Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 6.0.182.0

June 11, 2009

These release notes describe open and resolved caveats for software release 6.0.182.0 for Cisco 2100, 4400, and 5500 Series Wireless LAN Controllers; Cisco Wireless Services Modules (WiSMs); Cisco Wireless LAN Controller Network Modules; Catalyst 3750G Integrated Wireless LAN Controller Switches; Cisco 3201 Wireless Mobile Interface Cards (WMICs); Cisco Aironet 1100, 1130, 1140, 1200, 1230AG, 1240, 1250, 1300, and AP801 Series Lightweight Access Points; Cisco Aironet 1130AG, 1240AG, 1522, and 1524 Mesh Access Points, which comprise part of the Cisco Unified Wireless Network (UWN) Solution.

Note Unless otherwise noted, all of the Cisco wireless LAN controllers are hereafter referred to as *controllers*, and all of the Cisco lightweight access points are hereafter 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:

- Software release 6.0.182.0 for all Cisco controllers and lightweight access points
- Cisco autonomous to lightweight mode upgrade tool release 3.0
- Cisco Wireless Control System (WCS) software release 6.0.132.0
- Cisco WCS Navigator 1.5.132.0
- Location appliance software release 6.0.75.0
- Cisco 2700 Series Location Appliances
- Mobility services engine software release 6.0.75.0 and Context Aware Software

Note Client and tag licenses are required in order to retrieve contextual (such as location) information within the Context Aware Software. See the *Release Notes for Cisco 3350 Mobility Services Engine for Software Release 6.0* for more information.

- Cisco 3350 Mobility Services Engines
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 5500 Series Wireless LAN Controllers
- Cisco Wireless Services Module (WiSM) for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers

Note The 6.0.182.0 release does not support the NM-AIR-WLC6 platform.

- Catalyst 3750G Wireless LAN Controller Switches
- Cisco 3201 Wireless Mobile Interface Card (WMIC)
- Cisco Aironet 1130AG, 1240AG, 1522, and 1524 Mesh Access Points

Note This release does not support Cisco Aironet 1505 and 1510 access points.

- Cisco Aironet 1100, 1130, 1140, 1200, 1230AG, 1240, 1250, 1300, and AP801 Series Lightweight Access Points

Note Controller software release 5.0.148.0 or later is not compatible with Cisco Aironet 1000 series access points.

Note The AP801 is an integrated access point on the Cisco 800 Series Integrated Services Routers (ISRs).

Note The 801 access point (the access point embedded in the 88xW ISR), the 1250 series access point, and the 1140 series access point have a hardware limitation where beacons can only be output at intervals that are multiples of 17 milliseconds. When these APs are configured for a 100-millisecond beacon interval, they transmit beacons every 102 milliseconds. Similarly, when the beacon interval is configured for 20 milliseconds, these APs transmit beacons every 17 milliseconds.

Note Only Cisco Aironet 1200 Series Access Points that contain 802.11g (AIR-MP21G) or second-generation 802.11a radios (AIR-RM21A or AIR-RM22A) are supported for use with controller software releases. The AIR-RM20A radio, which was included in early 1200 series access point models, is not supported. To see the type of radio module installed in your access point, enter this command on the access point: **show controller dot11radio** *n*, where *n* is the number of the radio (0 or 1).

Controller Requirements

The controller GUI requires the following operating system and web browser:

- Windows XP SP1 (or later) or Windows 2000 SP4 (or later)
- Internet Explorer 6.0 SP1 (or later) or Mozilla Firefox 2.0.0.11 (or later)

Note Internet Explorer 6.0 SP1 (or later) and Mozilla Firefox 2.0.0.11 (or later) are the only browsers supported for using the controller GUI and web authentication.

MIB Files

Cisco controllers support standard SNMP Management Information Base (MIB) files. MIBs can be downloaded from the Software Center on Cisco.com. Only one MIB is posted per major release (6.0, 5.2, 5.1, and so on). If an updated MIB becomes available, the previous version is removed from the Software Center and replaced by the new version.

New Features

The following new features are available in controller software release 6.0.182.0.

Note Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 6.0* for more details and configuration instructions.

New Controller Platform

- **Cisco 5508 Wireless LAN Controller**—This controller supports up to 250 lightweight access points and 7000 wireless clients (or 5000 wireless clients and 2500 RFID tags when using the client location feature) through eight Gigabit Ethernet distribution system ports. Cisco 5508 controllers have no restrictions on the number of access points per port. However, Cisco recommends using link aggregation (LAG) or configuring dynamic AP-manager interfaces on each Gigabit Ethernet port to automatically balance the load. If more than 100 access points are connected to the 5500 series controller, make sure that more than one gigabit Ethernet interface is connected to the upstream switch.

  You are not required to configure an AP-manager interface for 5500 series controllers. The management interface acts like an AP-manager interface by default, and the access points can join on this interface.

  Note The 5500 series controllers can run only controller software release 6.0 or later. Refer to the *Cisco 5500 Series Wireless Controller Installation Guide* for more information on this controller.

- **Licensing**—Two types of licenses are required in order to use the 5500 series controllers: an image-based license (base or wplus), which determines the feature set that the controller uses, and an ap-count license (base-ap-count or wplus-ap-count), which determines the number of access points that the controller supports (12, 25, 50, 100, or 250). The base license supports the standard base software set, and the wplus license supports the premium wireless plus (wplus) software set. The wplus software set provides the standard base feature set as well as this functionality:
  - Datagram Transport Layer Security (DTLS) data encryption for added security across remote WAN and LAN links
  - Support for OfficeExtend access points, which are used for secure mobile teleworking
  - Support for the 1130AG and 1240AG series indoor mesh access points, which dynamically establish wireless connections in locations where it might be difficult to connect to the wired network.

    Note Outdoor mesh access points can be used with the 5500 series controller without a wplus license.

    Note Other controller platforms (such as the 2100 and 4400 series controllers) also require a license for use with indoor mesh access points. See the *Cisco Enterprise Wireless Mesh Licensing and Ordering Guide* for details: http://www.cisco.com/en/US/products/ps8368/products_data_sheets_list.html

  Note No licensing steps are required after you receive your 5500 series controller because the licenses you ordered are installed at the factory. However, as your wireless network evolves, you might want to add support for additional access points or upgrade from the standard software set to the wplus software set. To do so, follow the instructions in the controller configuration guide to obtain and install an upgrade license.

- **Data Encryption**—Cisco 5500 series controllers enable you to encrypt CAPWAP control packets (and optionally CAPWAP data packets) that are sent between the access point and the controller using Datagram Transport Layer Security (DTLS). If an access point does not support DTLS data encryption, DTLS is enabled only for the control plane, and a DTLS session for the data plane is not established.

  Note Only 5500 series controllers support data encryption. This feature is not available on other controller platforms. If an access point with data encryption enabled tries to join any other controller, the access point joins the controller, but data packets are sent unencrypted.

  Note Only 1130, 1140, 1240, and 1250 series access points support DTLS data encryption, and data-encrypted access points can join a 5500 series controller only if the wplus license is installed on the controller. If the wplus license is not installed, the access points cannot join the controller. DTLS data encryption is enabled automatically for OfficeExtend access points but disabled by default for all other access points.

New Controller Features

- **Auto-Immune Feature**—A potential attacker can use specially crafted packets to mislead the intrusion detection system (IDS) into treating a legitimate client as an attacker. It causes the controller to wrongly disconnect this legitimate client and launches a DoS attack. The auto-immune feature, when enabled using the **config wps auto-immune enable** command, is designed to protect against such attacks.

  Note If "auto-immune" messages appear for certain clients (for example, "*mac_address* Suspected Auto-Immune attack: Not Sending Assoc Response to station on BSSID 00:11:22:33:44:50 (status 1) statusCode=0)," you can enter this CLI command to disable the auto-immune feature: **config wps auto-immune disable** (CSCsx74467).

  Note Conversations using Cisco 792x phones might be interrupted intermittently when the auto-immune feature is enabled.

- **Beamforming (also called ClientLink)**—Cisco Aironet 1140 and 1250 series access points support *beamforming*, a spatial-filtering mechanism used at a transmitter to improve the received signal power or signal-to-noise (SNR) ratio at an intended receiver (client). Beamforming uses multiple transmit antennas to focus transmissions in the direction of an 802.11a or 802.11g client, which increases the downlink SNR and the data rate to the client, reduces coverage holes, and enhances overall system performance. Beamforming works with all existing 802.11a and 802.11g clients. It is disabled by default.
- **Core Dump Files**—You can upload the core dump file from the flash memory of a 5500 series controller to a TFTP or FTP server using the controller CLI. The 5500 series controllers save the core dump file to flash memory following a crash. Also, to help troubleshoot controller crashes, you can now use the controller GUI to configure the controller to automatically upload its core dump file to an FTP server after experiencing a crash; previously this functionality was configurable only from the CLI.

- **IPv6 Support for Layer 2 Security**—In controller software release 6.0, all Layer 2 security policies are supported and can be configured when you enable IPv6 bridging on a WLAN. Clients must support IPv6 with either static stateless auto-configuration (such as Windows XP clients) or stateful DHCPv6 IP addressing (such as Windows Vista clients). For stateful DHCPv6 IP addressing to operate properly, you need a switch or router that supports the DHCP for IPv6 feature (such as the Cisco Catalyst 3750 switch) and is configured to act like a DHCPv6 server, or you need a dedicated server such as a Windows 2008 server with a built-in DHCPv6 server.

  Note Currently, DHCPv6 is supported for use only with Windows Vista clients. For these clients, you must manually renew the DHCPv6 IP address after the client changes VLANs.

  Note To load the SDM IPv6 template in the Cisco Catalyst 3750 switch, enter this command and then reset the switch: **sdm prefer dual-ipv4-and-v6 default**. For more information, refer to the Cisco Catalyst 3750 switch configuration guide for Cisco IOS Release 12.2(46)SE.

- **Login Banner File**—You can download a login banner file using either the controller GUI or CLI. The login banner is the text that appears on the screen before user authentication when you access the controller GUI or CLI using Telnet, SSH, or a console port connection.
- **Packet Capture Files**—When a 5500 series controller's data plane crashes, it stores the last 50 packets that the controller received in flash memory. You can use the controller GUI or CLI to upload the packet capture file from the controller. You can then use Wireshark or another standard packet capture tool to view and analyze the contents of the file.
- **Pinning and Cascading**—In controller software releases prior to 6.0, the dynamic channel assignment (DCA) search algorithm attempts to find a good channel plan for the radios associated to controllers in the RF group, but it does not adopt a new channel plan unless it is considerably better than the current plan. The channel metric of the worst radio in both plans determines which plan is adopted. Using the worst-performing radio as the single criterion for adopting a new channel plan can result in *pinning* (when the worst radio in the RF group could potentially prevent other radios in the group from seeking better channel plans) or *cascading* (when one radio's channel change results in successive channel changes to optimize the remaining radios in the RF neighborhood). In controller software release 6.0, the DCA algorithm has been redesigned to prevent pinning and cascading. These changes have been implemented: multiple local searches, multiple channel plan change initiators (CPCIs), localization (limiting the propagation of channel plan changes), and non-RSSI-based cumulative cost metric.
- **TCP MSS**—If a client's maximum segment size (MSS) in a Transmission Control Protocol (TCP) three-way handshake is greater than the maximum transmission unit can handle, the client might experience reduced throughput and the fragmentation of packets. To avoid this problem in controller software release 6.0, you can specify the MSS for all access points joined to the controller or for a specific access point.
- **VoIP Snooping**—Controller software release 6.0 supports Voice over IP (VoIP) Media Session Aware (MSA) snooping and reporting. This feature enables access points to detect the establishment, termination, and failure of Session Initiation Protocol (SIP) voice calls and then report them to the controller and WCS. It can be enabled or disabled for each WLAN. When VoIP MSA snooping is enabled, the access point radios that advertise this WLAN look for SIP voice packets that comply with SIP RFC-3261. They do not look for non-RFC-3261-compliant SIP voice packets or Skinny Call Control Protocol (SCCP) voice packets.

GUI Enhancements

- **802.11a (or 802.11b/g) > RRM > Tx Power Control (TPC) page**—You can now configure the power threshold using the controller GUI. Previously, it could be configured only from the controller CLI. The power threshold value specifies the cutoff signal level used by RRM when determining whether to reduce an access point's power. The default value is –70 dBm but can be changed when access points are transmitting at higher (or lower) than desired power levels. The range is –80 to –50 dBm. Increasing this value (between –65 and –50 dBm) causes the access points to operate at higher transmit power rates.
- **802.11a/n (or 802.11b/g/n) Radios page and All APs page**—On these GUI pages, you can search for specific access points or access point radios. To do so, you create a filter to display only access points or radios that meet certain criteria (such as MAC address, status, access point mode, and certificate type). This feature is especially useful if your list of access points or radios spans multiple pages, preventing you from viewing them all at once.
- **All APs > Details for (Advanced) page**—In addition to showing the link latency results, this page now shows the data latency results, specifically the current, maximum, and minimum round-trip times of CAPWAP data packets from the access point to the controller and back.
- **AP Join Stats page**—You can now use the controller GUI to view join statistics for an access point that sends a CAPWAP discovery request to the controller. Previously, this information could be viewed only from the controller CLI.
- **Controller > Multicast page**—The Ethernet Multicast Mode parameter has moved from the Controller > General page to the Controller > Multicast page.
- **DHCP Parameters page**—You can now configure DHCP option 82 using the controller GUI. Previously, it could be configured only from the controller CLI.
- **Local Significant Certificates (LSC) page**—An AP Provisioning tab has been added to this page to assist in provisioning an LSC on the access point. Previously, this functionality could be configured only from the controller CLI.
- **Priority Order > Management User page**—This page has been modified to help you more easily specify which servers have priority when the controller attempts to authenticate management users.

Access Point Additions and Changes

- **OfficeExtend Access Points**—Cisco Aironet 1130 series and 1140 series access points that are joined to a Cisco 5500 series controller with a wplus license can be configured to operate as OfficeExtend access points. This feature provides secure communications from a controller to an access point at a remote location, seamlessly extending the corporate WLAN over the Internet to an employee's residence. The teleworker's experience at the home office is exactly the same as it would be at the corporate office. Datagram Transport Layer Security (DTLS) encryption between the access point and the controller ensures that all communications have the highest level of security.

Note In order to use OfficeExtend access points, a wplus license must be installed and in use on the 5500 series controller. After the license is installed, you can enable the OfficeExtend mode on the 1130 series or 1140 series access point.

- **Power over Ethernet (PoE)**—When a dual-radio 1250 series access point is powered using 15.4-W PoE, it cannot operate at full functionality, which requires 20 W. The access point can operate with dual radios on 15.4-W PoE, but performance is reduced in terms of throughput and range. If full functionality is required on 15.4 W, you can remove one of the radios from the 1250 series access point chassis or disable it in controller software release 6.0 so that the other radio can operate in full 802.11n mode. After the access point radio is administratively disabled, the access point must be rebooted for the change to take effect. The access point must also be rebooted after you re-enable the radio to put it into reduced throughput mode.

Mesh Access Point Additions and Changes

- Controller software release 6.0 supports the following Cisco Aironet mesh access points:
  - **Cisco Aironet 1522 and 1524 outdoor mesh access points**

    The 1522 access point has two simultaneously operating radios: a 2.4-GHz radio used for client access and a 5-GHz radio used for data backhaul.

    The 1524PS access point has three radios: 2.4 GHz, 4.9 GHz, and 5.8 GHz. The 2.4-GHz radio is for client access (non-public safety traffic), and the 4.9-GHz radio is for public safety client access traffic only. The 5.8-GHz radio is used as the backhaul for both public safety and non-public safety traffic.

    The 1524SB access point has three radios: a 2.4-GHz radio and two 5.8-GHz radios. The 2.4-GHz radio is for client access. The two 5.8-GHz radios are used for the serial backhaul, which provides uplink and downlink access. The downlink radio also provides universal client access. The 1524SB access points are supported in the US, Canada, and Singapore regulatory domains.

    Note Universal client access applies to mesh access points with two or more radios (1524SB, 1522, 1240, and 1130), excluding the 1524PS.

  - **Cisco Aironet 1130AG and 1240AG indoor mesh access points**

    The 1130AG and 1240AG access points have two simultaneously operating radios: a 2.4-GHz radio used for client access and a 5-GHz radio used for data backhaul.

    Note You must convert these access points in order for them to operate as indoor mesh access points.

- **Dynamic Rate Adaptation**—You can now set the bridge data rate to **auto**. When you do so, the mesh backhaul chooses the highest rate such that the next higher rate cannot be used due to unsuitable conditions for that specific rate (and not because of conditions that affect all rates).
- **Intrusion Detection System (IDS)**—You can disable IDS reports on outdoor mesh access points. When you disable this feature, no IDS reports are generated, which preserves bandwidth on the backhaul. When you enable this feature, IDS reports are generated for all traffic on the backhaul.

  Note IDS reporting is enabled for all indoor mesh access points and cannot be disabled.

- **Licensing**—In order to use indoor mesh access points with a 5500 series controller, a wplus license must be used on the controller.

  Note Outdoor mesh access points do not require a wplus license.

  Note Other controller platforms (such as the 2100 and 4400 series controllers) also require a license for use with indoor mesh access points. See the *Cisco Enterprise Wireless Mesh Licensing and Ordering Guide* for details: http://www.cisco.com/en/US/products/ps8368/products_data_sheets_list.html

- **Serial Backhaul**—The 1524SB access point has two 5.8-GHz backhaul radios: one uplink and one downlink. Each radio is configured with a different backhaul channel, so there is no need to use the same shared wireless medium between the north-bound and south-bound traffic in a mesh tree-based network.
- **Telnet**—In previous mesh software releases, Telnet is enabled by default. However, in controller software release 6.0, controllers block Telnet sessions by default, so you need to enable Telnet if you want to use it.

Other Changes

These additional changes are applicable to controller software release 6.0:

- **128-Bit WEP**—The 128-bit key size option for static WEP has been removed from the controller GUI and CLI.
- **Access Point Groups**—Before deleting an access point group in controller software release 6.0, you must move all access points in the group to another group. The access points are not moved to the default-group access point group as in previous releases.
- **Access Point Level Domain and Name Server**—When configuring a static IP address, you can now specify a domain name server and access point domain.
- **DHCP Option 82**—You can now use the controller CLI to override the global DHCP option 82 setting and disable (or enable) this feature for the AP-manager or management interface on the controller.
- **IPv6 Bridging Changes**—The following changes have been made with regard to IPv6 bridging:
  - To use IPv6 bridging, multicast must be enabled on the controller.
  - Clients must support IPv6 with either static stateless auto-configuration (such as Windows XP clients) or stateful DHCPv6 IP addressing (such as Windows Vista clients).

    Note Currently, DHCPv6 is supported for use only with Windows Vista clients. For these clients, you must manually renew the DHCPv6 IP address after the client changes VLANs.

  - For stateful DHCPv6 IP addressing to operate properly, you need a switch or router that supports the DHCP for IPv6 feature (such as the Cisco Catalyst 3750 switch) and is configured to act like a DHCPv6 server, or you need a dedicated server such as a Windows 2008 server with a built-in DHCPv6 server.

Note To load the SDM IPv6 template in the Cisco Catalyst 3750 switch, enter this command and then reset the switch: **sdm prefer dual-ipv4-and-v6 default**. For more information, refer to the Cisco Catalyst 3750 switch configuration guide for Cisco IOS Release 12.2(46)SE.

- **Local Database Entries**—You can now use the controller GUI or CLI to view the number of entries that are currently in the local database.
- **Network Mobility Services Protocol (NMSP)**—The CLI commands to set the NMSP notification interval value for clients, RFID tags, and rogue clients and access points have been modified, and some new commands have been added to view NMSP information and debug NMSP issues.
- **RADIUS Configuration**—The **config radius** {**auth** | **acct**} **mac-delimiter** {**colon** | **hyphen** | **single-hyphen** | **none**} CLI command has been added to enable you to specify the delimiter to be used in the MAC addresses that are sent to the RADIUS authentication or accounting server in Access-Request messages.
- **Rogue Detection**—Rogue detection is enabled by default for all access points joined to the controller (except for OfficeExtend access points). However, in controller software release 6.0, you can enable or disable it for individual access points.
- **Telnet-SSH Configuration**—You can now use the controller GUI to configure Telnet and Secure Shell (SSH) sessions or to troubleshoot lightweight access points. Previously, these operations could be configured only from the controller CLI. In addition, the CLI commands for configuring Telnet and SSH sessions have changed.

  Note By default, controllers block Telnet sessions. You must use a local connection to the serial port and then enable Telnet sessions.

- **Pico Cell Configuration**—You can no longer configure Pico cells using the controller GUI and CLI.

Software Release Information

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. As new releases become available for the controllers and their access points, consider upgrading.

Note The Cisco WiSM requires software release SWISMK9-32 or later. The Supervisor 720 12.2(18)SXF2 supports the Cisco WiSM software release 3.2.78.4 or later, and the Supervisor 720 12.2(18)SXF5 (Cisco IOS Software Modularity) supports the Cisco WiSM software release 4.0.155.5 (with Cisco IOS Software Modularity).

Note To use the Cisco WiSM in the Cisco 7609 and 7613 Series Routers, the routers must be running Cisco IOS Release 12.2(18)SXF5 or later.

Note The Cisco Wireless LAN Controller Network Module is supported on Cisco 28/37/38xx Series Integrated Services Routers running Cisco IOS Release 12.4(11)T2, 12.4(11)T3, and 12.5.

Note To use the controller in the Catalyst 3750G Wireless LAN Controller Switch, the switch must be running Cisco IOS Release 12.2(25)FZ, 12.2(35)SE or later, 12.2(37)SE or later, 12.2(44)SE or later, or 12.2(46)SE or later. The following Cisco IOS Releases and any variants are not supported: 12.2(25)SEC, 12.2(25)SED, 12.2(25)SEE, 12.2(25)SEF, and 12.2(25)SEG. All Catalyst 3750 software feature sets (IP Base, IP Service, and Advanced IP Services) are supported for use with the controller.

Note You can use the 2112 and 2125 controllers only with software release 5.1.151.0 or later.

Note Cisco 526 Wireless Express Mobility Controller is supported only until the Cisco Wireless LAN Controller, Release 5.2.193.0. The later releases do not support the Cisco 526 Wireless Express Mobility Controller.

Finding the Software Release

To find the software release running on your controller, click **Monitor** and look at the Software Version field under Controller Summary on the controller GUI or enter **show sysinfo** on the controller CLI.

Special Rules for Upgrading to Controller Software Release 6.0.182.0

Caution Before upgrading your controller to software release 6.0.182.0, you must comply with the following rules.

