Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.0.116.0

First Published: April 14, 2011
OL-19342-05

These release notes describe open and resolved caveats for release 7.0.116.0 for Cisco 2100, 2500, 4400, 5500, and Cisco Flex 7500 Series Wireless LAN Controllers; Cisco Wireless Services Modules (WiSMs), Cisco Wireless Services Module (WiSM2); Cisco Wireless LAN Controller Network Modules; Catalyst 3750G Integrated Wireless LAN Controller Switches; Cisco 3201 Wireless Mobile Interface Cards (WMICs); Cisco Aironet 1100, 1130, 1200, 1230AG, 1240, 1250, 1522, 1524, 1550, AP3500, AP1260, AP 1040, AP801, and AP 802 Series Lightweight Access Points; Cisco OEAP 600 Series 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 referred to as *controllers*, and all of the Cisco lightweight access points are referred to as *access points*.

Contents

These release notes contain the following sections.

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

Cisco Unified Wireless Network Solution Components

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

- Software release 7.0.116.0 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 7.0.172.0
- Cisco WCS Navigator 1.6.172.0
- Mobility services engine software release 7.0.201.0 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, 3310 Mobility Services Engines
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 2500 Series Wireless Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 5500 Series Wireless LAN Controllers
- Cisco Flex 7500 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 7.0.116.0 release does not support the NM-AIR-WLC6 platform. The NME-AIR-WLC platform is supported.

- Catalyst 3750G Wireless LAN Controller Switches
- Cisco 3201 Wireless Mobile Interface Card (WMIC)
- Cisco Aironet 1130AG, 1240AG, AP 1550, 1522, and 1524 Mesh Access Points

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

- Cisco Aironet 1100, 1130, 1200, 1230AG, 1240, 1250, AP1260, AP3500, AP 1040, OEAP 600 Series Access Points, 1522, 1524, 1550, 3500p, AP801, and AP802 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 AP802 is an integrated access point on the Next Generation Cisco 880 Series Integrated Services Routers (ISRs).

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).

Note The 1250 series access points 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.

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 (7.0.116.0, 7.0.98.0, 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 7.0.116.0.

Note See the *Cisco Wireless LAN Controller Configuration Guide, Release 7.0*, for more details and configuration instructions.

wIPS ELM

wIPS now includes the ability to visualize, analyze, and proactively prevent attacks on customer networks and equipment. The objective of the ELM (Enhanced Local Mode) is the ability to detect on-channel attacks while simultaneously providing client access and services. The feature offers full 802.11, nonstandard channel and nonWi-Fi threat detection. It uses an extensive threat library and supports forensics and reporting. Pre-processing at the access points minimizes the data backhaul because it works over very low bandwidth links.

In this release, the regular local mode or H-REAP mode access point has been extended with a subset of Wireless Intrusion Prevention System (wIPS) capabilities. This feature enables you to deploy your access points to provide protection without needing a separate overlay network.

Local mode or H-REAP mode access points with a subset of wIPS capabilities is referred to as Enhanced Local Mode AP or just ELM AP. You can configure an access point to work in wIPS mode if the access point is in any of the following modes:

- Monitor
- Local
- Hybrid REAP

Note wIPS ELM is not supported on 1130 and 1240 access points.

This feature has limited capability of detecting off-channel alarms. The access point periodically goes off-channel, and monitors the non-serving channels for a short duration, and triggers alarms if any attack is detected on the channel. But the off-channel alarm detection is best effort and it takes longer time to detect attacks and trigger alarms, which might cause the ELM AP intermittently detect an alarm and clear it because it is not visible.

Voice Diagnostics

The 7.0.116.0 release introduces a test debug command that details the call flow between a pair of client MACs involved in an active call. This command enables customers and partners to troubleshoot any voice problems to determine the next steps.

Rogue Containment and RLDP Enhancements

This feature significantly improves on rogue containment effectiveness and bandwidth usage. For Monitor mode access points, rogue clients and adhoc clients are contained using unicast deauthentication and disassociation frames exchanged between an access point and a wireless client. which reduces bandwidth usage, because the containment frames are sent only on active rogue clients. On Local or HREAP mode access points, the containment policy remains the same as previous release.

The auto-containment level is made programmable and you can choose to use only monitor mode access points for auto-containment. RLDP is supported on hybrid-REAP access points (central switching), which enables rogue detection on wire.

Calibration Enhancements

This feature offers an improved response time when collecting data during calibration. The S60 or the Enhanced Location Measurements-based calibration scheme creates a Path Loss Model (PLM) based on S60 measurements to provide better location accuracy for S60 devices.

Hybrid REAP: Local Authentication

The hybrid REAP local authentication feature places the authentication capability directly at the access point level in a hybrid REAP deployment (when in local switching mode), instead of the wireless controller. When a client associates with a hybrid REAP access point, the access point authenticates the client locally and switches the data packets locally.

One of the requirements when using hybrid REAP is that the roundtrip latency must not exceed 300 milliseconds for data and 100 milliseconds for voice and data between the access point and the controller, and CAPWAP control packets must be prioritized over all other traffic. To remove the requirement the round trip latency on the network connection, local authentication of hybrid REAP is used.

Hybrid REAP Fault Tolerance

Starting in release 7.0.116.0 and later releases, the controller software release has added a more robust fault tolerance methodology to hybrid REAP access points. In previous releases, whenever a hybrid REAP access point disassociates from a controller, it moves to the standalone mode. The clients that are centrally switched are disassociated. However, the hybrid REAP access point continues to serve locally switched clients. When the hybrid REAP access point rejoins the controller (or a standby controller), all clients are disconnected and authenticated again. In the controller software 7.0.116.0 release and later releases, this functionality has been enhanced and the connection between the clients and the hybrid REAP access points are maintained intact and the clients experience seamless connectivity.

Hybrid REAP OKC Feature

Starting in 7.0.116.0 release, Hybrid-REAP Groups enable Optimistic Key Caching (OKC) to enable fast roaming of clients. OKC facilitates fast roaming by using PMK Caching in access points that are in the same Hybrid- REAP group.

This feature prevents the need to perform a full authentication as the client roams from one access point to another. Whenever a client roams from one hybrid-REAP access point to another, the hybrid-REAP group access point calculates the PMKID using the cached PMK.

Note The Hybrid-REAP access point must be in connected mode when the PMK is derived during WPA2/802.1x authentication.

CDP Over Air

The feature enables you to configure Cisco Discovery Protocol (CDP) on an Ethernet or radio interface of the access point. By default, CDP is disabled on the radios on nonmesh access points. It is enabled by default on mesh access points.

Preferred Call Support

The Preferred Call feature enables you to specify the highest priority to SIP calls made to some specific numbers. The high priority is achieved by allocating bandwidth to such preferred SIP Calls even when there is no available voice bandwidth in the configured voice pool. This feature is supported only for those clients that use SIP-based CAC for bandwidth allocation in WCS or WLC.

