Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.5.102.0

First Published: July 2013
Last Revised: November 2013
OL-28977-01

These release notes describe what is new in this release, instructions to upgrade to this release, and open and resolved caveats for this release. Unless otherwise noted, all of the Cisco Wireless LAN controllers are referred to as *controllers*, and all of the Cisco lightweight access points are referred to as *access points* or *Cisco APs*.

For more information about compatibility with the other wireless products and their releases, see:

www.cisco.com/en/US/docs/wireless/controller/5500/tech_notes/Wireless_Software_Compatibility_Matrix.html

Contents

These release notes contain the following sections:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Controller and Access Point Platforms

The section contains the following subsections:

Controller Platforms Supported

The following controller platforms are supported in this release:

- Cisco 2500 Series Wireless LAN Controllers
- Cisco 5500 Series Wireless LAN Controllers
- Cisco Flex 7500 Series Wireless LAN Controllers
- Cisco 8500 Series Wireless LAN Controllers
- Cisco Virtual Wireless Controllers on Cisco Services-Ready Engine (SRE) or Cisco Wireless LAN Controller Module for Integrated Services Routers G2 (UCS-E)
- Cisco Wireless Controllers for high availability (HA controllers) for 2500 Series, 5500 Series, WiSM2, Flex 7500 Series, and 8500 Series controllers
- Cisco Wireless Services Module 2 (WiSM2) for Catalyst 6500 Series switches

Access Point Platforms Supported

The following access point platforms are supported in this release:

- Cisco 1040, 1130, 1140, 1240, 1250, 1260, 1600, 2600, 3500, 3500p, 3600, Cisco 600 Series OfficeExtend Access Points, 700 Series, AP801, and AP802
- Cisco Aironet 1550 (1552) series outdoor 802.11n mesh access points; Cisco Aironet 1520 (1522, 1524) series outdoor mesh access points
- The AP801 and AP802 are integrated access points on the Cisco 800 Series Integrated Services Routers (ISRs). For more information about the stock-keeping units (SKUs) for the access points and the ISRs, see the following data sheets:
  - AP860:

    http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78_461543.html
  - AP880:

    http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78_459542_ps380_Products_Data_Sheet.html

    http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78-613481.html

    http://www.cisco.com/en/US/prod/collateral/routers/ps380/ps10082/data_sheet_c78_498096.html

http://www.cisco.com/en/US/prod/collateral/routers/ps380/ps10082/data_sheet_c78-682548.html

- AP890:

  http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78-519930.html

Note The AP802 is an integrated access point on the Next Generation Cisco 880 Series ISRs.

Note Before you use an AP802 series lightweight access point with controller software release 7.5.102.0, you must upgrade the software in the Next Generation Cisco 880 Series ISRs to Cisco IOS 151-4.M or later releases.

Controller Platforms Not Supported

The following controller platforms are not supported:

- Cisco 4400 Series Wireless LAN Controller
- Cisco 2100 Series Wireless LAN Controller
- Cisco Catalyst 3750G Integrated Wireless LAN Controller
- Cisco Wireless LAN Controller software on Cisco Services-Ready Engine (SRE) running on ISM 300, SM 700, SM 710, SM 900, and SM 910
- Cisco Catalyst 6500 Series/7600 Series Wireless Services Module (WiSM)
- Cisco Wireless LAN Controller Module (NM/NME)

What's New in This Release?

This section provides a brief description of what is new in Release 7.5. For more information about instructions on how to configure these features, see the *Cisco Wireless LAN Controller Configuration Guide, Release 7.5* (hereafter referred to as the configuration guide) at

http://www.cisco.com/en/US/products/ps10315/products_installation_and_configuration_guides_list.html.

- The 802.11ac radio module, which is based on the IEEE 802.11ac Wave 1 standard, is available on the Cisco Aironet 3600 Series access points (Cisco AP3600). The 802.11ac module provides enterprise-class reliability and wired-network-like performance. The 802.11ac module supports three spatial streams and 80 MHz-wide channels for a maximum data rate of 1.3 Gbps. The 802.11ac standard is a 5-GHz-only technology, which is faster and a more scalable version of the 802.11n standard.

  Some important points to note:

  - If you downgrade from Release 7.5.102.0 to an earlier controller software release and you connect the Cisco AP3600 with the 802.11ac module to the controller, the Cisco AP3600 works as expected, but the 802.11ac is not visible. When you upgrade to Release 7.5.102.0 again, all the 802.11ac parameters are set to default values.

  - When FlexConnect APs switch to standalone mode (WAN link down), the 802.11ac clients move to the 802.11n radio and the 802.11ac module is disabled. When WAN link comes up, the 802.11ac module is enabled and the 802.11ac clients will move back to the 802.11ac radio.
  - The LED scheme for Cisco AP3600 has changed to reflect the presence of the 802.11ac module. When you enter a command to locate an AP, the AP LEDs now flash the red and green lights as opposed to the blue light previously.

  For more information about the 802.11ac module on Cisco AP3600, see:

  http://www.cisco.com/en/US/products/ps11983/products_relevant_interfaces_and_modules.html.

  For more information about configuring the 802.11ac parameters, see the "Configuring 802.11ac Parameters" section in the configuration guide.

- New –Z Product IDs are introduced for Cisco 3600 Series access points. The –Z PIDs provide enhanced 5-GHz spectrum coverage for Australia and New Zealand.

  The UNII-2 Extended channels in 5470-5725 (excluding 5600 to 5650) are supported.

  The following are the complete set of channels in the 5-GHz bandwidth with –Z:

  - 5150 to 5250
  - 5250 to 5350
  - 5470 to 5725 (excluding 5600 to 5650)
  - 5750 to 5850

  For more information, see the Declaration of Conformity at:

  http://www.cisco.com/web/dofc/1087946.pdf

- Cisco Aironet 700 Series access points are supported. Cisco AP700 supports high-performing two spatial stream rates over a deployable distance with high reliability when they serve clients. For more information, see:

  http://www.cisco.com/en/US/products/ps12968/tsd_products_support_series_home.html.

- Starting in this release, the Cisco Wireless Controller on Cisco Services-Ready Engine (SRE) running on ISM 300, SM 700, and SM 900 using native controller software is not supported. However, SRE or UCS-E with Cisco Virtual Wireless Controllers is supported.
- Wireless Policy Classification engine is a wireless device profiler and policy classification feature introduced on the Cisco Wireless LAN Controller. The onboard wireless policy engine enables profiling of wireless devices and policy enforcement to address your Bring Your Own Device (BYOD) deployments.
- Cisco 8500 Series Wireless LAN Controllers can act as anchor controllers in high-scale deployments that can have as many as 64000 clients.
- The Cisco SFP-10G-LR module is supported on the Cisco Flex 7500 Series and the Cisco 8500 Series Wireless LAN Controllers.

  The Cisco SFP-10G-LR module supports a link length of 10 kilometers (6.2 miles) on a standard single-mode fiber (SMF, G.652).

- The RADIUS and TACACS+ server lists in AAA are manually configurable options that are based on statically-defined IP addresses of the servers. You can configure up to 17 servers in the global server list. In this release, you have an option to use a Fully Qualified Domain Name (FQDN) that enables you to change the IP address when needed, for example, for load balancing updates.

  A new submenu, DNS has been added to the **Security > AAA > RADIUS** and the **Security > AAA > TACACS+** menus, which you can use to get RADIUS or TACACS+ IP information from the DNS server.

Note DNS is disabled by default.

For more information about configuring DNS, see the "Configuring RADIUS" and "Configuring TACACS+" sections in the configuration guide.

- It is now possible to choose the interface name from which you ping:
  - Get the interface details by entering this command:

    show interface summary
  - Ping from an interface of your choice by entering this command:

    ping *ip-addr interface-name*
- You can view the IP address of the AP and the client count on the controller:
  - On the controller CLI, enter the **show ap summary** command.
  - On the controller GUI, choose **Wireless > All APs**.

  You can view the IP address of the AP when you see the client summary:
  - On the controller CLI, enter the **show client summary** command.
  - On the controller GUI, choose **Monitor > Clients**.
- You can now use the **grep** command to print only the lines that match a pattern. This is especially useful when the output of certain **show** commands is lengthy and you have to scroll multiple times to get to the information that you need. For example, to view only the system uptime from the **show sysinfo** command output, enter the following **grep** command:

  ```
  grep include 'Up Time' "show sysinfo"
  ```

  Output that is similar to the following is displayed:

  ```
  Press yes to continue(y)y
  System Up Time................................ 0 days 5 hrs 30 mins 7 secs

  There are 1 lines matching the pattern Up Time
  ```

  Similarly, you can exclude the lines that match a given string by entering the **grep exclude** command.

  The search string is case sensitive. Use single-quotes (' ') if your string contains spaces.

  The search string cannot contain only wild cards (*, ?, and so on). However, you can include wild cards along with the search string that contains other text. For example, if you want to see all the information that starts with the string 'Sys' in the output of the **show sysinfo** command, enter this command:

  ```
  grep include 'Sys*' "show sysinfo"

  Press yes to continue(y)y
  Manufacturer's Name.......................... Cisco Systems Inc.
  System Name.................................. Test
  System Location.............................
  System Contact..............................
  System ObjectID.............................. 1.3.6.1.4.1.9.1.1069
  System Up Time............................... 0 days 5 hrs 38 mins 0 secs
  System Timezone Location....................
  System Stats Realtime Interval............... 5
  System Stats Normal Interval................. 180
  ```

```
                                                    There are 9 lines matching the
pattern Sys*
```

- You can include wild cards when you use the Change Filter option in your search for APs, WLANs, and so on. For example, if you want to search for all the WLANs whose names start with the string wlan:
  1. On the controller GUI, choose **WLANs**.
  2. On the **WLANs** page that is displayed, click **Change Filter**.
  3. In the **Search WLANs** dialog box that is displayed, select the **Profile Name** check box and enter *wlan** in the adjacent text box.
  4. Click **Find**.

  The wildcard option is available for all menus that have the Change Filter option:
  - **Monitor > Access Points > Radios > 802.11a/n/ac | 802.11b/g/n | Dual-Band Radios**

    (MAC Address and AP name)
  - **Monitor > Cisco CleanAir > 802.11a/n/ac | 802.11b/g/n > Interference Devices**

    (Cluster ID and AP name)
  - **Monitor > Cisco CleanAir > 802.11a/n/ac | 802.11b/g/n > Air Quality Report**

    (AP name)
  - **WLANs > WLANs**

    (Profile Name and SSID)
  - **Wireless > Access Points > All APs**

    (MAC Address, AP Name, AP Model)
  - **Wireless > Access Points > Radios > 802.11a/n/ac | 802.11b/g/n**

    (MAC Address and AP Name)
- Prior to this release, the Ethernet wired lightweight APs in the Bridge mode (either the RAP mode or the MAP mode) were not responding to nor were able to send the Internet Control Message Protocol (ICMP) traffic unless they were associated with the controller. This resulted in issues where it is expected that the controller and AP should be able to ping each other before the Control And Provisioning of Wireless Access Points (CAPWAP) association process can begin.

  In this release, the mesh APs can ping and be pinged even before they are associated with the controller.
- Prior to this release, the Cisco AP1552 GI2 interface could not be configured for VLAN. This was because the GI2 interface was used as a cable modem interface on the Cisco AP1552C. This restriction is removed in this release.
- You can now deauthenticate a client by specifying the username or the IP address of the client. In the earlier releases, you could do this by specifying only the MAC address of the client. This enhancement allows multiple client sessions with the same username to be deauthenticated. Overlapping IP addresses across different interfaces result in the MAC addresses of the clients being listed. In such as scenario, you must use the MAC address of a client to deauthenticate the client.

  Deauthenticate a client by entering this command:

  ```
  config client deauthenticate {mac-addr | ipv4-addr | ipv6-addr | user-name}
  ```

Note It is not possible to configure this enhancement on the controller GUI.

- Use the Telnet Authority Management feature to selectively manage local users who have credentials to use Telnet to connect to the controller.

  In the earlier releases, you could configure Telnet only for all local management users at the global level. By default, all the local management users were allowed to use Telnet to connect to the controller.

  Now, the Telnet Authority Management feature is enabled only after you enable Telnet globally. By default, all Telnet user capability is in an enabled state.

  Also, the SSH connection behavior is not affected by the Telnet Authority Management feature.

  For more information, see the "Configuring Telnet Privileges for Selected Management Users" section in the configuration guide.

- You can configure the controller to support a maximum number of APs, with the number not exceeding the one allowed in the license. The controller limits the number of APs supported depending on the licensing information and the controller model that is used.

  The licensing information overrides the configured value if the configured number of APs is greater than that is allowed in the license.

  You must reboot the controller after you change the configured number of APs supported.

  For more information, see the "Configuring the Maximum Number of Access Points Supported" section in the configuration guide.

- New Mobility (converged access) enables the controller to be compatible with converged access controllers with a Wireless Control Module (WCM) such as the Cisco Catalyst 3850 switch and the Cisco 5760 Wireless LAN Controller.

  The Cisco 2500 Series, Cisco 5500 Series, Cisco WiSM2, or the Cisco 5760 Wireless LAN Controller functions as a mobility controller with the Cisco Catalyst 3850 switch. The mobility controller is part of a hierarchical architecture that consists of a mobility agent and a mobility oracle.

  For more information, see the "Configuring New Mobility" chapter in the configuration guide.

Note The epings are not available in Cisco 5500 Series WLC when New Mobility is enabled.

- High Availability enhancements:
  - Redundancy ports can operate over a Layer 2 connection (multiple intermediate switches or routers). Therefore, a direct connection is not required.
  - A client stateful switchover (SSO) across geographical locations is supported. Clients that are not in Run state are removed after the switchover. During a stateful switchover of a client (client SSO), the information of the client is synchronized with the standby controller when the client associates with the controller, or is configured. Clients that are fully authenticated, that is, clients that are in the Run state, are synchronized with the peer controller. The data structures of clients are synchronized based on the client state. Clients that are in a transient state are dissociated after a switchover.
- The controller can profile wireless devices based on protocols, such as HTTP and DHCP, to identify the clients. You can configure device-based policies and enforce per-user or per-device policies on the wireless network. You can view statistics that are based on per-user or per-device endpoints and policies that are applicable to a wireless device.

  For more information, see the "Configuring Local Policies" section in the configuration guide.
- Protocol packs are a means to distribute protocol updates outside the controller software releases, and can be loaded on the controller without replacing the controller software release.

The Application Visibility and Control Protocol Pack (AVC Protocol Pack) is a compressed file that contains multiple Protocol Description Language (PDL) files and a manifest file. A set of required protocols can be loaded, which helps AVC to recognize additional protocols for classification on your wireless network. The manifest file gives information about the protocol pack, such as the protocol pack name, version, and information about the available PDLs in the protocol pack.

For more information, see:

http://www.cisco.com/en/US/products/ps10315/products_installation_and_configuration_guides_list.html

- Multicast DNS-related enhancements:
  - The processing of Multicast DNS (mDNS) service advertisements and mDNS query packets are enhanced to support Location Specific Services (LSS). All valid mDNS service advertisements that are received by the controller are tagged with the MAC address of the AP that is associated with the service advertisement from the service provider while inserting the new entry into the service provider database. The response formulation to the client query filters the wireless entries in the service provider database using the MAC address of the AP associated with the querying client.

