Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.3.101.0

First Published: August 2012
Revised Date: December 2012
OL-26898-01

These release notes describe what is new in this release, instructions to upgrade to this release, and open and resolved caveats for this release.

Note 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*.

Contents

These release notes contain the following sections:

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

Cisco Unified Wireless Network Solution Components

The following components are part of the Cisco UWN Solution and are compatible in this release:

Note For more information on the compatibility of wireless software components across releases, see the *Cisco Wireless Solutions Software Compatibility Matrix*.

Note The 7.3.101.0 controller software release is not compatible with Cisco Prime Network Control System (NCS) 1.1.1.24. Cisco Prime Infrastructure 1.2 is required to support the new features in controllers introduced in the 7.3.101.0 controller software release. Cisco Prime Infrastructure 1.2 is the subsequent version of Cisco Prime Network Control System (NCS) 1.1.1.24.

- Cisco IOS Release 15.2(2)JA
- Cisco Prime Infrastructure 1.2
- Mobility services engine software release 7.3.101.0 and context-aware software

  Note Client and tag licenses are required to get contextual (such as location) information within the context-aware software. For more information, see the *Release Notes for Cisco 3350 Mobility Services Engine for Software Release 7.3*.

- Cisco 3350, 3310, 3355 Mobility Services Engine, Virtual Appliance
- 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 LAN Controllers
- Cisco Wireless Controllers for high availability (HA controllers) for 5500 series, WiSM2, Flex 7500 series, and 8500 series controllers
- Cisco Wireless Services Module 2 (WiSM2) for Catalyst 6500 Series switches
- Cisco Wireless Controller on Cisco Services-Ready Engine (SRE) (WLCM2) running on ISM 300, SM 700, SM 710, SM 900, and SM 910
- Cisco Aironet 1550 (1552) series outdoor 802.11n mesh access points; Cisco Aironet 1520 (1522, 1524) series outdoor mesh access points
- Cisco 1040, 1130, 1140, 1240, 1250, 1260, 2600, 3500, 3500p, 3600, Cisco 600 Series OfficeExtend Access Points, AP801, and AP802

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 7.3.101.0, 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 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 this release. For more information about instructions on how to configure these features, see the *Cisco Wireless LAN Controller Configuration Guide*.

- The virtual wireless LAN controller is software that can run on hardware that is compliant with an industry standard virtualization infrastructure. Virtual wireless LAN controllers provide flexibility for users to select the hardware based on their requirement.

  We recommend that you have the following hardware to host a virtual controller:

  - Cisco UCS R210-2121605W Rack Mount Server (2 RU)
  - IBM x3550 M3 server
  - ISR G2 Services Ready Engine (SRE) using UCS Express

  For more information, see
  http://www.cisco.com/en/US/products/ps12723/tsd_products_support_series_home.html

The virtual wireless LAN controller does not have a Manufacturer Installed Certificate (MIC). Therefore, APs cannot validate the virtual controller unless they are using a 7.3-based image such as the follows:

- 12.4(25e)JAL for 1130/1240 series APs
- 15.2(2)JA for 1250/1260/1140/2600/3500/3600 series APs

Follow either of the following two ways to resolve this:

- Install the abovementioned IOS images manually on the AP, join the APs to a hardware based controller using the 7.3 software release to download the image, and disable hash validation by entering the **config certificate ssc hash validation disable** command.
- Configure the virtual controller as a mobility member and include the hash value so that the APs can validate the virtual controller.

Note It is not possible to directly join an AP that has a 7.2 or older image of the controller with the virtual wireless LAN controller. You must first join the AP with a different controller model, say a 5500 or Flex 7500 series controller that is using the 7.3 software or later releases, and then join the AP with the virtual wireless LAN controller.

- Cisco 8500 Series Controllers are introduced with support for local mode, FlexConnect, and mesh modes. The Cisco 8500 Series Controllers support 6000 APs, 64,000 clients, 2000 FlexConnect groups, 6000 AP groups, 100 APs per FlexConnect group, and up to 4095 VLANs. A Cisco 8500 Series Controller can support up to 24,000 rogue APs and 32,000 rogue clients. For more information, see http://www.cisco.com/en/US/products/ps12722/tsd_products_support_series_home.html
- Increased scale for Cisco Flex 7500 Series Controllers to support 6000 APs, 64000 clients, 2000 FlexConnect groups, 6000 AP groups, 100 APs per FlexConnect group, and up to 4096 VLANs.
- The number of rogue APs and rogue clients that can be detected per platform is increased (see Table 1-1).

Table 1-1 Number of Rogue APs and Rogue Clients that Can Be Detected

Controller Platform	Number of Rogue APs	Number of Rogue Clients
Cisco 2500 Series Controller	2000	2500
Cisco 5500 Series Controller	2000	2500
Cisco WiSM2	4000	5000
Cisco Flex 7500 Series Controller	24000	32000
Cisco 8500 Series Controller	24000	32000
Cisco Virtual Wireless LAN Controller	800	1500

- This release extends the number of radio frequency identifiers (RFIDs) to be supported (see Table 1-2).

Table 1-2 Number of RFIDs Supported on Controller Platforms

Controller Platform	Number of RFIDs Supported
Cisco WiSM2	10000
Cisco Flex 7500 Series Controller	50000
Cisco 8500 Series Controller	50000
Cisco Virtual Wireless LAN Controller	3000

- The Cisco Aironet 2600 Series Access Points are supported. For more information, see http://www.cisco.com/en/US/products/ps12534/index.html.
- High availability (HA) in controllers allows you to reduce the downtime of the wireless networks, due to the failover of controllers. In this release, a 1:1 (Active:Standby-Hot) AP stateful switchover (AP SSO) is supported. In an HA architecture, one controller is configured as the primary controller and another controller as the secondary controller.

  After you enable HA, the primary and secondary controllers are rebooted. During the boot process, the primary controller role is negotiated as active and the secondary controller as standby-hot. After a switchover, the secondary controller becomes the active controller and the primary controller becomes the standby-hot controller. After subsequent switchovers, the roles are interchanged between the primary and the secondary controllers. The reason for switchovers could be due to manual trigger or a controller or network failure.

Note Internal DHCP is not supported.

- FlexConnect-related features:
  - Split tunneling allows the traffic sent by a client to be classified based on the packet contents. The matching packets are locally switched and the rest of the traffic is centrally switched. The traffic that is sent by the client that matches the IP address of the device present in the local site can be classified as locally switched traffic and the rest of the traffic as centrally switched.