DHCP Option 60

This feature enables service providers to differentiate their access points from others[1] on the network by appending the string *-ServiceProvider* to the Vendor Class Identifier during a DHCP request.

PCI Compliance for Neighbor Packets

The Cisco Neighbor Discovery Protocol (NDP) is the fundamental tool for RRM and other wireless applications that provide information about the neighbor radio information. Starting in release 7.0.116.0 and later releases, you can configure the controller to encrypt neighbor discovery packets.

This feature enables you to be compliant with PCI.

In order to have backward compatibility, a command-line interface (CLI) is added to allow the reception and transmission of the legacy NDP that is disabled by default.

RF Grouping

This feature provides wireless controller enhancements to Radio Resource Management (RRM). An RF grouping algorithm provides optimal channel allocation and power settings for access points in a network. This feature enables you to configure RF group leaders based on two criteria:

- Static leader: You can select an RF group leader rather than have the leader chosen automatically by the grouping algorithm.
- Type-based leader: Type-based leadership is a configuration where the controller with a lower version should not be allowed to be made a leader for higher version controller.

You can statically select a controller as RF group leader with the best physical capabilities and the most recent software load. Load balancing between group leaders when you have different coverage areas allows the controllers to communicate effectively.

Additionally, when access points see each other, they are aware of the controllers they are associated with, which enables you to make predictable decisions.

This enhancement minimizes the limitations of the current approach to RF group management and reporting tools for predictability of RF group forming.

Chile Regulatory Enhancements

Starting in the 7.0.116.0 release, the controller software has obtained regulatory approval for Chile.

Russia Regulatory Enhancements

Starting the in 7.0.116.0 release, the controller software has obtained regulatory approval for Russia.

Licensing Changes for 5500 Series Controllers

The Cisco 5500 Series Controller is now available with two license options. One allows data DTLS without any license requirements and another image requires a license to use data DTLS. The images for the DTLS and licensed DTLS images are as follows:

- Licensed DTLS—AS_5500_LDPE_x_x_x_x.aes
- Non licensed DTLS—AS_5500_x_x_x_x.aes

Cisco 2500, WiSM2, WLC2—These platforms by default do not contain DTLS. To turn on data DTLS, a license needs to be installed. That is, these platforms have a single image with data DTLS turned off. To use data DTLS you must have a license.

If your controller does not have a data DTLS license and if the access point associated with the controller has DTLS enabled, the data path will be unencrypted.

Non-Cisco WGB Support

Starting in release 7.0.116.0, the controller software has been updated to accommodate non-Cisco workgroup bridges so that the controller can forward ARP, DHCP, and data traffic to and from the wired clients behind workgroup bridges. This processes is accomplished by enabling the passive client feature. To configure your controller to work with non-Cisco workgroup bridges, you must enable the passive clients feature. All traffic from the wired clients is routed through the work group bridge to the access point.

Note The Non-Cisco WGB feature is supported only on the 5508, 2500 and 2100 Controllers. NPU based platforms (4400/wism/3750w) do not support this feature.

Cisco Identity Services Engine Support

Cisco Identity Services Engine (ISE) is a comprehensive next-generation, context-based access control solution that provides the functions of Cisco Secure Access Control System (ACS) and Cisco Network Admission Control (NAC) portfolios in one integrated platform.

ISE has been introduced in the 7.0.116.0 release of the Cisco Unified Wireless Network. ISE can be used to provide advanced security for your deployed network. It is an authentication server that you can configure on your controller. This first release of the next-generation Network Admission Control (NAC) product delivers base network access policy services across wired, wireless, and VPN environments as well as additional services like device administration, profiling, guest, posture, TrustSec, and Advanced Monitoring and Troubleshooting.

This feature offers security enhancements using ISE, the next-generation, single platform for 802.1X. As a result, you can take advantage of wired/wireless AAA services, profiling, guest, posture and more. The release adds ISE and controller integration for simplified URL-Redirect, Access Control List (ACL), VLAN override, and CoA-Reauth. You can flexibly apply policies in your network based on device profiling.

PSB Enhancements

This feature enhancement forces validation requirements that will be enforced on the new password. The rules reject weak passwords and force better passwords in general to improve baseline security.

DHCP Option 82 Support for Ethernet MAC ID

Starting in the 7.0.116.0 release, DHCP option 82 is added to the controller-based WLAN system. An access point can forward all DHCP requests that are incoming from a client to the controller. The controller adds the DHCP option 82 payload with the contents and then forwards it to the DHCP server. As per the RFC requirement, the DHCP packets that already have a relay agent option in them are dropped at the controller.

This feature enables validation of the location from where a request came in, making it easier to identify the specific access point from which the request comes. This feature helps to do the following:

- Simplify tracking radio MAC
- Limit security concerns when an attacker requests available IP addresses with a fabricated client MAC address.
- Prevent spoofing of client identifier fields used to assign IP addresses
- Prevent denial of service by spoofing other client's MAC addresses

VLAN Select and Related Features

Integration of the VLAN Select feature in the 7.0.116.0 release enables a WLAN to be mapped to multiple interfaces using an interface group. Wireless clients associating to this WLAN will get an IP address from a pool of subnets identified by the interfaces in round-robin fashion.

This feature extends the current access point group and AAA override architecture where access point groups and AAA override can override the interface group WLAN that the interface is mapped to, with multiple interfaces using interface groups.

This feature also provides the solution to guest anchor restrictions where a wireless guest user at a foreign location can get an IP address from multiple subnets on the foreign locations/foreign controllers from the same anchor controller.

VLAN Select L2 and L3 Multicast Optimization

With the introduction of the VLAN select feature, there is a possibility of increasing the number of duplicate packets over the air, which creates as many multicast packets as there are VLANs in the pool and clients may receive multiple copies of the multicast packets. To suppress the duplication of a multicast stream on the wireless medium and between the controller and access points, the multicast VLAN method is introduced. A multicast VLAN is used for multicast traffic. One of the VLANs of the WLAN is configured as a multicast VLAN on which multicast groups are registered. Configuring the multicast VLAN for the WLAN is controlled by the user. Clients can listen to a multicast stream on the multicast VLAN.

When using Layer 2 multicast/broadcast, Layer 2 MGID is used to forward packets to the access point. The Layer 2 Multicast Broadcast from all the VLANs in the group are sent on WLAN, which causes duplication packets on AIR. To limit these the duplication, Layer 2 multicast or broadcast is now a configurable option per interface.