    LSS applies only to wireless service provider database entries. There is no location awareness for wired service provider devices.
  - In Release 7.4, a configured service was learned from wired or wireless devices and there was no option to restrict the learning to only wired devices or only wireless devices or both types of devices. In this release, you can configure a service to filter inbound traffic that is based on its origin and is either wired or wireless. All the services that are learned from the mDNS AP are treated as wired. When the learn origin is wired, the LSS cannot be enabled for the service because LSS applies only to wireless services.
  - In Release 7.4, there was a limit of 100 service providers per service type. In this release, this restriction is removed. However, there is a global service provider limit per controller model as shown in this table:

Table 1 Per-Service Service Provider Count Limit

Controller Model	Service Provider Count Limit
Cisco 8500 Series Wireless LAN Controller	16000
Cisco Flex 7500 Series Wireless LAN Controller	16000
Cisco 5500 Series Wireless LAN Controller	6400
Cisco 2500 Series Wireless LAN Controller	6400

  - You can configure up to 50 MAC addresses per service; these MAC addresses are the service provider MAC addresses that require priority. This guarantees that any service advertisements originating from these MAC addresses for the configured services are learned even if the service provider database is full by deleting the last nonpriority service provider from the service that has the highest number of service providers. When you configure the priority MAC address for a service, there is an optional parameter called ap-group, which allows only wired service providers to associate a sense of location to the wired service provider devices. When a client mDNS query originates from the ap-group, the wired entries with priority MAC and ap-group are looked up and those entries are listed first in the aggregated response.
  - In Release 7.4, the controller could learn the mDNS services that are visible only on the network. In this release, the mDNS AP feature allows the controller to have visibility of wired service providers, which are on VLANs that are not visible to the controller. You can configure

any AP as an mDNS AP to allow the AP to forward mDNS packets to the controller. VLAN visibility at the controller is achieved by APs that forward the mDNS advertisements to the controller. The mDNS packets between the AP and the controller are forwarded through a CAPWAP data tunnel that is similar to mDNS packets from a wireless client. Only CAPWAP v4 tunnels are supported. APs can be in either access port or the trunk port to learn the mDNS packets from the wired side and forward them to the controller.

  - Multicast DNS stateful switchover (mDNS SSO) is part of the Client SSO where mDNS configuration on an active controller is synchronized with the standby controller. Synchronization of mDNS AP information is not required.

  For more information, see the "Configuring Multicast DNS" section in the configuration guide.

- Guest access clients that have had successful web authentication are allowed to sleep and wake up without having to go through another authentication process. You can configure the duration for which the sleeping clients are to be remembered for reauthentication. The valid range is 1 hour to 720 hours (30 days), with the default duration being 12 hours. You can configure the duration on a WLAN and on a user group policy that is mapped to the WLAN.

Table 2 Maximum Number of Sleeping Clients Supported Per Platform

Controller Model	Maximum Number of Sleeping Clients Supported
Cisco 2500 Series Wireless LAN Controller	500
Cisco 5500 Series Wireless LAN Controller	1000
Cisco Wireless Services Module 2	1000
Cisco Flex 7500 Series Wireless LAN Controller	9000
Cisco 8500 Series Wireless LAN Controller	9000
Cisco Virtual Wireless Controller on Cisco Service-Ready Engine (SRE) or UCS-E	500

  For more information, see the "Configuring Authentication for Sleeping Clients" section in the configuration guide.

- Rogue-policy-related enhancements:
  - In the earlier releases, you had to configure security policies manually. In this release, you can choose a security level that is defined in the system for your rogue policy. The available options are: Low, High, Critical, and Custom (default).
  - In the earlier releases, the unicast deauthentication messages were sent at broadcast rates. The lowest supported rate was 1 Mbps on a 2.4-GHz band and 6 Mbps on a 5-GHz band. In this release, you can choose to optimize the rate to use the best rate for the target rogue. The AP selects the best rate based on rogue RSSI.
  - In the earlier releases, you could validate rogue clients against AAA. This required you to statically enter each valid client MAC address into AAA. In this release, you can validate the rogue clients against the Cisco Mobility Services Engine.
  - In the earlier releases, access points in the local mode and the monitor mode, and FlexConnect access points in the connected mode could be used to contain rogues. However, FlexConnect access points that moved to the standalone mode stopped containing rogues. In this release, FlexConnect access points that move to the standalone mode continue to contain rogues. They also apply the policy that is received from the controller.

  - In the earlier releases, you had to manually define how many APs must be used to contain rogues. This depended on the time and location. In this release, you can configure the controller to automatically assign the number of APs to contain rogues. For each rogue to be contained, the controller calculates the available number of APs based on rogue RSSI and the AP utilization level and channel, and then dynamically selects the number of APs to use.
  - In the earlier releases, you could create rogue policy rules based on SSID, but the SSID had to be an exact match. In this release, you can create rogue policy rules based on wildcard SSID, where the rule is enforced by any SSID that contains the wildcard SSID string. You can configure up to 25 wildcard rule per rogue rule.
  - In the earlier releases, if a rogue that was already classified by a rule, then the rogue was not classified again. In this release, this behavior is enhanced to allow reclassification of rogues based on the priority of the rogue rule. The priority is determined by using the rogue report that is received by the controller.
  - In the earlier releases, when you configure rogue policy rules, you could set the state to Alert, Internal, or External. In this release, you can also set the state to Delete. If a rogue device matches a rule, the alarm is silently deleted from the controller database. No trap is sent to Cisco Prime Infrastructure. This helps you to delete unwanted AP or ad hoc entries in the controller, which you do not want to be alerted about, thus avoiding the unnecessary action of adding the MAC address to a friendly or ignore list.

    For more information about the rogue policy enhancements, see the "Managing Rogue Devices and Classifying Rogue Access Points" sections in the configuration guide.

- Cisco Virtual Wireless LAN Controller-related (virtual controller) enhancements:
  - In the earlier releases, CAPWAP control was encrypted by default and CAPWAP data was encapsulated, but not encrypted by default. In the virtual controllers, the option to encrypt data traffic for specific APs was not present. In this release, DTLS data encryption between APs and virtual controller is supported. Without Data DTLS, the average virtual controller throughput is about 200 Mbps. With all the APs using Data DTLS, the average virtual controller throughput is about 100 Mbps.

    For Cisco 600 Series OEAP to associate with Cisco Virtual Wireless LAN Controller, follow these steps: First, configure the OEAP to associate with a physical controller that is using Release 7.5 and download the corresponding AP image. Next, configure the OEAP so that the OEAP does not associate with the physical controller again; for example, you can implement an ACL in the network to block CAPWAP between the OEAP and the physical controller. Next, configure the OEAP to associate with the Cisco Virtual Wireless LAN Controller.
  - You can now assign rate limiting to client traffic. You can configure rate limiting at the QoS profile level or the WLAN level. The WLAN configuration overrides the QoS profile-level configuration.

    Rate limiting is enforced at the AP level. It is not possible to enforce rate limiting at the virtual controller level because per client downstream rate limiting is not supported for central switching WLANs when traffic is terminated at the virtual controller.

    Per client downstream rate limiting is supported if the virtual controller is a foreign controller tunneling traffic to another controller platform, for example, a Cisco 5500 Series Wireless LAN Controller.

Table 3 Rate Limiting with Cisco Virtual Wireless LAN Controller

Traffic	FlexConnect Central Switching	FlexConnect Local Switching	FlexConnect Standalone
Per client Downstream	Not Supported	Supported	Supported
Per SSID Downstream	Supported	Supported	Supported
Per client Upstream	Supported	Supported	Supported
Per SSID Upstream	Supported	Supported	Supported

- FlexConnect-related enhancements:
  - In the earlier releases, you could use the FlexConnect AP for local authentication using LEAP and EAP-FAST. In this release, additional options are provided using which you can also use EAP-TLS and PEAP.

    EAP-TLS and PEAP are supported in the FlexConnect APs that are in the standalone mode and when local authentication is enabled on a WLAN.

    FlexConnect APs perform 802.1X authentication on the AP itself using the local RADIUS server.

    When EAP-TLS and PEAP are enabled, regardless of the authentication method, up to 100 clients per radio are supported.
  - In the earlier releases, you could configure WLAN-to-VLAN mapping for FlexConnect APs. However, it was not possible to apply WLAN-to-VLAN mapping to several FlexConnect APs that belonged to a FlexConnect group. In this release, you can configure a WLAN-to-VLAN mapping to a FlexConnect group, thereby configuring the mapping for all the APs in the FlexConnect group.

    The individual AP settings have precedence over the FlexConnect group and global WLAN settings. The FlexConnect group settings have precedence over global WLAN settings.

    The AP-level configuration is stored in Flash; WLAN and FlexConnect group configurations are stored in RAM.

    When an AP moves from one controller to another, the AP can keep its individual VLAN mappings. However, the FlexConnect group and global mappings will be from the new controller.
  - In the earlier releases, you could have a per client access control list (ACL) in a centrally switched traffic. In this release, this feature has been enhanced to support ACL for local switching traffic with both central and local authentication. Client ACL is returned from AAA on successful client Layer 2 authentication as part of Airespace RADIUS attributes. As the Airespace RADIUS attribute is an ACL name, the ACL must be already present on the FlexConnect AP.

    In downstream traffic, VLAN ACL is applied first and then the client ACL is applied. In upstream traffic, the client ACL is applied first and then the VLAN ACL is applied.
  - In Release 7.4, AAA could override individual client bandwidth contract, in the downstream direction, for the APs in the local mode and the FlexConnect APs with central switching. AAA override allows for configuration of per client rate limiting for downstream traffic for UDP (real-time) and TCP (data) traffic. Both the average rate and the burst rate can be configured. In this release, this feature is enhanced to support FlexConnect APs with local switching.

  - In Release 7.4, the 802.11w standard for Management Frame Protection was introduced and supported on all the 802.11n-capable APs. In this release, this feature has been enhanced to support FlexConnect APs. The following scenarios are supported: central authentication and local authentication; local switching and central switching; key is maintained when the AP switches from the connected to the standalone mode and then back to the connected mode if there is no change on the WLAN in the controller; key is maintained when HA SSO becomes effective. Besides these, both flat and new mobility are supported.

    This feature is supported on all controller platforms including Cisco Virtual Wireless LAN Controller and Cisco Flex 7500 Series Wireless LAN Controller.

Note This feature is not supported on Cisco AP1130 and Cisco AP1240.

  - The point-to-point protocol over the Ethernet (PPPoE) submode on FlexConnect access points, that was supported until Release 7.4, is not supported in this release.
  - With this release, the FlexConnect access points support client load balancing.

- You can configure rules for Layer 2 access control lists (ACLs) based on the Ethertype associated with the packets. Using this feature, if a WLAN with central switching is required to support only PPPoE clients, you can apply Layer 2 ACL rules on the WLAN to allow only PPPoE packets after the client is authenticated and the rest of the packets are dropped. Similarly, if the WLAN is required to support only IPv4 clients or only IPv6 clients, you can apply Layer 2 ACL rules on the WLAN to allow only IPv4 or IPv6 packets after the client is authenticated and the rest of the packets are dropped. For a locally-switched WLAN, you can apply the same Layer 2 ACL either for the WLAN or a FlexConnect AP. AP-specific Layer 2 ACLs can be configured only on FlexConnect APs. This is applicable only for locally-switched WLANs. The Layer 2 ACL that is applied to the FlexConnect AP takes precedence over the Layer 2 ACL that is applied to the WLAN.
- The 802.11w standard for Management Frame Protection is supported on mesh access points.
- Proxy Mobile IPv6-related enhancements:
  - Central external web authentication is supported.
  - You are not required to force the mobility type as PMIPv6 on a WLAN. Instead, you can enable AAA override, and the AAA server can send the PMIPv6 attributes to the client.
- You can configure split tunneling for the Cisco OEAP to enable or disable local printer access. You can enable or disable split tunneling on a per WLAN or per remote LAN basis, or you can enable or disable split tunneling globally on the Cisco OEAP themselves.
- IPv6-framed-prefix and IPv6-framed-address AAA attributes are supported for RADIUS accounting request packets.

  Configure the framed IPv6 AAA attributes for RADIUS accounting request packets by entering this command:

  config wlan radius_server acct framed-ipv6 {**address** | **prefix** | **both**} *wlan-id*

Note At present, the IPv6-framed-address attribute value is encoded with a dummy attribute number of 190 because the Internet Engineering Task Force (IETF) is yet to define a value.

- The Cisco License Manager (CLM) is not supported from this release onwards.

  If your network contained various Cisco-licensed devices, you could use the Cisco License Manager (CLM) to manage all of the licenses using a single application. CLM was a secure client/server application that managed Cisco software licenses network wide.

The license agent was an interface module that ran on the controller and mediated between CLM and the controller's licensing infrastructure. CLM could communicate with the controller using various channels, such as HTTP, Telnet, and so on.

- The default values of the 802.1p tags for the following QoS profiles are changed:
  - Platinum—5 (previously 6)
  - Gold—4 (previously 5)
  - Silver—2(previously 3)

Note If, after an upgrade to Release 7.5.102.0, you prefer to retain the previous tag values, you must disable the networks and configure the tag values manually.

Software Release Support for Access Points

Table 4 lists the controller software releases that support specific Cisco access points. The First Support column lists the earliest controller software release that supports the access point. For access points that are not supported in ongoing releases, the Last Support column lists the last release that supports the access point.

Note Third-party antennas are not supported with Cisco indoor accesss points.

Table 4 Software Support for Access Points

Access Points		First Support	Last Support
700 Series	AIR-CAP702I-x-K9	7.5.102.0	—
	AIR-CAP702I-xK910	7.5.102.0	—
1000 Series	AIR-AP1010	3.0.100.0	4.2.209.0
	AIR-AP1020	3.0.100.0	4.2.209.0
	AIR-AP1030	3.0.100.0	4.2.209.0
	Airespace AS1200	—	4.0
	AIR-LAP1041N	7.0.98.0	—
	AIR-LAP1042N	7.0.98.0	—
1100 Series	AIR-LAP1121	4.0.155.0	7.0.x
1130 Series	AIR-LAP1131	3.1.59.24	—
1140 Series	AIR-LAP1141N	5.2.157.0	—
	AIR-LAP1142N	5.2.157.0	—
1220 Series	AIR-AP1220A	3.1.59.24	7.0.x
	AIR-AP1220B	3.1.59.24	7.0.x

Table 4 Software Support for Access Points (continued)

Access Points		First Support	Last Support
1230 Series	AIR-AP1230A	3.1.59.24	7.0.x
	AIR-AP1230B	3.1.59.24	7.0.x
	AIR-LAP1231G	3.1.59.24	7.0.x
	AIR-LAP1232AG	3.1.59.24	7.0.x
1240 Series	AIR-LAP1242G	3.1.59.24	—
	AIR-LAP1242AG	3.1.59.24	—
1250 Series	AIR-LAP1250	4.2.61.0	—
	AIR-LAP1252G	4.2.61.0	—
	AIR-LAP1252AG	4.2.61.0	—
1260 Series	AIR-LAP1261N	7.0.116.0	—
	AIR-LAP1262N	7.0.98.0	—
1300 Series	AIR-BR1310G	4.0.155.0	7.0.x
1400 Series	Standalone Only	—	—
1600 Series	AIR-CAP1602I-x-K9	7.4.100.0	—
	AIR-CAP1602I-xK910	7.4.100.0	—
	AIR-SAP1602I-x-K9	7.4.100.0	—
	AIR-SAP1602I-xK9-5	7.4.100.0	—
	AIR-CAP1602E-x-K9	7.4.100.0	—
	AIR-SAP1602E-xK9-5	7.4.100.0	—
AP801		5.1.151.0	—
AP802		7.0.98.0	—
AP802H		7.3.101.0	—
2600 Series	AIR-CAP2602I-x-K9	7.2.110.0	—
	AIR-CAP2602I-xK910	7.2.110.0	—
	AIR-SAP2602I-x-K9	7.2.110.0	—
	AIR-SAP2602I-x-K95	7.2.110.0	—
	AIR-CAP2602E-x-K9	7.2.110.0	—
	AIR-CAP2602E-xK910	7.2.110.0	—
	AIR-SAP2602E-x-K9	7.2.110.0	—
	AIR-SAP2602E-x-K95	7.2.110.0	—
3500 Series	AIR-CAP3501E	7.0.98.0	—
	AIR-CAP3501I	7.0.98.0	—
	AIR-CAP3502E	7.0.98.0	—
	AIR-CAP3502I	7.0.98.0	—
	AIR-CAP3502P	7.0.116.0	—
3600 Series	AIR-CAP3602I-x-K9	7.1.91.0	—

Table 4 Software Support for Access Points (continued)

Access Points		First Support	Last Support
	AIR-CAP3602I-xK910	7.1.91.0	—
	AIR-CAP3602E-x-K9	7.1.91.0	—
	AIR-CAP3602E-xK910	7.1.91.0	—
600 Series	AIR-OEAP602I	7.0.116.0	—
Note The Cisco 3600 Access Point was introduced in 7.1.91.0. If your network deployment uses Cisco 3600 Access Points with release 7.1.91.0, we highly recommend that you upgrade to 7.2.103.0 or a later release.			
1500 Mesh Series	AIR-LAP-1505	3.1.59.24	4.2.207.54M
	AIR-LAP-1510	3.1.59.24	4.2.207.54M
1520 Mesh Series	AIR-LAP1522AG	-A and N: 4.1.190.1 or 5.2 or later[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-LAP1522HZ	-A and N: 4.1.190.1 or 5.2 or later[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-LAP1522PC	-A and N: 4.1.190.1 or 5.2 or later[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-LAP1522CM	7.0.116.0 or later.	—
	AIR-LAP1524SB	-A, C and N: 6.0 or later	—
		All other reg. domains: 7.0.116.0 or later.	—
	AIR-LAP1524PS	-A: 4.1.192.22M or 5.2 or later[1]	—
1550	AIR-CAP1552I-x-K9	7.0.116.0	—

Table 4 Software Support for Access Points (continued)

Access Points		First Support	Last Support
	AIR-CAP1552E-x-K9	7.0.116.0	—
	AIR-CAP1552C-x-K9	7.0.116.0	—
	AIR-CAP1552H-x-K9	7.0.116.0	—
	AIR-CAP1552CU-x-K9	7.5.102.0	—
	AIR-CAP1552EU-x-K9	7.5.102.0	—
1552S	AIR-CAP1552SA-x-K9	7.0.220.0	—
	AIR-CAP1552SD-x-K9	7.0.220.0	—

1. These access points are supported in the separate 4.1.19x.x mesh software release or with release 5.2 or later releases. These access points are not supported in the 4.2, 5.0, or 5.1 releases.