    This feature is supported on the AP1040, AP1140, AP1260, AP2600, AP3500, and AP3600 access points.
  - Support to configure Network Address Translation (NAT) and Port Address Translation (PAT) on FlexConnect locally switched WLANs is added. You must enable Central DHCP Processing to enable NAT and PAT.

    This feature is supported on the AP1040, AP1140, AP1260, AP2600, AP3500, and AP3600 access points.
  - Support for the Point to Point Protocol (PPP) and the Point to Point Protocol over Ethernet (PPPoE) is added for APs in FlexConnect mode. You must configure PPPoE submode when the AP is in FlexConnect mode.

    This feature is supported on the AP1040, AP1140, AP1260, AP2600, AP3500, and AP3600 access points.
  - This release extends WGB/uWGB support to FlexConnect APs for locally switched WLANs.

    WGB is supported on all FlexConnect APs: AP1040, AP1130, AP1140, AP1240, AP1250, AP1260, AP1520, AP2600, AP3500, AP3600, AP801, and AP802.
  - This release extends support for 802.11u in FlexConnect mode.

  - 802.11r Fast Transition is now supported on FlexConnect APs in central and locally switched WLANs.
  - VLAN-based local and central switching is supported. When a AAA server returns a VLAN configured for a client, the VLAN is configured on the local IEEE 802.1Q link, the AP bridges the traffic locally. If the VLAN is not configured on the AP uplink, the AP tunnels the traffic back to the controller. The controller bridges the traffic into the corresponding VLAN from where the traffic is transported toward the next routing instance for further processing.

- Table 1-3 lists the 802.11r L2 and L3 roaming rates that are supported in this release on the 5500 and WiSM2 controllers:

Table 1-3 802.11r L2 and L3 Roaming Rates Supported in the 7.3 Release

Roaming Type	Controller Platform	Roaming Rate	Failure Rate (Roam Time > 20 milliseconds)
Intracontroller Roam	Cisco WiSM2	400 roams per second	Less than 1%
	Cisco 5500 Series Controller	350 roams per second	Less than 1%
Intercontroller Roam	Cisco WiSM2	200 roams per second	Less than 5%
	Cisco 5500 Series Controller	200 roams per second	Less than 5%

- This release extends support for HotSpot 2.0 specifications, where APs in mesh mode and APs in FlexConnect mode in locally switched WLANs are also supported.
- IPv6 address support is added for rogue client and wIPS alarms. Three new wIPS signatures are supported.
- This release extends support for IPv6 on Cisco Wireless Controller on Cisco Services-Ready Engine (SRE).
- Right to Use (RTU) licensing allows you to enable a desired AP license count on the controller after you accept the End User License Agreement (EULA). This process enables you to add AP counts on a controller without interacting with external tools.

  RTU licensing is supported only on Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN Controllers.
- This release extends support to video CAC for calls that are based on TSpec and SIP. For example:
  - TSpec-based video calls including 802.11n clients.
  - Facetime and Cius video call applications that use SIP unencrypted signaling.
- You can configure WLANs to do 802.1X authentication of clients if MAC authentication with static WEP fails. Clients are deauthenticated if they fail the 802.1X authentication. If MAC authentication is successful and clients send a request to start 802.1X authentication, clients have to pass the 802.1X authentication to be allowed to send data traffic. Otherwise, clients are deauthenticated. If clients choose not to have 802.1X authentication, they can be declared as authenticated if they pass MAC authentication.
- Proxy Mobile IPv6 is a network-based mobility management protocol that supports a mobile node by acting as the proxy for the mobile node in any IP mobility-related signaling. The mobility entities in the network track the movements of the mobile node and initiate the mobility signaling and set up the required routing state.

The main functional entities are the Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG). The LMA maintains the reachability state of the mobile node and is the topological anchor point for the IP address of the mobile node. The MAG performs the mobility management on behalf of a mobile node. The MAG resides on the access link where the mobile node is anchored. The controller implements the MAG functionality.

Note PMIPv6 MAG functionality is supported only on Cisco 5500 Series Controllers, Cisco 8500 Series Controllers, and Cisco WiSM2.

Note In this release, the Cisco 8500 Series Controllers can support a maximum of 40,000 PMIPv6 clients out of the 64,000 clients that are supported.

- You can enable or disable IPv6 globally by entering this command:

  config ipv6 {**enable** | **disable**}

- You can upload the output of the **show run-config** command onto an FTP server by entering this command:

  transfer upload datatype run-config

- Support for detection and forwarding of the first HTTP packet with a user-agent attribute from a client per session to profile the client, where the controller acts as a collector, is added in this release.
- To resolve issues such as voice and security on wireless networks, you might need to dump packets from the AP for analysis while the AP continues to operate normally. The packets can be dumped onto an FTP server. This process of dumping packets for analysis is called Packet Capture. Use the controller to start or stop packet capture for clients. You can choose the type of packets that need to be captured using the controller.
- In this release, RF profiles incorporate new configurations, which are specially targeted at high-density and stadium environments. These new configurations are as follows:
  - High-density configurations
  - Stadium vision configurations
  - Out-of-the-box AP configurations
  - Band select configurations
  - Load balancing configurations
  - Coverage hole mitigation configurations
- VLAN tagging on Ethernet interfaces is supported. You can configure VLAN tagging on the Ethernet interface either directly from the AP console or through the controller and Cisco Prime Infrastructure. You must save the configuration in flash and all CAPWAP packets use the VLAN tag as configured with all the locally switched traffic, which is not mapped to a VLAN. When enabled, the CAPWAP packets from the AP are forwarded through the trunk VLAN. If it fails, the AP falls back to the untagged mode.
- DHCP Option 82 enhancement—You can also specify the name and the SSID of the access point to the DHCP Option 82 payload.
- RADIUS CallStationID enhancement—You can also specify the name and the SSID of the access point to determine the RADIUS CallStationID.