Dynamic Anchoring Support for Static IP Clients

At times, you may want to configure static IP addresses for wireless clients. When these wireless clients move about in a network, they could try associating with other controllers. If the clients try to associate with a controller that does not support the same subnet as the static IP, the clients fail to connect to the network. Administrators can now enable dynamic tunneling of clients with static IP addresses. Using this feature, clients with static IP addresses can be associated with other controllers where the client's subnet is supported by tunneling the traffic to another controller in the same mobility group. This feature enables you to configure your WLAN so that the network is serviced even though the clients use static IP addresses.

Fast Controller Failover

This feature enables customers to configure retransmission count and retry intervals when access points try to reconnect with a controller. When a controller goes out of service, the access point associated to it will fall back to the next available controller. Before associating itself to a new controller, the access point first tries to establish a connection with the existing controller that it is associated to. It does so by sending a retransmission request at regular intervals to the controller and for a specified number of times. If the access point does not get an acknowledgement from the controller, it tries to associate itself to the next available controller. You can configure the retransmission intervals and retry count for an access point.

Webauth Proxy

This feature enables clients that have manual web proxy enabled in the browser to facilitate authentication with the controller. If the user's browser is configured with manual proxy settings with a configured port number as 8080 or 3128 and if the client requests any URL, the controller responds with a web page prompting the user to change the Internet proxy settings to automatically detect the proxy settings. This process prevents the browser's manual proxy settings from getting lost. After configuring this feature, the user can get access to the network through the web authentication policy. This functionality is provided for port 8080 and 3128 because these are the most commonly used ports for web proxy server.

Client Limits Per WLAN

You can set a limit to the number of clients that can connect to a WLAN, which is useful in scenarios where you have a limited number of clients that can connect to a controller. For example, consider a scenario where the controller can serve up to 256 clients on a WLAN and these clients can be shared between enterprise users (employees) and guest users. You can set a limit on the number of guest clients that can access a given WLAN. The number of clients that you can configure per WLAN depends on the platform that you are using.

FIPS Support

Cisco Controller Release 7.0.116.0 has been awarded Federal Information Processing Standard (FIPS) 140-2 validation. The following Cisco Wireless LAN Controllers and access points have received FIPS 140-2 Level 2 validation: Cisco 5508 WLAN Controller, Cisco Wireless Integrated Services Module (WiSM), Cisco 4400 Series WLAN Controllers, Cisco 3750G WLAN Controller. Cisco Aironet Lightweight Access Points: 3502i, 3502e, 1262, 1142, 1252, 1524, 1522, 1131, and 1242. The NIST Security Policies and FIPS certificates for these modules can be downloaded at the NIST web site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm.

Software Release Information

The 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, you should consider upgrading.

Note The Cisco WiSM requires software release SWISMK9-32 or later releases. 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.

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 7.0.116.0

Before upgrading your controller to software release 7.0.116.0, 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 7.0.116.0, 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 that 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 7.0.116.0 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 7.0.116.0 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 7.0.116.0. Table 1 shows the upgrade path that you must follow before downloading software release 7.0.116.0.
- The AP-count evaluation licenses for the 7.0 and the 6.0 releases are different. If you downgrade from a 7.0 release to a 6.0 release, you must activate the AP-count evaluation license of the 6.0 release after you downgrade. Similarly, if you upgrade from a 6.0 release to a 7.0 release, you must activate the AP-count evaluation license of the 7.0 release after you upgrade. If you do not activate the AP-count license, then the AP-count is shown as 0.
- Before you use an AP802 series lightweight access point with controller software release 7.0.116.0, you must upgrade the software in the Next Generation Cisco 880 Series Integrated Services Routers (ISRs) to Cisco IOS 151-4.M or later releases.

Table 1 Upgrade Path to Controller Software Release 7.0.116.0

Current Software Release	Upgrade Path to 7.0.116.0 Software
3.2.78.0 or later 3.2 release	Upgrade to 4.0.206.0 or later 4.0 release, then upgrade to 4.2.176.0, before upgrading to 7.0.116.0.
4.0.155.5 or later 4.0 release	Upgrade to 4.2.176.0 before upgrading to 7.0.116.0.
4.1.171.0 or later 4.1 release	Upgrade to 4.2.176.0 before upgrading to 7.0.116.0.

Table 1 Upgrade Path to Controller Software Release 7.0.116.0 (continued)

Current Software Release	Upgrade Path to 7.0.116.0 Software
4.1.191.xM	Upgrade to 4.1.192.35M and then to 6.0.182.0 before upgrading to 7.0.116.0.
4.1.192.22M or 4.1.192.35M	Upgrade to 6.0.182.0 before upgrading to 7.0.116.0.
4.2.130.0 or earlier 4.2 release	Upgrade to 4.2.209.0 before upgrading to 7.0.116.0.
4.2.173.0 or later 4.2 release	Upgrade to 4.2.209.0 before upgrading to 7.0.116.0.
4.2.209.0 or later 4.2 release	You can upgrade directly to 7.0.116.0.
5.0.148.0 or later 5.0 release	You can upgrade directly to 7.0.116.0.
5.1.151.0 or later 5.1 release	Upgrade to a 5.2 or a 6.0 release and then upgrade to 7.0.116.0.
5.2.157.0 or later 5.2 release	You can upgrade directly to 7.0.116.0.
6.0.188.0 or later 6.0 release	You can upgrade directly to 7.0.116.0.
6.0.196.0 or later 6.0 release	You can upgrade directly to 7.0.116.0.
7.0.98.0	You can upgrade directly to 7.0.116.0.
7.0.98.218	You can upgrade directly to 7.0.116.0.

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 7.0.116.0 software. In large networks, it can take some time to download the software on each access point.

Note You cannot install the Cisco Unified Wireless Network Controller Boot Software 7.0.116.0ER.aes file on Cisco 5500 Controller platform.

Note If you upgrade to the controller software release 7.0.116.0 from an earlier release, you must also upgrade WCS to 7.0.172.0 and MSE to 7.0.201.0.

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 (7.0.116.0 ER.aes) ensures that the boot software modifications in all of the previous and current boot software ER.aes files are installed.

- It is not possible to upgrade or downgrade a new image if FIPS is enabled.
- Downgrading from 7.0.116.0 ER to 5.2.157.0 ER release version on a Cisco 4400 Series Controller fails. The downgrade fails reporting insufficient disc space.

Note Consider a network deployment scenario where an OfficeExtend Access Point is configured with the Least Latency Join option enabled and the controller is configured with NAT enabled. The Least Latency Join feature enables the access point to choose a controller with the least latency when joining, that is, when the feature is enabled, the access point calculates the time between the discovery request and the

response and joins the controller that responds first. NAT enables a device such as a router to act as an agent between the Internet and the local network. NAT enables you to map the controller's intranet IP address to a corresponding external address.