- Before you download a software image or an ER.aes file to a 2100 series controller or a controller network module, use the **show memory statistics CLI** command to see the current amount of free memory. If the controller has less than 90 MB of free memory, you need to reboot it before downloading the file.
- Before you use an AP801 series lightweight access point with controller software release 6.0.182.0, you must upgrade the software in the Cisco 860 and 880 Series Integrated Services Routers (ISRs) to Cisco IOS 12.4(22)T and the software in the Cisco 890 Series Integrated Services Router to Cisco IOS 12.4(22)YB.
- Make sure you have a TFTP or FTP server available for the software upgrade. Keep these guidelines in mind when setting up a TFTP or FTP server:
  - Controller software release 6.0.182.0 is larger than 32 MB; therefore, you must make sure that your TFTP server supports files that are larger than 32 MB. Some TFTP servers that support files of this size are tftpd and the TFTP server within the WCS. If you attempt to download the 6.0.182.0 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 service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
  - 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.
  - A third-party TFTP or FTP server cannot run on the same computer as WCS because the WCS built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.

- 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 6.0.182.0. Table 1 shows the upgrade path that you must follow before downloading software release 6.0.182.0.

Table 1 Upgrade Path to Controller Software Release 6.0.182.0

Current Software Release	Upgrade Path to 6.0.182.0 Software
3.2.78.0 or later 3.2 release	Upgrade to a 4.1 release and then upgrade to 4.2.176.0 before upgrading to 6.0.182.0.
4.0.155.5 or later 4.0 release	Upgrade to 4.2.176.0 before upgrading to 6.0.182.0.
4.1.171.0 or later 4.1 release	Upgrade to 4.2.176.0 before upgrading to 6.0.182.0.
4.1.191.xM	Upgrade to 4.1.192.35M before upgrading to 6.0.182.0.
4.1.192.xM	You can upgrade directly to 6.0.182.0.
4.2.130.0 or earlier 4.2 release	Upgrade to 4.2.176.0 before upgrading to 6.0.182.0.
4.2.173.0 or later 4.2 release	You can upgrade directly to 6.0.182.0.
5.0.148.0 or later 5.0 release	You can upgrade directly to 6.0.182.0.
5.1.151.0 or later 5.1 release	You can upgrade directly to 6.0.182.0.
5.2.157.0 or later 5.2 release	You can upgrade directly to 6.0.182.0.

Note When you upgrade the controller to an intermediate software release, wait until all of the access points joined to the controller are upgraded to the intermediate release before you install the 6.0.182.0 software. In large networks, it can take some time to download the software on each access point.

- Cisco recommends that you install the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file on all controller platforms. This file resolves CSCsm03461 and is necessary in order for you to view the version information for ER.aes files in the output of the **show sysinfo** CLI command. If you do not install this ER.aes file, your controller does not obtain the fix for this defect, and “N/A” appears in the Emergency Image Version field in the output of this command.

  Note The ER .aes files are independent from the controller software files. You can run any controller software file with any ER.aes file. However, installing the latest boot software file (5.2.157.0 ER.aes) ensures that the boot software modifications in all of the previous and current boot software ER.aes files are installed.

Caution If you require a downgrade from one release to another, you may 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.

Special Rules for Upgrading to Controller Software 6.0.182.0 in Mesh Networks

Caution Before upgrading your controller to software release 6.0.182.0 in a mesh network, you must comply with the following rules.

Upgrade Compatibility Matrix

Table 2 outlines the upgrade compatibility of controller mesh and non-mesh releases and indicates the intermediate software releases required as part of the upgrade path.

Software Upgrade Notes

- You can upgrade from all mesh releases to controller software release 6.0.182.0 without any configuration file loss. See Table 2 for the available upgrade paths.

  Note If you downgrade to a mesh release, you must then reconfigure the controller. Cisco recommends that you save the configuration from the mesh release before upgrading to release 6.0.182.0 for the first time. Then you can reapply the configuration if you need to downgrade.

- You cannot downgrade from controller software release 6.0.182.0 to a mesh release (for example, 4.1.190.5, 4.1.191.22M, or 4.1.192.xM) without losing your configuration settings.
- Configuration files are in the binary state immediately after upgrade from a mesh release to controller software release 6.0.182.0. After reset, the XML configuration file is selected.
- Do not edit XML files.
- Any field with an invalid value is filtered out and set to default by the XML validation engine. Validation occurs during bootup.
- If you upgrade the controller from software release 4.1.191.xM to 4.1.192.xM and then to software release 6.0.182.0, the controller might reboot without a crash file. To work around this problem, manually reset the controller without saving the configuration after you upgrade the controller to software release 6.0.182.0. Also, make sure to check the RRM configuration settings after the reset to verify that they are correct (CSCsv50357).

Table 2 Upgrade Compatibility Matrix for Controller Mesh and Non-Mesh Releases

Upgrade to	6.0	5.2	4.1.192.35M	4.1.191.24M	4.1.190.5	4.1.185.0	4.1.171.0	4.0.219.0	4.0.217.204	4.0.217.0	4.0.216.0	4.0.206.0	4.0.179.11	4.0.179.8	4.0.155.5	4.0.155.0	3.2.195.10	3.2.193.5	3.2.171.6	3.2.171.5	3.2.150.10	3.2.150.6	3.2.116.21	3.2.78.0	3.1.111.0	3.1.105.0
Upgrade from																										
4.1.192.35M	Y	Y																								
4.1.192.22M	Y	Y	Y																							
4.1.191.24M			Y	–																						
4.1.190.5			Y[1]	Y	–																					
4.1.185.0				Y	Y[2]	–																				
4.1.181.0					Y[2]	Y[2]																				
4.1.171.0					Y[2]	Y[2]	–																			
4.0.219.0						Y[2]	Y[2]	–																		
4.0.217.204				Y[2]		Y[2]	Y[2]	Y[2]	–																	
4.0.217.0						Y[2]	Y[2]	Y[2]	Y[3]	–																
4.0.216.0						Y[2]	Y[2]	Y[2]	Y[3]	Y	–															
4.0.206.0						Y[2]	Y[2]	Y[2]	Y[3]	Y		–														
4.0.179.11										Y		Y[4]	–													
4.0.179.8										Y		Y[4]	Y	–												
4.0.155.5										Y		Y[4]	Y	Y	–											
4.0.155.0										Y		Y[4]	Y	Y	Y	–										
3.2.195.10										Y		Y[4]	Y	Y	Y		–									
3.2.193.5										Y		Y[4]	Y	Y	Y		Y	–								
3.2.171.6										Y		Y[4]	Y	Y	Y		Y		–							
3.2.171.5										Y		Y[4]	Y	Y	Y		Y		Y	–						

Table 2 Upgrade Compatibility Matrix for Controller Mesh and Non-Mesh Releases (Continued)

Upgrade to	6.0	5.2	4.1.192.35M	4.1.191.24M	4.1.190.5	4.1.185.0	4.1.171.0	4.0.219.0	4.0.217.204	4.0.217.0	4.0.216.0	4.0.206.0	4.0.179.11	4.0.179.8	4.0.155.5	4.0.155.0	3.2.195.10	3.2.193.5	3.2.171.6	3.2.171.5	3.2.150.10	3.2.150.6	3.2.116.21	3.2.78.0	3.1.111.0	3.1.105.0
3.2.150.10										Y		Y[4]	Y	Y	Y		Y		Y		–					
3.2.150.6										Y		Y[4]	Y	Y	Y		Y		Y		Y	–				
3.2.116.21										Y		Y[4]	Y	Y	Y		Y		Y		Y		–			
3.2.78.0										Y		Y[4]	Y	Y	Y		Y		Y		Y		Y	–		
3.1.111.0																	Y		Y		Y		Y	Y	–	
3.1.105.0																	Y		Y		Y		Y	Y	Y	–
3.1.59.24																	Y		Y		Y		Y	Y	Y	Y

1. You can upgrade directly from software release 4.1.190.5 to 4.1.192.35M; however, upgrading to 4.1.191.24M before upgrading to 4.1.192.35M is highly recommended.
2. CUSTOMERS WHO REQUIRE DYNAMIC FREQUENCY SELECTION (DFS) FUNCTIONALITY SHOULD NOT USE THIS RELEASE. This release does not provide DFS functionality fixes found in release 4.0.217.204. Additionally, this release is not supported in ETSI-compliant countries or Singapore.
3. Release 4.0.217.204 provides fixes for DFS on 1510 series access points. This functionality is needed only in countries where DFS rules apply.
4. An upgrade to 4.0.206.0 is not allowed in the following country codes when operating with the following access points: Australia (1505 and 1510), Brazil (1505 and 1510), Hong Kong (1505 and 1510), India (1505 and 1510), Japan (1510), Korea (1505 and 1510), Mexico (1505 and 1510), New Zealand (1505 and 1510), and Russia (1505 and 1510). Note: The 1505 mesh access point is not supported in release 5.0 and later. The 1510 mesh access point is supported only in mesh releases 4.1.190.5, 4.1.191.22M, and 4.1.192.xxM.

Software Release Support for Access Points

Table 3 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 3 Software Support for Access Points

Access Points		First Support	Last Support
1000 Series	AIR-AP1010	3.0.100.0	4.2.207.0
	AIR-AP1020	3.0.100.0	4.2.207.0
	AIR-AP1030	3.0.100.0	4.2.207.0
	Airespace AS1200	—	4.0

Table 3 Software Support for Access Points (Continued)

Access Points		First Support	Last Support
1100 Series	AIR-LAP1121	4.0.155.0	—
	AIR-LAP1131	3.1.59.24	—
	AIR-LAP1141N	5.2.157.0	—
	AIR-LAP1142N	5.2.157.0	—
1200 Series	AIR-AP1220A	3.1.59.24	—
	AIR-AP1220B	3.1.59.24	—
1230 Series	AIR-AP1230A	3.1.59.24	—
	AIR-AP1230B	3.1.59.24	—
	AIR-LAP1231G	3.1.59.24	—
	AIR-LAP1232AG	3.1.59.24	—
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	—
1300 Series	AIR-BR1310G	4.0.155.0	—
1400 Series	Standalone Only	N/A	—
1500 Mesh Series	AIR-LAP-1505	3.1.59.24	4.2.176.51M
	AIR-LAP-1510	3.1.59.24	4.2.176.51M

Table 3 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-LAP1524SB	-A, C and N: 6.0 or later	—
	AIR-LAP1524PS	-A: 4.1.192.22M or 5.2 or later[1]	—

[1] These access points are supported in the separate 4.1.19x.x Mesh Software Release train or with Release 5.2 or later. These access points are not supported in the 4.2, 5.0, or 5.1 Release trains.

Upgrading to a New Software Release

When you upgrade the controller's software, the software on the controller's associated access points is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession. Up to 10 access points can be concurrently upgraded from the controller.

Note The 5500 series controllers can download the 6.0.182.0 software to 100 access points simultaneously.

Caution Do not power down the controller or any access point during this 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 in software release 4.0.206.0 and later, the upgrade time should be significantly reduced. The access points must remain powered, and the controller must not be reset during this time.

Note In controller software release 5.2 or later, the WLAN override feature has been removed from both the controller GUI and CLI. If your controller is configured for WLAN override and you upgrade to controller software release 6.0.182.0, the controller deletes the WLAN configuration and broadcasts all WLANs. You can specify that only certain WLANs be transmitted by configuring access point groups. Each access point advertises only the enabled WLANs that belong to its access point group. Access point groups do not enable WLANs to be transmitted on per radio interface of AP.

Note Do not install the 6.0.182.0 controller software file and the 5.2.157.0 ER.aes boot software file at the same time. Install one file and reboot the controller; then install the other file and reboot the controller.

Follow these steps to upgrade the controller software using the controller GUI.

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

Note Cisco highly recommends that you back up your controller's configuration files prior to upgrading the controller software. Otherwise, you must manually reconfigure the controller.

Step 2 Follow these steps to obtain the 6.0.182.0 controller software and the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file from the Software Center on Cisco.com:

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

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875243

b. Click **Wireless Software**.

c. Click **Wireless LAN Controllers**.

d. Click **Standalone Controllers** or **Integrated Controllers and Controller Modules**.

e. Click a controller series.

f. If necessary, click a controller model.

g. If you chose Standalone Controllers in Step d., click **Wireless LAN Controller Software**.

h. If you chose Cisco Catalyst 6500 Series/7600 Series Wireless Services Module (WiSM) in Step e., click **Wireless Services Modules (WiSM) Software**.

i. 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. Cisco recommends that you migrate to an upgraded release.

j. Click a software release number.

- **k.** Click the filename (*filename*.aes).
- **l.** Click **Download**.
- **m.** Read Cisco's End User Software License Agreement and then click **Agree**.
- **n.** Save the file to your hard drive.
- **o.** Repeat steps a. through n. to download the remaining file (either the 6.0.182.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file).

Step 3 Copy the controller software file (*filename*.aes) and the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file to the default directory on your TFTP or FTP server.

Step 4 Disable the controller 802.11a and 802.11b/g networks.

Step 5 Disable any WLANs on the controller.

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

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

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

Step 9 In the IP Address field, 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 and 6 seconds for the Maximum Retries and Timeout fields should work fine 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 field and the amount of time (in seconds) that the TFTP server attempts to download the software in the Timeout field.

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

Step 12 In the File Name field, 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 field, enter the username to log into the FTP server.
- **b.** In the Server Login Password field, enter the password to log into the FTP server.
- **c.** In the Server Port Number field, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 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.

Note Do not wait to reboot the controller. Reboot it immediately after downloading the software. Otherwise, the access points might start downloading the software before the controller is running it.

Step 18 After the controller reboots, repeat Step 6 to Step 17 to install the remaining file (either the 6.0.182.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file).

Step 19 Re-enable the WLANs.

Step 20 For Cisco WiSMs, re-enable the controller port channel on the Catalyst switch.

Step 21 Re-enable your 802.11a and 802.11b/g networks.

Step 22 If desired, reload your latest configuration file to the controller.

Step 23 To verify that the 6.0.182.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

Step 24 To verify that the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file is installed on your controller, enter the **show sysinfo** command on the controller CLI and look at the Emergency Image Version field.

Note If you do not install the 5.2.157.0 ER.aes file, the Emergency Image Version field shows "N/A."

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.**

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

Warning **Do not locate any antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing antennas, take extreme care not to come in contact with such circuits, as they may cause serious injury or death. For proper installation and grounding of the antenna, refer to national and local codes (e.g. U.S.: NFPA70, National Electrical Code, Article 810, in Canada: Canadian Electrical Code, Section 54).**

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 120 VAC, 15A U.S. (240vac, 10A International)**

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.**

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

⚠ **Warning** **Do not work on the system or connect or disconnect cables during periods of lightning activity.**

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

⚠ **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.**

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

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 may 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

Refer to 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 professionally installed.

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.

Using the Cisco 5500 Series Controller USB Console Port

The USB console port on the 5500 series controllers connects directly to the USB connector of a PC using a USB Type A-to-5-pin mini Type B cable.

Note The 4-pin mini Type B connector is easily confused with the 5-pin mini Type B connector. They are not compatible. Only the 5-pin mini Type B connector can be used.

For operation with Microsoft Windows, the Cisco Windows USB console driver must be installed on any PC connected to the console port. With this driver, you can plug and unplug the USB cable into and from the console port without affecting Windows HyperTerminal operations.

Note Only one console port can be active at a time. When a cable is plugged into the USB console port, the RJ-45 port becomes inactive. Conversely, when the USB cable is removed from the USB port, the RJ-45 port becomes active.

USB Console OS Compatibility

- Microsoft Windows 2000, XP, Vista (Cisco Windows USB console driver required)
- Apple Mac OS X 10.5.2 (no driver required)
- Linux (no driver required)

To install the Cisco Windows USB console driver, follow these steps:

Step 1 Follow these steps to download the USB_Console.inf driver file:

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

   http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875243

b. Click **Wireless LAN Controllers**.

c. Click **Standalone Controllers**.

d. Click **Cisco 5500 Series Wireless LAN Controllers**.

e. Click **Cisco 5508 Wireless LAN Controller**.

f. Choose the USB driver file.

g. Save the file to your hard drive.

Step 2 Connect the Type A connector to a USB port on your PC.

Step 3 Connect the mini Type B connector to the USB console port on the controller.

Step 4 When prompted for a driver, browse to the USB_Console.inf file on your PC. Follow the prompts to install the USB driver.

Note Some systems might also require an additional system file. You can download the Usbser.sys file from this URL:
http://support.microsoft.com/kb/918365

The USB driver is mapped to COM port 6. Some terminal emulation programs do not recognize a port higher than COM 4. If necessary, change the Cisco USB systems management console COM port to an unused port of COM 4 or lower. To do so, follow these steps:

Step 1 From your Windows desktop, right-click **My Computer** and choose **Manage**.

Step 2 From the list on the left side, choose **Device Manager**.

Step 3 From the device list on the right side, double-click **Ports (COM & LPT)**.

Step 4 Right-click **Cisco USB System Management Console 0108** and choose **Properties**.

Step 5 Click the **Port Settings** tab and click the **Advanced** button.

Step 6 From the COM Port Number drop-down box, choose an unused COM port of 4 or lower.

Step 7 Click **OK** to save; then close the Advanced Settings dialog box.

Step 8 Click **OK** to save; then close the Communications Port Properties dialog box.

Important Notes for Controllers and Non-Mesh Access Points

This section describes important information about controllers and non-mesh lightweight access points.

One-Time Password (OTP) Support

One Time Passwords (OTP) are supported on controllers using TACACS and RADIUS. For OTP support, you must install a controller release that resolves defects CSCsh29597 and CSCsk21007. Without fixes for those defects, the WLC continuously requires users to authenticate. When the user clicks an option on the controller GUI, the controller sends the request to TACACS for authentication.

In this configuration, the controller acts as a transparent pass-thru device. The controller forwards all client requests to the TACACS/RADIUS server without inspecting the client behavior. When using OTP the client must only establish a single connection to the controller to function properly. The controller currently does not have any intelligence or checks to correct a client that is trying to establish multiple connections.

RADIUS Called-station-id and Calling-station-id Attributes

In software releases prior to 6.0, the controller sends uppercase alpha characters in the MAC address. In software release 6.0 or later, the controller sends lowercase alpha characters in the MAC address for the RADIUS called-station-id and calling-station-id attributes. If you enabled these attributes for 802.1X authentication in previous releases and upgrade to software release 6.0, client authentication fails. Therefore, you must change the MAC addresses to lowercase characters on the RADIUS server before upgrading to software release 6.0.

Access Point Groups

You can create up to 50 access point groups for 2100 series controllers and controller network modules and up to 192 access point groups for 4400 series controllers, 5500 series controllers, the Cisco WiSM, and the 3750G wireless LAN controller switch.

Using Access Points in Sniffer Mode

You must disable IP-MAC address binding in order to use an access point in sniffer mode if the access point is joined to a 5500 series controller, a 2100 series controller, or a controller network module running software release 6.0. To disable IP-MAC address binding, enter this command using the controller CLI: **config network ip-mac-binding disable**.

WLAN 1 must be enabled in order to use an access point in sniffer mode if the access point is joined to a 5500 series controller, a 2100 series controller, or a controller network module running software release 6.0. If WLAN 1 is disabled, the access point cannot send packets.

EDCA CLI Commands

The following enhanced distributed channel access (EDCA) CLI command appears in controller software release 6.0.182.0, but this command is not configurable and cannot be used:

config advanced {**802.11a** | **802.11b**} **edca-parameters custom** *profile_name* {**aifs** | **ecwmin** | **ecwmax** | **txop**} *value*

Band Select and Load Balancing CLI Commands

The **config band-select** and **config wlan band-select** CLI commands appear in controller software release 6.0.182.0, but they are not supported and should not be used. Also, you can ignore the Band Select Stats information in the output of the **show ap stats** {**802.11a** | **802.11b**} *Cisco_AP* command.

The **config load-balancing denial** and **config wlan load-balance** CLI commands appear in controller software release 6.0.182.0, but they are not supported and should not be used. Also, you can ignore the Denial Count information in the output of the **show load-balancing** command.

Inter-Release Controller Mobility

When controllers in the mobility list are running different software releases (such as 4.2, 5.0, 5.1, 5.2, and 6.0), Layer 2 or Layer 3 client roaming is not supported between them. It is supported only between controllers running the same release.

Guest tunneling works only between controllers running the same software release or between controllers running software release 4.2 and controllers running any later software release (for example, 4.2 to 5.0, 4.2 to 5.1, 4.2 to 5.2, or 4.2 to 6.0). Guest tunneling does not work among controllers running other combinations of software.

RLDP Limitations in This Release

Rogue Location Discovery Protocol (RLDP) is a controller feature that detects the presence of rogue access points that are connected to your wired network. In this software release, RLDP operates with these limitations:

- RLDP detects rogue access points that are configured for open authentication.
- RLDP detects rogue access points that use a broadcast BSSID (that is, the access point broadcasts its SSID in beacons).
- RLDP detects only rogue access points that are on the same network. In other words, if an access list in the network prevents the sending of RLDP traffic from the rogue access point to the controller, RLDP does not work.
- RLDP does not work on 5-GHz dynamic frequency selection (DFS) channels.
- If the automatic RLDP attempt does not detect the rogue (due to a noisy RF environment, for example), the controller does not retry. However, you can initiate RLDP manually on a rogue at any time.

Also, in controller software release 6.0, the rogue containment packet transmission times have changed as follows:

- For monitor mode, rogue containment deauthentication packets are still sent at 100-msec intervals.

- For non-monitor mode, deauthentication packets are sent at 500 msec (minimum). In previous releases, they are sent at 100-msec intervals.

Internal DHCP Server

When clients use the controller's internal DHCP server, IP addresses are not preserved across reboots. As a result, multiple clients can be assigned the same IP address. To resolve any IP address conflicts, clients must release their existing IP address and request a new one.

Bootloader Menu

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 series controllers are different than for 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, or enter **4** (on a 5500 series controller) or **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 Only options 1 through 3 are available on 5500 series controllers in FIPS mode.

Note Refer to the Installation Guide or Quick Start Guide for your controller for more details on running the bootup script and power-on self-test.

Fragmented Pings

Cisco 5500 series controllers do not support fragmented pings on any interface. Similarly, Cisco 4400 series controllers, the Cisco WiSM, and the Catalyst 3750G Integrated Wireless LAN Controller Switch do not support fragmented pings on the AP-manager interface.

802.11g Controller and 802.11b Clients

When a controller is configured to allow only 802.11g traffic, 802.11b client devices are able to successfully associate to an access point but cannot pass traffic. When you configure the controller for 802.11g traffic only, disable any channels (such as channel 14 in Japan) that allow associations from 802.11b client devices.

FIPS 140-2

The Cisco 4400 series controllers, the Cisco WiSM, and the Catalyst 3750G Wireless LAN Controller Switch have received NIST FIPS 140-2 Level 2 certification. Click this link to view the NIST Security Policies and compliant software versions:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

CAPWAP Problems with Firewalls and ACLs

If you have a firewall or access control list (ACL) between the controller and its access points that allows LWAPP traffic, before upgrading to software release 5.2 or later and CAPWAP, you should allow CAPWAP traffic from the access points to the controller by opening the following destination ports:

- UDP 5246
- UDP 5247

The access points use a random UDP source port to reach these destination ports on the controller. In controller software release 5.2, LWAPP was removed and replaced by CAPWAP, but if you have a new out-of-the-box access point, it could try to use LWAPP to contact the controller before downloading the CAPWAP image from the controller. Once the access point downloads the CAPWAP image from the controller, it uses only CAPWAP to communicate with the controller.