- The bandwidth contract feature is enhanced so that rate limits can be defined on both upstream and downstream traffic. Rate limits can be defined per SSID and/or specified as a maximum rate limit for all clients. These rate limits can be individually configured. This feature is supported on AP1140, AP1040, AP3500, AP3600, AP1250, and AP1260. In centrally switched WLANs, the downstream traffic is rate limited by the controller and the upstream is rate limited by the APs. In local switched WLANs, both upstream and downstream are traffic are rate limited by the APs.
- RADIUS source interface is aware of the AP group, which allows sourcing the RADIUS packets from the interface assigned to the AP group. To allow partitioning of a network into different subnets, AP groups can be used to provide site-specific VLANs, where each VLAN has its own IP subnet that can be identified. For all client associations to the site-specific VLAN on the AP, all RADIUS interactions must be sourced from the IP address of that site-specific VLAN, which maps an AP group to a site-specific VLAN and maps the VLAN to a unique IP subnet.
- Increased RADIUS servers per WLAN from 3 to 6.
- Added SNMP support to swap controller images (primary and standby).
- AP searches and renaming of APs are based on serial numbers.
- Usernames are displayed in client summaries.
- This release is compliant with the Federal Information Processing Standard (FIPS) 140-2 standard for wireless controllers and APs.
- This release introduces two new AP1552 models:
  - AP1552CU
  - AP1552EU
- AP802H, a newer version of AP802 is supported. For more information, see http://www.cisco.com/en/US/prod/collateral/routers/ps10906/ps380/qa_c67-678460.html.
- Support is added to the following features on the AP1552 models to match the ones with the indoor APs:
  - Local, FlexConnect, Monitor, Rogue Detector, and Sniffer modes
  - VideoStream in Local mode
  - HotSpot 2.0 in Local mode
  - VoWLAN
  - Band Select
  - Datagram Transport Layer Security (DTLS)

Note Support is added for DTLS data plane encryption for the AP1552s in Local and FlexConnect mode.

  - CleanAir of 5-GHz radio
- Mesh outdoor access points support local mode. In this mode, the AP can handle clients on its assigned channel or while monitoring all channels on the band over a 180-second period. During this time, the AP listens on each channel for 50 milliseconds for rogue client beacons, noise floor measurements, interference, and IDS events. The AP also scans for CleanAir interference on the channel.
- The operating frequency in the 5-GHz band for the 1550 series access points has been increased from 5.850 GHz to 5.875 GHz.

- A new country domain has been added for India. The –D domain supports the 20-MHz channels, which are 169 (5.845 GHz) and 173 (5.865 GHz), and the 40-MHz channel pair, which is 169/173 (5.855 GHz).
- You can activate CleanAir Advisor when you enable CleanAir on a backhaul radio. CleanAir Advisor generates Air Quality Index (AQI) and Interfere Detection Reports (IDRs), but the reports are displayed only in the controller. No action is taken through Event Driven RRM (ED-RRM).
- You can order AP1552E/EU with an Ethernet Passive Optical Network (EPON) SFP as an add-on. The EPON SFP provides Gigabit data rates. EPON SFP is not an orderable feature on the AP1552. You must order it separately and install it.

Software Release Support for Access Points

Table 1-4 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.

Table 1-4 Software Support for Access Points

Access Points		First Support	Last Support
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
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	—

Table 1-4 Software Support for Access Points (continued)

Access Points		First Support	Last Support
	AIR-LAP1262N	7.0.98.0	—
1300 Series	AIR-BR1310G	4.0.155.0	7.0.x
1400 Series	Standalone Only	—	—
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	—
	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

Table 1-4 Software Support for Access Points (continued)

Access Points		First Support	Last Support
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	—
	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	7.3.101.0	—
	AIR-CAP1552EU-x-K9	7.3.101.0	—
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 7.3.101.0

Guidelines and Limitations

- The 7.3.101.0 controller software release is not compatible with Cisco Prime Network Control System (NCS) 1.1.1.24. Cisco Prime Infrastructure 1.2 is required to support the new features in controllers introduced in the 7.3.101.0 controller software release. Cisco Prime Infrastructure 1.2 is the subsequent version of Cisco Prime Network Control System (NCS) 1.1.1.24
- 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 7.3.101.0 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 7.3.101.0. Table 1-5 shows the upgrade path that you must follow before downloading software release 7.3.101.0.

Table 1-5 Upgrade Path to Controller Software Release 7.3.101.0

Current Software Release	Upgrade Path to 7.3.101.0 Software
7.0.98.0 or later 7.0 releases	You can upgrade directly to 7.3.101.0
7.1.91.0	You can upgrade directly to 7.3.101.0
7.2. or later 7.2 releases	You can upgrade directly to 7.3.101.0

- 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 7.3.101.0 from an earlier release, you must also upgrade to Cisco Prime Infrastructure 1.2 and MSE 7.3.101.0.
- 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.
- 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.
- Ensure that you have a TFTP or FTP server available for the software upgrade. Follow these guidelines when setting up a TFTP or FTP server:
  - Ensure that your TFTP server supports files that are larger than the size of the controller software release 7.3.101.0. 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 7.3.101.0 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 Configuration Guide*.

Note Predownloading a 7.3.101.0 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 7.3.101.0 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
- Ensure that you apply the calibration fix for AP1260 and AP3500 models (see the resolved caveat CSCty68030). This addresses a manufacturing calibration issue on the AP1260 and AP3500 models (VID V01). For more information, see https://supportforums.cisco.com/docs/DOC-25460.

Upgrading to Controller Software Release 7.3.101.0 (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 7.3.101.0 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 or FTP 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** or **FTP.**

Step 9 In the IP Address text box, enter the IP address of the TFTP or FTP 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 7.3.101.0 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 7.3.101.0" section on page 12.

Interoperability With Other Clients in 7.3.101.0

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

Table 1-6 describes the configuration used for testing the clients.

Table 1-6 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	7.3.101.0
Controller	Cisco 5500 Series Controller
Access points	1131, 1142, 1242, 1252, 3500e, 3500i, and 3600

Table 1-6 Test Bed Configuration for Interoperability

Radio	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 1-7 lists the client types on which the tests were conducted. The clients included laptops, handheld devices, phones, and printers.