When an OfficeExtend Access Point that is configured with the "Least Latency Join" option and is upgraded to the controller release 7.0.116.0 tries to associate to the controller with NAT enabled, the access point fails to join the controller. Due to an update to the software code of 7.0.116.0, the OEAP always tries to join the non-NAT IP address and fails to join, and tries a rediscovery which fails again. The OEAP can never connect to the controller.

This problem can be fixed by moving the access point to local mode to the controller and let the access point join the controller. On joining, disable least latency join and upgrade to 7.0.116.0 release.

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.

Software Release Support for Access Points

Table 2 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 2 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
	AIR-LAP1041N	7.0.98.0	
	AIR-LAP1042N	7.0.98.0	
1100 Series	AIR-LAP1121	4.0.155.0	7.0.x
	AIR-LAP1131	3.1.59.24	
	AIR-LAP1141N	5.2.157.0	
	AIR-LAP1142N	5.2.157.0	
1220 Series	AIR-AP1220A	3.1.59.24	7.0.x
	AIR-AP1220B	3.1.59.24	7.0.x
1230 Series	AIR-AP1230A	3.1.59.24	7.0.x
	AIR-AP1230B	3.1.59.24	7.0.x
	AIR-LAP1231G	3.1.59.24	7.0.x
	AIR-LAP1232AG	3.1.59.24	7.0.x

Table 2 Software Support for Access Points (continued)

Access Points		First Support	Last Support
1240 Series	AIR-LAP1242G	3.1.59.24	—
	AIR-LAP1242AG	3.1.59.24	—
1250 Series	AIR-LAP1250	4.2.61.0	—
	AIR-LAP1252G	4.2.61.0	—
	AIR-LAP1252AG	4.2.61.0	—
1260 Series	AIR-LAP1261N	7.0.116.0	
	AIR-LAP1262N	7.0.98.0	
1300 Series	AIR-BR1310G	4.0.155.0	7.0.x
1400 Series	Standalone Only	N/A	—
3500 Series	AIR-CAP3501E	7.0.98.0	
	AIR-CAP3501I	7.0.98.0	
	AIR-CAP3502E	7.0.98.0	
	AIR-CAP3502I	7.0.98.0	
	AIR-CAP3502P	7.0.116.0	
1500 Mesh Series	AIR-LAP-1505	3.1.59.24	4.2.207.54M
	AIR-LAP-1510	3.1.59.24	4.2.207.54M

Table 2 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-LAP1523CM	7.0.116.0 or later.	
	AIR-LAP1524SB	-A, C and N: 6.0 or later	—
		All other reg. domains: 7.0.116.0 or later.	
	AIR-LAP1524PS	-A: 4.1.192.22M or 5.2 or later[1]	—
1550	AIR-CAP1552I-x-K9	7.0.116.0	
	AIR-CAP1552E-x-K9	7.0.116.0	
	AIR-CAP1552C-x-K9	7.0.116.0	
	AIR-CAP1552H-x-K9	7.0.116.0	

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

Interoperability With Other Clients in 7.0.116.0

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

Table 3 describes the configuration used for testing the clients.

Table 3 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	7.0.116.0
Controller	Cisco 4400 Series Controller and Cisco 5500 Series Controller
Access points	1131, 1142, 1242, 1252, AP 3500e and AP3500i
Radio	802.11a, 802.11g, 802.11n2, 802.11n5
Security	Open, WEP, PSK (WPA and WPA2), 802.1X (WPA-TKIP and WPA2-AES) (LEAP, PEAP, EAP-FAST, EAP-TLS)
RADIUS	ACS 4.2
Type of tests	Connectivity, traffic, and roaming between two access points

Table 4 lists the versions of the clients. The traffic tests included data or voice. The clients included laptops, handheld devices, phones, and printers.

Table 4 Client Type

Client Type and Name	Version
Laptop	
Intel 3945/4965	11.5.1.15 or 12.4.4.5
Intel 5100/5300/6200/6300	13.1.1.1
Dell 1395/1397/Broadcom 4312HMG(L)	XP/Vista: 5.60.18.8 Win7: 5.30.21.0
Dell 1505/1510/Broadcom 4321MCAG/4322HM	5.60.18.8
Dell 1520/Broadcom 43224HMS	5.60.48.18
Atheros HB92/HB97	8.0.0.320
Atheros HB95	7.7.0.358
MacBook Pro (Broadcom)	5.10.91.26
Handheld Devices	
Falcon 4200/WinCE 4.2	5.60.21
Intermec CK31/WinCE 4.2:	3.00.19.0748
Intermec CN3/Windows Mobile 5.0	3.25.15.0065
Psion 7535/WinCE 5.0	1.02.09
Psion WAP/WinCE 5.0	1.02.42
Symbol 8846/Pocket PC 4.20	2.4.2273

Table 4 Client Type (continued)

Symbol MC70 /Windows Mobile 5.0	3.0.0.226
Symbol MC9060/Pocket PC 4.2	3.1.7
Symbol MC9090/WinCE 5.0	3.1.7
Phones and Printers	
Ascom i75	1.4.25
Nokia e61	3.0633.09.04
Spectralink 8030	104.025
Spectralink e340/PTE110	110.036/091.047/104.025
Spectralink i640/PTX110	110.036/091.047/104.025
Vocera B1000A	4.1.0.2817
Vocera B2000	4.0.0.269
Zebra QL320	HTNVK49s
Monarch 9855	3.2AB
Cisco 7921G	CP7921G-1.3.4.LOADS
Cisco 7925G	CP7925G-1.3.4.LOADS

Special Rules for Upgrading to Controller Software 7.0.116.0 in Mesh Networks

Caution Before upgrading your controller to software release 7.0.116.0 in a mesh network, you must comply with the following rules.

Upgrade Compatibility Matrix

Table 5 outlines the upgrade compatibility of controller mesh and nonmesh releases and indicates the intermediate software releases required as part of the upgrade path.

Software Upgrade Notes

The software upgrade notes are as follows:

- You can upgrade from 4.1.192.22M and 4.1.192.135M to 6.0.182.0 without any configuration file loss. See Table 5 for the available upgrade paths.

Note If you downgrade to a mesh release, you must then reconfigure the controller. We recommend that you save the configuration from the mesh release before upgrading to release 7.0.116.0 for the first time. Then, you can reapply the configuration if you need to downgrade.

- You cannot downgrade from controller software release 7.0.116.0 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 7.0.116.0. After a 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 7.0.116.0. Also, make sure to check the RRM configuration settings after the reset to verify that they are correct (CSCsv50357).