Note After 60 seconds of trying to join a controller with CAPWAP, the access point falls back to using LWAPP. If it cannot find a controller using LWAPP within 60 seconds, it tries again to join a controller using CAPWAP. The access point repeats this cycle of switching from CAPWAP to LWAPP and back again every 60 seconds until it joins a controller.

Note An access point with the LWAPP recovery image (an access point converted from autonomous mode or an out-of-the-box access point) uses only LWAPP to try to join a controller before downloading the CAPWAP image from the controller.

Messages Appearing Upon Controller Bootup

Several messages might flood the message logs when the controller boots up. These messages appear because of a failure to read or delete several different configuration files. These are low-severity messages that can safely be ignored. They do not affect controller functionality. These are some examples:

```
Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Failed to delete the file :
sshpmInitParms.cfg. file removal failed.
-Process: Name:fp_main_task, Id:11ca7618
Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Failed to delete the file :
bcastInitParms.cfg. file removal failed.
-Process: Name:fp_main_task, Id:11ca7618
```

Web Authentication Redirects

The controller supports web authentication redirects only to HTTP (HTTP over TCP) servers. It does not support web authentication redirects to HTTPS (HTTP over SSL) servers.

Note For 5500 series controllers, 2100 series controllers, and controller network modules, you must configure a preauthentication access control list (ACL) on the WLAN for the external web server and then choose this ACL as the WLAN preauthentication ACL under Security Policies > Web Policy on the WLANs > Edit page.

Cisco 1250 Series Access Points and Cisco 7920 IP Phones

Cisco 1250 series access points are not supported for use with the Cisco 7920 IP phone. They can, however, be used with the Cisco 7921 and 7925 IP phones.

Crash Files for 1250 Series Access Points

The 1250 series access points may contain a bootloader older than version 12.4(10b)JA. Units with old bootloaders do not generate a crash log when a crash occurs. The crash log is disabled so that a crash does not corrupt the flash file system. Units with bootloader versions 12.4(10b)JA or later generate a crash log if the access point is associated to a controller running software release 4.2.112.0 or later.

New 1250 series access points shipped from the factory contain new bootloader images, which fixes the flash file system after it is corrupted during a crash (without losing files). This new bootloader automatically sets a new CRASH_LOG environment variable to "yes," which enables a crash log to be generated following a crash but only on controllers running software release 4.2.112.0 or later. Therefore, no user configuration is needed to enable a crash log on new 1250 series access points shipped from the factory.

These examples show the output from the CLI commands (in bold) that you use to check the bootloader version on lightweight and autonomous 1250 series access points:

Commands entered on the controller CLI:

debug ap enable AP001b.d513.1754

debug ap command "show version | include BOOTLDR" AP001b.d513.1754

```
Thu Apr 23 09:31:38 2009: AP001b.d513.1754: BOOTLDR: C1250 Boot Loader
```

```
(C1250-BOOT-M) Version 12.4(10b)JA, RELEASE SOFTWARE (fc1)
```

Command entered on the access point CLI:

show version | include BOOTLDR

```
BOOTLDR: C1250 Boot Loader (C1250-BOOT-M) Version 12.4(10b)JA, RELEASE SOFTWARE (fc1)
```

Configuration File Stored in XML

In controller software release 4.2.61.0 and later, the controller's bootup configuration file is stored in an Extensible Markup Language (XML) format rather than in binary format. When you upgrade a controller to 4.2.61.0 or a later software release, the binary configuration file is migrated and converted to XML.

Note You cannot download a binary configuration file onto a controller running software release 6.0.182.0. Also, do not attempt to make changes to the configuration file. If you do so and then download the file to a controller, the controller displays a cyclic redundancy checksum (CRC) error while it is rebooting and returns the configuration parameters to their default values.

Note You cannot modify the configuration files for 2000, 4000, and 4100 series controllers. The ability to modify configuration files is available in controller software release 5.2 or later, and these controllers support only earlier software releases (up to the 4.2 release for 2000 series controllers and up to the 3.2 release for 4000 and 4100 series controllers).

LWAPP Mode Changes

When you upgrade to controller software release 5.0.148.0 or later, the LWAPP mode changes to Layer 3 if it was previously configured for Layer 2.

If you downgrade from controller software release 6.0.182.0, 5.2.178.0, 5.2.157.0, 5.1.151.0, or 5.0.148.0 to 4.2.61.0 or an earlier release, the LWAPP mode changes from Layer 3 to Layer 2. Access points might not join the controller, and you must manually reset the controller to Layer 3 to resolve this issue.

Access Points Send Multicast and Management Frames at Highest Basic Rate

Access points running recent Cisco IOS versions transmit multicast and management frames at the highest configured basic rate, which could cause reliability problems. Access points running LWAPP or autonomous IOS should transmit multicast and management frames at the lowest configured basic rate. Such behavior is necessary to provide good coverage at the cell's edge, especially for unacknowledged multicast transmissions where multicast wireless transmissions may fail to be received.

Because multicast frames are not retransmitted at the MAC layer, clients at the edge of the cell may fail to receive them successfully. If reliable reception is a goal, then multicast frames should be transmitted at a low data rate. If support for high data rate multicast frames is required, then it may be useful to shrink the cell size and disable all lower data rates.

Depending on your specific requirements, you can take the following action:

- If you need to transmit multicast data with the greatest reliability and if there is no need for great multicast bandwidth, then configure a single basic rate, one that is low enough to reach the edges of the wireless cells.
- If you need to transmit multicast data at a certain data rate in order to achieve a certain throughput, then configure that rate as the highest basic rate. You can also set a lower basic rate for coverage of non-multicast clients.

Disabling Radio Bands

The controller disables the radio bands that are not permitted by the configured country of operation (CSCsi48220).

40-MHz Channels in the 2.4-GHz Band

Cisco recommends that you do not configure 40-MHz channels in the 2.4-GHz radio band because severe co-channel interference is likely to occur.

802.11a Channels 120, 124, and 128 Disabled

802.11a channels 120, 124, and 128 are disabled to achieve compliance with draft EN 301 893 version 1.5.1 on the following -E regulatory domain products: AP1131AG, AP1243AG, and AP1252AG.

Impact of External Antenna Gain on Transmit Power

In controller software release 4.2 or later, external antenna gain is factored into the maximum transmit power of the access point. Therefore, when you upgrade from an earlier software release to 4.2 or later, you might see a decrease in transmit power output.

Supporting Oversized Access Point Images

Controller software release 4.2 or later allows you to upgrade to an oversized access point image by deleting the recovery image to create sufficient space. This feature affects only access points with 8 MB of flash (the 1100, 1200, and 1310 series access points). All newer access points have a larger flash size than 8 MB.

Note As of August 2007, there are no oversized access point images, but as new features are added, the access point image size will continue to grow.

The recovery image provides a backup image that can be used if an access point power-cycles during an image upgrade. The best way to avoid the need for access point recovery is to prevent an access point from power-cycling during a system upgrade. If a power-cycle occurs during an upgrade to an oversized access point image, you can recover the access point using the TFTP recovery procedure.

Follow these steps to recover the access point using the TFTP recovery procedure.

Step 1 Download the required recovery image from Cisco.com (c1100-rcvk9w8-mx, c1200-rcvk9w8-mx, or c1310-rcvk9w8-mx) and install it in the root directory of your TFTP server.

Step 2 Connect the TFTP server to the same subnet as the target access point and power-cycle the access point. The access point boots from the TFTP image and then joins the controller to download the oversized access point image and complete the upgrade procedure.

Step 3 After the access point has been recovered, you may remove the TFTP server.

Multicast Queue Depth

The multicast queue depth is 512 packets on all controller platforms. However, the following message might appear on 2106 controllers: “Rx Multicast Queue is full on Controller.” This message does not appear on 4400 series controllers because the 4400 NPU filters ARP packets while all forwarding (multicast or otherwise) and multicast replication are done in the software on the 2106.

This message appears when too many multicast messages are sent to the CPU. In controller software releases prior to 5.1, multicast, CDP, and ARP packets share the same queue. However, in software releases 5.1 and later, these packets are separated into different queues. There are currently no controller commands that can be entered to determine if the multicast receive queue is full. When the queue is full, some packets are randomly discarded.

MAC Filtering for WGB Wired Clients

Controller software release 4.1.178.0 or later enables you to configure a MAC-filtering IP address for a workgroup bridge (WGB) wired client to allow passive WGB wired clients, such as terminal servers or printers with static IP addresses, to be added and remain in the controller’s client table while the WGB is associated to a controller in the mobility group. This feature, activated by the **config macfilter ipaddress** *MAC_address IP_address* CLI command, can be used with any passive device that does not initiate any traffic but waits for another device to start communication.

This feature allows the controller to learn the IP address of a passive WGB wired client when the WGB sends an IAPP message to the controller that contains only the WGB wired client’s MAC address. Upon receiving this message from the WGB, the controller checks the local MAC filter list (or the anchor controller’s MAC filter list if the WGB has roamed) for the client’s MAC address. If an entry is found and it contains an IP address for the client, the controller adds the client to the controller’s client table.

Note Unlike the existing MAC filtering feature for wireless clients, you are not required to enable MAC filtering on the WLAN for WGB wired clients.

Note WGB wired clients using MAC filtering do not need to obtain an IP address through DHCP to be added to the controller’s client table.

CKIP Not Supported with Dynamic WEP

In controller software release 4.1.185.0 or later, CKIP is supported for use only with static WEP. It is not supported for use with dynamic WEP. Therefore, a wireless client that is configured to use CKIP with dynamic WEP is unable to associate to a wireless LAN that is configured for CKIP. Cisco recommends that you use either dynamic WEP without CKIP (which is less secure) or WPA/WPA2 with TKIP or AES (which are more secure).

Setting the Date and Time on the Controller

Cisco Aironet lightweight access points do not connect to the controller if the date and time are not set properly. Set the current date and time on the controller before allowing the access points to connect to it.

Synchronizing the Controller and Location Appliance

For controller software release 4.2 or later, if a location appliance (release 3.1 or later) is installed on your network, the time zone must be set on the controller to ensure proper synchronization between the two systems. Also, Cisco highly recommends that the time be set for networks that do not have location appliances. Refer to Chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide, Release 5.2* for instructions for setting the time and date on the controller.

Note The time zone can be different for the controller and the location appliance, but the time zone delta must be configured accordingly, based on Greenwich Mean Time (GMT).

FCC DFS Support on 1130 Series Access Points

Federal Communications Commission (FCC) dynamic frequency selection (DFS) is supported only on 1130 series access points in the United States, Canada, and the Philippines that have a new FCC ID. Access points use DFS to detect radar signals such as military and weather sources and then switch channels to avoid interfering with them. 1130 series access points with FCC DFS support have an FCC ID *LDK102054E* sticker. 1130 series access points without FCC DFS support have an *LDK102054* (no *E* suffix) sticker. 1130 series access points that are operating in the United States, Canada, or the Philippines; have an FCC ID *E* sticker; and are running the 4.1.171.0 software release or later can use channels 100 through 140 in the UNII-2 band.

Inaccurate Transmit Power Display

After you change the position of the 802.11a radio antenna for a lightweight 1200 or 1230 series access point, the power setting is not updated in the controller GUI and CLI. Regardless of the user display, the internal data is updated, and the transmit power output is changed accordingly. To see the correct transmit power display values, reboot the access point after changing the antenna’s position. (CSCsf02280)

Setting the Retransmit Timeout Value for TACACS+ Servers

Cisco recommends that the retransmit timeout value for TACACS+ authentication, authorization, and accounting servers be increased if you experience repeated reauthentication attempts or the controller falls back to the backup server when the primary server is active and reachable. The default retransmit timeout value is 2 seconds and can be increased to a maximum of 30 seconds.

Configuring an Access Point's Prestandard Power Setting

An access point can be powered by a Cisco prestandard 15-watt switch with Power over Ethernet (PoE) by entering this command:

config ap power pre-standard {**enable** | **disable**} {**all** | *Cisco_AP*}

A Cisco prestandard 15-watt switch does not support intelligent power management (IPM) but does have sufficient power for a standard access point. The following Cisco prestandard 15-watt switches are available:

- AIR-WLC2106-K9
- WS-C3550, WS-C3560, WS-C3750
- C1880
- 2600, 2610, 2611, 2621, 2650, 2651
- 2610XM, 2611XM, 2621XM, 2650XM, 2651XM, 2691
- 2811, 2821, 2851
- 3631-telco, 3620, 3640, 3660
- 3725, 3745
- 3825, 3845

The **enable** version of this command is required for full functionality when the access point is powered by a Cisco prestandard 15-watt switch. Disable the pre-standard option if power is being provided by a power injector or by a switch not on the above list. This is the default value.

It is safe to use if the access point is powered by either an IPM switch or a power injector or if the access point is not using one of the 15-watt switches listed above.

You might need this command if your radio operational status is "Down" when you expect it to be "Up." Enter the **show msglog** command to look for this error message, which indicates a PoE problem:

```
Apr 13 09:08:24.986 spam_lrad.c:2262 LWAPP-3-MSGTAG041: AP 00:14:f1:af:f3:40 is unable to
verify sufficient in-line power. Radio slot 0 disabled.
```

Controller Functions that Require a Reboot

After you perform these functions on the controller, you must reboot the controller in order for them to take effect:

- Enable or disable link aggregation (LAG)
- Enable a feature that is dependent on certificates (such as HTTPS and web authentication)
- Add new or modify existing SNMP v3 users

- Install a license, change the license feature set, or change the priority of an AP-count evaluation license on a 5500 series controller

2106 Controller LEDs

The 2106 controller's Status LED and AP LED do not flash amber when software is being uploaded to the controller or downloaded to an access point, respectively.

Note Some versions of the *Cisco 2106 Wireless LAN Controller Quick Start Guide* might incorrectly state that these LEDs flash amber during a software upload or download.

Rate-Limiting on the Controller

Rate-limiting is applicable to all traffic destined to the CPU from either direction (wireless or wired). Cisco recommends that you always run the controller with the default **config advanced rate enable** command in effect in order to rate-limit traffic to the controller and protect against denial-of-service (DoS) attacks. You can use the **config advanced rate disable** command to stop rate-limiting of Internet Control Message Protocol (ICMP) echo responses for testing purposes. However, Cisco recommends that you reapply the **config advanced rate enable** command after testing is complete.

Pings Supported to the Management Interface of the Controller

Controller software release 4.1.185.0 or later is designed to support ICMP pings to the management interface either from a wireless client or a wired host. ICMP pings to other interfaces configured on the controller are not supported.

Pinging from a Network Device to a Controller Dynamic Interface

Pinging from a network device to a controller dynamic interface may not work in some configurations. When pinging does operate successfully, the controller places Internet Control Message Protocol (ICMP) traffic in a low-priority queue, and the reply to ping is on best effort. Pinging does not pose a security threat to the network. The controller rate limits any traffic to the CPU, and flooding the controller is prevented. Clients on the WLAN associated with the interface pass traffic normally.

GLBP Not Supported

Controller software release 4.2 or later is not compatible with the Gateway Load Balancing Protocol (GLBP). Make sure to configure the controller's default gateway to a fixed address and not to the GLBP virtual address.

IPSec Not Supported

Software release 6.0.182.0 does not allow you to choose IPSec as a Layer 3 security option. None and VPN Passthrough are the only available options. If you upgrade to this release from a previous release that supported IPSec as a Layer 3 security option, any WLANs that are configured for this feature become disabled. If you want to configure IPSec, you must use a version of controller software prior to 4.0.

4400 Series Controllers Do Not Forward Subnet Broadcasts through the Guest Tunnel

As designed, 4400 series controllers do not forward IP subnet broadcasts from the wired network to wireless clients across the EoIP guest tunnel.

Connecting 1100 and 1300 Series Access Points

You must install software release 4.0.179.8 or later on the controller before connecting 1100 and 1300 series access points to the controller.

Preventing Clients from Accessing the Management Network on a Controller

To prevent or block a wired or wireless client from accessing the management network on a controller (from the wireless client dynamic interface or VLAN), the network administrator should ensure that there is no route through which to reach the controller from the dynamic interface or use a firewall between the client dynamic interface and the management network.

Voice Wireless LAN Configuration

Cisco recommends that aggressive load balancing always be turned off either through the controller GUI or CLI in any wireless network that is supporting voice, regardless of vendor. When aggressive load balancing is turned on, voice clients can hear an audible artifact when roaming, and the handset is refused at its first reassociation attempt.

Changing the IOS LWAPP Access Point Password

Cisco IOS Lightweight Access Point Protocol (LWAPP) access points have a default password of *Cisco*, and the pre-stage configuration for LWAPP access points is disabled by default. To enable it, you must configure the access point with a new username and password when it joins the controller. Enter this command using the controller CLI to push a new username and password to the access point:

config ap username *user_id* **password** *password* {*Cisco_AP* | **all**}

- The *Cisco_AP* parameter configures the username and password on the specified access point.
- The **all** parameter configures the username and password on all the access points registered to the controller.

The password pushed from the controller is configured as “enable password” on the access point.

There are some cases where the pre-stage configuration for LWAPP access points is disabled and the access point displays the following error message when the CLI commands are applied:

> "ERROR!!! Command is disabled."

For more information, refer to *Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode.*

Exclusion List (Blacklist) Client Feature

If a client is not able to connect to an access point, and the security policy for the WLAN and client are correct, the client has probably been disabled. In the controller GUI, you can view the client's status on the Monitor > Summary page under Client Summary. If the client is disabled, click **Remove** to clear the disabled state for that client. The client automatically comes back and, if necessary, reattempts authentication.

Automatic disabling happens as a result of too many failed authentications. Clients disabled due to failed authorization do not appear on the permanent disable display. This display is only for those MACs that are set as permanently disabled by the administrator.

RADIUS Servers and the Management VLAN

If a RADIUS server is on a directly connected subnet (with respect to the controller), then that subnet must be the management VLAN subnet.

RADIUS Servers

This product has been tested with CiscoSecure ACS 4.2 and later and works with any RFC-compliant RADIUS server.

Management Usernames and Local Netuser Names

Management usernames and local netuser names must be unique because they are stored in the same database. That is, you cannot assign the same name to a management user and a local netuser.

Using the Backup Image

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.

Home Page Retains Web Authentication Login with IE 5.x

Because of a caching problem in the Internet Explorer 5.x browser, the home page retains the web authentication login. To correct this problem, clear the history or upgrade your workstation to Internet Explorer 6.x.

Ad-Hoc Rogue Containment

Client card implementations may mitigate the effectiveness of ad-hoc containment.

Changing the Default Values of SNMP Community Strings

The controller has commonly known default values of “public” and “private” for the read-only and read-write SNMP community strings. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values. Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 5.2* for configuration instructions.

Changing the Default Values for SNMP v3 Users

The controller uses a default value of “default” for the username, authentication password, and privacy password for SNMP v3 users. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values. Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 5.2* for configuration instructions.

Note SNMP v3 is time sensitive. Make sure that you have configured the correct time and time zone on your controller.

Features Not Supported on 2100 Series Controllers

This hardware feature is not supported on 2100 series controllers:

- Service port (separate out-of-band management 10/100-Mbps Ethernet interface)

These software features are not supported on 2100 series controllers:

- VPN termination (such as IPSec and L2TP)
- VPN passthrough option

  Note You can replicate this functionality on a 2100 series controller by creating an open WLAN using an ACL.

- Termination of guest controller tunnels (origination of guest controller tunnels is supported)
- External web authentication web server list
- Spanning Tree Protocol (STP)
- Port mirroring
- AppleTalk
- QoS per-user bandwidth contracts
- IPv6 pass-through
- Link aggregation (LAG)
- Multicast-unicast mode

Features Not Supported on 5500 Series Controllers

These software features are not supported on 5500 series controllers:

- Static AP-manager interface

Note For 5500 series controllers, you are not required 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.

- Asymmetric mobility tunneling
- 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)

Note The 5500 series controllers bridge these packets by default. If desired, you can use ACLs to block the bridging of these protocols.

Some Clients See Only 64 Access Point MAC Addresses (BSSIDs) at a Time

In a crowded RF environment, clients may not be able to detect the desired SSID because of internal table limitations. Sometimes disabling and then enabling the client interface forces a rescan. Your RF environment needs to be controlled. Cisco UWN rogue access point detection and containment can help you to enforce RF policies in your buildings and campuses.

2106 Image Not Supported for 3504 Controllers

The 2106 controller image is supported for use with only 2100 series controllers. Do not install the 2106 image on a 3504 controller. Otherwise, errors may occur. Install only the 3504 image on a 3504 controller.

Running a 3504 Image on a 2106 Series Controller

It is possible to run a 3504 controller image on a 2106 series controller, but Cisco Aironet 1130, 1200, and 1240 series access points will not be able to connect to the controller.

Upgrading External Web Authentication

When upgrading a controller from operating system release 2.0 or 2.2.127.4 to release 3.2.116.21 or later, update the external web authentication configuration as follows:

1. For 5500 series controllers, 2100 series controllers, and controller network modules, you must configure a preauthentication access control list (ACL) on the WLAN for the external web server and then choose this ACL as the WLAN preauthentication ACL under **Security Policies > Web Policy** on the WLANs > Edit page.
2. For 4400 series controllers and the Cisco WiSM, instead of using a preauthentication ACL, the network manager must configure the external web server IP address using this command:

   config custom-web ext-webserver add *index IP-address*

   Note *IP-address* is the address of any web server that performs external web authentication.