Table 1-7 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
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 5.0.1
Apple iPad3	iOS 5.1.1
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

Table 1-7 Client Types (continued)

Client Type and Name	Version
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
Spectralink 8030	119.081/131.030/132.030
Vocera B1000A	4.1.0.2817
Vocera B2000	4.0.0.345
Apple iPhone 4	iOS 5.0.1
Apple iPhone 4S	iOS 5.1.1
Ascom i62	2.5.7
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 Wireless Controller on Cisco Services-Ready Engine
- Features Not Supported on Cisco Virtual Wireless LAN Controllers
- Features Not Supported on Mesh Networks

Features Not Supported on Cisco 2500 Series Controllers

- Wired guest access
- Cisco 2500 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.
- Bandwidth contract
- Service port
- AppleTalk Bridging
- LAG
- Right to Use licensing
- Multicast-to-unicast
- High Availability
- PMIPv6

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
- Layer 2 access control list (ACL) support
- 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
- LAG
- 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
- PMIPv6

Features Not Supported on Cisco 8500 Controllers

- LAG
- Cisco 8500 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.
- TrustSec SXP
- Local authentication (controller acting as authentication server)
- Internal DHCP server
- Wired guest access

Features Not Supported on Cisco Wireless Controller on Cisco Services-Ready Engine

- Wired guest access

- Cisco Wireless Controller on Cisco Services-Ready Engine (SRE) 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.
- Bandwidth contract
- Access points in direct connect mode
- Service port support
- AppleTalk Bridging
- LAG

Features Not Supported on Cisco Virtual Wireless LAN Controllers

- Data DTLS
- Cisco 600 Series OfficeExtend Access Points
- Wireless rate limiting (bandwidth contract)
- Internal DHCP server
- TrustSec SXP
- Access points in local mode
- Mobility/guest anchor
- Multicast-unicast mode
- IPv6
- PMIPv6
- WGB
- VideoStream
- High Availability
- Outdoor mesh access points

Note Outdoor APs such as AP1552 are supported in FlexConnect mode are supported if the APs are not used in a mesh deployment.

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 7.3.101.0. 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 1-8 lists the open caveats in the 7.3.101.0 controller software release.

Table 1-8 Open Caveats

ID	Description
CSCub67462	Ethernet bridged clients on AP3600 models are unable get IP. **Symptom**: Ehternet bridging does not work with AP3600e/i models. **Conditions**: AP3600 in bridge mode and Ethernet bridging enabled. **Workaround**: None.
CSCub26289	Controller does not raise alarm after automatic configuration changes after an upgrade. **Symptom**: Following the resolution for the CSCty45920 issue in the 7.3 release, the controller changes the overlapping subnet interface IP addresses to all zeros without raising any visible alarm on the GUI or the CLI. The controller does not log a message on msglog, traplog, or after entering the **show invalid-config** command. After the controller is upgraded and the controller reboots with all the zero IP address interfaces, there could be network outages if you do not know about these silent configuration changes. **Conditions**: Controller had overlapping subnet interfaces before upgrading the controller software release that had the fix for the CSCty45920 issue. **Workaround**: Ensure that the controller does not have overlapping interfaces before the upgrade.
CSCtz07676	Controller cannot establish SXP connection with a Cisco Nexus 7000 Series switch. **Symptom**: An SXP connection from the controller to the Cisco Nexus 7000 Series switch reports the On state on the controller side while the switch reports the Waiting for Response state. **Conditions**: Establishing SXP connection between the controller and ASA. **Workaround**: Add an intermediate device that supports SXPv2 between the controller and the Cisco Nexus 7000 Series switch.
CSCua45032	Outer DSCP is 46 with client gold QoS level policy. **Symptom**: The outer DSCP is 46 with a gold QoS level policy for the client. **Conditions**: During AAA override of QoS values. **Workaround**: None.
CSCub42439	An AP sends CAPWAP control frame incorrectly to the client. **Symptom**: AP Sends CAPWAP control frame to client incorrectly when gateway IP address of AP is assigned to the client. **Conditions**: The gateway IP address of the AP is assigned to the client. The client is pinging the AP for a few seconds, but the AP starts to send CAPWAP control frames to the client incorrectly. **Workaround**: None.

Table 1-8 Open Caveats (continued)

ID	Description
CSCtz76132	AP stops working during check HEAP while validating allocated memory pool. **Symptom**: AP1130 stops working with crashlog entries including messages such as the following: `%SYS-3-CPUHOG: Task is running for (1992)msecs, more than (2000)msecs (29/26),process = Check heaps.` **Conditions**: AP1130 connected to a controller on the 7.0.230.0 software release. **Workaround**: None.

CSCtz93407	Mesh traps have invalid content.
	Symptom: All mesh traps have invalid information on SNR, hop counts, and so on:
	`Mesh node '88:f0:77:XX:XX:XX' has detected low SNR '0' from its parent Mesh node '00:02:cd:fc:00:00'.`
	`Mesh node '88:f0:77:XX:XX:XX' has detected high SNR '255 db' from its parent Mesh node '00:01:2e:bf:00:00'.`
	Parent MAC does not exist, and SNR is incorrect.
	Excessive hop count of 56 on mesh node 88:f0:77:XX:XX:XX. It is not possible to have 56 hops on the topology.
	Conditions: No associated condition.
	Workaround: None.

CSCua45747	AP stops working during ARP processing. **Symptom**: AP stops working. This is a very low-frequency event (one AP, once a month). **Conditions**: ARP processing. **Workaround**: Reboot the AP.

Table 1-8 Open Caveats (continued)

ID	Description

CSCtw67184	Controller loses RAID after a power interruption.
	
	Symptom: During the boot process, the following error message appears on the attached monitor or on the 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 Spacebar key is pressed, the system could not boot from the disk.
	
	Conditions: The Cisco Flex 7500 Series Controller had an unexpected power interruption (the power plug was pulled while the system was operational). After the reboot, the RAID card could not find its configuration in the flash memory and therefore it could not boot.
	
	Workaround: Enter the WebBIOS, which is a RAID management tool. 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-line interface (CLI).
	
	The CLI version can be accessed from the serial console. You are prompted for this on the serial console after the error message is displayed.
	
	1. Press **Ctrl-Y** to enter the CLI version of the WebBIOS tool in the following command:
	
	`-CfgForeign -Import -a0`
	
	2. Reboot the server.
	
	Further Problem Description: When the Spacebar key is pressed, the system could not boot from the disk. During bootup, the LSI WebBIOS loads correctly and shows two physical disks but no virtual disks. It appears that the RAID configuration that was present in the system was lost.
	
	The controller encountered an unexpected power interruption (the power plug was pulled while the system was operational). After the reboot, the RAID card could not find its configuration in the flash memory and therefore it could not boot. The flash configuration was corrupted or deleted 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, the card does not automatically get the backup configuration information from the hard drives. The information on the hard drives is considered a foreign configuration that requires your intervention.
	
	The system waits for you to take action. Note that all the data on the hard drives are still intact.