Table 5 Upgrade Compatibility Matrix for Controller Mesh and NonmeshReleases from 4.0.206.0 release and above

Upgrade to	7.0.116.0	7.0.98.218	7.0.98.0	6.0.199.0	6.0.196.0	6.0.188.0	6.0.182.0	5.2	4.2.207.54M	4.2.176.51M	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
Upgrade from																		
7.0.98.0	Y	Y	-															
6.0.199.0	Y	Y																
6.0.196.0	Y	Y	Y															
6.0.188.0	Y	Y	Y	Y	Y	-												
6.0.182.0	Y	Y	Y	Y	Y	Y	-											
5.2	Y	Y	Y					-										
4.2.207.54M	Y	Y	Y															
4.2.176.51M	Y	Y	Y															
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]	–	

Upgrade to	7.0.116.0	7.0.98.218	7.0.98.0	6.0.199.0	6.0.196.0	6.0.188.0	6.0.182.0	5.2	4.2.207.54M	4.2.176.51M	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
4.0.217.0														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

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.

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 7.0.116.0 software to 500 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 7.0.116.0, 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.

Note If a WiSM controller is heavily loaded with access points and clients and is running heavy traffic, a software upgrade sometimes causes an Ethernet receive-path lockup and the hardware watchdog sometimes trips. You might need to reset the controller to return to normal operation.

Note Do not install the 7.0.116.0 controller software file and the 7.0.116.0 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.

Note When upgrading from 5.2.193.0 to 7.0.116.0 release, access points with names that contain spaces will lose their configured name. For example, if an access point was named "APTestName 12", after upgrade, when the access point rejoins the controller, the name is truncated to "APTestName".

Caution If you want to downgrade from 7.0.116.0 release to a previous release, do either of the following:

> Delete all WLANs that are mapped to interface groups and create new ones.
> Ensure that all WLANs are mapped to interfaces rather than interface groups.

Caution If you are using controller software release 7.0.116.0 and if you have configured multicast interfaces, do not use the same configuration file for the 7.0.98.0 release. Using the 7.0.116.0 configuration file with multicast interfaces in 7.0.98.0 release might cause the controller to be unresponsive.

To upgrade the controller software using the controller GUI, follow these steps.

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

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

Step 2 Follow these steps to obtain the 7.0.116.0 controller software and the Cisco Unified Wireless Network Controller Boot Software 7.0.116.0 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. We recommend 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 7.0.116.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 7.0.116.0 ER.aes file).

Step 3 Copy the controller software file (*filename*.aes) and the Cisco Unified Wireless Network Controller Boot Software 7.0.116.0 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 list, choose **Code**.

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

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

Step 10 If you are using a TFTP server, the default values of 10 retries for the Maximum Retries text field, and 6 seconds for the Timeout text field should work 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 text box and the amount of time (in seconds) that the TFTP server attempts to download the software in the Timeout text box.

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

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

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

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

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

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

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

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

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

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

Step 18 After the controller reboots, repeat Step 6 to Step 17 to install the remaining file (either the 7.0.116.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 7.0.116.0 ER.aes file).

Step 19 Reenable the WLANs.

Step 20 Reenable your 802.11a and 802.11b/g networks.

Step 21 If desired, reload your latest configuration file to the controller.

Step 22 To verify that the 7.0.116.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

Step 23 To verify that the Cisco Unified Wireless Network Controller Boot Software 7.0.116.0 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 7.0.116.0 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. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.** Statement 1071

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

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

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

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

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

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

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

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

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

Safety Information

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

FCC Safety Compliance Statement

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

Safety Precautions

For your safety, and to help you achieve a good installation, read and follow these safety precautions. **They 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 list, choose an unused COM port of 4 or lower.

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

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

Important Notes for Controllers and Nonmesh Access Points

This section describes important information about controllers and nonmesh lightweight access points.

Cisco 2106, 2112, 2125, and 2500 Series Controllers support only up to 16 WLANs.

Cisco 2106, 2112, 2125, and 2500 Series Controllers can support only up to 16 WLANs. To support more than 16 WLANs, you can use WISM2 or Cisco 5508 Controller.

Cisco 1040/1140 Series Access Points may record "watchdog timer expired" as last reset reason

The following error message sometimes appears as the last reset reason when the access points are power cycled:

```
Watchdog timer expired
```

This symptom is observed only in Cisco 1040/1140 Series Access Point and does not have any impact on functionality. Ignore the watchdog timer expired after power cycled. You can also overwrite the reset reason to"reload" by rebooting with command operation.

WPlus License Features Included in Base License

All features included in a Wireless LAN Controller WPlus license are now included in the base license; this change is introduced in release 7.0.116.0. There are no changes to WCS BASE and PLUS licensing.

These WPlus license features are included in the base license:

- Office Extend AP
- Enterprise Mesh
- CAPWAP Data Encryption

The licensing change can affect features on your wireless LAN when you upgrade or downgrade software releases, so you should be aware of these guidelines:

- If you have a WPlus license and you upgrade from 6.0.18x to 7.0.116.0: Your license file contains both Basic and WPlus license features. You will not see any disruption in feature availability and operation.
- If you have a WPlus license and you downgrade from 7.0.116.0 to 6.0.196.0, 6.0.188 or 6.0.182, the license file in 7.0.116.0 contains both Basic and WPlus license features, so you will not see any disruption in feature availability and operation.

- If you have a base license and you downgrade from 7.0.116.0, 6.0.196.0, 6.0.188.0 or 6.0.182.0, when you downgrade, you lose all WPlus features.

Note Some references to Wireless LAN Controller WPlus licenses remain in WCS and in the controller CLI and GUI in release 7.0.116.0. However, WLC WPlus license features have been included in the Base license, so you can ignore those references.

Additive Licenses Available for 5500 Series Controllers

You can now purchase licenses to support additional access points on 5500 series controllers. The new additive licenses (for 25, 50, or 100 access points) can be upgraded from all license tiers (12, 25, 50, 100, and 250 access points). The additive licenses are supported through both rehosting and RMAs.

One-Time Password (OTP) Support

One Time Passwords (OTP) are supported on the Wireless Lan Controller (WLC) using TACACS and RADIUS. In this configuration, the controller acts as a transparent passthrough 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 alphabetic characters in the MAC address. In software release 6.0 or later, the controller sends lowercase alphabetic 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 300 access point groups for 4400 series controllers, 500 AP Groups on 5500 Series Controllers, and 192 access point groups for 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.

Inter-Release Controller Mobility

To know more about inter-release controller mobility compability across releases, see http://www.cisco.com/en/US/docs/wireless/controller/5500/tech_notes/Wireless_Software_Compatibility_Matrix.html#wp80877.

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. However, this works when the managed access point is a monitor mode AP on a DFS channel.

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 with 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 and Flex 7500 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 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.

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.

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 fix 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 7.0.116.0. 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 7.0.116.0, 6.0.196.0, 6.0.188.0, 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 frames at the highest configured basic rate and management frames at lowest basic mandatory rates, which can cause reliability problems. Access points running LWAPP or autonomous Cisco 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 nonmulticast clients.