3. The network manager must use the new login_template shown here:

   Note Make sure to format the script to avoid any extra characters or spaces before using the web authentication template.

```
<html>
<head>
<meta http-equiv="Pragma" content="no-cache"> <meta HTTP-EQUIV=”Content-Type”
CONTENT="text/html; charset=iso-8859-1"> <title>Web Authentication</title> <script>

function submitAction(){
     var link = document.location.href;
     var searchString = "redirect=";
     var equalIndex = link.indexOf(searchString);
     var redirectUrl = "";
     var urlStr = "";
     if(equalIndex > 0) {
            equalIndex += searchString.length;
            urlStr = link.substring(equalIndex);
            if(urlStr.length > 0){
   redirectUrl += urlStr;
         if(redirectUrl.length > 255)
        redirectUrl = redirectUrl.substring(0,255);
       document.forms[0].redirect_url.value = redirectUrl;
  }
     }

     document.forms[0].buttonClicked.value = 4;
     document.forms[0].submit();
}

function loadAction(){
     var url = window.location.href;
     var args = new Object();
     var query = location.search.substring(1);
     var pairs = query.split("&");
     for(var i=0;i<pairs.length;i++){
          var pos = pairs[i].indexOf('=');
          if(pos == -1) continue;
          var argname = pairs[i].substring(0,pos);
          var value = pairs[i].substring(pos+1);
          args[argname] = unescape(value);
     }
     //alert( "AP MAC Address is " + args.ap_mac);
     //alert( "The Switch URL is " + args.switch_url);
     document.forms[0].action = args.switch_url;

     // This is the status code returned from webauth login action
     // Any value of status code from 1 to 5 is error condition and user
     // should be shown error as below or modify the message as it suits
     // the customer
     if(args.statusCode == 1){
        alert("You are already logged in. No further action is required on your 
part.");
     }
     else if(args.statusCode == 2){
        alert("You are not configured to authenticate against web portal. No further 
action is required on your part.");
     }
     else if(args.statusCode == 3){
        alert("The username specified cannot be used at this time. Perhaps the user is 
already logged into the system?");
     }
     else if(args.statusCode == 4){
        alert("Wrong username and password. Please try again.");
     }
     else if(args.statusCode == 5){
        alert("The User Name and Password combination you have entered is invalid. 
Please try again.");
     }

}

</script>
</head>
<body topmargin="50" marginheight="50" onload="loadAction();"> <form method="post"> 
<input TYPE="hidden" NAME="buttonClicked" SIZE="16" MAXLENGTH="15" value="0"> <input 
TYPE="hidden" NAME="redirect_url" SIZE="255" MAXLENGTH="255" VALUE=""> <input 
TYPE="hidden" NAME="err_flag" SIZE="16" MAXLENGTH="15" value="0">

<div align="center">
<table border="0" cellspacing="0" cellpadding="0"> <tr> <td>&nbsp;</td></tr>

<tr align="center"> <td colspan="2"><font size="10" color="#336699">Web 
Authentication</font></td></tr>

<tr align="center">

<td colspan="2"> User Name &nbsp;&nbsp;&nbsp;<input type="TEXT" name="username" 
SIZE="25" MAXLENGTH="63" VALUE=""> </td> </tr> <tr align="center" > <td colspan="2"> 
Password &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<input type="Password" name="password" 
SIZE="25" MAXLENGTH="24"> </td> </tr>

<tr align="center">
<td colspan="2"><input type="button" name="Submit" value="Submit" class="button" 
onclick="submitAction();"> </td> </tr> </table> </div>

</form>
</body>
</html>
```

Important Notes for Controllers and Mesh Access Points

This section describes important information about controllers and mesh access points.

Access Point Support Limit on Cisco WiSMs

The Cisco WiSM supports only up to 300 mesh access points reliably. Therefore, do not allow more than 300 mesh access points to associate to a Cisco WiSM.

Bridge MAC Filter Config Status Shown in Error

The **show network** command mistakenly shows a status for the Bridge MAC Filter Config parameter. This parameter is not a configurable option in software release 4.1.192.35M or later (CSCsk40572).

Limit Bridge Group Names to 11 Characters

Entering more than 11 characters into the bridge group name (BGN) field on the controller GUI mesh access point configuration page generates an error message. An error also appears when you configure this parameter through the **config ap bridgegroupname set groupname** *Cisco_MAP* CLI command or WCS (CSCsk64812).

Monitoring Port LED Status on a 1520 Series Access Point

When you disconnect a cable from a 1520 series access point, the port LED associated with that connection might remain lit for up to 3 seconds.

Data Rate Considerations in Short Link Deployments of 1520 Series Access Points

For dynamic frequency selection (DFS) bands, the current Hammer 5-GHz radio does not meet the receiver saturation specification of –30 dBm for some of the higher data rate modes due to a transceiver chipset optimization made to lower the DFS false detect probability. The typical receiver saturation input level is –37 dBm at 24 and 36 Mbps. The receiver saturation performance impact can be mitigated by reducing transmit power and antenna gain where possible. For typical deployments where radios are separated by reasonable distances, there is no impact to high data rate support.

Warning Message for Access Point Bridging Disable Requests

When you disable access point bridging using either the controller GUI (All APs > *AP_Name* > Mesh) or CLI (**config ap bridging disable**), the following message appears: “Disabling ethernet bridging will affect servicing of ethernet bridged clients. Are you sure you want to continue?” (CSCsi88127 and CSCsm16458).

Warning Message for Antenna Gain Changes

When you change the antenna gain on either the 1522 or 1524 access point radio using the controller GUI (Wireless > Access Points > Radios) or CLI (**config 802.11a antenna extAntGain**), the following message appears: "Changing antenna gain can make current channel unusable. The AP will be rebooted. A new channel must be chosen once the AP rejoins. If no channel is available with the new antenna gain, it will return back to the original value. Are you sure you want to continue?" (CSCsl75327).

Message for LinkTest Limitations

When you run a linktest that might oversubscribe the link using the controller GUI (Wireless > All APs > *Access_Point_Name* > *Neighbor_Info*) or CLI (**config mesh linktest**), the following message appears: "Warning! Data Rate (100 Mbps) is not enough to perform this link test on packet size (2000 bytes) and (1000) packets per second. This may cause AP to disconnect or reboot. Are you sure you want to continue?" (CSCsm11349).

Features Not Supported on Mesh Networks

The following controller features are not supported on mesh networks:

- Multi-country support
- Load-based CAC (Mesh networks support only bandwidth-based, or static, CAC.)
- High availability (fast heartbeat and primary discovery join timer)
- EAP-FASTv1 and 802.1X authentication
- Access point join priority (Mesh access points have a fixed priority.)
- Locally significant certificate
- Location-based services

Caveats

This section lists Open Caveats and Resolved Caveats for Cisco controllers and lightweight access points.

Open Caveats

The open caveats are divided into two sections:

- New Open Caveats, page 45
- Caveats Open in Previous Releases, page 51

New Open Caveats

These new caveats are open in controller software release 6.0.182.0.

Major New Open Caveats

These caveats are open in controller software release 6.0.182.0 and have a severity of 1 or 2.

- CSCsz12429—On rare occasions, the **show controller** CLI command on a controller running software release 6.0 might show this message: "Transmitter seems to have stopped."

  Workaround: None.

- CSCsz18085—In a large wireless network deployment with 1240 series access points, the closest access point does not report RSSI values when S60 calibration is performed.

  Workaround: None.

- CSCsz34724—A 2100 series controller or controller network module automatically reboots during a software image download. When multiple management sessions (SSH, Telnet, GUI) are concurrently open, the controller can reserve up to 2 MB of memory per session. Depending on the number of concurrent sessions, the controller can reserve a significant amount of memory, which is then no longer available during image downloads.

  Workaround: Before an image download, reboot the controller if it has less than 90 MB of free memory. Use the **show memory statistics CLI** command to see the current amount of free memory.

- CSCsz38828—An 1130 or 1230 series access point radio might experience a core dump or reset and stop transmissions.

  Workaround: None.

- CSCsz43474—An 1142 access point in hybrid-REAP mode sometimes enters stand-alone mode. If the access point is rebooted while in stand-alone mode, the 802.11a radio changes to a different channel than the one configured by the controller after a few minutes.

  Workaround: None.

- CSCsz47181—The 1130 series access points might reboot during a system upgrade and become stuck in a constant discovery loop. This behavior occurs in a large-scale environment when many access points are unable to join a controller simultaneously.

  Workaround: Make sure that the access point can reach a controller at all times. If the access point requires AAA authentication, the AAA server should have the access point entry to avoid any loops of discovery.

- CSCsz72774—1240 series access points in monitor mode sometimes reboot in the Dot11 driver software process.

  Workaround: None.

- CSCsz89669—Access point radios sometimes toggle between beacons disabled and enabled when packets are pending in the radio.

  Workaround: None.

Moderate New Open Caveats

These caveats are open in controller software release 6.0.182.0 and have a severity of 3.

- CSCsv33662—When you try to upgrade a 4400 series controller from software release 4.2 to 6.0, the controller might display the following Linux kernel panic message: "Open Device file Failed while writing Watchdog Data<0>Kernel panic - not syncing: No init found. Try passing init= option to kernel."

  Workaround: None. The controller recovers after 180 seconds.

- CSCsy01118—When noise sources are present in the network, 1130 and 1240 series access point radios might experience channel fluctuations because off-channel noise measurements are not done properly in legacy access point radios.

  Workaround: Change the dynamic channel assignment (DCA) schedule to run infrequently, or remove noise as a metric for DCA.

- CSCsy20525—The **config mesh secondary-backhaul** {**enable** | **disable**} command is ignored by the controller.

  Workaround: It is not valid in controller software release 6.0.

- CSCsy27483—The access point LWAPP uptime might be reported incorrectly during a Daylight Saving Time (DST) change.

  Workaround: Reboot the access point that reports an incorrect LWAPP uptime.

- CSCsy40776—When two workgroup bridges (along with clients) are connected through a hub and associate to an 1130 or 1240 series access point, a traceback occurs when the access point attempts to join a controller.

  Workaround: Separate the workgroup bridges between two hubs.

- CSCsy47656—When you enter the **config guest-lan security splash-page-web-redir** {**enable** | **disable**} *guestlan_id* command, it is applied to the WLAN with the corresponding WLAN ID instead of to the guest LAN.

  Workaround: It is not applicable for guest LANs.

- CSCsy55985—SSH/HTTPS access becomes sluggish for a 5500 series controller during an access point image upgrade.

  Workaround: None.

- CSCsy56469—An 1130 series access point reboots when a workgroup bridge is connected to the same switch as the access point through which it is trying to associate to the controller.

  Workaround: It is very unusual to have such a connection. A workgroup bridge should never have a wired connection to the switch. If there is such a connection, it should be removed.

- CSCsy57435—You should not be able to delete a WLAN if a guest user is using it.

  Workaround: None.

- CSCsy61338—If you use WCS to enable the quantraine VLAN on a controller management interface, WCS shows an SNMP error. The error appears only if an active WLAN is having that interface mapped.

  Workaround: Enable the quantraine VLAN on the management interface of an individual controller rather than from WCS.

- CSCsy62781—CAPWAP instructs an access point to disable beacons and probes over and over again, even after the access point has already executed the instructions.

  Workaround: None.

- CSCsy77851—If you use WCS to push more than 50 WLAN templates to a 5500 series controller with 250 access points associated, WCS takes a long time to create the WLANs.

Workaround: Push one or just a couple WLAN templates at a time.

- CSCsy79435—When Ethernet bridging is enabled for a mesh access point, VLAN information is not deleted when the access point's configuration is erased from the controller GUI or CLI.

  Workaround: Set the Ethernet port mode to Normal from the controller GUI or CLI.

- CSCsz06811—When multicast-multicast is configured on a 5500 series controller, the downstream multicast throughput is low for packet sizes of 1518 bytes.

  Workaround: None.

- CSCsz06820—When you configure an access control list (ACL) with 64 rules and the last rule is set to permit all, packets pass the sixty-fourth rule, but the permit counter does not increment. It shows 0.

  Workaround: None.

- CSCsz07277—The controller does not show the complete output of the **show auth-list** CLI command.

  Workaround: None.

- CSCsz08530—The client details page on a 5500 series controller might take 5 to 10 seconds to show the details for a CCXv5 client.

  Workaround: None. The page comes up after awhile.

- CSCsz10515—When paging is enabled and you try to see the list of available commands for the **config** command by using a **?**, the last command on the page gets truncated and overflows to the next page.

  Workaround: Disable paging.

- CSCsz11308—A runtime edit of the RADIUS server is not being saved.

  Workaround: Click the index of the RADIUS server, update the status, save the configuration, and reboot the controller.

- CSCsz11493—When the WLAN diagnostics channel is enabled and security is configured, XML validation errors appear while downloading a configuration file onto the controller.

  Workaround: Manually configure the commands that were rejected because of the XML validation errors.

- CSCsz13710—If you add a non-default SNMP user, upload the configuration, and download it again, the default SNMP user is removed.

  Workaround: Reconfigure the default SNMP user using this CLI command:
  config snmp v3user create default rw hmacsha aescfb128 *authkey privkey*

- CSCsz14422—When 802.1X clients are roaming, the output of the **show process memory** CLI command does not show the correct BlocksInUse value for the RadiusTransportThr process because of an error in per-task memory statistics accounting.

  Workaround: None.

- CSCsz16449—When you change the management IP address on a 2106 controller and other mobility members are updated with this new management IP address in the mobility group configuration, the data path on the 2106 controller for other mobility members never comes up.

  Workaround: To bring the mobility path up, delete the mobility member entry on the 2106 controller and reconfigure it or reboot the 2106 controller.

- CSCsz16489—If management via wireless and management via dynamic are enabled, you can open the controller GUI using the virtual interface IP address.

Workaround: Create a CPU ACL to block GUI access to the virtual interface.

- CSCsz18431—The controller GUI shows the wrong syslog facility when configured through the controller CLI.

  Workaround: Use the controller GUI to configure the syslog facility.

- CSCsz19715—RF configuration parameters for client roaming are not reflected after a configuration upload or download.

  Workaround: None.

- CSCsz20162—QoS rate limiting is not accurate for a 5500 series controller for both TCP and UDP. The resulting allowed traffic is around 50% lower than the expected traffic.

  Workaround: Configure the limits to a higher than desired value.

- CSCsz23896—A software release prior to 6.0 can be downloaded to a 5500 series controller without a warning or an error message.

  Workaround: None.

- CSCsz26737—When Rogue Location Detection Protocol (RLDP) is enabled for local mode access points, the access points move to the rogue channel but continue to beacon and serve clients.

  Workaround: None.

- CSCsz26973—The CHDM client threshold check currently passes only if the number of failed clients exceeds the current threshold. So if the threshold is set to 3, four failed clients are required to detect a coverage hole.

  Workaround: Configure the threshold to be one less than the expected number.

- CSCsz29877—Ports 7 and 8 on the 2112 and 2125 controllers do not correctly support Power over Ethernet (PoE) to lightweight access points.

  Workaround: Console to the access points and issue the following command:
  power inline negotiation injector installed

- CSCsz29925—On a 2100 series controller, the **show cdp neighbor detail** CLI command provides invalid power drawn information.

  Workaround: None.

- CSCsz32085—The local SSID defined on the OfficeExtend access point has a malformed wireless multimedia (WMM) information element (IE). The QoS information bits, EDCA parameters, and advertised access categories are incorrect.

  Workaround: None.

- CSCsz32401—A 5500 series controller does not generate a trap when the wplus or base evaluation license expires.

  Workaround: Enter the **show logging** CLI command to view the message log.

- CSCsz37352—If 250 access points are joined to a 5500 series controller, the GUI does not show all of the access points on the Management Frame Protection Settings page.

  Workaround: None.

- CSCsz37520—When channel utilization (CU) for 1140 and 1250 series access points is calculated, non-802.11 noise is not taken into account. Noise detection works correctly and is used properly in dynamic channel assignment (DCA); it is just not accounted for in the CU.

  Workaround: None.

- CSCsz37571—For 5500 series controllers, client statistics are always 0 for wired guest clients.

Workaround: None.

- CSCsz46499—A client might fail EAP-FAST PAC provisioning using generic token card (GTC).

  Workaround: Configure the client to use MSCHAPv2 to provision the PAC and then change back to GTC after it has the PAC. Alternatively, you can enable anonymous provisioning on the client so it uses MSCHAPv2 for the PAC provisioning phase, or you can manually provision the PAC.

- CSCsz47597—When you change management and AP-manager IP address to different subnets, multicast data stops flowing. The controller receives multicast traffic from the wired network but does not forward it to access points in CAPWAP. The same problem occurs when you change the management and AP-manager VLAN configuration from tagged to untagged or from untagged to tagged.

  Workaround: Disable and re-enable multicast globally after editing IP addresses or VLAN tags for management and AP-manager interfaces.

- CSCsz52953—You can enable 128-bit WEP using SNMP in some controller releases even though support for 128-bit WEP has been removed from the controller CLI and the GUI.

  Workaround: None.

- CSCsz53077—When you remove and re-insert radio modules from a 1250 series access point into different slots, the access point learns the MFP keys generated from radios on neighboring access points in different slots.

  Workaround: Insert radio modules only in defined slots; for example, Radio A module should be inserted in slot 1 and Radio B/G module should be inserted in slot 0.

- CSCsz56454—Controller logs are sometimes flooded with messages about access points impersonating legitimate access points.

  Workaround: None.

- CSCsz59488—When an MSE is connected to a 5500 series controller, the controller's client count that appears in WCS sometimes drops unexpectedly to an inaccurate number and then recovers to the correct number within five minutes.

  Workaround: None.

- CSCsz68445—Local Auth sometimes fails with EAP-FAST, especially when using Funk Odyssey supplicant.

  Workaround: Use a client supplicant other than Odyssey, or use LEAP.

- CSCsz69190—Messages similar to this one sometimes appear on the controller console when client devices are disconnected abruptly, or when access points or the controller are rebooted:

  PPX:~CONSOLE--> cmdDelTclas:XXXX acldb_delete failed for aclId XXXX

  Workaround: None.

- CSCsz71417—When dozens of access points join a controller at the same time, this message sometimes appears on the controller console:

  ```
  PP1:~CONSOLE-> fp_egress_capwap:573 inside_l2_hdr_and_cw_len = 64
  PP1:~CONSOLE->
  PP1:~CONSOLE-> fp_egress_capwap:574    dtlsHdr->length:1520
  ```

  Workaround: Limit the number of access points that are allowed to join the controller at the same time.

- CSCsz73516—License operation sometimes fails on 5500 series controllers after a series of "clear license base-ap-count" and "clear license wplus-ap-count" messages.

  Workaround: None.

- CSCsz75076—An SNMP error sometimes appears when you configure physical mode for a controller port.

  Workaround: Set the physical mode to Auto for the port.

- CSCsz77786—You cannot disable HTTP on a hybrid-REAP access point.

  Workaround: None.

- CSCsz81149—Access points do not use RTS/CTS to send frames using MIMO when a client device requests dynamic SM power save.

  Workaround: None.

- CSCsz90565—When dozens of access points join a controller at the same time, the controller console displays messages like these:

  ```
  PP2:~CONSOLE-> cp_debug_printf: Could not allocate buffer. Log message dropped.
  PP8:~CONSOLE-> cp_debug_printf: Could not allocate buffer. Log message dropped.
  PP4:~CONSOLE-> cp_debug_printf: Could not allocate buffer. Log message dropped.
  ```

  Workaround: None.

- CSCsz93036—Output for the **show traplog** command sometimes fails to show coverage hole trap events. When coverage holes are detected, the CHD module generates a trap which is sent to WCS for monitoring. On the controller, the **show traplog** command should list all the traps, but it does not. However, CH detection traps are displayed in WCS.

  Workaround: View the traps in WCS.

- CSCsz94920—When the controller checks the status of an access point's 2.4-Ghz and 5-Ghz radios, it checks the power-over-Ethernet (PoE) state for the access point. If the PoE state is set to 15.4 power, the controller automatically indicates that the e 2.4-Ghz and 5-Ghz radios are in "degraded state." The controller could indicate the actual state of the radio if a field accompanied the radio CAPWAP config response to indicate whether a radio is in Powered Down, Single Transmitter, or Full Power mode.

  Workaround: None.

- CSCsz96027—The login banner is displayed after the user prompt appears. This issue is seen when the login banner is downloaded and the controller displays the user prompt first, followed by the banner. The login banner should be completely displayed and then the prompt should appear.

  Workaround: None.

- CSCsz97089—Multicast traffic sometimes fails in inter-NPU network configurations when IGMP snooping is enabled.

  Workaround: None.

- CSCta00445—The current controller logging and debugging method makes it difficult to identify which task is logging the message. Ideally, the thread name should be part of the logging message.

  Workaround: None.

- CSCta08942—Appletalk does not work with Lexmark printers. Frames from Lexmark printers come to 4400 series controllers as DSAP: SNAP (0xaa) but go to the wire as DIX (Digital Intel Xerox).

  Workaround: None.

Minor New Open Caveats

These caveats are open in controller software release 6.0.182.0 and have a severity of 4 or 5.

- CSCsx68322—When dynamic channel assignment (DCA) is scheduled for 1-hour intervals, it does not run at the exact hour. It runs about 35 minutes later.

  Workaround: None.
- CSCtf90722—ACL on WLC4400/WiSM can cause low throughput and packet loss.

  Workaround: Move the ACL elsewhere on the network.

Caveats Open in Previous Releases

These caveats are open in controller software release 6.0.182.0 and in prior releases.

Major Caveats Open in Previous Releases

These caveats are open in controller software release 6.0.182.0 and in prior releases and have a severity of 1 or 2.

- CSCsm82725—Clients are able to connect to the Internet without authenticating when using web authentication and port 53 on a proxy server.

  Workaround: None.
- CSCso10678—The controller might hang when you attempt to upgrade the controller software.

  Workaround: Upgrade to a more recent controller software release. Make sure to follow the upgrade instructions in the *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points* for that release.
- CSCsq26051—When a Cisco terminal server connects to the controller but the user is not logged in through the console, the controller might hang after a reboot.

  Workaround: None.
- CSCsr02102—Non-mesh 4.2 software should not allow 1505 or 1510 mesh access points to join the controller and download software. The access points generally do not join, but they can become inoperable.

  Workaround: None.
- CSCsr39536—An error message appears if you make any changes on the AP Details page on the controller GUI and do not re-enter the access point credentials.

  Workaround: Re-enter the access point credentials.
- CSCsu09424—Cisco 2100 series controllers sometimes reboot unexpectedly when you upgrade from software release 4.2.121.0 to 5.2.157.0.

  Workaround: Upgrade to a more recent controller software release. Make sure to follow the upgrade instructions in the *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points* for that release.
- CSCsu38925—After you upgrade a 2106 controller to software release 5.1, access points sometimes fail to join the controller automatically.

  Workaround: Downgrade the controller to a software release earlier than 5.1.
- CSCsv12308—When the controller has to use its default gateway to talk to an access point, the access point never sees the join reply from the controller because the AP-manager uses the wrong MAC address for the default gateway.

Workaround: Clear the default gateway on the AP-manager or reboot the controller.

- CSCsw45913—The wrong access control list (ACL) is applied when the AAA override feature is enabled for ACLs.

  Workaround: Do not use the AAA override feature with ACLs.

- CSCsw49486—When many access points are joining at the same time, they may reboot during a software error.

  Workaround: Wait for the access points to join.

- CSCsx96815—After you upgrade a Cisco WiSM controller from software release 4.1.192xM to 5.2.157.0, the virtual interface becomes corrupted.

  Workaround: Reconfigure the virtual interface with a new IP address and reboot the controller. Then reconfigure the original IP address and reboot the controller again.

- CSCsy15897—Cisco Aironet 1232 access points do not go off channel to perform background scanning even with no clients and all WLANs disabled.

  Workaround: None.

- CSCsy59254—802.11n access points use long packet retries (the full packet is retried instead of the RTS mechanism), which can lead to degraded voice quality in extreme fringe coverage areas.