Table 1-8 Open Caveats (continued)

ID	Description

CSCua09530	Invalid tar magic error on custom WebAuth download on a Cisco Wireless Controller on Cisco Services-Ready Engine (SRE).
	Symptom: Downloading a custom WebAuth bundle tar file to a Cisco Wireless Controller on Cisco Services-Ready Engine (SRE) might fail with the following output:
	`TFTP receive complete... extracting webauth files.`
	`tar: invalid tar magic`
	
	`Error extracting webauth files.`
	
	Conditions: Tar file created with 7zip. The same tar file might successfully download to other controller platforms.
	Workaround: Tar the custom WebAuth files using the unix tar utility.
	`tar -cvf <output.tar> login.html`

CSCua45762	AP stops working during RRM packet validation. **Symptom**: AP stops working during RRM message processing. This is a very low-frequency event (one AP, once a month). **Conditions**: Unknown. **Workaround**: Reboot the AP.
CSCua58695	Controller responds to SNMPv1 query when SNMPv1 is disabled. **Symptom**: If the controller is queried through SNMPv1 when SNMPv1 is disabled but SNMPv2 and/or SNMPv3 is enabled, the controller responds to the SNMPv1 query with a null response. The controller should not respond to the SNMPv1 query if this version is explicitly disabled. **Conditions**: None. **Workaround**: None.
CSCub03023	WebAuth redirect to custom page, gets credential information, redirects to internal page. **Symptom**: WebAuth redirects to custom page, gets user credential information, again redirects to internal page, gets user credential information, and eventually succeeds. **Conditions**: HTTPs/HTTP WebAuth redirection when using custom WebAuth bundle. **Workaround**: Use internal WebAuth page.
CSCub14541	Need an option to enable and disable S-60 messages on the controller CLI and GUI. **Symptom**: Teklogix scanners do not work when connecting to the WLAN. This issue is due to the S-60 messages sent by the controller, which the scanners drop. **Conditions**: CCX is enabled on the client. The devices do not respond and need to reboot. **Workaround**: Turn off CCX on the client devices.

Table 1-8 Open Caveats (continued)

ID	Description
CSCub04273	Controller rogue detector falsely reports rogue AP to be on the network. **Symptom**: The controller rogue detector mode AP incorrectly reports the rogue AP to be on the network near crowded locations such as an airport. **Conditions**: Rogue detector mode APs in their network connected to a switch in trunk mode configuration seeing all the VLANs. The APs are not on a wired infrastructure. A debug on the rogue detector gets the MAC address of the rogue AP, but the wired sniffer traces do not show the ARP traffic entries of the rogue AP, which implies that it is a false positive that is reported to be on the network. **Workaround**: None.
CSCub13415	AP3502 in H-REAP local switching does not forward broadcast ARP. **Symptom**: Wireless phones are experiencing sporadic one-way or no-way audio. **Conditions**: Wireless phones (7925) connected to APs in H-REAP, Local Switching, Local Authentication, WPA2/AES/PSK. **Workaround**: • Reboot the AP (works for a short time). • Roam away and back (works for a short time). • Use WEP instead.
CSCub14813	APs with CDP disabled returns to enabled state after a failover. **Symptom**: A redundant topology with primary and secondary controllers are configured. CDP is disabled on all APs by entering the **config ap cdp disable all** command on the primary controller. After APs failed over to the secondary controller, the CDP of some APs returned to the enabled state. **Conditions**: Failover. **Workaround**: None.
CSCub23546	AP1130 stops working during MFP validation. **Symptom**: AP1130 stops working. **Conditions**: • AP1130 and AP1240 on the 7.2.x.x controller software release • MFP enabled **Workaround**: None. Low frequency issue, AP reboots.

Table 1-8 Open Caveats (continued)

ID	Description

CSCub21596	Duplicate and invalid association identifier entries for FlexConnect clients.
	Symptom: Multiple issues are seen with invalid and duplicate AID entries on the 7.2.103.0 controller software release. The following error messages appear:
	`*apfReceiveTask: Jul 18 18:22:01.632: %LWAPP-3-INVALID_AID2: spam_api.c:1226 Association identifier 8 for client cc:52:af:7f:d8:8b is already in use by cc:52:af:7f:d2:1`
	`*apfReceiveTask: Jul 18 18:03:45.096: %LWAPP-3-INVALID_AID2: spam_api.c:1226 Association identifier 2 for client cc:52:af:7f:cd:4e is already in use by cc:52:af:7f:d6:a1`
	Also, clients do not respond to ARP or broadcast issues, and the APs do not move to the standalone mode.
	Conditions: FlexConnect mode APs on the 7.2.103.0. controller software release.
	Workaround: None.

CSCub24389	AP stops working during the spamProcessCertPayload process. **Symptom**: Stack Trace: `[0x001A1A60] crashdump(0x1a18dc)+0x184 [0x001A19B0] crashdump(0x1a18dc)+0xd4 [0x001CB2F8] get_block(0x1cb130)+0x1c8 [0x001BA118] malloc(0x1b9e9c)+0x27c [0x005AAA08] spamProcessCertPayload(0x5aa9e8)+0x20 [0x00585BAC] lwapp_client_process_q(0x5859c0)+0x1ec [0x00586BB4] lwapp_client_process(0x58679c)+0x418 [0x001A5AF0] process_execute(0x1a5964)+0x18c</B></B>` **Conditions**: Using LSC on a Cisco 5508 Controller results in multiple APs (AP3500 and AP1131 models). **Workaround**: Disable LSC on the controller.
CSCub24566	WebAuth redirect fails. All token entries are already in use. **Symptom**: Some clients fail to redirect to the web authentication page. **Conditions**: • Per-user bandwidth contracts are in use • Auto-anchor mobility (Guest Anchoring) • Anchor controller on the 7.2.103.0 software release • Foreign controllers on the 7.0.230.0 software release **Workaround**: Reboot the anchor controller.
CSCub25051	Mesh 1524SB radio0 excessive reset with code 50. **Symptom**: 1524SB radio0 excessive reset with code 50 causes client drops. **Conditions**: Not applicable. **Workaround**: None.