Disabling Radio Bands

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

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, AP1242AG, 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.

Note The Transmit Power level can range between -10 dBM to 30 dBM.

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.

To recover the access point using the TFTP recovery procedure, follow these steps:

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. We recommend 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, we highly recommend 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 7.0,* 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

We recommend 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. 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)
- 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). We recommend 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, we recommend 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 Support

This version of the controller software release 7.0.116.0 is compatible with the Gateway Load Balancing Protocol (GLBP).

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.

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

We recommend 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.

Enabling/Disabling Band Selection and Client Load Balancing

It is not possible to enable or disable band selection and client load balancing globally through the controller GUI or CLI. You can, however, enable or disable band selection and client load balancing for a particular WLAN. Band selection and client load balancing is enabled globally by default.

Changing the IOS LWAPP Access Point Password

Cisco IOS Lightweight Access Point Protocol (LWAPP) access points have a default password of *Cisco*, and the prestage 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 mgmtuser add *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 prestage 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.

Client exclusion can happen both statically and dynamically. In a static exclusion, the client is disabled permanently. In dynamic exclusion, the client is excluded until the configured exclusion timeout is reached in the WLAN.

The following client exclusion policies are available:

- Excessive 802.11 association failure
- Excessive 802.11 authentication failure
- Excessive 802.1X authentication failure
- IP theft or reuse
- Excessive web authentication failure

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 7.0,* 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 7.0,* for configuration instructions.

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

DirectStream Feature Is Not Supported With WGB

The DirectStream feature from the controller does not work for clients behind workgroup bridges and the stream is denied. This feature is not supported in 7.0 release.

Features Not Supported on 2100 Series Controllers

This hardware feature is not supported on Cisco 2100 Series Controllers:

- Service port (separate out-of-band management 10/100-Mbps Ethernet interface)
- The Cisco 2100 Series Controllers do not support AP801 and AP802 access points.

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 Cisco 2500 Series Controllers

These software features are not supported on Cisco 2500 Series Controllers:

- Support for wired guest access.
- Cisco 2500 Series Controller cannot be configured as an auto anchor controller. However you can configure it as a foreign controller.
- Supports only multicast-multicast mode.
- Bandwidth Contract feature is unsupported.
- Access points in direct connect mode is unsupported
- Service port support
- Apple Talk Bridging
- LAG
- Wired Guest

Features Not Supported on 5500 Series Controllers

These software features are not supported on Cisco 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 Cisco 5500 Series Controllers bridge these packets by default. If desired, you can use ACLs to block the bridging of these protocols.

Features Not Supported on Cisco Flex 7500 Series Controllers

These software features are not supported on Cisco Flex 7500 Series Controllers:

- Static AP-manager interface

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

- L3 Roaming
- VideoStream
- WGB
- Client rate limiting for centrally switched clients
- Access points in local mode

Note AP associated with the controller in local mode should be converted to H-REAP mode or Monitor mode.

- Mesh
- LAG
- Spanning Tree Protocol (STP)
- Cisco Flex 7500 Controller as a guest controller
- Multicast
- ACLs
- P2P Blocking

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 2504 Image on a 2106 Series Controller