Note The access point must always be connected to the POE-IN port to associate with the controllers. The POE-OUT port is for connecting external devices only.

Upgrading to Controller Software Release 7.5.102.0

Guidelines and Limitations

- When upgrading from Release 7.3.x to Release 7.5.102.0, the primary controller gets upgraded while the secondary controller does not get upgraded because of an error of application timeout while transferring the image from the primary controller to the secondary controller. This causes the controllers to go to maintenance mode when rebooting after upgrade because of image mismatch.

  This issue occurs when HA is enabled and when you try to upgrade from Release 7.3.x to Release 7.5.102.0.

  The workaround is as follows:

  a. Unpair the HA controllers.

  b. Upgrade the individual controllers to Release 7.5.102.0.

  c. Pair up the controllers after they are upgraded.

  This issue will not occur in future releases as the new images have the bug fixes and design changes, which will avoid this issue.

- Controller using Release 7.3.112.0, configured for new mobility, might revert to old mobility after upgrading to Release 7.5, even though Release 7.5 supports new mobility. This issue occurs when new mobility, which is compatible with Cisco 5760 Wireless LAN Controller and Cisco Catalyst 3850 Series Switch, is in use. Old mobility is not affected.

  The workaround is as follows:

  a. Enter the following commands:

  ```
  config boot backup
  show boot
  ```

```
Primary Boot Image.................. 7.5.102.0
Backup Boot Image................... 7.3.112.0 (default) (active)
```

b. After the reboot, press Esc on the console, and use the boot menu to select Release 7.5.

c. After booting on Release 7.5, set back the primary boot, and save the configuration by entering the following command:

```
config boot primary
```

- When FlexConnect access points (known as H-REAP access points in the 7.0.x releases) that are associated with a controller that has all the 7.0.x software releases that are prior to 7.0.240.0 upgrade to the 7.5.102.0 release, the access points lose their VLAN support configuration if it was enabled. The VLAN mappings revert to the default values of the VLAN of the associated interface. The workaround is to upgrade from 7.0.240.0 or a later 7.0.x release to the 7.5.102.0 release.
- If you have disabled the ‘learn-ip-address' functionality for locally switched WLANs with the security type configured as ‘WEB-AUTH’ or ‘DHCP-Req’ or if PMIPv6 is in enabled state and you upgrade to Release 7.5.102.0, the ‘learn-ip-address’ feature is enabled after you upgrade. This is to avoid the WLAN from being disabled in Release 7.5.102.0 because of changes committed for CSCuf24517. The IP-based functionality might be impacted if the ‘learn-ip-address’ feature is disabled in Release 7.5.102.0 due to changes committed for CSCuf24517.

  In Release 7.5.102.0, when the WLAN is locally switched, you must use the **config wlan flexconnect learn-ipaddr** *wlan-id* {**enable** | **disable**} command. When the WLAN is centrally switched, you must use the **config wlan learn-ipaddr-cswlan** *wlan-id* {**enable** | **disable**} command.
- While a client sends an HTTP request, the Controller intercepts it for redirection to login page. If the HTTP request intercepted by Controller is fragmented, the Controller drops the packet as the HTTP request does not contain enough information required for redirection.
- A client whose home page is an HTTPS (HTTP over SSL, port 443) one is not redirected by Web Auth to the web authentication dialog box. Therefore, it is not possible for such a client to get authenticated and eventually fails to connect to the network. A workaround is for the client to attempt to open any HTTP (port 80) web page.
- We recommend that you install Wireless LAN Controller Field Upgrade Software for Release 1.7.0.0-FUS, which is a special AES package that contains several system-related component upgrades. These include the bootloader, field recovery image, and FPGA/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, see http://www.cisco.com/en/US/docs/wireless/controller/release/notes/fus_rn_1_7_0_0.html.
- If you are using a Cisco 2500 Series controller and you intend to use the Application Visibility and Control (AVC) and NetFlow protocol features, you must install Wireless LAN Controller Field Upgrade Software for Release 1.8.0.0-FUS. This is not required if you are using other controller hardware models. For more information, see http://www.cisco.com/en/US/docs/wireless/controller/release/notes/fus_1_8_0_0.html.
- After you upgrade to the 7.4 release, networks that were not affected by the existing preauthentication ACLs might not work because the rules are now enforced. That is, networks with clients configured with static DNS servers might not work unless the static server is defined in the preauthentication ACL.
- On Flex 7500 controllers if FIPS is enabled, the reduced boot options are displayed only after a bootloader upgrade.

Note Bootloader upgrade is not required if FIPS is disabled.

- If you require a downgrade from one release to another, you might lose the configuration from your current release. The workaround is to reload the previous controller configuration files saved on the backup server or to reconfigure the controller.
- It is not possible to directly upgrade to the 7.5.102.0 release from a release that is older than 7.0.98.0.
- You can upgrade or downgrade the controller software only between certain releases. In some instances, you must first install an intermediate release prior to upgrading to software release 7.5.102.0. Table 5 shows the upgrade path that you must follow before downloading software release 7.5.102.0.

Table 5 Upgrade Path to Controller Software Release 7.5.102.0

Current Software Release	Upgrade Path to 7.5.102.0 Software
7.0.x releases	You can upgrade directly to 7.5.102.0 **Note** If you have VLAN support and VLAN mappings defined on H-REAP access points and are currently using a 7.0.x controller software release that is prior to 7.0.240.0, we recommend that you upgrade to the 7.0.240.0 release and then upgrade to 7.5.102.0 to avoid losing those VLAN settings.
7.1.91.0	You can upgrade directly to 7.5.102.0
7.2.x releases	You can upgrade directly to 7.5.102.0 **Note** If you have an 802.11u HotSpot configuration on the WLANs, we recommend that you first upgrade to the 7.3.101.0 controller software release and then upgrade to the 7.5.102.0 controller software release. You must downgrade from the 7.5.102.0 controller software release to a 7.2.x controller software release if you have an 802.11u HotSpot configuration on the WLANs that is not supported.
7.3.x releases	You can upgrade directly to 7.5.102.0
7.4.x releases	You can upgrade directly to 7.5.102.0

- When you upgrade the controller to an intermediate software release, you must wait until all of the access points that are associated with the controller are upgraded to the intermediate release before you install the latest controller software. In large networks, it can take some time to download the software on each access point.
- If you upgrade to the controller software release 7.5.102.0 from an earlier release, you must also upgrade to Cisco Prime Infrastructure 1.4 and MSE 7.5.
- You can upgrade to a new release of the controller software or downgrade to an older release even if Federal Information Processing Standard (FIPS) is enabled.

- When you upgrade to the latest software release, the software on the access points associated with the controller is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession.
- We recommend that you access the controller GUI using Microsoft Internet Explorer 6.0 SP1 (or a later release) or Mozilla Firefox 2.0.0.11 (or a later release).
- Cisco controllers support standard SNMP Management Information Base (MIB) files. MIBs can be downloaded from the Software Center on Cisco.com.
- The controller software is factory installed on your controller and automatically downloaded to the access points after a release upgrade and whenever an access point joins a controller. We recommend that you install the latest software version available for maximum operational benefit.
- Ensure that you have a TFTP, FTP, or SFTP server available for the software upgrade. Follow these guidelines when setting up a server:
  - Ensure that your TFTP server supports files that are larger than the size of the controller software release 7.5.102.0. Some TFTP servers that support files of this size are tftpd32 and the TFTP server within the Prime Infrastructure. If you attempt to download the 7.5.102.0 controller software 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 or a different subnet because the distribution system port is routable.
- When you plug a controller into an AC power source, the bootup script and power-on self-test run to initialize the system. During this time, you can press **Esc** to display the bootloader Boot Options Menu. The menu options for the 5500 differ from the menu options for the other controller platforms.

  Bootloader Menu for 5500 Series Controllers:

```
   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:
```

  Bootloader Menu for Other 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 a 5500 series controller), or enter **5** (on another controller platform) to run the current software and set the controller 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 for your controller for more details on running the bootup script and power-on self-test.

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

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

- Control which address(es) are sent in CAPWAP discovery responses when NAT is enabled on the Management Interface using the following command:

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

  where:

  - **enable**— Enables use of NAT IP only in a discovery response. This is the default. Use this command if all APs are outside of 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 of the NAT gateway; for example, Local Mode and OfficeExtend APs are on the same controller.

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

- You can configure 802.1p tagging by using the **config qos dot1p-tag** {**bronze** | **silver** | **gold** | **platinum**} tag. For the 7.2.103.0 and later releases, if you tag 802.1p packets, the tagging has impact only on wired packets. Wireless packets are impacted only by the maximum priority level set for QoS.
- You can reduce the network downtime using the following options:
  - You can predownload the AP image.
  - For FlexConnect access points, use the FlexConnect AP upgrade feature to reduce traffic between the controller and the AP (main site and the branch). For more information about the FlexConnect AP upgrade feature, see the *Cisco Wireless LAN Controller FlexConnect Configuration Guide*.

Note Predownloading a 7.5.102.0 version on a Cisco Aironet 1240 access point is not supported when upgrading from a previous controller release. If predownloading is attempted to a Cisco Aironet 1240 access point, an AP disconnect will occur momentarily.

- Do not power down the controller or any access point during the upgrade process; otherwise, you might corrupt the software image. Upgrading a controller with a large number of access points can take as long as 30 minutes, depending on the size of your network. However, with the increased number of concurrent access point upgrades supported, the upgrade time should be significantly reduced. The access points must remain powered, and the controller must not be reset during this time.
- If you want to downgrade from the 7.5.102.0 release to a 6.0 or an older release, do either of the following:
  - Delete all WLANs that are mapped to interface groups and create new ones.
  - Ensure that all WLANs are mapped to interfaces rather than interface groups.

- After you perform these functions on the controller, you must reboot the controller for the changes to take effect:
  - Enable or disable link aggregation (LAG)
  - Enable a feature that is dependent on certificates (such as HTTPS and web authentication)
  - Add a new license or modify an existing license
  - Increase the priority for a license
  - Enable the HA
  - Install SSL certificate
  - Configure the database size
  - Install vendor device certificate
  - Download CA certificate
  - Upload configuration file
  - Install Web Authentication certificate
  - Changes to management or virtual interface
  - TCP MSS

Upgrading to Controller Software Release 7.5.102.0 (GUI)

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

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

Step 2 Follow these steps to obtain the 7.5.102.0 controller software:

a. Click this URL to go to the Software Center:

http://www.cisco.com/cisco/software/navigator.html

b. Choose **Wireless** from the center selection window.

c. Click **Wireless LAN Controllers**.

The following options are available:

- Integrated Controllers and Controller Modules
- Standalone Controllers

d. Depending on your controller platform, click one of the above options.

e. Click the controller model number or name. The **Download Software** page is displayed.

f. Click a controller software release. The software releases are labeled as follows to help you determine which release to download:

- **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 a software release number.

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

i. Click **Download**.

j. Read Cisco's End User Software License Agreement and then click **Agree**.

k. Save the file to your hard drive.

l. Repeat steps a. through k. to download the remaining file.

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

Step 4 (Optional) Disable the controller 802.11a/n and 802.11b/g/n networks.

Note For busy networks, controllers on high utilization, or small controller platforms, we recommend that you disable the 802.11a/n and 802.11b/g/n networks as a precautionary measure.

Step 5 Disable any WLANs on the controller.

Step 6 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 7 From the File Type drop-down list, choose **Code**.

Step 8 From the Transfer Mode drop-down list, choose **TFTP**, **FTP**, or **SFTP**.

Step 9 In the IP Address text box, enter the IP address of the TFTP, FTP, or SFTP server.

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

Step 11 In the File Path text box, enter the directory path of the software.

Step 12 In the File Name text box, enter the name of the software file (*filename*.aes).

Step 13 If you are using an FTP server, follow these steps:

a. In the Server Login Username text box, enter the username to log on to the FTP server.

b. In the Server Login Password text box, enter the password to log on to the FTP server.

c. In the Server Port Number text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 14 Click **Download** to download the software to the controller. A message appears indicating the status of the download.

Step 15 After the download is complete, click **Reboot**.

Step 16 If prompted to save your changes, click **Save and Reboot**.

Step 17 Click **OK** to confirm your decision to reboot the controller.

Step 18 After the controller reboots, repeat Step 6 to Step 17 to install the remaining file.

Step 19 Reenable the WLANs.

Step 20 For Cisco WiSM2 on the Catalyst switch, check the port channel and reenable the port channel if necessary.

Step 21 If you have disabled the 802.11a/n and 802.11b/g/n networks in Step 4, reenable them.

Step 22 To verify that the 7.5.102.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

Special Notes for Licensed Data Payload Encryption on Cisco Wireless LAN Controllers

Datagram Transport Layer Security (DTLS) is required for all Cisco 600 Series OfficeExtend Access Point deployments to encrypt data plane traffic between the APs and the controller. You can purchase Cisco Wireless LAN Controllers with either DTLS that is enabled (non-LDPE) or disabled (LDPE). If DTLS is disabled, you must install a DTLS license to enable DTLS encryption. The DTLS license is available for download on Cisco.com.

Important Note for Customers in Russia

If you plan to install a Cisco Wireless LAN Controller in Russia, you must get a Paper PAK, and not download the license from Cisco.com. The DTLS Paper PAK license is for customers who purchase a controller with DTLS that is disabled due to import restrictions but have authorization from local regulators to add DTLS support after the initial purchase. Consult your local government regulations to ensure that DTLS encryption is permitted.

Note Paper PAKs and electronic licenses available are outlined in the respective controller datasheets.

Downloading and Installing a DTLS License for an LDPE Controller

Step 1 Download the Cisco DTLS license.

a. Go to the Cisco Software Center at this URL:

https://tools.cisco.com/SWIFT/LicensingUI/Home

b. On the Product License Registration page, choose **Get New > IPS, Crypto, Other Licenses**.

c. Under **Wireless**, choose **Cisco Wireless Controllers (2500/5500/7500/8500/WiSM2) DTLS License**.

d. Complete the remaining steps to generate the license file. The license file information will be sent to you in an e-mail.

Step 2 Copy the license file to your TFTP server.

Step 3 Install the DTLS license. You can install the license either by using the controller web GUI interface or the CLI:

- To install the license using the web GUI, choose:

  Management > Software Activation > Commands > Action: Install License

- To install the license using the CLI, enter this command:

  license install tftp:*//ipaddress /path /extracted-file*

After the installation of the DTLS license, reboot the system. Ensure that the DTLS license that is installed is active.

Upgrading from an LDPE to a Non-LDPE Controller

Step 1 Download the non-LDPE software release:

a. Go to the Cisco Software Center at this URL:

http://www.cisco.com/cisco/software/navigator.html?mdfid=282585015&i=rm

b. Choose the controller model from the right selection box.

c. Click **Wireless LAN Controller Software**.

d. From the left navigation pane, click the software release number for which you want to install the non-LDPE software.

e. Choose the non-LDPE software release: AIR-X-K9-X-X.X.aes

f. Click **Download**.

g. Read Cisco's End User Software License Agreement and then click **Agree**.

h. Save the file to your hard drive.