Table 1-8 Open Caveats (continued)

ID	Description
CSCub38930	Controller loses time zone after reboot. **Symptom**: The controller loses the time zone after a reboot. This is specific to time zone location index 30 and 31 (New Zealand). **Conditions**: When the time zone is configured on the controller, the configuration is saved and rebooted. **Workaround**: Use the **delta** command. Do not set the time zone location.
CSCub42900	Cisco 5508 Controller stops working on the 7.0.220.0 controller software release. **Symptom**: Cisco 5508 Controller stops working. **Conditions**: Cisco 5508 Controller on the 7.0.220.0 controller software release. The controller had been operational for 100 days. **Workaround**: Reboot the controller. **Further Problem Description**: It was found that the Ethernet driver stopped working. The controller was rebooted after which it became operational. The controller stopped working again, after which it was rebooted, and the cycle continued.
CSCub40170	AAA VLAN override fails when a client moves from 802.1X to MAC authentication WLAN. **Symptom**: If a wireless client moves from an 802.1X WLAN to a RADIUS MAC authenticated WLAN on the same controller, the AAA override VLAN mapping might not succeed. **Conditions**: • 7.2.110.0 controller software release • All involved WLANs have AAA override enabled **Workaround**: Two options: • Deauthenticate the client • Decrease the session timeout of the MAC authentication WLAN.
CSCub41983	Maximum allowed clients per AP radio does not work for two APs. **Symptom**: With one controller and one AP, when the Maximum Allowed Clients Per AP Radio for WLAN is set to 1, it works as expected. With one controller and two APs, when the Maximum Allowed Clients Per AP Radio for WLAN setting is still set as 1, it was found that two clients were associated to the same AP. **Conditions**: None. **Workaround**: None.

Table 1-8 Open Caveats (continued)

ID	Description

CSCub23677	Aggregate probe request interval became 0 seconds.
	Symptom: Aggregate probe request interval is 500 milliseconds by default.
	Advanced configuration:
	`Probe request filtering.....  Enabled`
	`Probes fwd to controller per client per radio....  2`
	`Probe request rate-limiting interval.....  500 msec`
	`Aggregate Probe request interval.....  500 msec <<`
	
	This value will be 0 millisecond under a particular condition.
	Advanced Configuration:
	`Probe request filtering.....  Enabled`
	`Probes fwd to controller per client per radio....  2`
	`Probe request rate-limiting interval.....  500 msec`
	`Aggregate Probe request interval.....  0 msec  <<`
	
	Conditions: This issue occurs if the following is done on the controller:
	1. Client load balancing is enabled on one WLAN.
	The aggregate probe request interval is shown as 0 as expected.
	2. The WLAN is deleted and created again.
	Client load balancing is disabled.
	3. The aggregate probe request interval is 0.
	Workaround: The following step returns to the default value of 500 milliseconds.
	0. Problematic controller shows an aggregate probe request interval as 0 millisecond.
	`Aggregate Probe request interval.....  0 msec`
	1. Disable the WLAN by entering the **config wlan disable** *wlan-id* command.
	2. Enable client load balancing by entering the **config wlan load-balance allow enable** *wlan-id* command.
	3. Disable client load balancing by entering the **config wlan load-balance allow disable** *wlan-id* command.
	4. Enable the WLAN by entering the **config wlan enable** *wlan-id* command.
	5. The aggregate probe request interval returns to the default value of 500 milliseconds.
	`Aggregate Probe request interval.....  500 msec`

Table 1-8 Open Caveats (continued)

ID	Description

CSCub44007	SSHPM rule leak on service port address renewal.
	
	Symptom: The controller displays error messages such as the following:
	
	`*sshpmMainTask: Jun 28 15:18:20.121: %SSHPM-4-SSH_ALERT: sshglue.c:1437 SSH ERROR Auth): The maximum number of policy rules reached`
	
	`sshpmMainTask: Jun 28 15:18:20.121: %SSHPM-3-RULE_CREATION_FAILED: sshpmrules.c:2250 inbound WCP rule creation failed for peer 0.0.0.0`
	
	Conditions:
	• Cisco WiSM
	• Service port with DHCP in use with relatively low lease time
	
	Workaround: Use the service port with a static IP address, or long lease time. Reboot the controller after the error is observed to recover the controller.

CSCua76243	SRE710 does not boot after upgrade. **Symptom**: SRE becomes corrupt during the image upgrade process on rare occasions, which causes the unit to be unable to boot because the flash image is corrupted on both sides. **Conditions**: Upgrading SRE to the 7.3 release sometimes causes the flash to be corrupted, and a manual image download needs to be performed. **Workaround**: If the flash is corrupted during an image download, manual image recovery must be done through the router that this device is plugged into. A manual image transfer must include the files with these extensions on the tftp server to allow software download: .aes, .install.sre, .install.sre.header, .installer, .key, ER.aes, ism_bl, and sm_bl.
CSCub46092	H-REAP is central switched when WLAN is set for local switching. **Symptom**: Client sometimes is left in central switched mode even though WLAN is set for local switching. **Conditions**: MAC filtering Web-Auth on fail enable for local switched H-REAP. **Workaround**: Bounce the client wireless adapter.
CSCub50981	GTK key update breaks for clients on FlexConnect AP using local authentication. Symptom: ARP issues seen with wireless clients on FlexConnect APs using local authentication. **Conditions**: Wired server on the same network cannot ARP for wireless clients. **Workaround**: Move to central authentication for the FlexConnect APs.

Table 1-8 Open Caveats (continued)

ID	Description
CSCub52566	HA: Active controller stops working during the rsyncmgrXferMain task. **Symptom**: In an HA environment, the active controller might stop working during an image and/or configuration download to the standby-hot controller with the rsyncmgrXferMain task if the standby-hot controller detects gateway and/or peer unreachability and reloads in the middle of a download. **Conditions**: • HA pair is up • Image download started on the active controller • Image successfully written on the active controller • Image transfer successful to the standby-hot controller • Image write in progress on the standby-hot controller • Standby-hot controller unable to reach gateway, detected gateway failure, and started rebooting • If the standby-hot controller detects peer unreachable and starts reloading during download process from the active controller **Workaround**: Always schedule an image download, configuration download during a scheduled maintenance window to avoid disruption in the wireless service.
CSCub52499	In an HA environment, Cisco 8500 Series controller as the active controller stops working. **Symptom**: HA paired 7500 or 8500 controller might abruptly stop working. **Conditions**: None. **Workaround**: If the active controller stops working, the standby-hot controller takes over, and the wireless service is restored automatically. Then, you must manually power off/on the controller that has stopped working. If the standby-hot controller stops working, the active controller continues to operate. You must manually power off/on the controller that has stopped working.
CSCub15299	AP1242 is registered to one controller, ignoring the primary configuration. **Symptom**: AP1242 is registered to one controller and is unable to switch to another controller. Rebooting the access point does not resolve the issue. **Conditions**: Not applicable. **Workaround**: Clear the configuration on the AP.
CSCua37498	License module stops working and the controller prompts saying another user has transfer in progress. **Symptom**: While trying to install a license, it was found out that the controller does not allow any transfer stating that "another user has transfer in progress." The controller could not be reset. The controller then had a “devshell crash.” **Conditions**: None. **Workaround**: None.