  Workaround: None.

- CSCsy80680—A client is unable to obtain an IP address after a Layer 3 roam event.

  Workaround: None.

- CSCsy95660—Under rare conditions, the radio of an 1140 series access point might enter a state in which the transmitter is stuck with probes disabled and beacons enabled. The following message appears in the output of the **show controllers** access point CLI command: “Beacons enabled, Probes disabled.”

  Workaround: None.

- CSCsz37124—When a Cisco WiSM controller crashes, it fails to display a crash log.

  Workaround: To capture a crash dump to a text file, console a machine directly into the controller with a terminal emulation program such as HyperTerminal and monitor the controller for a few days.

- CSCsz40659—Sometimes during a controller software upgrade, the file transfer of the new image fails.

  Workaround: Reboot the controller.

- CSCsz40856—Intermittently, a client associated to a hybrid-REAP access point using EAP-TLS is not able to pass traffic although it is listed in the Run state.

  Workaround: You can get the client to pass traffic again by moving to and from the primary and secondary controller.

- CSCsz41350—If you disable the auto-containment SSID and reboot 1140 and 1250 series access points, the watchdog timer for some of the access points expires within a minute of rebooting.

  Workaround: None.

- CSCsz48244—The mobility control path for controllers to the DMZ sometimes flap up and down. However, the data path for the same controllers does not flap.

  Workaround: None.

- CSCsz53434—When the DHCP address required flag is not enabled for a WLAN, wireless client devices can sometimes forge the IP address for the VLAN if the selected IP address is not in the ARP table.

Workaround: None.

- CSCsz57113—Controllers sometimes send IPv6 Routing Advertisement, Layer-2 Multicast packets on the wrong (old) VLAN.

  Workaround: Reset the controller.

- CSCsz64049—Controllers sometimes reboot unexpectedly, and console output suggests that nf_iterate causes a kernel panic/exception. After rebooting the controllers operates normally until it unexpectedly reboots again.

  Workaround: None.

- CSCsz67401—When a 1252 access point is joined to a 4400 series controller running software release 4.2.176.0 and a Catalyst 3750 switch running 12.2(44) SE2, the access point does not negotiate 18.5 W of power.

  Workaround: Use the **power inline static** command.

- CSCsz76248—When an 1130 or 1240 series access point is powered up with insufficient power, the access point radios are sometimes stuck in a reset state and do not function, and the access point fails to send a low-power alert to the controller.

  Workaround: None.

- CSCsz80820—When you enable AP join priority and access points are connected to a secondary controller when the primary is already full, the access points will not fall back automatically to the primary.

  Workaround: Reboot the access points.

- CSCsz87643—Controllers sometimes become unreachable when you add an interface to the controller through WCS.

  Workaround: Reboot controller.

- CSCsz92558—Ethernet interface statistics from access points sometimes fail to appear on the controller GUI.

  Workaround: Enter the **show interface g0** command on the controller CLI to see access point Ethernet statistics.

Moderate Caveats Open in Previous Releases

These caveats are open in controller software release 6.0.182.0 and in prior releases and have a severity of 3.

- CSCek49781—When you use the lightweight access point 802.1X wired supplicant with EAP-FAST and in-band PAC provisioning, the access point fails to refresh the tunnel PAC when it expires and loses connectivity to the network.

  Workaround: Restart the access point so that it requests a new PAC instead of refreshing it. Disable 802.1x on the switch port.

- CSCsd54928—The CPU ACL is unable to block LWAPP packets that are destined for the IP address of the dynamic interface.

  Workaround: None.

- CSCsd84706—Containment information for ad-hoc rogue access points is not shown on the controller GUI.

  Workaround: Use the controller CLI.

- CSCsg87111—After you edit a WLAN configured for WPA1+WPA2 with a conditional redirect to 802.1X, the MIB browser shows a commit failure error.

  Workaround: Do not directly change from WPA1+WPA2+Conditional Web Redirect to 802.1X+Conditional Web Redirect. Instead, follow these steps:

  a. Remove **Conditional Web Redirect** and save your change.

  b. Change Layer 2 to **802.1X** and save your change.

  c. Change Layer 3 to **Conditional Web Redirect** and save your change.

- CSCsi17242—If a controller starts a timer (such as reauthentication or keylife time) after running for approximately 52 days, the timer might take a long time to fire (up to another 52 days).

  Workaround: Clean up the timers. If the problem is related to the client, deauthenticate the client to clean the timer. If the problem is related to the WLAN, such as a broadcast key update, disable and then re-enable the WLAN.

- CSCsi26248—After a failed link aggregation (LAG) link recovers, you might lose connectivity for approximately 30 seconds.

  Workaround: Recover the LAG link when service is not in use. You might also want to consider not using this type of configuration.

- CSCsj03124—RLDP behavior is inconsistent when initiated from a Cisco 1250 series access point.

  Workaround: Use access points other than the 1250 when RLDP needs to be used.

- CSCsj17054—A misleading message appears on the controller GUI when you upload software or certificates.

  Workaround: Ignore the message and choose the correct options to upload files on the controller.

- CSCsj29501—When the **session slot** or **telnet** command times out on the supervisor on the Cisco WiSM and you try to log in again, any character that you enter is duplicated.

  Workaround: Use a direct console connection to the Cisco WiSM.

- CSCsj62507—An access point in sniffer mode might report incorrect timestamps.

  Workaround: None.

- CSCsj87925—When you create a new rule for an access control list (ACL) using the controller GUI, the source and destination netmasks accept any value between 0 and 255, which are not actual netmask values.

  Workaround: Enter a valid netmask.

- CSCsj88889—WGB and wired WGB clients are shown using different radios.

  Workaround: None.

- CSCsk08360—The following message log entry needs further clarification: "APF-1-DISCONECT_MOBILE_DUE_TO_WLAN_SWITCH: Disconnecting mobile 00:16:6f:79:82:75 due to switch of WLANs from 2 to 1."

  Workaround: None.

- CSCsk08707—The 1250 series access points receive console error messages indicating that the primary discover decode failed.

  Workaround: None.

- CSCsk17001—When a guest LAN with a blank ingress interface name is added to the controller, the application fails with an SNMP exception message.

  Workaround: Use the controller CLI to configure a guest LAN. You might need to delete a previous guest LAN if it has a blank ingress interface configured on it and then recreate it. By default, the ingress interface is blank.

- CSCsl03097—When a hybrid-REAP access point in standalone mode is on the DFS channel, the access point's radio goes down if a radar event occurs on its operating channel.

  Workaround: Wait until the access point's connectivity to the controller recovers, or reboot the access point.

- CSCsl34068—Guest roles for guest users configured on the controller should override the QoS parameters set for the WLAN. However, when a guest user is momentarily disconnected and reassociates, the WLAN parameters override the guest role.

  Workaround: None.

- CSCsm66780—Creating a WLAN with an access control list (ACL) that has no rules generates an SNMP error.

  Workaround: Create an access list with rules.

- CSCsm71573—When the following message appears, it fills up the entire message log:

  ```
  mm_listen.c:5078 MM-3-INVALID_PKT_RECVD: Received an invalid packet from 10.0.x.x.
  Source member:0.0.0.0. source member unknown.
  ```

  Workaround: None.

- CSCsm79901—Wired clients attached to a workgroup bridge (WGB) are retaining the previous IP address after the WGB obtains a new IP address. As a result, the wired client stops sending traffic to the infrastructure network.

  Workaround: Release and renew the DHCP IP address manually on the WGB wired client.

- CSCso02714—Throughput sometimes drops when you configure two 4400 series controllers (one as an anchor and one foreign) with symmetric tunneling and link aggregation (LAG).

  Workaround: Dedicate a port to mobility tunneling if performance is not adequate.

- CSCso07457—When the controller downloads a file using FTP, WCS shows the previous transfer state as the intermediate state, which is different from the final transfer state.

  Workaround: None.

- CSCso22875—During code download, some access points might disconnect and then reconnect to the controller.

  Workaround: None.

- CSCso31067—Some clients might experience failures during upstream-only prioritized traffic on 802.11a, despite radio resource management (RRM) features being disabled.

  Workaround: None.

- CSCso31640—When you downgrade a 2100 series controller from software release 5.1 to software release 4.2.112.0 or later, any hybrid-REAP groups configured on the controller are lost after the downgrade.

  Workaround: None. You must reconfigure the hybrid-REAP groups.

- CSCso38071—1252 series access points sometimes fail to connect to 2106 controllers when plugged into a port on the 2106.

  Workaround: Plug the access point into a switch port.

- CSCso60597—If a 1250 series access point is configured for the 20-MHz channel width and is then placed into sniffer mode, you cannot change the channel width to Above 40 MHz or Below 40 MHz. If the 1250 series access point was set to Above 40 MHz or Below 40 MHz before it was placed into sniffer mode, you can change it to 20 MHz but not to the other 40 MHz setting.

  Workaround: Configure the access point back to local mode in order to modify the channel width settings; then return it to sniffer mode. This sequence of actions requires a minimum of two access point reboots.

- CSCso97776—If you enable MFP when a guest LAN is configured, the controller might show unwanted logs.

  Workaround: None.

- CSCsq04411—Tracebacks from the RM measure process sometimes appear in the logs of 1250, 1240, and 1130 series access points when you change them from monitor mode to local mode.

  Workaround: None.

- CSCsq06451—On the controller, you cannot change the mapping of the guest LAN ingress interface to None.

  Workaround: None.

- CSCsq13610—WCS allows special characters in the primary, secondary, and tertiary controller names and access point names, but the controller does not, making the overall behavior inconsistent.

  Workaround: Do not use special characters in the primary, secondary, and tertiary controller names and access point names when you configure them on the controller.

- CSCsq19472—CCX radio measurement reports are not accurate if you trigger beacon, channel load, noise histogram, and frame requests together.

  Workaround: None.

- CSCsq21956—An error might occur when you try to edit guest user values.

  Workaround: Use the controller CLI.

- CSCsq25129—A controller software upgrade might fail with a Nessus scan running.

  Workaround: Stop the Nessus scan when upgrading the controller software.

- CSCsq29243—The 802.11h channel switch mode parameter accepts any value, even though only 0 or 1 should be accepted.

  Workaround: None.

- CSCsq30821—Web authentication is bypassed if a client associates to an access point on one controller, roams to an access point on another controller, and then roams back to the first controller. This behavior occurs if the WLAN is on different subnets on each controller, causing the client to be anchored to the first controller when roaming to the second.

  Workaround: None.

- CSCsq32038—The **config interface create** CLI command does not indicate the number of characters allowed for the interface name.

  Workaround: Do not enter an interface name containing more than 31 characters.

- CSCsq34262—When you add three controllers running software release 4.2.125.0 to the same mobility group and enable a dynamic interface on each, a traceback might appear on the controller console.

  Workaround: None.

- CSCsq35402—After you upgrade the controller to software release 4.2.125.0, the controller sometimes shows this message on the console: “dtlARPProtoRecv: Invalid ARP packet!”

  Workaround: You can safely ignore this message.

- CSCsq35590—A traceback might appear on the access point console when you change the access point country from Spain to the US.

  Workaround: None.

- CSCsq38075—A traceback might appear on the access point console when you set the access point country to Spain.

  Workaround: None.

- CSCsq38700—After you change the power level of an access point radio, the controller shows the radio’s operational status as DOWN. However, clients continue to pass traffic and function properly.

  Workaround: None.

- CSCsq47493—The hybrid-REAP access point VLAN ID is not being updated.

  Workaround: First change the native VLAN ID; then change the hybrid-REAP VLAN ID.

- CSCsq74144—The controller does not show the channel on which an access point in sniffer mode is currently sniffing. It shows only the last channel on which the access point was broadcasting in local mode.

  Workaround: None.

- CSCsq96655—The Controller Network Module in a Cisco Integrated Services Router (ISR) and clients associated to access points on this controller do not receive ARP replies from the gateway. As a result, NAC out-of-band integration does not work on this platform.

  Workaround: Configure the ISR so that ARPs are forwarded properly with the NAC setup.

- CSCsr02316—Some SNMPSet operations show successful despite the fact that the controller is truncating the string.

  Workaround: Set a smaller value.

- CSCsr09192—The FTP username and password can contain no more than 24 characters; however, the controller indicates that it allows up to 31 characters.

  Workaround: Enter a username and password containing no more than 24 characters each.

- CSCsr12961—The CLI help syntax does not indicate the value you should enter for the *mode* option in the **config 802.11h** command.

  Workaround: None.

- CSCsr16689—Wired hosts cannot manage the 2106 controller through the dynamic interface.

  Workaround: None.

- CSCsr18797—After you switch from local authentication on the controller to using an external RADIUS server, clients continue to use local authentication for several minutes.

  Workaround: None.

- CSCsr20151—If you attempt to change the power level for the 5-GHz radio in a 1250 series access point, the change does not take effect.

  Workaround: Enable 802.11n for the 802.11a radio.

- CSCsr27851—When you use WCS to create a diagnostic WLAN for a controller, the controller sometimes shows this error message even though the WLAN has been created: "SNMP operation to Device failed: Failed to create WLAN on device."

  Workaround: You can safely ignore this message.

- CSCsr43931—Large pings (10K bytes or larger) sometimes fail when sent to gigabit-Ethernet cards with hardwired chipsets.

  Workaround: None.

- CSCsr44439—The Web Authentication page does not load on the controller GUI when a client connects through the wired guest VLAN on software releases 4.2.130.0 and 5.0.148.2.

  Workaround: None.

- CSCsr49318—When you configure the power constraint feature for the 802.11a/n network, the access point does not include information element (IE) 32 (the power constraint IE) in beacons.

  Workaround: None.

- CSCsr49364—When a dynamic frequency selection (DFS) event occurs, the access point fails to populate the next 10 beacons with information element (IE) 37 (the channel switch announce IE). The access point also fails to send a broadcast channel switch announce action frame to alert associated 802.11h clients to move to the new channel.

  Workaround: None.

- CSCsr49559—The 802.11a radio in mesh access points sometimes adds an unnecessary extra byte in the country information element (IE 7) in the beacons.

  Workaround: None.

- CSCsr58532—This message sometimes appears on 2106 controllers: "SIM-3-INTFGET_GIG_ ETH_FAIL: Failed to get the interface number of the Gigabit Ethernet Port."

  Workaround: Cisco 2106 controllers do not contain a Gigabit Ethernet port, so you can safely ignore this message.

- CSCsr72091—The controller radio resource management (RRM) feature sometimes fails to adjust the transmit power on the radios in 1250 series access points.

  Workaround: None.

- CSCsr78181—When a controller running software release 5.1 boots up, you can press **ESC** for more options. Password recovery should be an option, but it is not.

  Workaround: Use the proper password recovery procedure. Follow the instructions in the "Restoring Passwords" section in Chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide, Release 5.2*.

- CSCsr85444—The link test does not work for non-Cisco Compatible Extension clients. The following error message appears on the access point CLI: "No response received."

  Workaround: None.

- CSCsu24001—The controller does not fragment outgoing CAPWAP packets according to MTU value.

  Workaround: Do not set the MTU below 800.

- CSCsu27886—When you configure conditional web direct without first configuring 802.1X security, the controller shows this error message: "Invalid parameter specified." The message should state that 802.1X is required when you configure conditional web direct.

  Workaround: None.

- CSCsu44722—When you enable a mobility anchor on a WLAN and then try to enable IPv6 support for the WLAN (which is not supported), the controller shows an invalid error message.

  Workaround: None.

- CSCsu80604—The memory monitor configuration returns to default values after the controller reboots.

  Workaround: None.

- CSCsv35010—In 40-MHz mode, the controller GUI should not allow channel 11 to be set.

  Workaround: None.

- CSCsv39373—When you enable the access point fallback feature on the controller, the controller might not recognize client associations (even when clients are associated) because the controller sends a non-MFP protected disassociation message.

  Workaround: Disable MFP client protection.

- CSCsv44917—You can configure diversity for 1250 series access points using the controller GUI, which should not be possible.

  Workaround: None.

- CSCsv54436—SSH is sometimes denied on the controller with the following message: "Sorry, telnet is not allowed on this port."

  Workaround: Retry the SSH connection.

- CSCsv76513—When you perform a wireless sniffer trace for a 2100 series controller, the same BSSID appears for the WLANs on both the 802.11a and 802.11b/g radios.

  Workaround: None.

- CSCsv84462—When you try to edit the parameters of a local network user from the controller GUI, the following error message appears: "Error in creating user."

  Workaround: Use the controller CLI to edit the local network user.

- CSCsw25810—When you attempt to configure a RADIUS server for a wired guest LAN using the controller GUI, a browser error might appear.

  Workaround: Use the controller CLI instead of the GUI.

- CSCsw80627—The controller might reboot because of a software failure of the emWeb task.

  Workaround: None.

- CSCsx07443—Traffic stream metric (TSM) WCS reports show the power loss ratio (PLR) at 100000%. It should be less than or equal to 100%.

  Workaround: None.

- CSCsx41062—Upon reboot, the controller sometimes starts rejecting valid Network Time Protocol (NTP) packets.

  Workaround: None.

- CSCsx51118—An access point might fail to join a controller running software release 5.2.157.0, and the following error message might appear: "WTP Board data: Failed to get serial."

  Workaround: None.

- CSCsx64115—The following error message might appear on the console of a 4400 series controller when you clear the configuration: "dtlArpRequest: Cannot send an ARP reply to 00:0B:85:32:58:C0."

  Workaround: None.

- CSCsx75872—When a client device connected to a workgroup bridge deauthenticates and then reauthenticates, it fails to receive an IP address through DHCP.

  Workaround: Force the workgroup bridge to reauthenticate to the wireless LAN. The client devices connected to the workgroup bridge then successfully receive IP addresses.

- CSCsx96204—The controller does not mark disabled clients as excluded.

  Workaround: None.

- CSCsx96410—The clMeshNodeBatteryRemainingCapacity and clMeshNodeBatteryChargingState OIDs return "0" values because the back end is not invoking the API to get the values.

  Workaround: None.

- CSCsy03762—Local EAP-TLS authentication is failing on the SubCA issuer check.

  Workaround: Do not use SubCA to enroll certificates for the controller and the clients, or do not check the certificate authority (CA).

- CSCsy05945—The "EAPOL-key M2 with invalid RSN IE" error message appears because of multiple PMKIDs. The clients send multiple PMKIDs, but the controller buffers only 64 bytes of the WPA/RSN information element (IE).

  Workaround: None.

- CSCsy06464—A 1242 hybrid-REAP access point running 12.4(18a)JA sometimes obtains an IP address on the wrong interface, which causes the locally switched wireless clients to obtain an IP address from the wrong subnet.

  Workaround: Use static IP instead of DHCP.

- CSCsy24030—You should be able to configure the world mode information element (IE) using the controller GUI, CLI, or SNMP.

  Workaround: Use the following remote debug commands to enable or disable the world mode IE in controller software release 6.0 or later:

  debug ap enable *Cisco_AP*

  debug ap command "debug dot11 d1/d0 world-mode-ie enable/disable" *Cisco_AP*

  debug ap disable *Cisco_AP*

  Or enter this command on the access point CLI: "debug dot11 d1/d0 world-mode-ie enable/disable."

- CSCsy31678—When you use the controller CLI to enter a fingerprint SHA value for the CIDS sensor, the fingerprint value does not appear on the controller GUI.

  Workaround: None.

- CSCsy66246—A 1250 series access point does not downshift rates for retries when low latency MAC is enabled. It sends three retransmissions, but the data rate for the retransmissions is the same rate at which the initial packet was sent.

  Workaround: Do not enable low latency MAC.

- CSCsy71912—Clients are redirected to an invalid URL after web authentication when a proxy server is configured.

  Workaround: Manually configure a redirect URL after login for the web authentication settings. Clients are not directed to the incorrect URL based on the initial request but instead are directed to the configured URL on the controller.

- CSCsy76474—Clients are showing as active and in the run state on multiple controllers at the same time.

  Workaround: None.

- CSCsy77091—When a 1242 access point is serving as a root access point (RAP) and trying to use VLAN tagging and Ethernet bridging, wired client traffic is not passed on the bridged VLAN.

  Workaround: Use another access point model, such as an 1131 or 1522, for the RAP.
- CSCsy83568—The mobility state is missing from external DHCP debugs.

  Workaround: None.
- CSCsy99807—RLDP sometimes fails to detect that Linksys 802.11n access points are wired to the infrastructure.

  Workaround: None.
- CSCsy99905—Rogue Location Detection Protocol (RLDP) consistently finds wired threats only when you use it manually.

  Workaround: None.
- CSCsz14243—If you try to enable an 802.1X WLAN on a controller network module when an access point is in the process of joining, the WLAN fails to be enabled, and this error message appears in the system log: "Request failed - refer to log."

  Workaround: Try again to enable the WLAN a few seconds later.
- CSCsz15011—The auto smartport views an AIR-AP1231G-A-K9 access point as an LWAPP access point and thus applies the LWAPP macro to the interface.

  Workaround: None.
- CSCsz19203—A controller running software release 4.2.176.0 might reboot because of a software failure of the sshpmMainTask.

  Workaround: None.
- CSCsz19970—Clients sometimes fail to associate when an access point moves from the primary controller to a standby controller and different data rates are configured on the controllers.

  Workaround: Configure identical data rates on the primary and standby controllers.
- CSCsz27295—With Rogue Location Detection Protocol (RLDP) set to monitor mode access points only and auto containment turned off, containment packets are still transmitted by local mode access points.

  Workaround: None.
- CSCsz32424—A 2100 series controller is not able to detect an identified rogue on the wire despite seeing it on the wired infrastructure.

  Workaround: None.
- CSCsz34552—If the battery of a Cisco 7921 phone is removed during a call, the TSPEC inactivity timer is not activated when the inactivity timeout expires.

  Workaround: None.
- CSCsz35570—Clients on the management interface cannot access the controller's dynamic interface, even though it can reach other IP addresses in the dynamic subnet.

  Workaround: None.
- CSCsz36028—Client devices connected to a webauth WLAN are sometimes not redirected to a login page where the user can enter login credentials and join the network.

  Workaround: None.

- CSCsz42191—When a 1252 access point running Cisco IOS Release 12.4(10b)JDA is upgraded to LWAPP using WCS, it sometimes fails to send the unicast LWAPP DISCOVERY obtained using the DNS discovery method.

  Workaround: Use alternative methods such as DHCP option 43, over-the-air provisioning (OTAP), or static LWAPP configuration.

- CSCsz49863—Local EAP authentication periodically fails for 792x phones using EAP-FAST. However, the authentication succeeds after some retries.

  Workaround: None.

- CSCsz53516—CAPWAP access points with static IP addresses sometimes take four hours to fall back to DHCP when they fail to join a controller or contact the default gateway. However, if the access point is using DHCP, it re-attempts DHCP after 100 failed discovery attempts (which takes around an hour).

  Workaround: None.