Step 2 Copy the controller software file (*filename*.aes) to the default directory on your TFTP or FTP server.

Step 3 Upgrade the controller with this version by following the instructions from Step 3 through Step 22 detailed in the "Upgrading to Controller Software Release 7.5.102.0" section on page 16.

Interoperability With Other Clients in 7.5.102.0

This section describes the interoperability of the version of controller software with other client devices.

Table 6 describes the configuration used for testing the clients.

Table 6 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	7.5.102.0
Controller	Cisco 5500 Series Controller
Access points	1131, 1142, 1242, 1252, 3500e, 3500i, and 3600
Radio	802.11ac, 802.11a, 802.11g, 802.11n2, 802.11n5
Security	Open, WEP, PSK (WPA and WPA2), 802.1X (WPA-TKIP and WPA2-AES) (LEAP, PEAP, EAP-FAST, EAP-TLS)
RADIUS	ACS 4.2, ACS 5.2
Types of tests	Connectivity, traffic, and roaming between two access points

Table 7 lists the client types on which the tests were conducted. The clients included laptops, handheld devices, phones, and printers.

Table 7 Client Types

Client Type and Name	Version
Laptop	
Intel 3945/4965	11.5.1.15 or 12.4.4.5, v13.4
Intel 5100/5300/6200/6300	v14.3.0.6
Intel 1000/1030/6205	v14.3.0.6
Intel 7260(11AC)	16.0.0.61 10.22.243.199
Broadcom 4360(11AC)	6.30.163.2005
Dell 1395/1397/Broadcom 4312HMG(L)	XP/Vista: 5.60.18.8 Win7: 5.30.21.0
Dell 1501 (Broadcom BCM4313)	v5.60.48.35/v5.60.350.11
Dell 1505/1510/Broadcom 4321MCAG/4322HM	5.60.18.8
Dell 1515(Atheros)	8.0.0.239
Dell 1520/Broadcom 43224HMS	5.60.48.18
Dell 1530 (Broadcom BCM4359)	v5.100.235.12
Cisco CB21	v1.3.0.532
Atheros HB92/HB97	8.0.0.320
Atheros HB95	7.7.0.358
MacBook Pro (Broadcom)	5.10.91.26
Handheld Devices	
Apple iPad	iOS 5.0.1
Apple iPad2	iOS 6.0(10A403)
Apple iPad3	iOS 6.0(10A403)
Asus Slider	Android 3.2.1
Asus Transformer	Android 4.0.3
Sony Tablet S	Android 3.2.1
Toshiba Thrive	Android 3.2.1
Samsung Galaxy Tab	Android 3.2
Motorola Xoom	Android 3.1
Intermec CK70	Windows Mobile 6.5 / 2.01.06.0355
Intermec CN50	Windows Mobile 6.1 / 2.01.06.0333
Symbol MC5590	Windows Mobile 6.5 / 3.00.0.0.051R
Symbol MC75	Windows Mobile 6.5 / 3.00.2.0.006R
Phones and Printers	
Cisco 7921G	1.4.2.LOADS
Cisco 7925G	1.4.2.LOADS
Ascom i75	1.8.0

Table 7 Client Types (continued)

Client Type and Name	Version
Spectralink 8030	119.081/131.030/132.030
Vocera B1000A	4.1.0.2817
Vocera B2000	4.0.0.345
Apple iPhone 4	iOS 6.0(10A403)
Apple iPhone 4S	iOS 6.0(10A403)
Apple iPhone 5	iOS 6.0(10A405)
Ascom i62	2.5.7
HTC One(11AC)	Android 4.1.2
Samsung Galaxy S4 - GT-I9500(11AC)	Android 4.2.2
HTC Legend	Android 2.2
HTC Sensation	Android 2.3.3
LG Optimus 2X	Android 2.2.2
Motorola Milestone	Android 2.2.1
RIM Blackberry Pearl 9100	WLAN version 4.0
RIM Blackberry Bold 9700	WLAN version 2.7
Samsung Galaxy S II	Android 2.3.3
SpectraLink 8450	3.0.2.6098/5.0.0.8774
Samsung Galaxy Nexus	Android 4.0.2
Motorola Razr	Android 2.3.6

Features Not Supported on Controller Platforms

This section lists the features that are not supported in the following platforms:

- Features Not Supported on Cisco 2500 Series Controllers
- Features Not Supported on WiSM2 and Cisco 5500 Series Controllers
- Features Not Supported on Cisco Flex 7500 Controllers
- Features Not Supported on Cisco 8500 Controllers
- Features Not Supported on Cisco Virtual Wireless Controllers
- Features Not Supported on Mesh Networks

Features Not Supported on Cisco 2500 Series Controllers

- Wired guest access
- Bandwidth contract
- Service port
- AppleTalk Bridging

- Right to Use licensing
- PMIPv6
- High Availability (1:1)
- Multicast-to-unicast

Note The features that are not supported on Cisco WiSM2 and Cisco 5500 Series Controllers are also not supported on Cisco 2500 Series Controllers.

Note Directly connected APs are supported only in Local mode.

Features Not Supported on WiSM2 and Cisco 5500 Series Controllers

- Spanning Tree Protocol (STP)
- Port mirroring
- VPN termination (such as IPsec and L2TP)
- VPN passthrough option

  Note You can replicate this functionality on a 5500 series controller by creating an open WLAN using an ACL.

- Configuration of 802.3 bridging, AppleTalk, and Point-to-Point Protocol over Ethernet (PPPoE)
- Fragmented pings on any interface
- Right to Use licensing

Features Not Supported on Cisco Flex 7500 Controllers

- Static AP-manager interface

  Note For Cisco 7500 Series controllers, it is not necessary to configure an AP-manager interface. The management interface acts like an AP-manager interface by default, and the access points can join on this interface.

- L3 Roaming
- VideoStream
- TrustSec SXP
- IPv6/Dual Stack client visibility

Note IPv6 client bridging and Router Advertisement Guard are supported.

- Internal DHCP server

- Access points in local mode

Note An AP associated with the controller in local mode should be converted to FlexConnect mode or Monitor mode, either manually or by enabling the autoconvert feature. On the Flex 7500 controller CLI, enable the autoconvert feature by entering the **config ap autoconvert enable** command.

- Mesh
- Spanning Tree Protocol (STP)
- Cisco Flex 7500 Series Controller cannot be configured as a guest anchor controller. However, it can be configured as a foreign controller to tunnel guest traffic to a guest anchor controller in a DMZ.
- Multicast

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

- PMIPv6

Features Not Supported on Cisco 8500 Controllers

- TrustSec SXP
- Internal DHCP server

Features Not Supported on Cisco Virtual Wireless Controllers

- Internal DHCP server
- TrustSec SXP
- Access points in local mode
- Mobility/guest anchor
- Multicast

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

- IPv6
- High Availability
- PMIPv6
- WGB
- VideoStream
- Outdoor mesh access points

Note Outdoor AP in FlexConnect mode is supported.

- Indoor mesh access points
- Application Visibility and Control (AVC)
- Client downstream rate limiting for central switching

Features Not Supported on Mesh Networks

- Multicountry support
- Load-based 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
- Access point join priority (mesh access points have a fixed priority)
- Location-based services

Caveats

The following sections lists Open Caveats and Resolved Caveats for Cisco controllers and lightweight access points for version 7.5.102.0. For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms might be standardized.
- Spelling errors and typos might be corrected.

Note If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

http://tools.cisco.com/Support/BugToolKit/

To become a registered cisco.com user, go to the following website:

http://tools.cisco.com/RPF/register/register.do

Open Caveats

Table 8 lists the open caveats in the 7.5.102.0 controller software release.

Table 8 Open Caveats

ID	Description
CSCui69732	**Symptom**: Platinum 802.1p tagging changed to 5. **Condition**: Platinum 802.1p is tagged at 6 and an upgrade was performed to Release 7.5.102.0. **Workaround**: Disable the networks and change the Platinum 802.1p tagging back to 6.
CSCui40233	**Symptom**: When upgrading from Release 7.3.x to Release 7.5.102.0, the primary controller gets upgraded while the secondary controller does not get upgraded because of an error of application timeout while transferring the image from the primary controller to the secondary controller. This causes the controllers to go to maintenance mode when rebooting after upgrade because of image mismatch. **Conditions**: This issue occurs when HA is enabled and when you try to upgrade from Release 7.3.x to Release 7.5.102.0. **Workaround**: 1. Unpair the HA controllers. 2. Upgrade the individual controllers to Release 7.5.102.0. 3. Pair up the controllers after they are upgraded. **Further Problem Description**: This issue will not occur in future releases as the new images have the bug fixes and design changes, which will avoid this issue.

CSCuf35841	**Symptom**: Controller using Release 7.3.112.0, configured for new mobility, reverted to old mobility after upgrading to Release 7.5, even though Release 7.5 supports new mobility.
	
	Condition:
	
	• New mobility in use (compatibility with Cisco 5760 Wireless LAN Controller and Cisco Catalyst 3850 Series Switch)
	• Old mobility mode is not affected
	
	Workaround:
	
	1. Enter the following commands:
	
	`config boot backup`
	`show boot`
	
	`Primary Boot Image..... 7.5.102.0`
	`Backup Boot Image..... 7.3.112.0 (default) (active)`
	
	2. After the reboot, press Esc on the console, and use the boot menu to select Release 7.5.
	3. After booting on Release 7.5, revert to the primary boot, and save the configuration by entering the following command:
	
	`config boot primary`

Table 8 Open Caveats (continued)

ID	Description
CSCui27029	**Symptom**: With maximum that is 64 IPv4 or IPv6 rules configured on the controller, and no Layer 2 ACL rules configured, web authentication clients are passing traffic in Web-auth required state. The issue is not seen with 63 rules configured. This issue occurs only when there is no ACL rule match. **Condition**: 1. Only with maximum (64) IPv4 or IPv6 rules 2. No Layer 2 ACL rules configured on the client or WLAN 3. Web authentication clients in Web-auth required state 4. None of the configured rules match the incoming packet 5. Release 7.5 **Workaround**: Configure only up to 63 rules.
CSCsv54436	**Symptom**: While doing SSH to controller, it is sometimes denied with "Sorry, telnet is not allowed on this port." If a retry is attempted immediately, the SSH connection is accepted. No changes are seen in between. **Condition**: SSH connection is done from a different Layer 3 network. This is breaking monitoring tools through SSH. **Workaround**: Retry SSH connection.
CSCsy66246	**Symptom**: An 802.11n AP does not downshift rates for retries when Low Latency MAC is enabled. The AP sends 3 retransmissions, but the data rate for the retransmissions is the same data rate at which the initial packet was sent. **Condition**: Using an 802.11n AP with Low Latency MAC enabled. **Workaround**: Do not enable Low Latency MAC. **Update**: The Low Latency MAC feature has been removed, for 802.11n APs, through CSCtc73527.

Table 8 Open Caveats (continued)

ID	Description
CSCtn52995	**Symptom**: FlexConnect: Reached the limit on the association ID for AP. **Condition**: 1. Client 1 is associated to the controller with AID =1 on SSID x. 2. Client 1 sends 802.11 Auth frame on SSID y; at this point AID = 1 is freed at the AP. Auth frames are not honored at the controller; and the controller is not informed. 3. No association frame arrives from client 1 at SSID 2. 4. Client 2 associates with the AP and gets AID = 1. 5. AP updates the controller about client 2 and AID = 1; now, the controller adds duplicate entries and increments the count (controller already has client 1 AID = 1). Counter gets incremented and reaching 256. It is due to the network conditions at the customer site in which the 802.11 authentication frames are sent (sometimes on different WLAN), but is not followed by association frames. **Workaround**: None.
CSCtq32444	**Symptom**: When a port in a LAG goes down and then comes back up, the controller does not send a UP trap via SNMP. **Condition**: Distribution ports are configured in a LAG, and an SNMP trap receiver is configured. **Workaround**: Look in the traplog on the controller (using the **show traplog** command on the controller CLI) for the UP trap. **Further Problem Description**: An attempt was made to fix this bug through CSCto58101, by delaying the transmission of the UP trap by 40 seconds. This attempted fix was implemented in Release 7.0.220.0; however, it caused the side effect that a dead port is not removed from the LAG (CSCtw56190, CSCtu13807), and therefore the CSCto58101 fix was rolled back in Release 7.0.230.0.

Table 8 Open Caveats (continued)

ID	Description

CSCtw67184	**Symptom**: Specific to Cisco Flex 7500 and 8500 Series Wireless LAN Controllers: While booting up, the following error message is displayed on the attached monitor or on serial console:
	`"All the disks from your previous configuration are gone. If this is an unexpected message, then please power off your system and check your system and check your cables to ensure all disks are present. Press any key to continue or C to load the configuration utility"`
	When the Space Bar is pressed, the system could not boot from the disk.
	Condition: Cisco Flex 7500 and 8500 Series Wireless LAN Controllers. This system went through an accidental power interruption; that is, the power plug was pulled while the system was operational. After a reboot, the RAID card could not find its configuration in the Flash memory and therefore it could not boot.
	Workaround: When this situation is encountered, you must enter the RAID management tool: WebBIOS. There are two versions of this tool: one that uses extensive menus and requires an attached monitor, and another that is based on the command lines (CLI).
	The CLI version of the tool can be accessed from the serial console. A prompt for this is visible on a serial console right after the error message is displayed.
	1. Enter the CLI version of the WebBIOS utility by pressing CTRL+Y and then enter the following command:
	`-CfgForeign -Import -a0`
	2. Reboot the server.
	Further Problem Description: When the Space Bar is pressed, the system could not boot from the disk. During the boot process, the LSI WebBIOS loads as expected and shows two physical disks, but no virtual disks. It appears that it lost the RAID configuration that was present in the system.
	The system went through an accidental power interruption, that is the power plug was pulled while the system was operational). After reboot, the RAID card could not find its configuration in the Flash memory and therefore it could not boot. The Flash configuration was affected due to the power interruption. The RAID card keeps a backup of the configuration on the hard drives. However, when the card loses the configuration information that is present in the Flash, it does not automatically pick up the backup configuration information from the hard drives. The information on the hard drives is considered a “foreign configuration” that requires user intervention.
	At this time, the system waits for you to take action. Note that all the data on the hard drives are still intact.

CSCtx68850	**Symptom**: After upgrading to Release 7.2, SSH connection to a controller sometimes fails randomly; a prompt for username is displayed, and then SSH is closed from the controller side. After several attempts in a row, the SSH connection is successful. **Condition**: Unknown. **Workaround**: Try several attempts in a row.

Table 8 Open Caveats (continued)

ID	Description
CSCtz41068	**Symptom**: Web Authentication on MAC Filter Failure authentication might sporadically fail. **Condition**: Controller using Release 7.0.116.0 or Release 7.0.230.0. Free RADIUS Server authentication for MAC authentication configured with default 1-second access-rejec. Clients might fail to get redirected to the web authentication splash page for authentication attempt, and remain in the 'DHCP Required' state. **Workaround**: Configure Free RADIUS access-reject response timer to zero.
CSCub14556	**Symptom**: If you use the **clear ap config** or the **clear all config** command on the controller CLI, under **Set to Factory Defaults** in the controller GUI, on an indoor AP that has been configured for the mesh (Bridge) mode, the AP remains in the Bridge mode. **Condition**: An indoor AP (such as an AIR-LAP1042) that has been configured for mesh. **Workaround**: 1. Remove the IOS_STATIC_AP_MODE environmental variable from the AP. This can be done on the console by reloading the AP, escaping into the boot loader, and entering the bootloader command `ap: unset IOS_STATIC_AP_MODE` OR Copy *flash:env_vars* from the AP to a TFTP server and edit the file to remove the IOS_STATIC_AP_MODE line, and copy the file back. 2. Clear the AP configuration. When the AP reboots, it should be back to factory defaults.
CSCub36414	**Symptom**: The change (enable/disable) in admin mode of the ports on Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN Controllers is not updated on upstream switch. **Condition**: Disable/enable admin mode of the ports on Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN Controllers. **Workaround**: Instead of enabling or disabling port admin from the controller, make it shut/no shut from upstream switch.
CSCuc49702	**Symptom**: Inter-SPG roam failures when MC (Cisco 2500 Series Wireless LAN Controller) goes down and comes back. **Condition**: Negative test case. MC is down and then comes back. **Workaround**: Idle timeout.
CSCuc60927	**Symptom**: Cisco 5508 Wireless LAN Controller fails to boot. SYS LED - Blinking Amber and ALM LED = OFF. **Condition**: Console logging set to debugging and high rate of console logs are generated while you reboot the controller. **Workaround**: Do not set console logging to debugging and reboot the controller at the same time, or send the debug output to an SSH/Telnet session, which is also a lower impact to the CPU.