Table 1-8 Open Caveats (continued)

ID	Description
CSCtu36088	MAP key error on failover recovery scenario between RAPs. **Symptom**: A MAP can stop working on decrypt errors for a long time and fail to recover when joining from the secondary controller to the primary controller, after a failure of the primary controller. The MAP might need a reboot to recover. **Conditions**: The problem can be reproduced consistently in the following conditions: 1. Two controllers: one primary and one backup. 2. Two RAPs, two MAPs. All mesh APs are associated with the primary controller. 3. Mesh tree is R1-M1, R2-M2. 4. Primary controller is disconnected from the network. 5. All APs are associated with the secondary controller, same mesh tree. 6. After some minutes, the primary controller is brought back online, and fallback is enabled. 7. APs reassociate with the primary controller. 8. MAP1 tries to join RAP2 instead of RAP1. 9. MAP1 authenticates and starts a join/discovery process, but a continuous set of decrypt errors is observed at the MAP and reported in traps at the controller. **Workaround**: Disable AP fallback, so that if there is a failure, the recovery can be done in a controlled manner.
CSCua79117	Incorrect error message and description displayed when editing mobility group members on the GUI. **Symptom**: Incorrect error message is displayed on the GUI when using the EditAll option. **Conditions**: On the controller GUI, choose **Controller > Mobility Management > Mobility Groups**, click **EditAll**, and then after editing, click **Apply**. An incorrect message might be displayed, but all the mobility group members are edited. From the 7.3 controller software release, the hash value is mandatory and must be added either as none or a proper hash value of the virtual controller. **Workaround**: Use the controller CLI.
CSCua62340	On the Monitor page, mesh link details: value is shown as 0 dB. **Symptom**: Mesh link detail is displayed as zero. **Conditions**: Monitor page on the controller GUI. **Workaround**: None.
CSCub26369	Incorrect data shown on the Monitor > Mesh AP > Mesh Statistics page. **Symptom**: Mesh statistics shows discrepancy in CLI and Cisco Prime Infrastructure. **Conditions**: Enter the **sh mesh stats** command. **Workaround**: None.

Table 1-8 Open Caveats (continued)

ID	Description
CSCub88941	802.1X clients fail to get authenticated with the maximum number of APs associated. **Symptom**: 802.1X clients fail to get authenticated with the maximum number of APs associated with the controller. **Conditions**: Issue is related to the number of APs supported per controller platform with the AP priority feature enabled. For example, Cisco WiSM2 can support a maximum of 1000 APs, which means 2000 802.1X control blocks are created in the controller (one per radio, two per AP). When a higher priority AP associates with the controller, the lower priority APs are dissociated. However, 802.1X control blocks are not deleted. As a result, when an 802.1X client tries to get authentcated from the newly joined AP, the controller fails to create 802.1X control block for that client, resulting in the failure of client authentication. **Workaround**: Disable the AP priority feature on the controller by entering this command: **config network ap-priority disable**
CSCtz39097	Enable DFS channels for FCC SKUs after FCC Cerification is done. **Symptom**: DFS channels are disabled for FCC SKUs of AP802AGN(AP802 Dual Radio) running on c8xx platforms pending FCC certification. **Conditions**: None. **Workaround**: None
CSCub24955	Traceback process_lock_semaphore seen during regression. **Symptom**: Following Traceback, the following message is seen after AP802 boots: `%SCHED-7-WATCH: Attempt to lock uninitialized watched semaphore (address 0). -Process= "Init", ipl= 4, pid= 3 -Traceback=` **Conditions**: None. **Workaround**: None.
CSCub22302	Error renaming "flash:/private-multiple-fs.new" seen on console. **Symptom**: AP802 displays the following errors during runtime: `Error renaming "flash:/private-multiple-fs.new" to "flash:/private-multiple-fs"` **Conditions**: When AP802 is running in Unified mode. **Workaround**: None.

Table 1-8 Open Caveats (continued)

ID	Description
CSCua23018	WCP status never comes to oper-up even after reconfiguring the service IP. **Symptom**: Static/DHCP service-vlan IP is lost after HA configuration. **Conditions**: Even after reconfiguration of service port IP, WCP status shows keep alive and never comes to oper-up state. **Workaround**: Enter `no wism service-vlan` *`vlan`* command in catalyst 6K device and add the configuration again.
CSCud23648	Controller stopped working on Release 7.3.101.0 **Symptom**: Controller stopped working on Release 7.3.101.0 **Conditions**: Task Name: osapiReaper User Crash: The system has encountered a fatal condition at broffu_fp_dapi_cmd.c:3679 **Workaround**: None.

Resolved Caveats

Table 1-9 lists the caveats that are resolved in the 7.3.101.0 controller software release.

Table 1-9 Resolved Caveats

ID	Title
CSCtz17483	HA: WebAuth redirect fails in wired guest when HA is enabled.
CSCua13332	Customized WebAuth login page not working for guest wired clients.
CSCua43558	Controller does not respond during a task with IPv6 traffic.
CSCub00341	Fast SSID change can bypass NAC RADIUS when switching SSIDs.
CSCty68030	AP3500 and AP1260: Upgrade bootloader automatically from IOS.
CSCsg32646	When LAG is enabled, CDP does not display proper port information.
CSCsq14833	Certain IPs used for management interface result in AP join issues.
CSCsu54884	Ad hoc rogues after being made internal are not displayed on the controller.
CSCti81379	show dot11 association all show encryption as off when using WEP.
CSCtj06776	Can enable band select on the controller CLI when WLAN radio policy is set to 802.11a.
CSCtr38446	AP is not displayed in the AP Group.
CSCts52226	Controller does not recognize the EAP-ID response from the client.
CSCts69268	**show run-config** command displays incorrect command syntax.
CSCtt15179	Two clients unable to communicate after inter-AP group roam to the home VLAN.
CSCtt32890	cckm timestamp-tolerance missing from the output of the **show run-config** command.