- CSCsz53825—Controllers sometimes report medium power on 1250 series access points connected to 3560E switches even when power is statically assigned at 20w.

  Workaround: None.

- CSCsz57828—Some counters for 1140 series access points, such as multiple retry count, fail to increment in the output of the **show ap stats** command.

  Workaround: None.

- CSCsz58747—CAPWAP data packets that contain wireless-specific information in the CAPWAP header have an extra field for the wireless ID in Wireless specific information. The extra field does not affect functionality.

  Workaround: None.

- CSCsz58917—Controllers log radio reset messages for access points running RLDP.

  Workaround: None.

- CSCsz59699—Controllers sometimes report that an access point radio resets due to a command timeout:

  ```
  *May 11 22:16:56.716: %DOT11-2-RESET_RADIO: Restarting Radio interface Dot11Radio0 due
  to command 0x16 timeout @0x9ED63498
  ```

  Workaround: None.

- CSCsz62286—Access points in sniffer mode do not work when the controller cannot resolve the ARP for the default gateway of the management interface.

  Workaround: Configure the default gateway of the management interface as the physical HSRP gateway and not the virtual one.

  These exceptions sometimes appear in WCS logs for 5500 series controllers:

  ```
  5/12/09 11:50:39.46 ERROR[snmpmed] [41] Response VarBind missing for class
  LradIfDot11Counters attribute multicastReceivedFrameCount
  5/12/09 11:50:39.46 ERROR[snmpmed] [41] SNMP Operation Error: sparse table not
  supported for class  LradIfDot11Counters
  5/12/09 11:50:39.46 ERROR[stspoll] [41] 171.71.128.78 SnmpTableQuery failed for
  LradIfDot11Counters com.cisco.server.common.errors.SnmpOperationException:
  MEDIATION-1,Sparse table not supported,LradIfDot11Counters
  ```

  Workaround: None.

- CSCsz63461—When WLAN DHCP override is enabled the DHCP Server check is broken.

  Workaround: None.

- CSCsz66726—A read-only local management user can enable or disable a WLAN using the drop-down WLAN menu on the main WLAN page of the controller GUI.

  Workaround: None.

- CSCsz66769—The output for the show boot command makes it difficult to tell which image is active.

  Workaround: None.

- CSCsz67652—Controller logs sometimes fill up with this error message:

  ```
  DOT11-3-RADIO_INVALID_FREQ_FOR_CHAN: Frequency not found for channel 133 in domain 0
  ```

  Workaround: None.

- CSCsz68239—On 2006 controllers, output for the **show acl detail** command is not properly formatted.

  Workaround: None.

- CSCsz69928—After inter-subnet roaming, web_auth_reqd_state wireless clients & wired clients continue to receive multicast traffic.

  Workaround: None.

- CSCsz72416—Roaming client devices are sometimes assigned to the wrong VLAN when the ACS server is configured for AAA override.

  Workaround: None.

- CSCsz74673—When you configure a 2106 controller for internal DHCP and upload the configuration to a TFTP server, the internal_dhcp_address pool value changes in the uploaded config.

  Workaround: None.

- CSCsz74983—Controllers sometimes display a memory error (pmallocProcessMemoryCorruption) when restoring a backup configuration.

  Workaround: None.

- CSCsz78003—Access points with 5-GHz radios sometimes incorrectly reporting radar detection on channel 157.

  Workaround: None.

- CSCsz78168—Access points connected to the same controller on a WiSM module, in the same Mobility and RF group, are sometimes reported as rogues by the controller.

  Workaround: None.

- CSCsz79621—EAP-TLS authentication sometimes times out on the controller. The controller reports that client is not answering the EAP request, but sniffer traces show that the client did send an answer, and it arrived at the controller port.

  Workaround: Use a different client supplicant or a different authentication type.

- CSCsz80099—Controllers on the same mobility group sometimes indicate that the mobility data and control paths are down. The controllers can't ping each other but can ping other devices on the network. A wired packet capture shows the controller responding to ICMP echo packets, and other packets sent to the other controllers in the mobility group with a destination MAC address containing all zeroes.

  Workaround: Delete the mobility group entry from both controllers and then re-add them.
- CSCsz80918—Controllers fail to filter CAPWAP debug messages by MAC address.

  Workaround: None.
- CSCsz82533—The username and password configured on an access point are lost when you upgrade from a 4.x controller release to a 5.x or 6.x controller release.

  Workaround: None.
- CSCsz86043—When a mix of 1130 series access points and 1522 access points are connected to a controller, the controller sometimes incorrectly displays four radio interfaces on the 1130 access points.

  Workaround: None.
- CSCsz87564—Access points sometimes send linktest retries with identical timestamps.

  Workaround: None.
- CSCsz88122—4400 series controllers sometimes reboot and report the reason as "Reaper Reset at task sshpmM," but recover without intervention.

  Workaround: None.
- CSCsz89135—Controllers sometimes fail to increase power after finding failed clients and prealarms.

  Workaround: None.
- CSCsz89606—When an access points initially running a recovery image discovers a controller through DNS, joins the controller, downloads a configuration, and reboots, the access point DNS query within the local domain fails and the access point cannot discover the controller.

  Workaround: Use DHCP option 43/60 or OTAP.
- CSCsz89858—Web authentication fails on controllers when the controller does not answer the SSL client hello during the handshake.

  Workaround: Reboot the controller.
- CSCsz89866—Controllers sometimes fail to send a redirection message during webauth.

  Workaround: None.
- CSCsz94843—Multicast traffic sometimes fails across NPU on 4404 controllers.

  Workaround: None.
- CSCsz95406—When an 1140 access point is connected to a 3750E switch that is configured to provide inline power up to 20w, the controller that the access point joins sometimes reports that the access point is receiving low power, and WCS creates an alarm.

  Workaround: None.

- CSCsz95595—Some access point IOS commands (**copy**, for example) may be unavailable from the access point CLI when you use Telnet or SSH to connect to the access point.

  Workarounds:

  - Connect a console cable to the access point. At the ap# prompt, enter one of the following hidden commands:

    #debug lwapp console cli (4.2 [12.4(10b)J*] or earlier)

    #debug capwap console cli (5.0 [12.4(13d)JA] or above)

  - On the controller controller CLI, enter the following command:

    debug ap enable *APname*

  Then you can enter any IOS CLI command using the following syntax:

  > debug ap command *COMMAND APname*

- CSCsz99331—1522 Mesh access points sometimes fail at software task mvl_show_controller(0x4ddf80).

  Workaround: None.

- CSCta00518—Controllers sometimes fail to identify rogue access points when the rogue unit is operating on a channel outside the configured regulatory domain.

  Workaround: None.

- CSCta00537—Controllers allow you to change an access point from HREAP mode to local mode even when the access point is in an H-REAP group.

  Workaround: None.

Minor Caveats Open in Previous Releases

These caveats are open in controller software release 6.0.182.0 and in prior releases and have a severity of 4 or 5.

- CSCsd95723—Some users might be confused when presented with the **None** and **DHCP** options for configuring the service port interface in the initial controller setup wizard. These options are available for a controller that has no configuration and the setup wizard is being used to configure it.

  Workaround: Users can interpret the **None** option as Static and a logical alternative to DHCP.

- CSCsg32646—If link aggregation (LAG) is enabled on the controller and the port channel is configured on the infrastructure switch, the controller displays only a single entry for its neighbor when you enter the sh cdp neighbor CLI command. When you enter the same command on the switch, it displays two entries for the controller for two different ports that are part of LAG. The controller should display two entries when the command is entered on the controller because the switch sends the CDP message from two different ports that are part of the port channel.

  Workaround: None.

- CSCsi30541—Loss of connectivity to the management interface occurs when you add a new dynamic interface and the configured DHCP server on all other interfaces is in the new dynamic interface subnet and the new interface has a shorter mask than the other interfaces.

  Workaround: Configure a 10/24 interface or a different 10/16 subnet such that the new dynamic interface does not contain the DHCP server IP address currently defined on all interfaces.

- CSCsi54588—Some 802.1X error messages have inadequate descriptions or incorrect severity levels. For example, the following messages, which can be caused by an incorrectly configured client, have a severity level of 1 when they should have a severity level of 3. As a result, they are logged even when the logging level is set to Critical.
  - DOT1X-1-MAX_EAPOL_KEY_RETRANS_FOR_MOBILE
  - DOT1X-1-ABORT_AUTH

  Workaround: Make sure that clients are correctly configured to minimize error logging.
- CSCsi62915—Static IP wireless devices are not shown on the controller until they send a packet. The IP address information should appear on the MAC Filtering > Details page of the controller GUI and in the output of the **show run-config** CLI command.

  Workaround: To see static IP wireless devices in the controller's local MAC filter list, enter a CLI command similar to the following:

  config macfilter add 00:01:02:03:04:05 3 200 "test prt" 192.168.200.10
- CSCsi72324—A service port with IP address 0.0.0.0 responds to an ARP for the AP-manager interface.

  Workaround: Unplug the service port and reconfigure it on the correct subnet.
- CSCsi73129—When you attempt to upgrade the controller using an associated wireless client as the TFTP or FTP server, the upgrade fails.

  Workaround: Place the server on a client that is not associated to the controller.
- CSCsj06245—Portions of the output of the **show tech-support** CLI command might be formatted incorrectly, making the information difficult to read.

  Workaround: None.
- CSCsk01633—The MAC address is truncated in the following EAPOL key message: "VALIDATE_REPLAY_CTR_FAILED: Couldnt Validate the replay counter in packet. EAPOL Key message with invalid replay counter from mobile.Got:00 00 00 00 00 00 00 00.Expected:0000 00 00 00 00 0001.Mobile:00:a0:f8:ed:."

  Workaround: None.
- CSCsk60655—The default frequency value in the intrusion detection system (IDS) file should be equal to or greater than the maximum deauthentication packets sent by an access point.

  Workaround: None.
- CSCsk63047—Dynamic transmit power control (DTPC) does not work on Cisco 1240 series access points in WGB mode.

  Workaround: None.
- CSCsk73574—Directed roam frames might be sent with an incorrect BSSID list. The frames include only the base addresses when they should include all the VLANs on the destination access point.

  Workaround: None.
- CSCsl19319—If you create a local user profile on the GUI of a 2106 controller with the WLAN profile "any WLAN" and then edit the profile, the following error message appears: "Error in setting WLAN ID for user." However, your change is applied.

  Workaround: Delete the local user profile and create a new one with the updated password or description or define a WLAN profile for the user.

- CSCsl67177—The Catalyst Express 500 (CE500) might lose connectivity to a 4400 series controller when one port of the portchannel is shut down.

  Workaround: Unplug and then plug in both Etherchannel links on the CE500 or the controller. Plug in or unplug any device on the CE500.

- CSCsl70043—When a client device connects to a secure EAP WLAN and immediately switches to an open WLAN, the access point sends a status 12 association response (which is normal) but sends it from the wrong MAC address and BSSID.

  Workaround: On the controller CLI, enter **config network fast-ssid-change** to allow the client devices to connect without incident.

- CSCsl95615—When a master controller exists on the network, an access point that is joined to a secondary or tertiary controller keeps going back to discovery.

  Workaround: Disable the master controller mode.

- CSCsm25943—The meaning of the following error message on the controller is not clear. This message does not necessarily imply that any actual "ARP poisoning" is occurring. Rather, this message appears when a WLAN is configured for DHCP Required and a client (after associating to this WLAN) transmits an ARP message without first using DHCP. The client is unable to send or receive any data traffic until it performs DHCP through the controller.

  ```
  DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (op 1) received with
  invalid SPA 192.168.1.152/TPA 192.168.0.206
  ```

  Workaround: Follow these steps:

  a. Determine whether you want to force your wireless clients to perform DHCP first, after associating, before they can send IP packets.

  - If you do, then disable DHCP Required, and you will not encounter this problem.
  - If you do not, then configure all clients to use DHCP.

  b. If the client is configured for DHCP but sometimes still sends IP packets after associating without performing DHCP, then perform the following:

  - Verify that the client eventually does perform DHCP without undergoing an unacceptable outage. If the outage before performing DHCP is acceptable, then you can ignore this message.

  If the client never does perform DHCP after associating, then it can never pass Layer 3 traffic. In this case, either determine how to change the client's behavior so that it always performs DHCP after associating, or simply accept that this client does not work in this application or reconsider your decision to use DHCP Required.

- CSCsm40870—The following error message should be reworded:

  ```
  Jan 24 15:20:55.374 apf_80211.c:2552 APF-4-ASSOCREQ_PROC_FAILED: Failed to process an
  association request from00:13:ce:37:8b:ff. WLAN:2, SSID:TMDInternal-WPA. mobile in
  exclusion list or marked for deletion
  ```

  The message should read as follows:

  ```
  ASSOCREQ_PROC_FAILED: Failed to process an association request from 00:13:ce:37:8b:ff.
  WLAN:2, SSID:TMDInternal-WPA. Mobile excluded or marked for deletion.
  ```

  Workaround: None.

- CSCsm74060—The word “received” is misspelled in this log message:

  ```
  %APF-4-ASSOCREQ_PROC_FAILED: apf_80211.c:3121 Failed to process an association request
  from xx:xx:xx:xx:xx:xx. WLAN:Y, SSID:<SSID>. message received from disabled WLAN.
  ```

  Workaround: None.

- CSCso18251—When you log into the controller as a lobby ambassador and create a guest user with a lifetime of zero (infinite), the user information appears only on the controller CLI. It does not appear on the controller GUI.

  Workaround: Use the controller CLI to display users.

- CSCso35129—If the controller is queried by SNMP for a virtual gateway interface address, it may generate messages such as “sim.c:1061 SIM-3-MACADDR_GET_FAIL: Interface 1 source MAC address is not found.”

  Workaround: None.

- CSCso38808—When a CCXv5 client associates to a WLAN that has Aironet IE extensions enabled, the client information table contains no information.

  Workaround: None.

- CSCso69011—After **config paging disable** is entered to disable page scrolling, the **show interface summary** command still shows a “paging” prompt, which could break customer scripts.

  Workaround: None.

- CSCso69016—After **config paging disable** is entered to disable page scrolling, the **show traplog** command still shows a “paging” prompt, which could break customer scripts.

  Workaround: None.

- CSCsq09590—The client details on the controller GUI and CLI show a session timeout of 0 and a reauthentication timeout of infinite when you connect. However, after the client roams to another access point on the controller, the session timeout remains at 0, but the reauthentication timeout shows 1800 regardless of the timeout configured on the controller. This issue occurs when the controller is configured for WPA2+802.1X with no AAA override.

  Workaround: Use the **show pmk-cache** *mac_address* CLI command to see the timeout.

- CSCsq14833—When using VLSM, if the fourth octet of the management IP address is the same as the fourth octet of the broadcast address of another interface on the controller, the controller does not respond to access point discoveries.

  Workaround: Change the IP address of the management interface.

- CSCsq40265—The statistics of a second RADIUS server are never incremented and stay at 0 in the **show radius auth stats** command or display incorrect values. This behavior occurs when the first RADIUS server does not reply and the request falls back to the second RADIUS server.

  Workaround: None.

- CSCsq55045—The IAPP-3-MSGTAG015 and other controller IAPP messages are not documented or documented inadequately.

  Workaround: None. The CAPWAP packet message format is documented in the IETF draft.

- CSCsq65895—If a DHCP server is not configured on a WLAN or interface, the **config dhcp proxy enable** CLI command returns the following message, even if all WLANs do not require DHCP: “Some WLAN configurations are inconsistent with the new configuration of the DHCP Proxy. Please check the message log ('show msglog') for details.”

  Workaround: Configure a valid (or dummy) DHCP address on the WLAN or interface.

- CSCsq78560—You can configure port mirroring on 4400 series controllers although this feature is not supported on those controllers.

  Workaround: Do not use port mirroring on 4400 series controllers.

- CSCsq83810—STP commands should be removed from the controller GUI and CLI. They are no longer supported and might cause undesired effects when interacting with PSVT.

  Workaround: None.

- CSCsq88010—You cannot clear the controller crash logs even though controllers show crash log information from versions prior to the current release.

  Workaround: Reset the controller configuration and crash logs to default values.

- CSCsr57256—A 1520 access point joined to a 4400 series controller running software release 4.1.192.22M reports an 802.11a radio operational state of UP when the radio is disabled after resetting the access point.

  Workaround: None.

- CSCsr61016—When you disable the 802.11a radio in a 1520 series access point in root access point (RAP) mode, the radio continues to send beacons, and client devices remain associated to it.

  Workaround: Disable 802.11a client access to force clients to disassociate. However, the radio remains enabled.

- CSCsu37392—If you connect a 1250 series access point directly to a PC running Tftpd32 without a firewall and use a mode button reset, a timeout might occur during a TFTP transfer.

  Workaround: Configure the TFTP server for a timeout of 45 seconds.

- CSCsu61354—When you attempt to set MAC filters on the controller from WCS, an error message appears indicating that the MAC address cannot be set because it already exists in the database. The error message should indicate that the MAC address is already associated by Auth-list.

  Workaround: Enter **config auth-list delete** *mac_address* and **config macfilter** *mac_address* using the controller CLI. Then enter **show mac-filter** to see the newly created MAC address.

- CSCsu84629—When 1250 series access points receive neighbor discovery packets (NDPs), they sometimes switch from maximum uniform transmit power to maximum transmit power.

  Workaround: None.

- CSCsu88885—When **debug locp interface events** is enabled, the **debug disable** command does not disable the debug.

  Workaround: Use the **debug dot11 locp disable** command.

- CSCsu89905—The following error message might appear on a controller running software release 4.2.130.0 during boot-up:

  ```
  dtl_cfg.c:714 DTL-3-CALLBACK_PROC_FAILED: Callback for command:26 failed for user
  port: 0/0/x
  ```

  Workaround: None.

- CSCsu90052—The following error message might appear on 4400 series controllers: “sim_config.c:194 SIM-3-INTFGET_GIG_ETH_FAIL: Failed to get the Interface number of the Gigabit Ethernet Port.”

  Workaround: Clear the configuration and reconfigure the controller.

- CSCsu90074—The following error message might appear on the controller at boot-up: “sim.c:272 SIM-3-INVALID_PORT: Using invalid port number. Port out of range. Port # 0.”

  Workaround: None.

- CSCsu90097—The following error message might appear on the controller: “spam.c:449 LWAPP-2-SEM_CREATE_ERR: Could not create semaphore for notifying AP registration.”

  Workaround: None.

- CSCsu90112—The following error message appears on the controller at boot-up, even though symmetric mobility tunneling is disabled: “dtl_ds.c:428 DTL-3-DSNET_CONF_FAILED: Unable to set symmetric mobility tunneling to enabled on Distribution Service interface.”

  Workaround: Clear the controller configuration and reconfigure the controller.

- CSCsv18730—Controllers sometimes unicast an ARP check to the default gateway every 5 to 7 seconds rather than using the configured ARP timeout interval.

  Workaround: None.

- CSCsv35162—One of the following messages appears when you try to designate a local controller as an anchor controller: “Request failed - Failed to add the IP into anchor list” (on the CLI) or “Failed to create anchor switch entry local” (on the GUI).

  Workaround: None. Mobility functionality is not broken.

- CSCsv63732—Controllers sometimes display an error message in which the word “heartbeat” is misspelled.

  Workaround: None.

- CSCsv79885—If you initially enter an incorrect mobility group name, the Edit All feature does not save the new mobility group name.

  Workaround: Delete the mobility member and re-enter it with the correct name.

- CSCsv87385—The controller logs this message when the DHCP packet received on the interface does not contain any DHCP options: “dhcpd.c:206 DHCP-3-MSGTAG095: Bad DHCP packet from *DHCP Server*, dropping.”

  Workaround: None.

- CSCsw52367—The controller CLI command **debug client** *mac_address* incorrectly shows the following error message when shared authentication is not enabled or shared authentication is failing: “*Dec 05 11:12:52.550: 00:1f:5b:c2:07:a4 Suspected Auto-Immune attack: Not Sending Assoc Response to station on BSSID 00:21:d8:93:cb:00 (status 13).” The message should be changed to reflect the actual problem.

  Workaround: None.

- CSCsw53035—When a controller running software release 4.2.176.0 (with hybrid-REAP local switching and hybrid-REAP VLAN mode enabled) sends a ping reply to a wireless client, the destination MAC address is the client MAC address. As a result, the Layer 3 switch cannot transfer the ping reply packet.

  Workaround: None.

- CSCsw62968—A CAPWAP access point logs the following error at bootup after the fastethernet0 gets an IP address from the DHCP server: “Not sending discovery request AP does not have an IP!!”

  Workaround: Ignore the message because the access point has an IP address.

- CSCsw79978—On the SNMP Trap Controls (Security) page on the controller GUI, the WEP Decrypt Error check box should be reworded because this setting also controls the SNMP decrypt error traps for WPA and WPA2. With the current wording, it is not clear whether this setting also disables the WPA decrypt traps.

  Workaround: None.

- CSCsw88545—The output of the **show client detail** *mac_address* CLI command is inconsistent for an EAP-FAST CCKM client. Sometimes the username is reported as “anonymous,” and sometimes it shows the actual username configured on the device. If local authentication is used on the controller, the username is reported as “PEAP-*mac_address*.”

  Workaround: None.

- CSCsw88727—When an unauthenticated wireless client changes IP addresses on a WLAN that has web authentication enabled, the controller sends level 1 syslog messages (immediate action required) to the syslog server. Here is a typical message:

  ```
  apf_foreignap.c:1285 Changing orphan packet IP address for station 00:23:32:xx:xx:xx
  from 192.168.X.Y --->192.168.X.Y
  ```

  Workaround: Change the open WLAN to WPA-PSK to prevent casual clients from trying a different IP address before obtaining an IP address on the open guest WLAN.

- CSCsw91395—“Trusted AP Missing or Failed” messages appear in the controller log even after you disable trusted access point alerts.

  Workaround: None.

- CSCsx05502—A guest-access anchor controller stops forwarding traffic to the wired clients.

  Workaround: Reset the PC card on the client.

- CSCsx09827—In controller software release 4.2.176.0, the **config ap** *?* CLI command does not list the possible subcommands in alphabetic order.

  Workaround: None.

- CSCsx18164—Undocumented “%DOT1X-4-INVALID_MSG_TYPE” messages appear when a client adapter experiences an EAP identity failure.

  Workaround: None.

- CSCsx21251—When a client successfully obtains a DHCP IP address with web authentication enabled on the WLAN and sends an orphan packet before authenticating, the controller marks the packet as an orphan and then sends out this erroneous debug message:

  ```
  Invalid MSCB state: ipAddr=X.Y.Z.A, regType=2, Dhcp required!
  ```

  Workaround: Ignore the erroneous debug message.

- CSCsx50408—The LWAPP DOS attack trap message always reports the source MAC address as all zeroes.

  Workaround: None.

- CSCsx53685—The default power type and mode are always displayed even when the access point is powered by Power over Ethernet (PoE).

  Workaround: None.