Table 8 Open Caveats (continued)

ID	Description

CSCuc68995	**Symptom**: A wireless web authentication client might be unable to authenticate to the network. When the client opens a browser, the window is blank.
	With the **debug web-auth redirect** command in effect, messages similar to the following might be displayed:
	`*webauthRedirect: Oct 15 18:43:19.470: #EMWEB-6-REQUEST_IS_NOT_GET_ERROR: webauth_redirect.c:1055 Invalid request not GET on client socket 72`
	or
	`*webauthRedirect: Oct 10 16:36:30.715: %EMWEB-3-PARSE_ERROR: parse error after reading. bytes parsed = 0 and bytes read = 189`
	Condition: The HTTP GET from the client comes at the controller in multiple TCP segments.
	Workaround: Reconfigure your network and the TCP/IP stack of the client to ensure that the HTTP GET comes in a single segment.
	One example of client software that is known to introduce TCP segmentation behavior that triggers this bug is AnyConnect Web Security 3.0.3054.

CSCuc80103	**Symptom**: Cisco WiSM2 is unreachable, unable to ping. All APs drop from the controller, and unable to ping the Management interface's gateway (via console) at the time of failure. Failure condition recovers on its own typically within minutes. **Condition**: Cisco WiSM2 using Release 7.3.101.0. Buffer pool leak messages are printed in the message log around the time of the failure as follows: `*broffu_SocketReceive: Oct 20 07:31:15.291: #BROFFU-0-DP_BUFFER_POOL_LOW_DETECTED: broffu_fp_dapi_cmd.c:5060 Warning: DP Early PacketBuffer low detected. DP1 PacketBuffer=26105(<?26200) WQE=102318(<?26200) *broffu_SocketReceive: Oct 20 07:31:15.291: #BROFFU-0-DP_BUFFER_POOL_LOW_DETECTED: broffu_fp_dapi_cmd.c:5060 Warning: DP Early PacketBuffer low detected. DP0 PacketBuffer=26025(<?26200) WQE=102322(<?26200)` **Workaround**: None.
CSCuc81911	**Symptom**: Cisco AP3600 remains in the ‘ap:’ mode when there is a power outage, requiring manual boot. **Condition**: When there was a power outage, there is a possibility of AP remaining in the boot mode. **Workaround**: On the AP console, enter the **flash_init** and **boot** commands to get the AP working again.
CSCud16984	**Symptom**: Access points are assigned to channels with lower maximum powers. **Condition**: Varying power levels in different channels of the new access points. The controller detects more neighbors with high RSSIs on channels with higher power. **Workaround**: None.

Table 8 Open Caveats (continued)

ID	Description
CSCud50209	**Symptom**: The system stopped working on management user form post manipulation. **Condition**: Field content/count is modified **Workaround**: None. **Further Information**: Form needs administrative access rights to be accessed. Management from wireless is disabled by default and has to be explicitly enabled. This can minimize exposure on the wireless side.
CSCud56753	**Symptom**: In a VMWare ESX cluster, when migrating a virtual controller from one host to another via vMotion, the virtual controller management might become unreachable for 15 to 30 seconds, which may cause APs to transition to the standalone mode temporarily and prevent centrally switched WLANs from communicating. **Condition**: The management interface of a virtual controller is configured with a 802.1q VLAN tag communicating through a virtual switch network configured with VLAN (4095 ALL) in promiscuous network; per virtual controller deployment guide. VMware network can be configured to "Notify Switches" causing RARP to be sent on VMs tagged interface for updating neighbors with CAM table seamlessly during vMotion transition. This is transparent to the VM. In the virtual controller deployment, hosts cannot know the virtual controller's management or other interface 802.1q tags; therefore, RARP is delivered untagged. This prevents CAM tables from learning MAC update on proper VLAN ID and therefore a loss of communication to the virtual controller. **Workaround**: Communication is established as soon as the virtual controller "generates or egresses" traffic through the new host after a vMotion event. No known workaround.
CSCud57046	**Symptom**: Client entry is seen on multiple controllers even when not anchored to the controller or part of its mobility group. **Condition**: Foreign to Foreign Roaming might cause it in the scenario when the 2 (Export) Foreigns are mobility peers of each other, but (Export) Anchor is mobility peer of only the first (Export) Foreign. **Workaround**: None.

Table 8 Open Caveats (continued)

ID	Description
CSCud57784	**Symptom**: 1. In Cisco 5508 Wireless LAN Controller, use MAC Filtering authentication. 2. On the controller GUI, choose **Security > AAA > RADIUS > Authentication**, and define more than 1 RADIUS server. 3. Choose **Security > AAA > MAC Filtering** and set **RADIUS Compatibility Mode** as **Free RADIUS**. 4. In the WLAN settings, check MAC Filtering, select the authentication server, which is defined in Step 1 and also has index number 1. 5. Choose **Security > AAA > RADIUS > Authentication** and delete the RADIUS server, which has index number 1. In the WLAN settings, select the authentication server, which has an index number other than 1. In this scenario, client authentication fails. **Workaround**: Choose **Security > AAA > RADIUS > Authentication** and define a dummy RADIUS server, which has the index as 1.
CSCud68413	**Symptom**: A controller functioning as a DHCP server with large DHCP scopes might stop servicing DHCP client requests. **Condition**: Release 7.2.110.0. **Workaround**: Reboot the controller.
CSCue38133	**Symptom**: Controller sends a message after 90 days of an AP associating with the controller, that the APs should be moved to a primary controller. **Condition**: A HA-SKU controller is used as a secondary controller in an N1 configuration and an AP has associated with the controller. **Workaround**: None.
CSCue55153	**Symptom**: Controller stops communicating with CAM with SNMPv3. **Condition**: 1. Enable High Availability. 2. Add controller to CAM with SNMPv3 (should have authorization and authentication passwords). 3. Failover from primary to backup controller. **Workaround**: Delete and add the controller in CAM again.
CSCue86878	**Symptom**: The controller software was downgraded from Release 7.5 to Release 7.0.240.0 using SFTP, configuration was saved, and controller was rebooted. Immediately after rebooting the controller, the **transfer download start** command was entered. The controller stopped working. **Condition**: This is a defect in Release 7.0.x. This is specific to SFTP downgrade procedure, and it does not apply to other mechanisms. **Workaround**: If the mode is changed to TFTP or FTP upon reboot, then the controller works as expected.

Table 8 Open Caveats (continued)

ID	Description
CSCuf03454	**Symptom**: Controller stops working intermittently. **Condition**: Web pass through clients anchored from foreign controller to anchor controller. Controller became unresponsive randomly. **Workaround**: Reboot the controller.
CSCuf52358	**Symptom**: First client that connects to an incorrect interface without an available subnet to assign will not work as expected. **Condition**: Multiple interfaces as part of an interface group with a client attempting to use an interface that has run out of available IP addresses in the relevant subnet to assign to this client. **Workaround**: Manually deauthenticate the client so that it can associate on a different interface to be assigned an IP address.
CSCuf60628	**Symptom**: When AP fails over from the primary controller to the secondary controller, the client protocol displays 802.11b, which was originally 802.11g. **Condition**: AP is in FlexConnect local switching mode. Controller using Release 7.3.112.0. **Workaround**: None.
CSCuf61599	**Symptom**: Clients are not able to associate. **Condition**: Release 7.3, Cisco 5500 Series Wireless LAN Controller with FlexConnect and NAT/PAT AP IP. **Workaround**: Enable data encryption.
CSCuf77488	**Symptom**: The FT and LT detection time for an alarm is ahead or later than the AP clock. This is causing a delay in Cisco NCS to detect the alarm. `LCAVIAX014-2AD1#show capwap am alarm 54 capwap_am_show_alarm = 54 <A id='139266813'> <AT>54</AT> <FT>2013/03/12 23:37:44</FT> <LT>2013/03/12 23:38:07</LT> <DT>2013/03/01 21:59:47</DT> <SM>D0:57:4C:08:FB:B2-g</SM> <SNT>1</SNT> <CH>1</CH> <FID>0</FID> pAlarm.bPendingUpload = 0 LCAVIAX014-2AD1# LCAVIAX014-2AD1#show clock *21:59:18.983 UTC Tue Mar 12 2013 In NCS we will not see the alarm until the actual AP time matches the time reported in the FT.` **Condition**: Cisco 5500 Series Wireless LAN Controller using Release 7.0.235.3; Cisco AP3500 wIPS ELM mode; Cisco MSE 3350 using Release 7.0.201.204. **Workaround**: None.
CSCug01143	**Symptom**: At times, Cisco AP3500 causes issues such as wireless client being unable to associate with the AP, unable to use telnet to connect to the AP, **show** command output being very slow. It seems to be a memory leak issue. **Condition**: Release 7.4.100.0. **Workaround**: Reboot the AP.

Table 8 Open Caveats (continued)

ID	Description
CSCug07559	**Symptom**: 1. Load the virtual controller with Release 7.4 or Release 7.5. 2. Reset the system and press Esc key 3. In the boot options, select **Change Active Boot Image**. Issue: Virtual controller is loading with the older active image, but it should load with the new or changed active image. **Condition**: Bootloader image change. **Workaround**: Use config boot commands to change the image order.
CSCug09947	**Symptom**: 1. Create a normal ACL with the name 'pre-webauth'. 2. Add some rules. 3. Create a webauth WLAN and map the 'pre-webauth' ACL name to the WLAN webauth preauth ACL 4. Create a FlexConnect ACL with the name 'pre-webauth'. 5. Attempt to remove the ACL. 6. Controller does not allow the operation and displays an error message as follows: "Error! ACL is in use." **Condition**: ACL and FlexConnect ACL with the same name. **Workaround**: Delete the ACL and create again with the different name.
CSCug21645	**Symptom**: Cisco WiSM2 stops working at Reaper Reset: Task "BootP" missed software watchdog. **Condition**: Release 7.3.112.0. **Workaround**: None.
CSCug25043	**Symptom**: The **config flexconnect group** *flex-group* **multicast overridden-interface enable** command is needed to enable multicast on AAA overridden interfaces. The command works if there are no spaces in the FlexConnect group name and then you do not have to use quotes in the command. When you have a FlexConnect group name that has spaces in it, then the command needs to use quotes to enclose the group name. The command does not work when quotes are used, thereby rendering this command unusable for FlexConnect group names with spaces in them. **Workaround**: Use FlexConnect group name without spaces.
CSCug27515	**Symptom**: Clients on 802.11n rates might experience disconnection or data transfer issues when certain segment number orders are used. **Condition**: 802.11n, when client leading segment number is lower than the window (lower order). **Workaround**: For Apple devices, disable AQM in the Apple wireless driver. Disable A-MPDU. **Further Information**: A workaround is being implemented through CSCug65693.

Table 8 Open Caveats (continued)

ID	Description
CSCug29742	**Symptom**: Wireless clients are not reachable when set with static IP and with the VLAN pooling feature. **Condition**: Initially, the wireless client is allowed to get IP through DHCP and it got IP from one of the subnets (any one VLAN from the interface group) for instance subnet A. If the static IP is set from the same subnet (subnet A) that is used previously to get IP through DHCP, the client reaches the controller very well with static IP. But, when static IP is set with other subnets (other than A), it does not reach the controller. **Workaround**: In Release 7.2, we can disable and enable the WLAN once and the client entry is deleted. Now, set the static IP from any other subnet among the interfaces in the group and the controller will be reachable. This workaround will not work in Release 7.3 and later releases.
CSCug32118	**Symptom**: Apple devices such as iPads running Apple iOS 6.1.2 and 6.1.3 stop working for 5 seconds every 30 seconds. Client does not get disconnected from the wireless network or roam to another AP. **Condition**: Cisco 5508 Wireless LAN Controller using Release 7.3.112.0; guest anchoring set up with ISE WPA2/AES/802.1x. **Workaround**: Use non-Apple devices.
CSCug32967	**Symptom**: When an AP stops working, the log file is not sent to the controller due to CAWAP queue being full. It seems like the incoming data rate is more than what the CAPWAP queue can handle. `RA045W02ALT430: *Apr 13 00:34:33.975: %CAPWAP-3-ERRORLOG: Queue already full. RA045W02ALT430: *Apr 13 00:34:33.975: %CAPWAP-3-ERRORLOG: Failed to send data transfer request. RA045W02ALT430: *Apr 13 00:34:33.975: %CAPWAP-3-ERRORLOG: Queue already full. RA045W02ALT430: *Apr 13 00:34:33.975: %CAPWAP-3-ERRORLOG: Failed to send data transfer request. RA045W02ALT430: *Apr 13 00:34:33.975: %CAPWAP-3-ERRORLOG: Queue already full. RA045W02ALT430: *Apr 13 00:34:33.975: %CAPWAP-3-ERRORLOG: Failed to send data transfer request. RA045W02ALT430: *Apr 13 00:34:33.979: %CAPWAP-3-ERRORLOG: Queue already full. RA045W02ALT430: *Apr 13 00:34:33.979: %CAPWAP-3-ERRORLOG: Failed to send data transfer request.` **Condition**: AP in Bridge mode (Mesh Role). **Workaround**: None.

Table 8 Open Caveats (continued)

ID	Description
CSCug32970	**Symptom**: Memory leak in EAP. Radio request process. `-Traceback = 195A30z 2758E0z 27BB40z 27BD90z 28A360z 275570z 27D78Cz C35128z 456530z 40734Cz 7B72 CAPWAP CLIENT -Traceback= 195A30z 2758E0z 27BB40z 27BD90z 28A360z 275570z 27D78Cz C35128z 8089D8z 8162F0z 806C58z 7DDC %SYS-2-MALLOCFAIL: Memory allocation of 65536 bytes failed from 0x28A35C, alignment 0 CAPWAP CLIENT -Traceback= 195A30z 2758E0z 27BB40z 27BD90z 28A360z 275570z 27D78Cz C35128z 8089D8z 8162F0z 806C58z 7DDC %SYS-2-MALLOCFAIL: Memory allocation of 6000 bytes failed from 0x30D6AC, alignment 0 CAPWAP CLIENT -Traceback= 195A30z 2758E0z 27C964z 30D6B0z 301314z 2AF628z 4C5634z 4DBCA4z 4DBE64z EEAFCz F52DCz F5AA8z CAPWAP CLIENT -Traceback= 195A30z 2AF8D8z 4C5634z 4DBCA4z 4DBE64z EEAFCz F52DCz F5AA8z 8169D0z 7FF130z 805088z 8065CCz %SYS-2-MALLOCFAIL: Memory allocation of 65536 bytes failed from 0x28A35C, alignment 0` **Condition**: Excessive mesh AP authentication. **Workaround**: None.
CSCug34700	**Symptom**: Controller sends keep active alive message as a wired packet instead of wireless. **Condition**: When the controller sends the keep alive as a wired packet, the ISE drops it because of license issues. **Workaround**: Use passive keep alive instead of active.
CSCug38794	**Symptom**: Cisco WiSM2 stops working and then reboots (bcastReceiveTask 1332). **Condition**: Unknown. **Workaround**: None.
CSCug38888	**Symptom**: Disabled SSID is being broadcast by a 2.4-GHz radio. **Condition**: SSID was created and disabled previously; this is a very rare occurrence, and only seen once; never reproduced in lab. **Workaround**: Reconfigure AP.
CSCug40463	**Symptom**: A Cisco AP might stop transmitting traffic after several days with a switchport speed/duplex micsonfiguration. **Condition**: Cisco AP2610 associated with a controller using Release 7.3.112.0. The default Ethernet interface of Cisco AP2600 is set to auto/auto; switchport: duplex full/speed 100. **Workaround**: Correct the speed/duplex misconfiguration (should match on the AP and switchport).
CSCug49148	**Symptom**: Status LED on Cisco AP1552 in the local mode is blinking green when working in normal operation. **Condition**: Cisco AP1552 in the local mode. **Workaround**: Convert the Cisco AP to the mesh mode.