It is possible to run a 2504 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> </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    <input type="TEXT" name="username"
SIZE="25" MAXLENGTH="63" VALUE=""> </td> </tr> <tr align="center" > <td colspan="2">
Password      <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>
```

Switch Port and Controller Port

When the port status on the controller changes, the switch status does not get changed. This is a known issue. For example, when the controller port goes down, the switch port is still in administrable state. This has been resolved in Cisco 5500 Series Controllers.

Unsupported mac-address Command for Unified and Autonomous Access Points

The unified and autonomous access point do not support the **mac-address** command for the wireless interfaces. When invoked, the command executes but can cause the access point to fail.

Fast Roaming and Authentication/Key Management for CCKM Clients

CCKM Fast-roaming clients in hybrid REAP mode works only with the following authentication or key management combinations:

- WPA2+AES
- WPA+TKIP

CCKM Fast-roaming clients in hybrid REAP mode is not supported with the following authentication or key management combinations:

- WPA+AES
- WPA2+TKIP

Errors when Using AAA with Active RADIUS Fallback

Consider a scenario where you configured the active RADIUS fallback feature using AAA for a controller. When using this feature, the controller sends the Accounting request probes without the session ID during fallback; which might be dropped by the RADIUS Server. This is because the controller cannot send accounting information with Session ID as during the fallback the controller will not have the context of the client. Some RADIUS Servers like ISE may report errors for Accounting probes sent to ISE. If your Authentication and Accounting servers are same then ignore the errors logged in ISE.

Roaming Clients when Access Points are in Standalone Mode

When access points are in standalone mode, they are not aware of each other's state and client statuses. For example, consider a scenario where two clients (Client 1 and Client 2) are communicating with each other. Also, assume that both the clients are associated with same access point (say, AP1). Let’s also assume that both AP1 and AP2 are in standalone mode. Now, if Client 1 roams to AP2, the packets sent from Client 2 will not reach Client 1.

Using Lightweight Access Points with NAT

You can place a lightweight access point under NAT. On the access point side, you can have any type of NAT configured. However, when you configure the controller, you can have only 1:1 (Static NAT) configured and the external NAT IP address configured on dynamic AP management interface. This is applicable only for Cisco 5500 Series Controllers. PAT cannot be configured on the controller because LAPs cannot respond to controllers if the ports are translated to ports other than 5246 or 5247, which are meant for control and data messages.

Note Select the Enable NAT Address check box and enter the external NAT IP address if you want to be able to deploy your Cisco 5500 Series Controller behind a router or other gateway device that is using one-to-one mapping network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a local network (private). In this case, it maps the controller's intranet IP addresses to a corresponding external address. The controller's dynamic AP-manager interface must be configured with the external NAT IP address so that the controller can send the correct IP address in the Discovery Response.

Note With CAPWAP, a controller behind NAT is not supported with the 4400 series, 2100 series Wireless LAN Controllers and the WiSM.

Default A-MPDU settings

By default, Aggregated MAC Protocol Data Unit (A-MPDU) is enabled for priority level 0, 4 and 5 and the rest are disabled. In releases prior to 6.0 release, only priority 0 was enabled by default. The video performance is enhanced when priorities 4 and 5 are enabled for A-MPDU aggregation.

Important Notes for Controllers and Mesh Access Points

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

New Features

The following new features are available in controller software release 7.0.116.0.

Note See the *Cisco Wireless LAN Controller Configuration Guide, Release 7.0*, for more details and configuration instructions.

Mesh LSC Support

This feature enables Locally Significant Certificates (LSC) to be used on access points. Wireless controllers use these certificates to join, authenticate, and derive a session key on access points configured in Mesh mode.

1524 SB Enhancements

The following two enhancements have been made to the 1524 SB access point.

Slot Bias

This feature provides an option to enable or disable slot bias. You can use directional antennas on both of the backhaul radios and the parent can be selected in either direction without the access point going into scanning mode after 15 minutes. The enhancements gives you dual 5-GHz backhaul and the freedom to select any type of antenna (omni or directional), which helps to reduce interference on 1524. By default, slot bias is enabled.

Note This feature is only applicable for serial backhaul access points like 1524 SB.

Preferred Parent

An option to configure a preferred parent for a mesh access point has been added to force a linear topology in a mesh environment. You can design the network the way that works best for your needs.

Mesh 11n Support in 7.0.116.0

With the 7.0.116.0 release, the mesh functionality is added in the Cisco Aironet 1040, 1140, 1250, 1260, 1520, and 3500 series indoor access points. The mesh backhaul radio supports the 802.11n data rate. When operating in mesh mode, their mesh backhaul will support both the 802.11a and 802.11n data rate.

The mesh functions are the same as that of indoor access points 1130/1240.

Because this is the first time the 802.11n rate is supported for Cisco access point mesh backhaul, both controller mesh backhaul-related GUI and CLI commands are modified to add 802.11n support. Both the controller and access point are modified to support mesh functions for access points. This feature enhancement extends mesh functionality to the 11n platform.

Caution Suppose an 11n indoor mesh access point (for example 1142 and 3502) on the 7.0.116.0 release roams because of parent loss or parent reset to a non-11n indoor parent on the 7.0.98.0 release (for example 1242). The 11n mesh access point joins the non-11n parent if it is authenticated (for example through MAC Filter) and then downloads the 7.0.98.0 release. When the mesh access point reboots, it becomes local because 7.0.98.0 does not support mesh for 11n APs. This results in the 11n mesh access point to be stranded. This scenario is possible when you upgrade your non-802.11n mesh network and have coexisting 11n mesh access points. We recommend that you have 802.11n RAPs instead of non-802.11n RAPs.

2.4-GHz Radio for Backhaul

Until the 7.0.98.0 release, mesh used the 5-GHz (802.11a) radio for backhaul, and the 2.4-GHz (802.11b/g) radio was used only for client access. The reasons for using only the 5-GHz radio for backhaul are as follows:

- More channels are available
- More EIRP is available
- Less interference occurs
- Most of the client access occurs over the 2.4-GHz band

However, under certain conditions, such as dense foliage areas, you might have needed to use the 2.4-GHz band for a backhaul because it has better penetration.

With the 7.0.116.0 release, you can configure an entire mesh network to use a single backhaul that can be either 5 GHz or 2.4 GHz.

Caution This feature is available only for AP1522 (two radios). This feature should be used only after exploring the 5-GHz backhaul option.

Caution We recommend that you use 5 GHz as the first option and use 2.4 GHz only if the 5-GHz option does not work.

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

The following sections lists Open Caveats and Resolved Caveats for Cisco controllers and lightweight access points for version 7.0.116.0. For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

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

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

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

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

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

Open Caveats

Table 6 lists open caveats in controller software release 7.0.116.0.

Table 6 Open Caveats

ID Number	Description
CSCsw93671	Controller sources packets for web authenticated clients from management or service-port interface. Symptom: When you see traffic on the network being sourced from the service port, all these packets are either SYN, ACK, or FIN acknowledgment packets with either a source port of TCP 2006 or TCP 2008. The service port is not connected to the network. On analyzing the sniffer captures, it is observed that no packet sent to the controller would cause these packets to be sent. Conditions: The condition happens rarely when a client associated to web-auth enabled WLAN sends only a TCP SYN packet for a web-session and terminates the connection. Workaround: None.
CSCtd14642	Controller fails to respond at task sshpmReceiveTask on controller with version 5.2.193. Symptom: Controller in WiSM fails to respond at sshpmReceiveTask on 5.2.193.0 Conditions: Controller using 5.2.193.0 with WiSM configuration. Workaround: Revert to the default configuration and build from scratch.

Table 6 Open Caveats (continued) (continued)

CSCte86144	AP fails to respond with %SYS-2-CHUNKBADMAGIC with message bad magic number in chunk header.
	Symptom: AP unresponsive with the message:
	`%SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk CCB638 data CCC2C0`
	`chunkmagic EF4321CD  chunk_freemagic 0`