Table 1-9 Resolved Caveats (continued)

ID	Title
CSCtt96265	Controller might fail to transfer or save configuration and then becomes unresponsive.
CSCtu07081	Unable to reboot Cisco Flex 7500 Series Controller after predownloading the AP image.
CSCtu19860	Cisco 5508 Controller does not set 802.1p marking for downstream CAPWAP packets.
CSCtu28535	APs unresponsive due to unexpected exception to CPUvector.
CSCtw55476	LWAPP Primary Discovery Request sent by newer AP.
CSCtw65316	LAG with CDP does not show all the physical ports correctly.
CSCtw70290	Inconsistent limitation of characters for guest username.
CSCtw74145	Creation of default SNMP entries with nondefault values is denied.
CSCtx49189	Preauthentication ACL is removed from web authentication WLAN.
CSCtx56334	H-REAP client does not experience a successful intercontroller L2 roam.
CSCtx60459	Retry count of 802.11 MAC counters display incorrect value in AP statistics.
CSCtx69189	Cisco WiSM2 multicast IGMP proxy delay under load.
CSCtx91550	When `sh wlan apgroups` is generated, an error message is generated in syslog for all nondefault group APs.
CSCtx95544	Packets from H-REAP and locally switched WLAN should never egress the controller.
CSCty28863	Client is deleted.
CSCty32663	**show run-config** commands: Invalid syntax for 802.11b rate disabled.
CSCty32730	**show run-config** commands: Invalid syntax for 802.11b mandatory command.
CSCty32761	**show run-config** commands: Invalid index numbers for RADIUS servers.
CSCty32823	**show run-config** commands: Missing quotes for names with spaces.
CSCty32835	**show run-config** commands: Missing DCA and Band select commands
CSCty32880	**show run-config** commands: Missing line-feeds on some lines.
CSCty36053	The **show client detail** *mac-addr* command does not display client statistics values.
CSCty40179	Unable to change H-REAP-VLAN mapping; WLAN ID 3 cannot be altered.
CSCty45920	Controller allows creation of dynamic interfaces with overlapping subnet.
CSCty47582	Controller unresponsive when executing the **show ap eventlog** *ap-name* command.
CSCty55275	Controller responds to ARP REQ for clients on a different VLAN rather than the source VLAN.
CSCtz13525	Controller secure password policies enforced for local net users on CLI.
CSCtz24275	FlexConnect AP with VLAN support: enabling SSH causes the radios to reset.
CSCtz28357	Accounting traffic statistics counters are unreliable with web authentication.
CSCtz31572	H-REAP local switching: ARP issues and wrong VLAN seen in NCS.
CSCtz43631	Controller keeps the ghost client entry.
CSCtz45133	TSM metrics collection setting not immediately pushed from controller to AP.

Table 1-9 Resolved Caveats (continued)

ID	Title
CSCtz52892	Wired client is unable to receive traffic after moving between WGB APs.
CSCtz58982	Unable to store CAPWAP fragment from XX:XX.
CSCtz63669	Error message is displayed when virtual interface is configured in the initial configuration wizard.
CSCtz76153	Interface name starting with the ‘all’ string is not accepted.
CSCtz79377	Controller unresponsive on an SNMP task.
CSCtz84782	On a Cisco Flex 7500 Series Controller, the **show run-config** command takes more time than expected to produce output.
CSCtz89535	Inconsistent Link Test results.
CSCtz92155	Web authentication guest access with custom bundle, passthrough and email.
CSCtz97752	Error logs for packet encryption failures and out-of-order issues.
CSCua00870	802.11a/802.11b shows in spite of 802.11n after H-REAP FT.
CSCua06724	WAN DNS entry does not work as expected on Cisco 600 Series OfficeExtend Access Points for static IP scenarios.
CSCua08891	Crash on Cisco Wireless Controller on Cisco Services-Ready Engine (SRE).
CSCua16846	"Invalid MTU (0) Discarding packet to AP" message is logged in the message log.
CSCua18971	RA client display page causes memory corruption for a list of more than 256 clients.
CSCua22875	H-REAP local switching client can show an incorrect VLAN on NCS.
CSCua24297	AP forwarding broadcast action frames to controller over CAPWAP.
CSCua27246	Unable to reset CM command sent via CMTS from AP to reset CM.
CSCua29504	802.11w-capable client fails pairwise key handshake with AES.
CSCua38960	Cisco 5508 controller running 7.2.103.0 release of the controller software does not update the default gateway MAC address for EoIP tunnel on the data plane after a failover on the default gateway via GARP.
CSCua39538	Controller with media snooping crashes due to memory corruption.
CSCua46511	CleanAir sensor stops working and requires a reboot.
CSCua56610	Core dump functionality needs to be added to SRE platforms.
CSCua69305	No DSCP on upstream data from a non-WMM client.
CSCua69563	Flex WAN controller: Receive failures for clients with longer usernames.
CSCua83334	Mesh AP does not initiate a CAPWAP discovery request to the primary controller.
CSCua93693	APs are not displayed in the configured AP groups for over 500 APs.
CSCua93936	Broadcast key rotation does not use rotated index 1 and 2, but sticks to slot 0.
CSCua95089	Knob to turn off IPv6 on controller.
CSCtj25124	HA: AP loses DTLS connection during DP crash switchover event.
CSCtt19734	AP3500 advertises rates that it is not capable of in the beacon.
CSCtw59905	Cisco WiSM2 unresponsive. Unable to recover after activating the new mobility architecture.
CSCtw61314	Controller unresponsive when SNMPv3 user is deleted.

Table 1-9 Resolved Caveats (continued)

ID	Title
CSCtx61062	Duplicate client entries are present in the ARP table of the controller.
CSCtx70704	**set cos** command is not present in show-running config.
CSCty29613	Continuous integration build failures introduced with CSCtx98731.
CSCty45423	AP unresponsive during pre-image.
CSCty80224	AP's radio core dump: transmitter appears to have stopped.
CSCty91749	High parallel QoS traffic streams cause Radio Tx watchdog resets.
CSCtz05016	Problem receiving multicast on wireless client on WiSM2.
CSCtz13994	The Cisco 5500 Series Controller became unresponsive and then rebooted after a successful upgrade from a 7.0 release to a 7.2 release.
CSCtz91180	Controller unresponsive with ‘emweb’ task while deleting a ARP entry.
CSCua52085	System unresponsive on lock for association processing.
CSCua59420	Active controller unresponsive when downgrade is performed.
CSCub11494	Controller unresponsive with "dtls_secret_delete+456" with simulated AP and client.
CSCub20309	Mesh AP3502 unresponsive with tbridge_clearif traceback.
CSCtx80743	Controller memory corruption with wIPS submode.
CSCty07036	CCKM EAPOL broadcast key rotation break at M5 exchange.
CSCty05792	Wireless clients receive GARP from a different VLAN.
CSCty38823	Controller memory leak in an EAP framework task.
CSCtz65426	Memory corruption seen on Cisco 8500 WLC with a large number of APs and clients associated with it.

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 additional information about the Cisco controllers and lightweight 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*

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.