Table 8 Open Caveats (continued)

ID	Description
CSCug50913	**Symptom**: After reenabling HA, post HA disable, the secondary unit rebooted with Reason: Standby timeout. Three attempts were made to reproduce the same issue, but without success. **Condition**: HA is disabled through GUI and no additional configuration change were attempted. The secondary unit rebooted and came up as active. After resetting both the primary and the secondary controller, the controllers pair up. **Workaround**: Low frequency/impact issue. Controllers will pair up and work after a reboot.
CSCug53680	**Symptom**: AP rebooted, log information was provided. **Condition**: There is no outstanding trigger. **Workaround**: None.
CSCug54426	**Symptom**: Release 7.3 introduced subinterface on the local mode APs. **Condition**: Customer requests a method to disable this on all APs because it is generating errors in the scripts. **Workaround**: None.
CSCug57216	**Symptom:** Ascom phone stops receiving voice packets. **Condition:** 802.11n in use; Voice traffic QoS markings are lost on downstream direction. **Workaround:** Either fix QoS markings or disable 802.11n.
CSCug57504	**Symptom:** Cisco AP702 is seen as an Impersonator. **Condition:** Cisco AP702 is seen as an Impersonator in controller trap logs. **Workaround:** None.
CSCug57545	**Symptom:** Clients are unable to connect to SNMP NAC SSID with an error message as follows: `"Unable to process out-of-band login request from MAC and IP Addr [device-filter]. Cause: OOB clientMAC and IP Addr not found."` **Condition:** Seen after upgrading from Release 7.4. **Workaround:** Enable the NAC Alert Client Trap.
CSCug69682	**Symptom:** Push a profile for autocontaining a device. If this fails for any reason, the mitigation status on Cisco Prime Infrastructure displays the following message: `Failed to start containment on device '34:a8:4e:d3:f7:a0'. Action failed due to 'Unable to contain the device.` This message should instead indicate the failure reason for auto containment. **Condition:** Failed containment. **Workaround:** None. It is a case of missing information.

Table 8 Open Caveats (continued)

ID	Description
CSCug73660	**Symptom:** As per the data sheet, the Cisco AP1600 should have 17 dBm of Tx power on 1 antenna and up to 22 with 3 antennas, as seen at http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps12555/data_sheet_c78-715702.html It is lesser in reality. The show controller's output shows that power level 1 is 13 dBm on 3 antennas (8 dBm per antenna). Comparing the show controller's output with a Cisco AP3600e clearly shows that Cisco AP1600 has less Tx Power. Field tests also show that it has a much smaller coverage area. This is on 2.4 GHz. On 5 GHz, the power meets expectations. This was noted in the -E reg domain. Also, modifying the antenna gain has no effect at all on the Tx power. **Condition:** Controller using Release 7.4.100.0 with European regulatory domain in countries where the expected power level is 17. **Workaround:** None.
CSCug76392	**Symptom:** It is specific to 'read-only' and 'lobby admin' users. If these users are prevented from accessing the controller due to successive failed attempts, the same users are able to logon to the controller through HTTP and, but cannot do any changes. However, it works as expected through SSH or Telnet; such users are not allowed to logon. **Condition:** Disabled user remote access. **Workaround:** None.
CSCug89084	**Symptom:** CleanAir sensor stops working and requires a reboot. **Condition:** First found on the monitor mode Cisco APs. **Workaround:** Reboot the Cisco AP.
CSCug90218	**Symptom:** Controller GUI has APs in unknown states. **Condition:** Unknown. **Workaround:** Reboot the controller.
CSCug91684	**Symptom**: Client does not get IP address even if it permits all Layer 2 ACLs that are mapped to the WLAN. This occurs only with CS WLAN; LS works as expected. **Condition**: Cisco Virtual Wireless LAN Controller with central switching and Layer 2 ACL applied. **Workaround**: Remove Layer 2 ACL.
CSCug92421	**Symptom:** Controller reports a large number of stale client entries. **Condition:** Cisco Flex 7510 Wireless LAN Controller using Release 7.3.103.x with numerous clients. **Workaround:** None.

Table 8 Open Caveats (continued)

ID	Description
CSCug98625	**Symptom:** Web authentication redirect fails when local switching is enabled on the WLAN. Manual redirect works. Redirect works when central switching is performed. **Condition:** Local switching enabled on the WLAN. **Workaround:** Add a dummy interface on the controller with IP assigned from the same VLAN, which is locally switched data VLAN for the client. VLAN identifier does not need to be the same, but IP address has to be. Also, it does not need be trunked to the controller.
CSCuh02340	**Symptom:** On the controller, CleanAir status is "N/A" even if AP supports and enables CleanAir. **Condition:** There are two controllers and many APs (more than 30), non-HA configuration. Each AP is configured as Primary or Secondary WLC. The symptom may happen when changing the joining WLC due to power down or network problem, for example, when Primary goes down and all APs are joined to Secondary WLC or vice versa. **Workaround:** Disable and re-enable radio on that AP to recover CleanAir status on the controller.
CSCuh03129	**Symptom:** FlexConnect AP does not delete Layer 2 ACL. **Condition:** When the AP moves from one controller to another controller, with the same WLAN on both the controllers but different Layer 2 ACL. **Workaround:** Reboot the AP.
CSCuh03648	**Symptom:** Controller might send accounting update with different framed IP address information. **Condition:** CWA in use with ISE, URL redirect pushed. **Workaround:** None.
CSCuh10735	**Symptom:** In the controller default configuration, the RADIUS failover occurs when the controller sends RADIUS request packets with the same ID to the RADIUS server for 6 times with no response from the server. However, sometimes RADIUS failover occurs even if the number of requests is less than 6. **Condition:** Release 7.3.112.0. **Workaround:** None.
CSCuh11730	**Symptom:** During WGB roaming test on FlexConnect local switching AP on Release 7.4.100.0, the following message is often observed on the AP CLI (**debug capwap client mgmt**): `*May 22 11:24:34.559: capwap_ap_mgmt: delete mn 0d0d.0d0d.0d0d *May 22 11:24:34.559: capwap_ap_mgmt: Deleting PMK for 0d0d.0d0d.0d0d The station mac address is not present in the network neither as a wlan client, or wired WGB client.` **Condition:** Roaming test on FlexConnect local switching Cisco AP on Release 7.4.100.0. Debugging using the **debug capwap client mgmt** command. **Workaround:** None.

Table 8 Open Caveats (continued)

ID	Description
CSCuh12796	**Symptom:** Consecutive SNMP **set** commands for same MIB variable on the controller fails. **Condition:** When a MIB object is set on the controller using SNMP **set** command, it works at the first attempt. However, if the command is entered repeatedly, the following message is displayed: `Error in packet. Reason: noCreation (That table does not support row creation or that object can not ever be created)` **Workaround:** Perform SNMP **get** before doing **set**.
CSCuh14797	**Symptom:** In Export Anchor-Foreign scenario, in both Foreign to Foreign as well as fresh association to a Foreign, if packets are not reaching to Export Anchor due to network issues, then after three retries, there will not be any further exchange. The request will go to Export Anchor and the client will stay in that state until it moves out. **Condition:** Network issues between mobility peers. **Workaround:** None. Instead, fix the underlying connectivity issues.
CSCuh16539	**Symptom:** After disabling the radio of a Cisco AP2600, it might become enabled after a reboot of the device. **Condition:** Cisco AP2600; controller using Release 7.4.100.0. **Workaround:** None.
CSCuh16842	**Symptom:** Client gets IPv6 address from a different VLAN. **Condition:** This is a combination of the following factors: 1. Interface group 2. Client sending traffic from either static IP or previously allocated IP. 3. Client traffic is not matching the assigned VLAN received initially. This message shows when this occurs: Overriding interface of client from 'vlan20' to 'vlan30' within interface group 'vlan20-30'. **Workaround:** Use DHCP required.
CSCuh16870	**Symptom:** Client with static IP loses connectivity on session timeout. **Condition:** This occurs only if the following set of conditions are met: 1. Interface that the client gets from the interface group does not match the interface corresponding to the static IP. 2. Client gets VLAN overridden with the following message: `apfReceiveTask: May 28 12:48:28.066: 00:1a:70:a5:2f:bd Overriding interface of client from 'vlan20' to 'vlan30' within interface group 'vlan20-30' *apfReceiveTask: May 28 12:48:28.066: 00:1a:70:a5:2f:bd Applying Interface policy on Mobile, role Local. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 20` This overriding is lost when PMK expires, and a new authentication takes place. This occurs even if the client is continuously sending traffic. **Workaround:** Either disable interface groups or set to DHCP required state.

Table 8 Open Caveats (continued)

ID	Description
CSCuh17680	**Symptom:** Cisco AP loses FlexConnect interface configuration when the AP is rebooted from the standalone mode. **Condition:** Cisco AP moves to standalone mode and is power cycled. **Workaround:** Wait for the Cisco AP to associate with the controller. After the Cisco AP has reassociated with the controller, the Cisco AP pulls the configuration from the controller.
CSCuh18983	**Symptom:** Using New Mobility, if the anchor controller for a client is lost, the traffic for the client might be locally terminated. **Condition:** Only on New Mobility (Cisco 5760 Wireless LAN Controller and Cisco Catalyst 3850 compatibility mode). This is not applicable to legacy mobility. **Workaround:** None for New Mobility; not present on legacy mobility scenarios.
CSCuh19195	**Symptom:** WLAN FlexConnect local switching is disabled on the active secondary controller after an HA failover. It causes WLAN-VLAN mapping to be changed on AP. **Condition:** After an HA failover; Release 7.3.x. **Workaround:** Reconfigure the WLAN-VLAN mapping.
CSCuh20385	**Symptom:** When using Internet Explorer 10 as the browser to access the GUI of the controller, it is not possible to use any filter options for clients and APs. The filter pop-up box is not displayed. **Condition:** None. **Workaround:** Switch the browser to compatibility view.
CSCuh20715	**Symptom:** Cisco 5508 Wireless LAN Controller stopped working on Reaper Reset: Task “LDAP DB Task 2” missed software watchdog. **Condition:** Reaper Reset: Task “LDAP DB Task 2” missed software watchdog. **Workaround:** None.

CSCuh25790	**Symptom:** With HA enabled Cisco 5508 Wireless LAN Controller set up with 430 real APs, the predownload was started on the 430 APs. Predownload was completed, but could not reset the system even after that. A message is displayed that says that the AP software upgrade is in progress, but remains unresponsive.
	`(HC-5508-01) reset system  AP Software being upgraded, please try again later.`
	`(HC-5508-01)`
	Condition: High AP count, failed predownload.
	Workaround: Reboot the controller with the **reset system forced** command.

Table 8 Open Caveats (continued)

ID	Description
CSCuh26716	**Symptom:** The output of the **show redundancy summary** command shows the following line regardless of its real SKU. `Unit = Secondary - HA SKU.` **Condition:** Used the **show redundancy summary** command on: 1. Secondary system which is converted from the Primary system. 2. HA-SKU system. **Workaround:** None.
CSCuh28190	**Symptom:** AP stopped working once and the log was found on the controller and TFTP server. **Condition:** None. **Workaround:** None. The AP will reset on its own. This was a one-time event and is still under investigation.
CSCuh29093	**Symptom:** LEAP authentication fails for FlexConnect mode local authentication and local switching. **Condition:** Primary and secondary server added in a FlexConnect group and they are not reachable. **Workaround:** Delete primary and secondary servers. The client right away authenticates with the local AP database. This caveat has been tested in controller software version 7.4.100.60 and customer version 7.4.100.0.
CSCuh31410	**Symptom:** AP radio may reset during FlexConnect state change. **Condition:** AP connectivity to the controller restored. **Workaround:** None.
CSCuh37173	**Symptom:** AP stops working on low memory condition. This is a request to implement WDT crash trigger mechanism in a low memory scenario, before reaching a breaking point. **Condition:** Unknown. **Workaround:** None.
CSCuh37960	**Symptom:** AP rebooted with log information provided. **Condition:** There is no outstanding trigger. **Workaround:** None.

Table 8 Open Caveats (continued)

ID	Description
CSCuh39893	**Symptom:** Controller using Release 7.3 or Release 7.4 fails to authenticate One Time Password (OTP) users when there is an attempt to authenticate to the controller using TACACS+. The following debug output is displayed when the **debug aaa tacacs enable** command was entered on the controller CLI. `TPLUS_AUTHEN_STATUS_GETPASS auth_cont get_pass reply: pkt_length=25 processTplusAuthResponse: Continue auth transaction No auth response from: SERVER IP, retrying with next server Preparing message for retransmit. Decrypting first Forwarding request to SERVER IP port=4900 AUTH Socket closed underneath No auth response from: SERVER IP, retrying with next server Preparing message for retransmit. Decrypting first Forwarding request to SERVER IP port=4900 AUTH Socket closed underneath Exhausted all available servers for Auth/Author packet.` **Condition:** Controller using Release 7.3 or Release 7.4; TACACS+ used for Management User Authentication; OTP used for TACACS+; static passwords are not impacted. **Workaround:** Extend the TACACS+ Management Server Timeout value by entering these commands: 1. **config tacacs auth disable server-index** 2. **config tacacs auth mgmt-server-timeout server-index** *10* 3. **config tacacs auth enable server-index**
CSCuh40464	**Symptom:** Topology: 5500 (MC/GC) MA1 MA2. To reproduce the issue, perform the following tasks: 1. Get the mobility between all is up and make Cisco 5500 Series Wireless LAN Controller as GA. 2. Try to connect a client to MA1. Client gets IP, anchor-foreign relationship is formed. 3. Roam the client to MA2. It is observed that it goes to IP learn state. **Condition:** Roaming between two mobility agents with Cisco 5508 Wireless LAN Controller as MC/GC. **Workaround:** None.
CSCuh41053	**Symptom:** When there is a duplex mismatch between the Cisco AP1142 port and upper layer switch port, both the switch and the Cisco AP display a warning message that is similar to the following: `"Duplex mismatch discovered"` The warning message is logged to the controller. However, when the controller is upgraded to Release 7.4.100.0, the warning message is not logged to the controller. **Condition:** This issue occurs only with Release 7.4.100.0, and not with Release 6.0.202.0. **Workaround:** None.

Table 8 Open Caveats (continued)

ID	Description
CSCuh42665	**Symptom:** Controller sends incorrect information for Rogue AP detection through traps. **Condition:** This issue occurs only with Release 7.4. **Workaround:** None.
CSCuh44119	**Symptom:** Cisco 8510 Wireless LAN Controller does not show the config line after disabling DHCP proxy. The **config dhcp proxy disable bootp-broadcast disable** command using Release 7.4.100.60. **Condition:** This issue occurs only with the Cisco 8510 Wireless LAN Controller using Release 7.4.100.60. **Workaround:** Enter the line in the configuration file or modify the configuration directly on the controller through the CLI or GUI.
CSCuh45072	**Symptom:** Cisco 5508 Wireless LAN Controller in HA configuration with two AAA servers in configuration sends TACACS+ authentication and authorization requests to different AAA servers. After some time, a user logging on through TACACS+ account to the controller is unable to logon because the controller sends authentication request to one AAA server, while at the same time and for the same user, the Authorization/Accounting request is sent to the second AAA server in the Authentication/Authorization servers list configuration on the controller. **Condition:** Controller with HA configuration. User logging on through TACACS+ account to the controller. Two or more AAA servers defined under controller TACACS+ authentication/authorization server list. **Workaround:** None.
CSCuh46442	**Symptom:** Cisco AP displays the %CAPWAP-3-ERRORLOG messages when the AP associates with the controller as follows: `%CAPWAP-3-ERRORLOG: Invalid event 10 & state 5 combination. %CAPWAP-3-ERRORLOG: CAPWAP SM handler: Failed to process message type 10 state 5. %CAPWAP-3-ERRORLOG: Failed to handle capwap control message from controller %CAPWAP-3-ERRORLOG: Failed to process encrypted capwap packet from 172.22.170.1` **Condition:** AP associating with a controller. **Workaround:** None.
CSCuh46996	**Symptom:** A wired device that scales behind a third-party bridge device fails to get an IP address. **Condition:** Third-party bridge is associating with an AP in H-REAP (FlexConnect) local switching mode and the controller is using a release that is later than the 7.0.116.0 release. **Workaround:** None.
CSCuh49135	**Symptom:** Beacon loss in Cisco AP1130. **Condition:** Random beacon drops are observed with Cisco AP1130 in FlexConnect mode. **Workaround:** None.