- CSCsx59100—When you enable SNMPv3 and create a user, it is not clear that you need to reboot the controller in order for your changes to take effect.

  Workaround: Reboot the controller.

- CSCsx65088—A Cisco WiSM running software release 5.2.157.0 causes “%WiSM-5-STATE: Oper-up” messages to appear in the supervisor logs.

  Workaround: None.

- CSCsx70458—The following message might appear on a controller running software release 5.2:

  ```
  Feb 11 11:30:48 <apname> 979: <mac>: *Feb 11 10:33:46.245: %LWAPP-3-CLIENTERRORLOG:
  Decode Msg: could not match WLAN ID 2
  ```

  This message is usually cosmetic. However, it should mention “CAPWAP” rather than “LWAPP,” should not appear because the WLAN override feature was removed in software releases 5.2 and later, and should not appear if your access point is broadcasting all SSIDs.

  Workaround: None.

- CSCsy00920—When you use the controller CLI to disable certain data rates, the controller returns “Invalid parameter specified” if the command to disable a given rate is for a rate that was previously disabled. This message is not particularly meaningful. A better message would be “Specified rate previously disabled.”

  Workaround: None.

- CSCsy03115—A Cisco WiSM controller might reboot because of a software failure at capwapAcStatemachine+2996 with time cb at ('dtlSendTimeoutMsg+76').

  Workaround: None.

- CSCsy04745—When you enable CAPWAP error debugs, this unclear message sometimes appears: “Invalid AP event (1) and state (8) combination.”

  Workaround: None.

- CSCsy18685—When access points are all assigned to the default-group access point group, clients cannot connect to all SSIDs.

  Workaround: Delete the WLANs on the controller. Then use the WCS WLAN template to recreate WLANs and repopulate the default-group. If you do not have WCS, manually recreate the WLANs on the controller.

- CSCsy19477—When a guest user logs in or out using web authentication, incorrect messages appear in the message and trap logs.

  Workaround: None.

- CSCsy20322—If a problem occurs when you upload or download a file to the controller, the “File transfer failed” error message appears, even if the file transfer is not the problem.

  Workaround: Use the **debug transfer all** command to view more information.

- CSCsy23776—If you issue the **config passwd-cleartext** {**enable** | **disable**} command to show or hide passwords and it fails, you might continue to be prompted for a password.

  Workaround: Issue the command again and make sure to enter **enable** or **disable**.

- CSCsy26457—On the controller GUI, the Base Radio MAC column for the list of access points in an access point group is labeled incorrectly. The column actually shows the Ethernet MAC address.

  Workaround: Use the **show wlan apgroups** CLI command to see the correct column name.

- CSCsy27532—“EAP-Identifier” is misspelled in AAA debug outputs.

  Workaround: None.

- CSCsy32145—Currently HTTP and HTTPS configurations on the controller are performed at a global level. You should be able to configure them on a non-global level. For example, you might want to manage the controller with HTTPS but want the web authentication login page to be HTTP.

  Workaround: None.

- CSCsy62007—Controllers sometimes drop the DHCP inform packet when a client device is in DHCP required state.

  Workaround: Use the **config dhcp proxy disabled** command to disable DHCP proxy on the controller.

- CSCsy74281—The **show interface detail** *interface_name* command for a guest LAN interface does not show the VLAN ID.

  Workaround: Use the controller GUI to see the VLAN ID for the guest LAN interface.

- CSCsy79744—The web authentication internal page shows a blue rectangle in the upper right-hand corner.

  Workaround: None. This is a cosmetic issue.

- CSCsy88149—When a client running IE6, IE7, or Firefox connects to the guest WLAN using web authentication, it receives the following error: “There is a problem with the website’s security certificate.” If the user chooses to continue, web authentication works, and the user is allowed access.

  Workaround: Do not use a wildcard * parameter in the hostname of the certificate (for example, use wifi.longueuil.ca instead of *.longueuil.ca).

- CSCsy98796—The controller web authentication Login Success page does not show the logical DNS name for the virtual interface when configured.

  Workaround: Use the raw IP address link provided by the success page for the logout.html call if needed.

- CSCsz03162—When a controller is configured to allow only 802.11g traffic, 802.11b client devices are able to successfully associate to an access point but cannot pass traffic.

  Workaround: When you configure the controller for 802.11g traffic only, disable any channels (such as channel 14 in Japan) that allow associations from 802.11b client devices.

- CSCsz09498—When a client device triggers the auto-immune code on a controller, it can be difficult to determine exactly how the client violated the auto-immune rules.

  Workaround: None.

- CSCsz25704—The VLAN and IP values are sometimes swapped in DHCP-4-INVALID_VLANID_ARP system messages.

  Workaround: None.

- CSCsz33810—The following error message might randomly fill the controller logs, preventing the clients from fully associating.

  ```
  Apr 23 16:30:15 10.10.10.10 WLC2: *Apr 23 16:29:48.576: APF-3-CHECK_SUPP_RATES_FAILED:
  apf_utils.c:268 Could not check supported rates. Missing Supported Rate. Length :0.
  Mobile MAC: xx:xx:xx:xx:xx:xx
  Apr 23 16:30:15 10.10.10.10 WLC2: *Apr 23 16:29:48.576: %APF-1-CONFLICT_IN_ASS_REQ:
  apf_80211.c:3664 Conflicting Supported Rates in Association Request fromxx:xx:xx:xx:xx
  Apr 23 16:30:15
  *tracebacks follow*
  Apr 23 16:30:17 10.10.10.10 WLC2: *Apr 23 16:29:48.926:
  %APF-4-REGISTER_IPADD_ON_MSCB_FAILED: apf_foreignap.c:1278 Could not Register IP Add
  on MSCB. MSCB still in init state. Address:xx:xx:xx:xx:xx:xx
  ```

  Workaround: Reconnect the client.

- CSCsz50249—Access points in local mode, connected to a controller running release 4.2.130.0 or later, sometimes sends 802.11g extended supported rates information elements, regardless of the supported rates on the client. The access point sends the information element only when 802.11g is enabled on the network. However, H-REAP access points never send 802.11g extended supported rates information elements; to be consistent with access point in local mode, they should.

  Workaround: None.

- CSCsz62198—Third-party certificates for web authentication are installed but sometimes indicate that they are locally generated.

  Workaround: None.

Resolved Caveats

These caveats are resolved in controller software release 6.0.182.0.

- CSCsd48349—Web authentication does not work when a clustered firewall is used as the client's default gateway.
- CSCse92557—Wireless clients, in various topologies, might be unable to send or receive large TCP segments.
- CSCsf98944—The AP-manager interface for 4400 series controllers does not respond to ICMP pings.
- CSCsi51966—The Clients > Detail page on the controller GUI does not show applied access control lists (ACLs).
- CSCsj25953—When 200 or more wireless clients try to associate to a controller at the same time, the clients become stuck in the DHCP_REQD state. Use this CLI command to limit the rate at which access point radios send association and authentication requests to the controller:

  config advanced assoc-limit {**enable** | **disable**} *associations_per_interval interval*

  The valid range for *associations_per_interval* is 1 to 100, and the valid range for *interval* is 100 to 10000 milliseconds. The default value is disabled.

- CSCsl79260—Wired guest LAN clients do not get an IP address if DHCP proxy is disabled.
- CSCsm19182—When an 802.11n radio is operating on channels 52 through 140, the channel width is configured for 40 MHz, and a radar event is detected, it is possible for the radio interface to become disabled instead of moving to another channel. This problem occurs when the access point is operating in the vicinity of radar operations or under extreme traffic conditions (when a false radar detection might occur).
- CSCsm25127—When you use the controller CLI in controller software release 4.2.61.0 to add a custom logo to the internal web authentication page, a light green border appears above and to the right of the logo.
- CSCsm32845—The Guest LAN parameter on the Interfaces > Edit page of the controller GUI might cause confusion for users because the guest LAN is used for interfaces involved in wired guest LANs, not for wireless guest WLANs.
- CSCsm50322—If you try to configure additional local net users when the database has reached the maximum number of entries, the controller does not show a valid message stating that the database has been exceeded.
- CSCso06740—When more than one controller belongs to an RF group, pressing the **Invoke Channel Update Once** button updates only the channels for the RF group leader but not the channels for the other RF group members.

- CSCso33491—The controller should report when it is experiencing high memory utilization.
- CSCso50723—When you use the controller's local RADIUS server for EAP-FAST authentications, authentication might fail if your client already has a protected access credentials (PAC) for the controller to which you are authenticating.
- CSCso59528—When you try to change the access VLAN to any VLAN that exists on the controller (either access VLAN or quarantine VLAN) from the GUI, the following error message appears: "Port number is incompatible with VLAN configuration." Similarly, when you try to change the quarantine VLAN to any VLAN that exists on the controller (either access VLAN or quarantine VLAN), the following error message appears: "Error setting vlan." These error messages should be more explanatory.
- CSCsq02092—The 1100 and 1200 series access points and 1310 series bridges fail to download image code from a 4400 series controller running software release 4.2. The following error message is logged:

```
Refusing image download to AP xx:xx:xx:xx:xx: - unable to open image file
/bsn/ap//c1yyy
xx:xx:xx:xx:xx:xx is the MAC address of the AP and c1yyy is the AP model number
```

- CSCsq13174—In controller software releases prior to 5.1.151.0, web authentication certificates can be only a device certificate and should not contain the certificate authority (CA) roots chained to the device certificate (no chained certificates). Starting with controller software release 5.1.151.0, the controller allows the device certificate to be downloaded as a chained certificate (up to a level of two).
- CSCsq23594—If you send a CCXv5 request to a workgroup bridge (WGB) or client, the following emergency level log message is generated:

```
May 13 00:22:45.795 timerlib_mempool.c:215 OSAPI-0-INVALID_TIMER_HANDLE: Task is using
invalid timer handle 836008400/272443620
- Traceback:  10786fc8 103da5d4 106d9c10 103d9b28 103d9da0 103d43cc 10b9585c 10d4ef2c
-Process: Name:osapiBsnTimer, Id:11d94ba8
```

- CSCsq23806—Guest tunneling does not work if the WLAN on the foreign controller is created by the controller GUI and the WLAN on the anchor controller is created by WCS.
- CSCsq25029—A 2106 controller running software release 4.2.112.0 might reboot because of a software failure of the bcastReceiveTask.
- CSCsq25762—Users cannot reduce the EAPOL-key timeout value. If a client does not send the EAP response, the access point should be able to retransmit faster than the default 1 second for voice clients.
- CSCsq30980—When you upgrade a 4400 series controller to software release 5.1, no more than 48 access points are able to join if link aggregation (LAG) is disabled. The controller enters this state when all the ports on the controller are administratively disabled and the configuration is saved before the controller is reset.
- CSCsq41190—In WLAN Layer 2 security for static WEP or 802.1X dynamic WEP, an error message appears when you choose a WEP key size of 128 bit, which is actually a 152 (128 + 24 IV) bit key. Few clients can operate with a 152-bit WEP key, and the only access points that can use 128 bit are no longer supported in controller software release 5.0 or later.
- CSCsq61533—The controller GUI and CLI do not allow a blank access point username, but SNMP can be used to enter a blank value.
- CSCsq76307—An 1130 series access point becomes stuck in image download after joining the controller.

- CSCsr16752—The Controller Network Module NM-AIR-WLC6 might experience interface flapping after the interface is reset.
- CSCsr40109—When a client roams from an access point joined to one controller to an access point joined to another controller, the client might experience a lack of data connectivity for a period equal to the configured user idle timeout. This problem occurs only if the mobility members are updated through the controller GUI using the Edit All button.
- CSCsr45163—When IPv6 clients move from an access point group or VLAN to a new access point group or VLAN, they lose connectivity because all traffic is forwarded to the old VLAN.
- CSCsr46256—If a Cisco Compatible Extensions v5 client associates and authenticates to a 1242 access point with management frame protection (MFP) enabled and then establishes a prioritized voice call, the client cannot perform a CCKM fast roam.
- CSCsl48639—An IP address can be configured on a dynamic interface on a controller when that IP address has already been assigned to another device on the network.
- CSCsr55450—In an environment with both LWAPP and CAPWAP controllers, the access points always join the CAPWAP controller, regardless of the controller type for which the access points are primed.
- CSCsr58034—Rogue rules and friendly access points are not being uploaded and downloaded properly.
- CSCsr60506—The controller might unexpectedly reboot at spamReceiveTask with a signal 11 error (segmentation fault).
- CSCsr70862—A Cisco WiSM controller running software release 4.2.130.0 might reboot because of a software failure of the instruction located at 0x1038a140(ewsInternalAbort+348).
- CSCsr75350—When a 1230 series access point joins a 4404 controller, the 2.4-GHz channel on which the access point is operating differs between the controller and the access point.
- CSCsr83684—When you enable link aggregation (LAG), the source MAC address for dynamic interfaces might change during operation.
- CSCsr89399—Cisco 1131AG access points that are connected to Cisco WiSM controllers might reboot unexpectedly.
- CSCsr89694—Cisco WiSM controllers running software release 4.2.130.0 generate trap logs indicating that the control path between two random mobility members is down. About 10 to 20 minutes later, the control path comes back up.
- CSCsr95295—The controller CLI allows you to disable all legacy data rates and with the network still enabled. This is an invalid configuration that disables the network.
- CSCsr97110—After you download an XML configuration file, a 4400 series controller running software release 5.1.151.0 might reboot continuously.
- CSCsu04447—If you enable TACACS+, you cannot classify rogue access points using the controller GUI.
- CSCsu05190—The AP-manager interface does not reply with the correct destination MAC address with GARP. As a result, access points cannot join the controller after a failover from the primary firewall to the secondary firewall.
- CSCsu22727—After WCS pushes an access point template to the controller, the controller might reboot.
- CSCsu26961—Using WCS or the controller CLI, you can configure the controller for WPA+WPA2 with 802.1X/CCKM and PSK. To see whether 802.1X/CCKM is configured at the same time with PSK, run the **show wlan 1** or **show run-config** command and look at the output.

- CSCsu39716—When an access point in workgroup bridge mode associates in a NAC-enabled WLAN, it should receive an IP address from the interface that is mapped in the access point group. Instead, the workgroup bridge receives an IP address from the interface to which the WLAN is mapped.
- CSCsu40636—The access point sometimes ignores the CTS duration when receiving U-APSD trigger frames and simply transmits.
- CSCsu42414—The controller CLI command **show client ccx rm** *mac_address* **pathloss** does not report correct information.
- CSCsu42445—WCS shows an audit mismatch and weird values in the syslog configuration when a clean controller is added to it.
- CSCsu50080—When you configure web authentication passthrough with email input on the controller, the controller allows any text to be entered. This feature implies that a client should have to enter an email address before proceeding. Although there is no way to verify that the email is valid, the controller should at least verify that it follows this format: name@company.com.
- CSCsu52812—When the controller is in multicast-unicast mode, it sends unicast traffic to an access point before that access point has fully joined the controller. This problem can be serious when the access point is running a recovery image such as 12.3(11)JX1, which does not drop LWAPP data packets. If the number of data packets sent to the access point before it loads the full image is large enough, the access point locks up and fails to join the controller.
- CSCsu52837—Pre-authenticated clients cannot reach web-authenticated clients on the same WLAN.
- CSCsu53020—When a CCXv5 client is associated to a controller with open authentication, the controller reboots if you navigate to the Clients > Detail page on the controller GUI.
- CSCsr53764—Some wired workgroup bridge (WGB) clients might randomly become stuck at specific access points while roaming.
- CSCsr91186—When you open a Telnet or SSH session to an access point running controller software release 5.1, the following CLI commands cannot be executed: **configure terminal**, **telnet**, **connect**, **ssh**, **rsh**, **ping**, **traceroute**, **clear**, **clock**, **crypto**, **delete**, **fsck**, **lwapp**, **mkdir**, **radius**, **release**, **reload**, **rename**, **renew**, **rmdir**, **save**, **set**, **test**, **upgrade**.
- CSCsu56269—A Cisco WiSM might reboot because of a software failure of the radiusTransportThread task.
- CSCsu57111—The following tracebacks might appear in the controller message logs: “apf_foreignap.c:1292 APF-1-CHANGE_ORPHAN_PKT_IP: Changing orphan packet IP address for station00:11:22:33:44:55 from x.x.x.x --->y.y.y.y- Traceback: 100cd4c0 100cddd0 100e40a8 10409864 10c064cc 10d748d8.”
- CSCsu62060—The 4400 series controller might reboot because of a software failure of the tplusTransportThread task.
- CSCsu69321—In controller software release 5.2.157.0, if you download a configuration with WPA + 802.1X and PSK security, no XML dependency errors appear.
- CSCsu71747—On a Catalyst 3750G Wireless LAN Controller Switch running software release 5.1.151.0, the integer value returned by the SNMP object ifNumber is 2, but IfIndex actually returns three indexes.
- CSCsu72077—Debug commands sometimes become disabled on the controller several minutes after you enable them.

- CSCsu74008—On a Catalyst 3750G Wireless LAN Controller Switch running software release 5.1.151.0, the results of ipRouteIfIndex for some routes point to an interface with index 5. However, the results of IfIndex show only three interfaces with their corresponding indexes.
- CSCsu75686—When you configure the DHCP Addr. Assignment option on a WLAN using the controller GUI, the controller CLI shows incorrect output in the **show running-config** command.

  When you use the controller GUI to enable the DHCP Server Override option and configure a DHCP address, and you do not enable the DHCP Addr. Assignment option, the **show running-config** command shows:

  ```
  wlan dhcp_server <wlan ID> x.x.x.x required
  ```

  The correct output should be:

  ```
  wlan dhcp_server <wlan ID> x.x.x.x
  ```

  When you use the controller GUI to enable the DHCP Server Override option, configure a DHCP address, and enable the DHCP Addr. Assignment option, the **show running-config** command shows:

  ```
  wlan dhcp_server <wlan ID> x.x.x.x required required
  ```

  The correct output should be:

  ```
  wlan dhcp_server <wlan ID> x.x.x.x required
  ```

- CSCsu84220—When a WAN outage occurs, the 1131AG and 1242AG access points joined to a controller running software release 4.2.130.0 come back online, but the radios remain in the “down” state, and the following message appears: “Unable to verify sufficient in-line power.”
- CSCsu84498—The 1240 series access point transmit diversity for multicast and broadcast packets does not alternate on antenna ports. It should alternate on consecutive packets (from A to B and so on).
- CSCsu86033—The controller might reboot a few minutes after approximately 100 access points join the controller with a local significant certificate (LSC).
- CSCsu87249—When you use the controller as the local authenticator for PEAP, you cannot successfully authenticate a user account using the domain-username format.
- CSCsu88956—System messages with tracebacks sometimes appear in the message logs of Cisco WiSM controllers when you edit and save a WLAN with only the 802.11a radio enabled.
- CSCsu90335—Intel 4965 cards might experience connectivity problems when another client connects to the same 1250 series access point in hybrid-REAP mode on a controller running software release 4.2.130.0. The loss of connectivity can last up to 1 minute.
- CSCsu92667—The controller might reboot after you make changes to the configuration.
- CSCsu96326—When you save the controller’s map on WCS, all of the 1520 series access points that are joined to the controller suddenly disconnect.
- CSCsu96916—When you issue the **show run-config** CLI command using SSH on a 4400 series controller running software release 4.2.130.0 with paging disabled, the output locks up at a certain point, probably because the controller runs out of buffers.
- CSCsv00108—The controller might report an invalid message integrity check (MIC) on beacon frames.
- CSCsv00342—When you clear the Back-up Primary Controller and Back-up Secondary Controller parameters on the Global Configuration page and click **Apply**, the controller does not clear the parameters.

- CSCsv01484—The controller prepends UID usernames with “CN=,” which can cause problems for LDAP authenticated binds. The controller should check for usernames with “UID” but not prepend them with “CN=.”
- CSCsv01840—During long-duration, dual-radio throughput to 802.11n clients, 1140 series access points sometimes show CAPWAP errors on the console. Traffic might be briefly interrupted but resumes at the same best rate.
- CSCsv01844—When you filter clients using the controller GUI, the controller repeats the last two characters of the filter text, and the filter does not work.
- CSCsv02613—The RxFragmentCount in the output of the **show ap stats** command shows an incorrect value. This issue seems to occur for 1100 and 1200 series access points and 1310 series bridges.
- CSCsv13068—An access request from the controller to the RADIUS server has the Authenticator field set to all zeros.
- CSCsv14863—When access points that have been converted to lightweight mode join a 4.2.130.0 controller with a channel of 0 and a power level of 0, the controller does not send the correct RF settings to the access point.
- CSCsv19291—When you are configuring the controller, WCS reports in alarms that the access point interface is down. WCS does not sufficiently indicate that these alarms are meant to inform users of access point radio status and are caused by the user during configuration.
- CSCsv21872—When a client associates to a WPA WLAN and does not have the correct security parameters (for example, the client is configured with the correct SSID but with static WEP instead of WPA-PSK or 802.1X), the controller generates this error message:

  ```
  %APF-1-PROC_RSN_WARP_IE_FAILED: apf_80211.c:2197 Could not process the RSN and WARP
  IEs. station not using RSN (WPA2) on WLAN requiring RSN.MobileStation:
  00:40:96:a1:4a:f6, SSID:RSN,AP: 00:1c:f9:05:92:80.
  ```

  The SSID: RSN incorrectly implies that WPA2 is being used when it is not.
- CSCsv23643—When you configure a WLAN with WPA2+802.1X and an infinite session timeout, any client that connects to a 5.1.151.0 controller actually has a session timeout of approximately 11.6 hours.
- CSCsv32280—Large bursts of data (usually greater than 6000 bytes) that are sourced from a wired node on the Ethernet and originating at 1Gbps might not be transmitted successfully downstream to a wireless client.
- CSCsv34136—When an RFC3576 message arrives, the controller enforces a source port check by searching for the server using the IP address and source port in the RFC3576 message rather than searching the configured RADIUS servers list using the same Find Server function as for any other RADIUS message.
- CSCsv34354—The access control list (ACL) name is set to None when you change the session timeout for the WLAN using SNMP.
- CSCsv34605—An access point using the Rogue Location Detection Protocol (RLDP) does not obtain a DHCP address if the DHCP server is on an autonomous access point. As a result, RLDP does not detect if a rogue access point is on the wire.
- CSCsv39950—Controllers running software release 4.2.130.0 sometimes reboot at apfMsCreateDeadlock+76 while configured for **debug pm ssh-engine enable**.
- CSCsv40946—When clients use WPA-PSK, the controller might not include the framed IP address attribute in every RADIUS accounting message sent to the RADIUS server.