Table 8 Open Caveats (continued)

ID	Description
CSCuh50219	**Symptom:** The mesh topology is: RAP - MAP1 - MAP2 (all AP are 1522s, using 5-GHz backhaul). When MAP1 does not have Ethernet bridge client, then MAP2 connects to MAP1 and associates with the controller. However, when MAP1 has an Ethernet bridge client, then MAP2 fails to connect to MAP1 in order to associate with the controller. The authentication process between MAP2 and MAP1 is never completed in this case. The problem also appears regardless of the radio used for backhaul; that is both 5-GHz backhaul and 2-GHz backhaul. **Condition:** Applies to Cisco AP1520. Not applicable to Cisco AP1550. **Workaround:** None.
CSCuh50505	**Symptom:** Cisco WiSM2 stops working and then reboots. **Condition:** Cisco WiSM2 stops working when TPCv2 is in an enabled state. **Workaround:** Disable TPCv2.
CSCuh51208	**Symptom:** On an HA pair, when the standby unit is active, it might display the evaluation license window showing the remaining time. **Condition:** HA in use. **Workaround:** None needed. The HA unit will continue to work because the local licenses are not used for AP join validation.
CSCuh52238	**Symptom:** False DFS detections related to client activity. **Condition:** Clients triggering DFS detections due to spurious emissions. **Workaround:** Use non-DFS channels. This bug is to track additional filtering for pulses generated by client activity.
CSCuh53168	**Symptom:** SNMP query to Cisco Wireless LAN Controllers return noSuchName during device sync operation done from Cisco NCS. **Condition:** Random event while Telnet is enabled. Only seen at two sites. **Workaround**: None.
CSCuh54815	**Symptom:** WPAv1 with AES and WPAv2 with TKIP are not supported in the FlexConnect standalone mode, local authentication in the connected mode and CCKM fast-roaming in the connected mode. This limitation is documented only in Wireless LAN Controller 7.0 configuration guide. See http://www.cisco.com/en/US/partner/docs/wireless/controller/7.0/configuration/guide/c70hreap.html For Wi-Fi Protected Access version 2 (WPA2) in H-REAP standalone mode or local authentication in the connected mode or CCKM fast-roaming in the connected mode, only Advanced Encryption Standard (AES) is supported. For Wi-Fi Protected Access (WPA) in H-REAP standalone mode or local authentication in the connected mode or CCKM fast-roaming in the connected mode, only Temporal Key Integrity Protocol (TKIP) is supported. WPA2 with TKIP and WPA with AES is not supported in the standalone mode, local authentication in the connected mode, and CCKM fast-roaming in the connected mode. This is true for Release 7.2 and later releases. **Condition:** None. **Workaround:** None.

Table 8 Open Caveats (continued)

ID	Description
CSCuh55653	**Symptom**: AIR-CT5508-K9 reboots unexpectedly using Release 7.4.100.0 and as a result the “apfMsConnTask_5” task gets suspended. **Condition:** This issue occurs under normal conditions without any hardware or software configuration changes or network topology changes. **Workaround**: None.
CSCuh60546	**Symptom**: There are no debugs or logs to troubleshoot 10-GB interface issues on Cisco 8500 or 7500 Series Wireless LAN Controllers. Unable to determine the issues between switches and the controller. **Condition:** Cisco 8500 or 7500 Series Wireless LAN Controllers with 10-GB uplinks SFP. **Workaround**: None.
CSCuh61659	**Symptom**: When the client tries to connect to snooped domain (such as google.com), the debug message on access point is incorrectly referencing the use of the Virtual IP. **Condition:** Using DNS snooping ACLs with Release 7.3.x; enable DNS snooping on one of the ACLs for any domain (such as google.com). Enter the **debug dot11 profiler events** command on the AP and connect to a client that is assigned with that ACL. **Workaround**: None.
CSCuh63491	**Symptom**: With RF profile created, certain clients (for example, Blackberry devices) are not able to associate with the AP, and the controller rejects the association indicating invalid client data rates. **Condition:** Create an RF profile for the AP group, disable standard rates in the profile, and map the profile to an AP group. **Workaround**: Disable standard rates in the global profile.
CSCuh65005	**Symptom**: Controller puts the client on Run state while the client is not actually authenticated by the RSA/RADIUS server using web authentication – PAP. **Condition:** This issue occurs when you use a two-factor authentication. **Workaround**: Do not use the two-factor authentication for web authentication because it is not supported on controllers.

Table 8 Open Caveats (continued)

ID	Description
CSCuh67653	**Symptom**: Stale client entries are seen when the **show dot11 associations** command is entered on the Cisco Autonomous Access Points. `- show dot11 associations all-client ------------------ Address : XXXX.XXXX.XXXX Name : NONE IP Address : 0.0.0.0 Interface : Dot11Radio 0 Device : unknown Software Version : NONE CCX Version : NONE Client MFP : Off State : Assoc Parent : self SSID : XXXXXX VLAN : 12 Hops to Infra : 1 Clients Associated: 0 Repeaters associated: 0` **Condition:** This issue occurs when a client connects and passes by or when the client gets disconnected and the entry still remains on the AP. **Workaround**: 1. Clear a particular client using the **clear dot11 client** *client-MAC-addr* command. 2. Reload the image. This clears all the ghost clients. 3. Enter the **shut** and **no shut** commands on the interface.
CSCuh69558	**Symptom**: Default interface takes precedence over foreign VLAN mapping with AAA override. **Condition**: Configure a guest anchor solution. Enable foreign controller-interface mapping in the anchor. Enable AAA override in the WLAN. If the AAA server does not send any interface details, the anchor controller uses the default interface configuration for the WLAN to assign an IP address to the client. The precedence should fall to the foreign controller-interface mapping and then to the default interface in the WLAN. **Workaround**: None.
CSCuh70825	**Symptom**: MAP becomes unreachable through ICMP and displays memory allocation failures. **Condition:** This issue occurs in Cisco AP1552UE MAP with an IP camera connected. **Workaround**: Reboot the AP.
CSCuh72474	**Symptom**: Controller assigns an interface within a group to an invalid list even though a response was received by the DHCP server. **Condition:** This occurs when some clients insist on requesting an IP outside their connected interface range in a DHCP flood. For each request, the DHCP server responds with DHCP NAK, and the DHCP NAK is received by the controller and forwarded to the clients. **Workaround**: None.

Table 8 Open Caveats (continued)

ID	Description
CSCuh76898	**Symptom**: The client communication fails after a controller failover. **Condition**: A system consists of two controllers and a Cisco AP, where the Cisco AP is in FlexConnect Local Switching mode with VLAN support disabled. This issue occurs when the Cisco AP fails over from controller1 to controller2 and then fails over back from controller2 to controller1. **Workaround**: Enable/disable the radio of the client.
CSCuh77093	**Symptom**: A Cisco 3500 Series access point stops responding under severe radio load. **Condition**: This issue occurs when several thousand clients attempt to use the access point at the same time, and when the affected Cisco APs are running an affected version of the software. This occurs due to an interrupt timing issue that is inherent to the CPU utilized in the Cisco APs. **Workaround**: None.
CSCuh78753	**Symptom**: Cisco AP3600 stops responding. **Condition**: This issue occurs when the Cisco AP is in FlexConnect mode and has continuous association and reassociation with clients having flapping WAN connection. **Workaround**: None.
CSCuh82907	**Symptom**: Cisco AP3500 experiences false radar detection. **Condition**: This issue occurs in Release 7.0.235.3. **Workaround**: Use the W52 band.
CSCuh86976	**Symptom**: Cisco NCS displays the “Table too large, possible agent loop” SNMP error message for bsnMeshNeighsTable. The controller sends too many rows to Cisco NCS due to which Cisco NCS SNMP polling stops responding. **Condition**: This issue occurs during an SNMP walk on bsnMeshNeighsTable for a controller using Release 6.0.199.4. **Workaround**: None.
CSCuh86993	**Symptom**: Cisco AP responds to an authentication request for a disabled BSSID. **Condition**: This issue occurs when the Cisco AP receives an authentication request from a client whose database is about to be deleted. **Workaround**: None.
CSCuh87571	**Symptom**: Image upgrade fails occasionally in an HA system. Even though the standby system is operational and in Standby Hot state, it does not show any activity when the image is downloaded, thereby causing failure in image transfer. **Condition**: This issue occurs in a Cisco 5508 Wireless LAN Controller and Cisco WiSM2 HA system. **Workaround**: Reset system and try to download again.

Table 8 Open Caveats (continued)

ID	Description
CSCuh92835	**Symptom**: The "WLAN with duplicate SSID and L2 security policy found." error message is displayed during a change of WLAN configuration. **Condition**: This issue occurs when an attempt is made to change configuration of two similar WLANs that use the same Layer 2 and Layer 3 security, that is QoS, Bandselect. **Workaround**: 1. Disable both WLANs from the controller GUI. 2. Make all WLAN configuration changes using the controller CLI and then enable the WLANs. 3. Delete and re-create the other WLAN from the controller GUI.
CSCuh94259	**Symptom**: When enabling the mDNS profile on an interface group, the "Active WLAN using interface group. Disable WLAN first." error message is displayed, if the interface group has already been mapped to a WLAN or an AP group. **Condition**: Using mDNS gateway on the interface group. **Workaround**: 1. Remove the interface group and then add the group again. 2. Enable the mDNS profile on the interface group before using it.
CSCuh94366	**Symptom**: FlexConnect Local Switching clients are unable to connect to some VLANs and get DHCP. **Condition**: After upgrading a Cisco Flex7510 Wireless LAN Controller to Release 7.4.100.60, clients associated to Cisco AP1242 are unable to connect to a FlexConnect Local Switching WLAN that is mapped to certain VLANs (301 is noted) in the AP's FlexConnect configuration. **Workaround**: Use other VLANs.
CSCuh97457	**Symptom**: Controller incompatibility behavior is observed on Change Of Authentication for RFC 3576 implementation. **Condition**: The attributes sent by the RADIUS server for the user session disconnect request are not acknowledged, when the RADIUS server sends a Change Of Authentication disconnect request. **Workaround**: The disconnect request is accepted when the following three AVP pair attributes are sent: 1. Calling-Station-ID MAC address of the device (lower case works) 2. Service-Type Login-user 3. Called-Station-ID (upper case MAC of AP SSID separated by colons).
CSCuh99194	**Symptom**: A client's first attempt to associate is unsuccessful; the second attempt is successful. **Condition**: Maximum number of clients per AP radio is configured on each Cisco AP1142. **Workaround**: None.

Table 8 Open Caveats (continued)

ID	Description
CSCui01948	**Symptom**: Cisco Prime Infrastructure, Release 1.3, displays the "SNMP operation to Device failed Table too large, possible agent loop" error message when monitoring a Cisco AP or a client associated with the Cisco AP. **Condition**: This occurs when the SSID is set to FlexConnect Local Switching and the Cisco AP is set to Local AP Mode. **Workaround**: None.
CSCui02779	**Symptom**: LDPE and non-LDPE controllers are allowed to form an HA pair. Cisco 600 Series OEAP fails to connect if the failover occurs from the LDPE to the non-LDPE controller. **Condition**: This issue occurs in an HA setup that has LDPE and non-LDPE controllers. **Workaround**: None.

CSCui05324	**Symptom**: Intermittently, after a period of operation, clients are unable to associate with the radio of a Cisco AP. The Cisco AP continues to beacon, but when the client sends an 802.11 authentication frame, the Cisco AP fails to respond with an authentication response because the transmit queues of the radio are filled up.
	Condition: When the current use of the transmit queues is equal to the limit, the radio is unable to transmit.
	For example, in Cisco AP1242, enter the following command:
	`ap#show controller dot11radio0 | include Transmit`
	`Transmit queues: Limit 650 Current 650 In-Progress 0`
	Workaround:
	1. Write a script that monitors the usage of the radio transmit queues in each access points. If a radio is found whose transmit queue usage is nearing its limit, enter the following command:
	`clear interface <interfacename>`
	2. Manually reset the radio of the impacted Cisco AP.

CSCui10841	**Symptom**: The Cisco AP arranges its own bandwidth for SIP Phone, though it is not on the phone. **Condition**: This issue occurs in Release 7.0.240.0. **Workaround**: None.
CSCui12365	**Symptom**: Cisco 5508 Wireless LAN Controller stops responding when a client is moved from a PMIPv6-enabled controller to a non-PMIPv6 enabled controller. **Condition**: This issue occurs if Fast SSID is enabled. **Workaround**: Disable Fast SSID.
CSCui13401	**Symptom**: Client exclusion feature does not become effective. **Condition**: This issue occurs due to repeated 802.1x authentication failures. **Workaround**: None.

Table 8 Open Caveats (continued)

ID	Description
CSCui15077	**Symptom**: Controller stops responding when AAA server pushes Cisco AV pair of url-redirect-acl longer than 32 characters. **Condition**: This issue occurs when the url-redirect-acl name is very long or when you put the URL in this Cisco-av-pair instead of the ACL name. **Workaround**: Use url-redirect-acl names which have less than 32 characters.
CSCui15110	**Symptom**: After adding WLAN to the AP group, it cannot be edited on the AP VLAN mapping page (FlexConnect mode). **Condition:** This issue occurs when you disable WLAN before adding it to the AP group. **Workaround**: 1. Enable the WLAN before adding to AP group. 2. Add another enabled WLAN. 3. Reboot the Cisco AP.
CSCui15562	**Symptom**: Controller stops working due to watchdog issues. **Workaround**: Controller recovers after reboot.
CSCui15800	**Symptom**: DCA assigns radar frequencies or channels that are not supported by AP's radio, but present in the DCA list. **Condition**: This occurs when DCA is enabled in the 40-MHz mode or running on an AP set on 40 MHz. **Workaround**: Use 20 MHz and remove unsupported channels from the list.
CSCui19316	**Symptom**: Voice client fluctuates while passing voice traffic. **Condition**: Create an open SSID in a Cisco AP702 and add it to the d0 radio interface. Try to associate two voice clients and then initiate a call from one to another. **Workaround**: None.
CSCui19817	**Symptom**: Location calibration fails indicating no data points were collected. Same setup works if you use other Cisco AP models (1140). **Condition**: This occurs if you do a location calibration, linear or by data points, in an area covered by Cisco AP2600 models. **Workaround**: Use an existing calibration model.
CSCui20773	**Symptom**: Broadcast queue becomes full. **Condition**: This issue occurs when the wireless clients sends an IGMP report as soon as the query is sent by the controller. **Workaround**: Increase the IGMP query interval and timeout value. If the queue is full and the IGMP query is not processed on the first try, the stream will not be affected until no report is received over the timeout value.
CSCui22463	**Symptom**: Controller using Release 7.4.x stops responding. **Condition**: This occurs when you enable mDNS snooping. **Workaround**: Disable mDNS snooping.

Table 8 Open Caveats (continued)

ID	Description
CSCui23123	**Symptom**: HA upgrade fails with the following error message displayed: `"Standby - Transfer failure: Upgrade from LDPE to non LDPE software is not allowed."` **Condition**: This issue occurs in an HA setup where the primary controller has a non-LDPE image and the secondary WLC has an LDPE image. Both the controllers have 7.4.100.0 software. **Workaround**: Disable HA on controller.
CSCui23134	**Symptom**: Controller stops responding. **Condition**: This issue occurs after you use the ap packet-dump feature. **Workaround**: Do not use the ap packet-dump feature.
CSCui23580	**Symptom**: RAP loses static channel on 5 GHz, and the 2.4-GHz channel gets set to static when configured for Auto. **Condition**: This issue occurs when you have the following settings: RAP-1: Set to Channel 100; 2.4 GHz = Auto RAP-2: Set to Channel 161. 2.4 GHz = Auto Both are initially joined with wired connection to the controller. When the RAP-1 Ethernet link is lost or goes down, it joins over wireless backhaul through RAP-2. When Ethernet connection is available, RAP-1 joins over Ethernet and gets set to channel 161 (remembers previous parents channel information) and 2.4 GHz gets set to static channel 11. **Workaround**: RAP Ethernet connection is never lost. If Ethernet connection is lost, RAP should not join another RAP.
CSCui24995	**Symptom**: During client authentication for a FlexConnect AP in the standalone mode, you will see that the Called-Station-ID attributes do not have the SSID information. **Condition**: This issue occurs in an AP that is configured for local RADIUS support. **Workaround**: Use controller for authentication.
CSCui25551	**Symptom**: FlexConnect Local Switching Local web authentication fails. **Condition**: This issue occurs when the controller using Release 7.4.100.0 performs local switching in a FlexConnect group. **Workaround**: Use central switching.

Table 8 Open Caveats (continued)

ID	Description
CSCui26077	**Symptom**: Fast Transition roam fails between FlexConnect APs. **Condition**: This issue occurs when a client tries to roam using 802.11r Fast Transition between two FlexConnect APs. **Workaround**: Normal roam occurs.
CSCui26223	**Symptom**: When performing an SNMP walk to the controller, there is no response from the device. **Condition**: This issue occurs in FlexConnect controllers with a particular configuration. **Workaround**: Contact Cisco Technical Assistance Center.

Resolved Caveats

Table 9 lists the caveats that are resolved in the 7.5.102.0 controller software release.

Table 9 Resolved Caveats

ID	Title
CSCue91034	Multicast: Handling link-local group addresses in CP/DP without L3 MGID
CSCtk58442	Controller needs forced reset option to recover if it stopped working in software download state
CSCtn54555	Cisco 600 Series OfficeExtend Access Points: Barker Preamble bit in IE42 is set when 802.11n clients associate
CSCtq82437	No CDP neighbor details for LAP
CSCtt47397	Cisco AP3500 watchdog stops working at random with CPU Hog while under light load
CSCtx61744	Cisco 600 Series OEAP low TCP throughput less than 50 Mbps for personal SSID
CSCty84682	AP not forwarding Multicast data and querier messages
CSCtz55837	Cisco Mesh AP cannot associate using mesh security EAP
CSCua97184	Aggr Sched Cat 1: AP stops working due to function pointer issue
CSCub24389	AP stopped working in spamProcessCertPayload
CSCub26654	Cisco AP3600/AP3500 DFS false detect
CSCuc02149	Local switching: Cisco AP3600 drops IP6to4 TCP SYN ACK packets received from LAN
CSCuc06605	Radio reset: SF3 radio ‘tx jammed’[BZ 809]
CSCuc32120	AP: %SYS-2-INTSCHED: ‘idle’ at level 0 interrupts -Process: CAPWAP CL
CSCuc52952	75Dup service IP address error messages on Cisco Catalyst 6500 for Cisco WiSM2 in HA setup
CSCuc72073	Cisco 5508 Wireless LAN Controller stopped working from mobilityCapwapSocketTask

Table 9 Resolved Caveats (continued)

ID	Title
CSCuc81022	Cisco AP1520 experienced excessive DFS detection for in-band/off-channel weather radar
CSCud04882	Cisco AP1142's display of Active Power levels was incorrect
CSCud04901	Cisco AP1550 excessive DFS detection for in-band/off-channel weather radar
CSCud12437	DHCPv6 solicits were sent over the air while it should not have been the case.
CSCud12582	Processing AAA error 'Out of Memory'
CSCud41398	Cisco AP sometimes failed to hear BA from clients that caused BA timeouts [BZ 786]
CSCud44269	Cisco AP should not have bridged ARP traffic for clients with DHCP required in WLAN
CSCud52785	Unable to create SNMP community on Cisco virtual controller
CSCud84135	Cisco AP without default route lacks IP connectivity with other subnets
CSCud97325	Cisco AP3600 sends invalid frames (0000.0104.xxxx) when changing primary controller.
CSCud97830	Telnet access to the controller was lost
CSCue01191	MAC flaps for wired guest MAC on switch connected to foreign controller
CSCue02718	HA redundancy did not fail over to the standby controller when removing Ethernet cable
CSCue02826	5-GHz radio fails on 1552-N in the non-bridge mode associated with the controller with Brazil (-T)
CSCue14501	WSSI interference triggered DCA to change channels on serving radios
CSCue32755	Wireless client was not able to associate with mesh access point with an Ethernet-bridged client
CSCue32955	Wired guest did not get IP address on the controller
CSCue33222	Controller stopped working using Release 7.4.100.0 with mDNS service enabled
CSCue34072	Controller leaking memory for the task: mmlisten
CSCue44986	Client could not detect SIP port while doing FaceTime call
CSCue50917	Root AP failed association as MAP when wired backhaul was lost
CSCue53220	Controller dropped wireless-to-wireless client traffic with source UDP/16666
CSCue54977	RF profile configuration not shown in **show run-config** commands
CSCue55191	Memory leak in mm_listen.c line 8826
CSCue56195	System MAC address is changed to all zeros
CSCue58727	Reaper reset controller due to mutex issue in spectrumRadSlotAQEnableGet
CSCue62388	"AP reloads with DOT11-3-NO_BEACONING ""Not Beaconing for too long"""
CSCue66506	Controller did not accept DHCP server address
CSCue66944	Remote LAN added MAC filtering after upgrade. Cisco 600 Series OEAP radios were disabled
CSCue69665	WebAuth FlexConnect ACL does not always bridge traffic outside of a CAPWAP tunnel

Table 9 Resolved Caveats (continued)

ID	Title
CSCue71856	AP did not send traffic indication to client in power saving mode in time
CSCue73385	Controller: 802.1x interface create failure — "Unable to find 802.1x interface"
CSCue76126	Cisco 5508 Wireless LAN Controller, Cisco 2504 Wireless LAN Controller, and Cisco WiSM2 using Release 7.0.240.0 stopped working due to memory buffer leak
CSCue80611	CLI Syscontact had more restrictive character list than GUI
CSCue83558	Cisco WiSM2 stopped working due to Task Name: apfMsConnTask_6
CSCue84694	Cisco AP did not clear L2 MGID information after Dynamic Interface Change
CSCue87238	Cisco 5508 Wireless LAN Controller using Release 7.4 stopped working without producing any log files.
CSCue89904	QoS per user rate limiting on the WLAN breaks client traffic on roaming
CSCue92521	Cisco 5508 Wireless LAN Controller stopped working due to memory corruption in task name spamApTask6
CSCue93244	Cisco 5500 Series Wireless LAN Controller using HA stopped working due to memory issues during AAA initialization
CSCue99040	Cisco Flex 7500 Series Wireless LAN Controller and Cisco WiSM2 have High Availability issues.
CSCue99208	Advanced 802.11 monitor noise command was lost after reboot
CSCuf03309	Small packet drop on Cisco WiSM2 with DTLS scenario
CSCuf30537	CalledStationId should have used MAC Address per CalledStationID change
CSCuf43147	All AP clears the L2 MGID when WLAN interface mapping deleted from 1 APG.
CSCuf49649	N domain type showed 36-48 as requiring DFS
CSCuf52235	Per WLAN user idle timeout broke global timeout after upgrade
CSCuf56192	Unable to delete an mDNS profile in a particular case
CSCuf61780	Cisco AP1600, Cisco AP2600, and Cisco AP3600 aIOS permitted only 7-dBm power setting
CSCuf65468	RRM was not working as expected on a controller with Cisco 600 Series OEAP
CSCuf74326	Valid Cisco Virtual Controller license misinterpreted by the virtual controller: no AP count
CSCuf76916	After a few failovers, only **clear** and **config** commands were available on the active controller
CSCuf86303	DP heartbeat lost; stopped working at longevity testbed
CSCuf93738	The **save config** command is not updating startup configuration with new AP group interface mapping
CSCug04801	After a few failovers, none of the clients get authenticated
CSCug08277	Cisco AP1260 stopped working in mvl_transmit_recover
CSCug08318	The new Cisco Flex 7500 Series Wireless LAN Controller M3 hardware version was unable to scale to 6000 Cisco APs.
CSCug14709	Controller does not recognize Airespace WLAN ID attribute in access-accept
CSCug16473	Standby controller using Release 7.4.100.0: DP failure in loop with Bluetooth adapter

Table 9 Resolved Caveats (continued)

ID	Title
CSCug19228	The **config mesh linktest** command does not work as expected
CSCug20166	'Network interrupt loop detected'; did not show AP traceback
CSCug22648	WSSI not supported in –S, –N regulatory Domains (possibly more)
CSCug25517	Layer 2 roam entry not initialized in HA standby controller
CSCug26521	Controller using Release 7.4 in DHCP Proxy mode: Option 255 missing in DHCP request packet
CSCug26650	CDP neighbor information was not shown correctly in **Monitor >APs** page
CSCug42677	Controller stopped working when applying CPU ACL in HA
CSCug45057	Radio disabled due to inline power using Release 7.4
CSCug46616	RRM grouping state did not work in computation state
CSCug46718	2.4-GHz client failures on Cisco AP3600, Cisco AP2600, and Cisco AP3500
CSCug49904	DTLS tunnel stopped working after configuration was restored
CSCug50611	Central DHCP Processing WLAN did not get added to the FlexConnect AP
CSCug51714	Clean up error messages about IPV6-3-INVALID_ADDR_ORPHAN
CSCug54108	AP memory leak - %SYS-2-MALLOCFAIL: Memory allocation failed
CSCug57376	Cisco WiSM2 with HA: AP disconnected the active controller and reassociated post switchover
CSCug57436	3502-Mesh Ethernet bridging does not exclude gig() failing to join over radio
CSCug59937	Controller stopped working in tpcv2ConstructApProfile
CSCug64750	ARP request unicast is dropped on anchor scenario
CSCug64950	AP group change to RAP in MAP mode results in stranded RAP
CSCug67289	Cisco Flex 7510 Wireless LAN Controller inverted Caller Station ID in TACACS+.
CSCug74606	Cable AP failed to switch between its cable modem and backhaul radio
CSCug78858	GSSO-CH:Layer 2 ACL worked differently in central switching and local switching.
CSCug79741	Cisco 5500 Series Wireless LAN Controller stopped working on Task: nmspRxServerTask
CSCug80060	PMIPv6 roam issue from Cisco 8500 Series to Cisco 5500 Series Wireless LAN Controllers with AAA override enabled
CSCug82362	All controllers using Release 7.4.100.0 schedule reboots at incorrect times
CSCug86782	AAA override disabled on WLAN was overridden with AAA attributes
CSCug86804	Controller using Release 7.4 stopped working on tplusTransportThread
CSCug86876	WSSI module showed as not working in dual-band section, but as working in the details
CSCug90440	Double 'client authenticated' Trap logs observed in a controller
CSCug91572	FlexConnect AID leak issue
CSCug99623	APs disconnect on software download in an HA pair
CSCuh01250	Cisco Flex 7500 Series Wireless LAN Controller stopped working on task emweb

Table 9 Resolved Caveats (continued)

ID	Title
CSCuh01892	Cisco 600 Series OEAP experienced client disassociation
CSCuh01980	HTTPS to an HA controller failed after reboot because the Web Admin key is missing
CSCuh11276	Client-specific AVC application graph not shown if the client is idle
CSCuh12457	Cisco Flex 7500 Wireless LAN Controller as HA primary controller reboots with gateway reachability issue
CSCuh29695	System stopped working on New Act on software over at acDtlsPlumbDataPlaneKeys
CSCuh41819	Controller: #LWAPP-3-VALIDATE_ERR: spam_lrad.c:10708 Validation of STAT_PAYLOAD
CSCuh48729	Cisco AP3600 stopped working on network interrupt loop (a finding from CSCtt47397)
CSCuh55612	Cisco 600 Series OEAP: WLAN client could not connect because the client database was full
CSCue87961	Controller GUI could not be accessed using management credentials through wireless on Release 7.4
CSCug65693	Apple Macbook client bug caused connectivity issues with the recent OS X update
CSCug23395	Cisco 5500 Series Wireless LAN Controller as HA Secondary controller did not work as expected
CSCug29258	FlexConnect ACL did not retain after AP reboot in standalone
CSCuf52235	Per WLAN user idle timeout broke global timeout after upgrade
CSCuh15491	Aggr_Sched_Stack Corruption (Intermediate Radio Reset Workaround Code)
CSCuh47735	Aggr_Scheduler_Crash - FWD_TRACE_L function (freed dtx in cpq)
CSCug99623	APs disconnect on software download in an HA Pair

Installation Notes

This section contains important information to keep in mind when installing controllers and access points.

Warnings

Warning **This warning means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.** Statement 1071

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death. For proper installation and grounding of the antenna, please refer to national and local codes (e.g. U.S.: NFPA 70, National Electrical Code, Article 810, Canada: Canadian Electrical Code, Section 54).** Statement 280

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).** Statement 13

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground connector. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

Warning **Read the installation instructions before you connect the system to its power source.** Statement 10

Warning **Do not work on the system or connect or disconnect any cables (Ethernet, cable, or power) during periods of lightning activity. The possibility of serious physical injury exists if lightning should strike and travel through those cables. In addition, the equipment could be damaged by the higher levels of static electricity present in the atmosphere.** Statement 276

Warning **Do not operate the unit near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.** Statement 364

Warning **In order to comply with radio frequency (RF) exposure limits, the antennas for this product should be positioned no less than 6.56 ft. (2 m) from your body or nearby persons.** Statement 339

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.** Statement 1017

Safety Information

Follow the guidelines in this section to ensure proper operation and safe use of the controllers and access points.

FCC Safety Compliance Statement

FCC Compliance with its action in ET Docket 96-8, has adopted a safety standard for human exposure to RF electromagnetic energy emitted by FCC-certified equipment. When used with approved Cisco Aironet antennas, Cisco Aironet products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper operation of this radio device according to the instructions in this publication results in user exposure substantially below the FCC recommended limits.

Safety Precautions

For your safety, and to help you achieve a good installation, read and follow these safety precautions. They might save your life!

1. If you are installing an antenna for the first time, for your own safety as well as others, seek professional assistance. Your Cisco sales representative can explain which mounting method to use for the size and type of antenna you are about to install.
2. Select your installation site with safety as well as performance in mind. Electric power lines and phone lines look alike. For your safety, assume that any overhead line can kill you.
3. Call your electric power company. Tell them your plans and ask them to come look at your proposed installation. This is a small inconvenience considering your life is at stake.
4. Plan your installation carefully and completely before you begin. Successfully raising a mast or tower is largely a matter of coordination. Each person should be assigned to a specific task and should know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.
5. When installing an antenna, remember:
   a. Do not use a metal ladder.
   b. Do not work on a wet or windy day.
   c. Do dress properly—shoes with rubber soles and heels, rubber gloves, long-sleeved shirt or jacket.
6. If the assembly starts to drop, get away from it and let it fall. Remember that the antenna, mast, cable, and metal guy wires are all excellent conductors of electrical current. Even the slightest touch of any of these parts to a power line completes an electrical path through the antenna and the installer: **you!**
7. If any part of an antenna system should come in contact with a power line, do not touch it or try to remove it yourself. Call your local power company. They will remove it safely.
8. If an accident should occur with the power lines, call for qualified emergency help immediately.

Installation Instructions

See the appropriate quick start guide or hardware installation guide for instructions on installing controllers and access points.

Note To meet regulatory restrictions, all external antenna configurations must be installed by experts.

Personnel installing the controllers and access points must understand wireless techniques and grounding methods. Access points with internal antennas can be installed by an experienced IT professional.

The controller must be installed by a network administrator or qualified IT professional, and the proper country code must be selected. Following installation, access to the controller should be password protected by the installer to maintain compliance with regulatory requirements and ensure proper unit functionality.

Service and Support

Information About Caveats

If you need information about a specific caveat that does not appear in these release notes, you can use the Cisco Bug Toolkit to find caveats of any severity. Click this URL to browse to the Bug Toolkit:

http://tools.cisco.com/Support/BugToolKit/

(If you request a defect that cannot be displayed, the defect number might not exist, the defect might not yet have a customer-visible description, or the defect might be marked Cisco Confidential.)

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at this URL:

http://www.cisco.com/en/US/support/index.html

Click **Product Support > Wireless**. Then choose your product and **Troubleshooting** to find information on the problem you are experiencing.

Related Documentation

For more information about the Cisco controllers, lightweight access points, and mesh access points, see these documents:

- The quick start guide or installation guide for your particular controller or access point
- *Cisco Wireless LAN Controller Configuration Guide*
- *Cisco Wireless LAN Controller Command Reference*
- *Cisco Wireless LAN Controller System Message Guide*
- *Cisco Wireless Mesh Access Points, Design and Deployment Guide*

You can access these documents at this URL: http://www.cisco.com/cisco/web/support/index.html.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.