- CSCsv41197—A new client can associate to a hybrid-REAP access point in standalone mode even though MAC filtering is enabled.
- CSCsv43156—The trap for an unsuccessful SSH login attempt sometimes shows the wrong IP address.
- CSCsv49302—If the SSID interface is different from the management interface, the SSID interface changes to the management interface after the diagnostic channel is disabled.
- CSCsv52889—The controller reboots because of a Reaper Reset error in the SNMPTask if a configuration file with a web authentication bundle is restored onto a controller without the bundle.
- CSCsv56016—When a 2106 controller running software release 5.1.151.0 logs messages to the syslog server, the following error appears: "Invalid IP address, x.x.x.255, x.x.x.0, 127.x.x.x or Class D/E is not permitted."
- CSCsv60932—If you use the GUI to set the RADIUS fallback mode to Active or Passive on a 2106 controller, the default value for the Interval parameter does not fall inside the allowable range.
- CSCsv62368—A CPU access control list (ACL) sometimes fails to block ICMP packets.
- CSCsv64590—After a reboot of the controller, SNMPv3 stops working. The controller running SNMPv3 shows as unreachable in WCS once the controller has been rebooted.
- CSCsv69899—The controller might reboot because of a software failure of the spamReceiveTask, dtlArpTask, or pemReceiveTask.
- CSCsv70260—When a Cisco WiSM running software release 5.1.151.0 has TCLAS enabled and uses wireless phones that support TCLAS, the controller might experience up to a 20% downstream packet loss.
- CSCsv70556—When you create a new dynamic interface, assign a VLAN tag, and then apply the interface settings on the controller GUI, a message appears indicating that no netmask or IP address was added; however, the interface is created.
- CSCsv73455—If you specify a value for the foreign 802.11a/b interference threshold percentage parameter on the controller, the uploaded configuration has a value that is 655 times the value that you entered. This value is incorrect and invalid because the percentage can be a maximum of 100.
- CSCsv74342—Clients associated to a WLAN with the diagnostic channel enabled cannot reach the 2106 controller default gateway management interface.
- CSCsv74572—In a non-link aggregation (non-LAG) setup with both ports plugged into a switch and the switch sending gratuitous ARPs on port 2 for the gateway when the dynamic interface is on port 1, the controller loses gateway access on a single VLAN, and off-subnet hosts (such as DHCP servers) cannot be reached for DHCP.
- CSCsv76635—When a controller running software release 4.2.130.0 generates either of the following traps, it sends an incorrect OID to the configured trap receiver: "All mobility anchors on wlan index 1 are down" or "Mobility anchoring is restored on wlan index 1." As a result, the configured trap receiver does not receive the proper trap message, and you are not notified that the anchor controller went down.
- CSCsv77075—HTTPS does not work on 4400 series controllers after you upgrade from software release 4.1.185.0.
- CSCsv77658—A 1250 or 1520 series access point reboots because the watchdog timer expired.
- CSCsv78027—When too many access points are close together, the controller might detect some of the access points as rogue and generate Honeypot traps against them. Normally, the controller generates a Honeypot trap alarm if a rogue access point is using WLANs that are configured on the controller.

- CSCsv79582—Controllers sometimes reboot because of a software failure of the SShpmMainTask task.
- CSCsv83452—A 4400 series controller with link aggregation (LAG) disabled might reboot when a large number of access points attempt to join.
- CSCsv84446—If you enter the **debug aaa all enable** CLI command during web authentication, the “Authentication failed for user” message appears even though the user was able to authenticate and pass traffic.
- CSCsv87375—The radios in an 1140 series access point might reset when operating in an environment with mixed clients and heavy traffic.
- CSCsv91377—If you use the following CLI command to download a configuration, the controller returns to factory default settings:

```
config country US,USX,CA,MX,FI,ES,EG,CO,CR,GB,HK,CH,IN,FR,IL,ILO,AU33333333333
```

- CSCsv91992—The controller does not remove DHCP option 82 in DHCP traffic from the server to the client.
- CSCsv94146—A 4400 series controller might reboot when using external web authentication.
- CSCsv94993—When you enable DHCP Required on a WLAN, passive wired clients behind a workgroup bridge (WGB) might lose their connection to the wireless network.
- CSCsv97224—If you configure a customized web authentication login window and then disable custom web authentication, the client continues to be prompted with customized pages.
- CSCsv98164—On the Priority Order > Management User page of the controller GUI, the authentication columns are not labeled, so it is difficult to tell if you are adding or removing a particular authentication type.
- CSCsv99579—Telnet or SSH settings configured through a controller running software release 5.2.157.0 are not saved across access point reboots.
- CSCsw14316—The RADIUS accounting and RADIUS authentication server key format should return a default value other than ASCII or HEX.
- CSCsw15327—When you configure rogue access point containment from WCS, the command appears to be accepted and processed. However, the controller does not contain the rogue access point because it is no longer available. WCS shows that the rogue access point is contained, but later the status returns to “Alert” without generating an error message.
- CSCsw17025—Controller software release 5.2 or later allows access point group VLANs to be mapped to the virtual interface.
- CSCsw19963—An SNMP trap message stating that the controller is out of sync with the central timebase appears when the controller reboots.
- CSCsw23723—On the controller, you should be able to format CALLING_STATION_ID and CALLED_STATION_ID with different characters (including no delimiter) for both RADIUS authentication and accounting messages.
- CSCsw25388—When you change the antenna gain setting on a 1520 series mesh access point, the access point reloads, which might cause downstream mesh access points to go out of service.
- CSCsw27841—A controller running software release 5.1.151.0 or 5.2.157.0 allows you to configure multiple untagged VLAN interfaces on the same physical port.
- CSCsw29731—A controller running software release 5.2.157.0 should (but does not) drop multicast traffic if the client has the same group address as the access point multicast group.

- CSCsw29804—Lexmark printers that are used with 4400 series controllers running software release 4.2.130.0 or 4.2.176.0 cannot have apple ARP entries on a Layer 3 router and cannot join the Appletalk zone.
- CSCsw30025—When you enter **show custom-web wlan** on the controller CLI, the controller sometimes reboots.
- CSCsw34627—When you enter the **show dhcp lease** CLI command on a controller running software release 5.2.157.0, the hours and minutes are omitted in the output.
- CSCsw38078—An anchor controller running software release 5.2.157.0 might reboot when DHCP leases are viewed from the controller GUI.
- CSCsw39752—When wireless multimedia (WMM) is enabled, some clients are not able to re-authenticate to the access point because they do not reset their sequence numbers. Roaming is affected for such clients.
- CSCsw40474—If you create a WLAN with WPA security using the controller GUI and then change the session timeout value using WCS, the security setting changes to WPA2.
- CSCsw40946—The controller might act as an ARP proxy for a locally switched hybrid-REAP client, which might cause problems with the MAC forwarding table of some switches and prevent client traffic from passing properly. This problem occurs only when all devices are on the same subnet and connected to a single switch.
- CSCsw41668—The Cisco WiSM might reboot and display the following error message on the console: "** LOCK ASSERT ** (pemReceiveTask) !! prio=332 root=400 word=1000."
- CSCsw44119—Mesh access points should consider Ethernet adjacency only once after a reboot. When a mesh access point loses its parent and does not have any potential parents in the neighbor list, it starts a new scan and tries to join through the Ethernet, which hampers the ability of an access point with Ethernet clients to re-converge quickly.
- CSCsw46354—The following traceback might appear in the controller message log:

```
Dec 12 08:48:16.957 apf_80211.c:3942 APF-1-SEND_ASSOC_RESP_FAILED: Could not send a
Client Association response to XX:XX:XX:XX:XX:XX. Suspected Auto-Immune attack Not
sending Assoc Response.
 - Traceback:  1051b51c 1051f7a0 100eaedc 100eb0a4 103e582c 10bb1168 10d6baac
```

- CSCsw49530—When the inline power configuration on the controller does not match the physical configuration of the access points, WCS problems (such as template apply failures and poor client tracking) can occur.
- CSCsw49636—A Cisco WiSM might reboot because of a software failure of the Reaper Watcher.
- CSCsw50747—The controller GUI should show the emergency/boot image on the controller.
- CSCsw51658—A Cisco WISM with factory default settings does not acquire an IP address during auto configuration. The behavior occurs only when the Catalyst 6500 switch is running Cisco IOS Release 12.2(33)SXI.
- CSCsw68564—The OID in the CISCO-LWAPP-MOBILITY-MIB needs to be changed from 9999 to 576.
- CSCsw68975—If you create an access point group and apply it to an access point, snmp-walk or snmp-get for the cLReapApVlanId MIB shows incorrect WLAN indexes after the access point reboots.

- CSCsw70888—A hybrid-REAP access point might reboot with an unexpected exception error when clients attempt to associate or reassociate to the access point:

  ```
  05:00:14 UTC Mon Dec 22 2008: Unexpected exception to CPUvector 1100, PC = 0x5CF75C  , 
  LR = 0x5CD148
  -Traceback= 0x5CF75C 0x5CD148 0x5CD200 0x1A28D0
  ```

  This error can be caused by clients switching from one band (such as 802.11a) to another band (such as 802.11b/g) on the same access point or by clients attempting to change from one security mode (such as WPA1/TKIP) to a different security mode (such as WPA2/AES) on the same access point.
- CSCsw71172—The controller might reboot when the local authenticator is in use.
- CSCsw73514—The backup controller configuration file does not properly reflect security and radio settings. All WLAN security settings are lost and reset to None. When you disable 802.11g rates, this change is not reflected in the uploaded configuration file. When the file is downloaded, the 802.11g rates are enabled and no security settings are enabled on the WLANs.
- CSCsw80042—An 1140 series access point might not join the controller. CAPWAP debugs on the controller show these messages:

  ```
  *Apr 03 14:03:53.077: xx:xx:xx:xx:xx:xx AP not registering with BASE MAC.
  *Apr 03 14:03:53.077: Failed to parse CAPWAP packet from ip-addr:port
  *Apr 03 14:03:53.077: Failed to process packet from ip-addr:port
  ```

- CSCsw80153—When a RADIUS server is used for web authentication, a controller running software release 5.1.151.0 might not send any RADIUS requests to the server. This problem pertains only to a specific configuration.
- CSCsw83779—Symbol scanners (MC9090) fail to connect to a local EAP WLAN after an extended time. When this issue occurs, all clients are unable to successfully authenticate to the WLAN. Client IDs for the WLAN are created and deleted with authentication sessions, but not all IDs are deleted with failed authentications for Symbol scanners.
- CSCsw84860—When you enter the **show 802.11b l2roam stat** CLI command in a Telnet or SSH session, the command output is improperly aligned and difficult to read.
- CSCsw85672—When you attempt to change the hybrid-REAP VLAN mapping through the controller GUI, the change appears to be made, but the VLAN tag reverts back to its original setting.
- CSCsw86749—When you upgrade a 4400 series controller to software release 5.1.151.0, irrelevant error messages like this one sometimes appear:

  ```
  Jan 06 08:35:08.785:%USMDB-4-MSGTAG027: usmdb_wcp.c:221 usmDbWcpGetParentRouterName(): 
  Non-WiSM platform.
  ```

- CSCsw87206—The service port interface must have an IP address on a different subnet from the management, AP-manager, and dynamic interfaces. The controller checks whether the IP address assigned to each interface is valid before the IP address setting is configured. However, this checking mechanism does not work when you change the subnet mask of each interface. As a result, the controller sometimes allows the service port interface to have an IP address on the same subnet as the other interface.
- CSCsw88108—When you add a MAC address to the access point authentication list using SNMP, the controller allows uppercase characters. However, the controller should reject or convert addresses with uppercase letters as it cannot handle mixed case in the database.
- CSCsw90266—For 2100 series controllers and controller network modules, clients associated to a WLAN pointing to a dynamic interface can access the HTTPS, Telnet, and SSH services of the management IP address, regardless of the state of the Management over Wireless setting.

- CSCsw91505—Log messages from mesh access points show the reason for disassociations and reboots but do not provide timestamps.
- CSCsw92335—If you use WCS to set the session timeout for a WLAN with 802.1X, WPA, or WPA2 security, the timeout is not set on the controller.
- CSCsw93865—The CLI help for the **config mesh battery-state** command shows only the **disable** option even though the **enable** option is also available.
- CSCsw97549—If a CCXv5 client with a trusted profile is associated to the controller, browsing to the client page in WCS causes the controller to reboot.
- CSCsx04986—WCS might receive reports from the controller that a rogue access point is on the network, even though a rogue access point is not actually on the network.
- CSCsx07340—The **show mesh env** controller CLI command sometimes shows incorrect Fahrenheit temperature values for 1520 series access points.
- CSCsx07538—When a TCP connection is open to port 1000, the controller responds with a reset.
- CSCsx07878—Clients might be unable to log into a WLAN configured for web authentication.
- CSCsx14840—The management interface source MAC address might change during operation.
- CSCsx19599—A controller running software release 5.2.170.0 might reboot because of a software failure of the spamReceiveTask.
- CSCsx20559—Point-to-Point Tunneling Protocol (PPTP) connections might fail to be established through a wireless connection with a 2106 controller running software release 5.2.
- CSCsx23643—When you back up the controller configuration using TFTP, some of the working configurations are changed.
- CSCsx27773—A 5500 series controller might hang after a Reaper Reset of the osapiBsnTimer task.
- CSCsx29643—802.11n access points might experience frequent channel changes, which can cause a disruption in service.
- CSCsx29956—A 4400 series controller reboots when it is configured to operate with an LDAP server because of a software failure of the LDAP DB Task 2 task.
- CSCsx39460—Configuration uploads from a 2100 series controller or controller network module do not include the **config network multicast mode** command.
- CSCsx39726—One of the controllers in a Cisco WiSM that is running software release 5.1.151.0 might reboot at sshpmMainTask (signal 11).
- CSCsx41861—An 1140 series access point might occasionally reboot for no apparent reason. If trace data is available, it might contain some indication of "PCI reset port *n*," where *n* is 0 or 1.
- CSCsx44137—A 4400 series controller might reboot when attempting to download a message log using FTP.
- CSCsx48164—The controller has insufficient debugs to troubleshoot web authentication while under a heavy load.
- CSCsx49921—The controller might receive CAPWAP Datagram Transport Layer Security (DTLS) packets out of sequence.
- CSCsx52830—A 1250 series access point radio might stop providing client access. The radio seems to lose client connectivity, and a reboot of the access point brings the clients back up.
- CSCsx53336—The management interface of a 2100 series controller running software release 5.2.157.0 cannot be accessed by a wired client in the same subnet as a dynamic interface on the controller.

- CSCsx57919—If any Layer 2 security is enabled on a WLAN with web authentication enabled, the controller does not send RADIUS packets to the external RADIUS server.
- CSCsx59156—Clients are unable to authenticate when a WLAN template using a PSK is pushed to the controller using WCS.
- CSCsx60137—The following error message might appear after wireless clients authenticate to an 1142 OfficeExtend access point and start sending multicast traffic: "sec_process_pkt: pd error, status=48."
- CSCsx60343—If you remove a WLAN from an access point group, the group does not display the WLAN; however, all of the access points still broadcast the SSID. Rebooting the access points resolves the issue.
- CSCsx67192—When the MTU path is set between 996 and 1494, the CAPWAP packets are dropped because they fail to be fragmented by the CAPWAP module.
- CSCsx69069—Cisco 1522 access points running software release 4.1.192.35M or 6.0 report incorrect dates for their neighbor update information.
- CSCsx69535—The controller sends a join reply to the wrong MAC address when the primary port on the switch is down, causing the access points on different subnets to lose connection with the controller.
- CSCsx70919—When you back up the configuration of a controller running software release 5.2.157.0, link aggregation (LAG) shows as disabled in the backed up configuration file even though LAG is enabled on the controller.
- CSCsx74467—For controllers running software release 4.2, 5.2, or 6.0, certain client conditions might cause "auto-immune" messages to appear (for example, "*mac_address* Suspected Auto-Immune attack: Not Sending Assoc Response to station on BSSID 00:11:22:33:44:50 (status 1) statusCode=0)." In software releases where this problem is fixed, enter this CLI command to disable the auto-immune feature: **config wps auto-immune disable**.
- CSCsx74494—The controller GUI does not show the status of mobility members.
- CSCsx78872—When an EAP session is closing, a 5500 series controller might crash because of a software failure of the PEAP or EAP-TLS task.
- CSCsx80743—If you configure link aggregation (LAG) more than once without rebooting the controller, you lose connectivity into the controller, though it is still pingable.
- CSCsx83406—The **config rogue ap rldp initiate** CLI command does not work when the controller tries to associate to a rogue access point using the 802.11a radio of a monitor mode access point. This behavior occurs because the channel on the monitor mode access point is not set to the rogue access point channel.
- CSCsx97002—When you upgrade the controller from software release 4.2.176.0 to 5.2.178.0, the controller fails to load the configuration and generates a large number of access control list (ACL) configuration errors in XML validation, and the controller keeps rebooting.
- CSCsx98249—A WLAN tied to an access point group VLAN sends client DHCP requests using the DHCP server IP address configured under the WLAN instead of using the server IP address configured under the interface that is tied to the access point group.
- CSCsx99923—After you upgrade a 2100 series controller to software release 5.2, the output of the **show stats port** command shows an FCS error. All discarded packets appear in the FCS error count, including BPDU packets.
- CSCsy05623—When you enter the **debug aaa tacacs enable** and **config ap logging syslog level alerts** CLI commands on a controller running software release 5.2, incorrect information is reported for TACACS+ accounting.

- CSCsy06689—The controller might reboot because of an out-of-memory situation, and memory-related messages appear in the crash file or message log of the controller.
- CSCsy13739—Hybrid-REAP access points might disconnect during the DTLS tunnel with a certificate validation error, but the controller shows them as connected with all zeroes in the Time Joined field.
- CSCsy13791—Cisco 1142 access points send out spurious error messages on initial bootup.
- CSCsy16331—The controller network module reboots when the Rogue Access Point Rule Group template is pushed from WCS.
- CSCsy17668—Cisco 1231 access point radios do not respond to the **cmd 1 (0,0,0) core dump** command.
- CSCsy18634—The controller might reboot because of a software failure of the apfOpenDtlSocket task.
- CSCsy20914—When 802.11 client association and disassociation traps are enabled, the controller sends multiple client association traps to WCS for the same client with the same timestamp, which causes WCS performance and processing issues.
- CSCsy23704—During heavy traffic conditions, 1242 and 1252 access points in hybrid-REAP, monitor, or wIPS mode might become stuck in the configuration, image, or join state.
- CSCsy24245—WLAN access point group configuration is missing from the output of the **show run-config** CLI command.
- CSCsy27502—Clients do not get DHCP IP addresses because of the following mobility message from the **debug mobility handoff enable** command: "Mon Mar 9 11:08:03 2009: xx:xx:xx:xx:xx:xx Mobility Response: IP 0.0.0.0 code 1, reason 5, PEM State DHCP_REQD, Role Unassociated(0)."
- CSCsy38629—A 5500 series controller with multiple TACACS+ servers configured might reboot when using remote debug commands and if one of the TACACS+ servers goes offline.
- CSCsy40717—A controller running software release 5.2 produces the following traceback when the service port IP address is changed:

```
*Mar 13 12:05:02.386: %SIM-6-MACADDR_GET_FAIL: sim.c:1165 Interface 255 source MAC
address is not found. Using the system MAC FF:FF:FF:00:00:01 instead.
-Traceback:  104e8570 104f10f8 10579a64 108bd698 107a8cc0 10485134 1047a034 10476cc4
1046940c 10491d64 104be944 10e42470 11033dec
```

- CSCsy48084—Cisco 1220 and 1250 series access points with a single radio in the D1 slot (5 GHz) are unable to join a controller running software release 5.2.
- CSCsy50654—A controller running software release 4.2.176.0 might experience a slow memory leak over a period of 60 days.
- CSCsy57573—A controller running software release 5.2.178.0 might reboot because of a software failure of the spamReceiveTask.
- CSCsy65347—When you configure the QoS profile for a WLAN, the downstream traffic is not restricted to the values configured for the per-user bandwidth contracts.
- CSCsy65401—A controller running software release 5.2 does not retain the customized web authentication settings configured for WLAN Layer 3 security across a reboot.
- CSCsy65598—A controller running software release 5.2.178.0 might experience a decrease in free system memory (of less than 15 MB) when a 1000 series access point tries to join.
- CSCsy76154—When link aggregation (LAG) is not enabled, packets might be sent on the wrong controller port using the wrong port MAC address, which can cause the packets to be lost.

- CSCsy84311—A controller running software release 5.2.178.0 might reboot because of a software failure of the emWeb task.
- CSCsy88329—An 1140, 1240, or 1310 series access point does not download code from a CAPWAP controller. CAPWAP debugs on the access point show a "Bad Record MAC Alert."
- CSCsy96340—An 1140 series access point drops clients and stops transmitting beacons although the beacon count on the interface keeps incrementing.
- CSCsy96551—A 1250 series access point with a channel width setting of 40 MHz shows the following error message when you set the Tx power level: "Error in setting TxPowerlevel configuration."
- CSCsy97077—The **show run-config** controller CLI command is truncated or incomplete.
- CSCsy98716—The following CLI command is not available in controller software release 5.2 or later: **config ap ethernet duplex** {**auto** | **half** | **full**} **speed** {**auto** | **10** | **100** | **1000**} {**all** | *Cisco_AP*}.
- CSCsz03239—This message might appear in the message log for a 4400 series controller running software release 5.2: "%RRM-3-RRM_LOGMSG: rrmLrad.c:2462 RRM LOG: RRM Verify Coverage Hole returned L7_FAILURE."
- CSCsz15249—When packets arrive out of sequence at the controller, a CAPWAP access point fails to join the controller.
- CSCsz15341—The AP Mode drop-down box on the All APs > Details for page of the controller GUI contains a Bridge option for 1142 and 1250 series access points even though bridge mode is not supported on these access points.
- CSCsz19675—A controller might reboot because LDAP authentication is enabled.
- CSCsz20036—CPU access control list (ACL) configurations are modified during configuration backups.
- CSCsz22520—You cannot disable the DHCP Required option on a WLAN without removing the DHCP override configuration.
- CSCsz43260—When you enable the access point latency report feature on the controller, the access point reports the wrong latency value to the controller.
- CSCsz43544—When more than 50 mobility group members are added using the controller GUI, the following error message appears: "The list cannot exceed 50 addresses," even though up to 72 members are supposed to be supported.
- CSCsz79080—When a WLAN template with Layer 3 web authentication policies is applied to the controller, the following message appears: "SNMP operation to Device failed: attempt to set conflicting attribute value."

If You Need More Information

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, refer to the Cisco TAC website at

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.

Documentation Updates

This section lists updates to user documentation that has not yet been added to either printed or online documents.

Omissions

The Package Contents section in the *Quick Start Guide: Cisco 4400 Series Wireless LAN Controllers* should be updated to include this item, which is included with the 4400 series controller:

- DB-9-to-DB-9 null modem cable

Related Documentation

For additional information on the Cisco controllers and lightweight access points, refer to 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 Control System Configuration Guide*

Click this link to browse to the Cisco Support and Documentation page:

http://www.cisco.com/cisco/web/support/index.html

Obtaining Documentation, Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html