	`-Process= "Check heaps", ipl= 0, pid= 4`
	`-Traceback= 196AC 14FA44 14FC10 14F88C 137190`
	Conditions: AP fails to respond with a bad magic number in the chunk header.
	Workaround: None

CSCtb78072	SNMPv3 communication breaks with NAC appliance CAM. Symptom: Wireless clients do not move into the access state even when the NAC agent on the client passed posture validation. This problem happens because of the following: 1. The controller reboots. 2. The CAM uses an old SNMPv3 session to communicate with the controller. The above clients are quarantined to access traps that are dropped by the controller due to a mismatch in their SNMP session (CAM - old , WLC- new after reboot). Conditions: SNMPv3 is used for traps originating from the NAC appliance CAM to controller. Workaround: Reset and reinitiate the SNMPv3 connection. You can do this by changing the SNMPv3 to SNMPv2 and then back to SNMPv3.
CSCtn04229	Signal strength increases for a while though TxPower is static. Symptom: Signal strength suddenly increases for a while though TxPower is static. During the issue, CRC error rate may increase and many packet retries may occur. It may cause packet loss/delay or may result in the client losing connectivity. Conditions: This problem is seen on CAP3502 with Controller version 7.0.98.0. Workaround: None.
CSCtn39219	Access point crashes on the access point 1130 with message dot11_radio_interrupt(0x493450)+0x150 Symptom: Access point is unresponsive and displays the following stack trace: `[0x4935A0] dot11_radio_interrupt(0x493450) 0x150 [0x2AA824] ISR_wrapper(0x2aa7d0) 0x54` Conditions: A hardware issue in the access point causes the access point to fail to handle certain interrupts. Workaround: Replace the access point.

Table 6 Open Caveats (continued) (continued)

CSCtn95179	No DSCP marking when CAPWAP data encryption enabled.
	Symptom: When CAPWAP data encryption is enabled, there are NO DSCP markings in the CAPWAP IP header (that is DSCP=0). The sniffer capture shows the following:
	`Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00) 0000 00.. = Differentiated Services Codepoint: Default (0x00)`
	`When CAPWAP data encryption is disabled, there are IP DSCP values in the CAPWAP IP header.`
	`Differentiated Services Field: 0x88 (DSCP 0x22: Assured Forwarding 41; ECN: 0x00)  1000 10.. = Differentiated Services Codepoint: Assured Forwarding 41(0x22)`
	Conditions: This problem happens when you want to prioritize voice traffic and the clients by running CUCIMOC on clients. However, no DSCP markings are found when CAPWAP data encryption is enabled.
	Workaround: None.

CSCto02968	Memory leak observed on controller on sshpm on sshencode line number 252. Conditions: Slow memory leak seen on controller configured with webauth and a custom webpage change every 20 minutes. The buffer allocation for the 64 pool increases rapidly in a few days. Workaround: Reload the controller.
CSCto06047	Access point does not respond after a while using 11n rates. Symptom: AP stops responding when using 11n rates. Conditions: While connected and on a audio call using 11n rates, the AP stops responding. Workaround: None.
CSCto08803	Controller leaks unencrypted frames for WGB clients. Symptom: Unencrypted frames are observed for WGB clients over the air. Conditions: This problem happens when the WGB roams across multiple access points. Workaround: None.
CSCto11157	Access point does not send an association response to client. Symptom: Client not able to associate to AP and WLC. Conditions: Some clients try to associate to an access point. The access point does not send an association response back to the client which causes the client to start the probe request and the cycle continues for about 10 to 15 minutes when eventually the access point sends a response. This problem is not reproducible in release 5.1. Workaround: This problem occurs when an intermediary device between the controller and the access point adds extra bytes to the association request. You can do one of the following: • Use controller software release 5.1, or • Eliminate the intermediary device that is adding the extra bytes to the association request.

Table 6 Open Caveats (continued) (continued)

CSCtl98942	CleanAir Trap types go back to default after configuration is restored. Symptom: CleanAir Trap types go back to default after configuration restored. Conditions: This problem is seen when using the controller version: 7.0.98.0 Workaround: The following workarounds are available: • Workaround 1: Reconfigure the controller with the desired configuration for CleanAir traps. • Workaround 2: Create a template for CleanAir using WCS and push the templates to other controllers. To know more about how to work with templates, refer to the *Cisco Wireless Control System Configuration Guide*.

CSCtn16281	Mesh access point is unresponsive on BVI restart by DHCP
	Symptom: Mesh AP crash on BVI restart by DHCP.
	Conditions: Mesh AP crash on BVI restart by DHCP
	`*Feb 9 04:00:45.911: %MESH-6-ADJ_VIDB_LINK: Mesh neighbor 0021.1bc0.XXXX VIDB Virtual-Dot11Radio2 dot1x control`
	`*Feb 9 04:01:03.199: %DHCP-5-RESTART: Interface BVI1 is being restarted by DHCP`
	`*Feb 9 04:01:06.023: %MESH-6-CAPWAP_RESTART: Mesh Capwap re-started`
	Workaround: None.

CSCtn16347	Controller does not rewrite DHCP ACK packets correctly for DHCP information. Symptom: DHCP Acknowledgement packets are not rewritten correctly to DHCP Inform packets by the controller (in DHCP proxy mode): The acknowledgement packets are sent as broadcast and server IP is not rewritten. Conditions: DHCP server replying to DHCP Inform Packets (Authoritative mode). Workaround: None.
CSCtn37462	The **show net user summary** command does not show users when the local database has more than 256 entries. Symptom: This problem is seen in release 7.0.98.0 with the command line interface. If your local database has more than 256 users, the command line only displays a maximum of 256 users. Conditions: The controller contains more than 256 users running software release 7.0.98.0. Workaround: Use the controller GUI.
CSCto00114	The iPhone 4 fails to authenticate with PEAP when using local EAP authentication on the controller. Symptom: iPhone 4 unable to authenticate using PEAP when the controller is configured for Local EAP Authentication. Conditions: Set WLC as Local EAP Authenticating Server with PEAP. Workaround: Use external RADIUS server if PEAP is desired. **Note** This problem only affects iPhone 4. iPhone 3 and iPhone 3GS work as expected.

Table 6 Open Caveats (continued) (continued)

CSCtj38889	Cisco Flex 7500 Series Controller- Locally authenticated PMK cache info gets deleted after the controller reboots. Symptom: The access point does not plumb the PMK cache for locally authenticated clients after the controller reboots because the controller does not have a cache. After the controller reboots, the access points that join the controller do not have the PMK cache. As a result of this, clients need to perform a full authentication. Conditions: This problem happens only for locally authenticated clients. Workaround: None
CSCtn42589	AP reboots while moving from connected to standalone mode if radios b/g is disabled. Symptom: This issue is seen when the g radio is disabled and the access point disconnects and connects back. The access point then reboots. Conditions: The access point fails to respond when it disconnects from the controller and joins back. Workaround: None.
CSCto06084	The access point summary report does not show any data for OEAP602 access point. Symptom: The access point summary report does not show any data because OEAP602 does not belong to the default-AP group. Conditions: Execute AP summary report with APs by using the Controller filter criteria. Workaround: The access point summary report does not show any data because the OEAP 602 does not belong to the default-ap group. Add another AP group and include the OEAP602. The report will show the data.
CSCto11060	Remote LAN fails to apply to Cisco 2500 Series Controller through WCS. Symptom: Remote LAN apply to Cisco 2500 Series Controller fails in WCS. Conditions: When you create a Remote LAN template using WCS and apply it to a Cisco 2500 Series Controller, the remote LAN fails. Workaround: Create the remote LAN using the controller GUI.
CSCto50248	Cisco Flex 7500 Series Controller-OKC fast roam fails in standalone mode while using EAPfast/PEAP EAP. Symptom: OKC fast roaming fails in standalone local authentication mode. During roaming, only a full authentication succeeds. Fast roaming works fine in connected mode with central authentication. Conditions: OKC fails with the other EAP methods such as EAP-Fast and PEAP. Workaround: Use the OKC feature with LEAP in connected mode or standalone mode with local authentication. Other EAP methods such as EAP-Fast/Peap can be used only in central authentication in connected mode.

Table 6 Open Caveats (continued) (continued)

CSCto59770	OEAP with least latency join are stranded. Symptom: OEAP or HREAP APs with Least Latency Join enabled on Wireless LAN controllers are not able to join a controller running version 7.0.116.0 when it sends the NAT and Non-NAT discovery responses. Conditions: This issue is seen when the least latency join feature is enabled on the controller. Workaround: Disable the least latency controller join from wireless LAN controllers. This feature should be disabled prior to the 7.0.116.0 upgrade to allow APs to join successfully to the controller.
CSCto34834	1520 and 1550 Series AP may change the 2.4-GHz channel when reloaded. Symptom: Cisco 1522 and 1552 access points may change the 2.4-GHz radio to another channel on AP reload. Conditions: This issue can occur when the channel selected is configured in Custom Mode and when another Cisco AP Network is nearby, utilizing the 2.4-GHz radio as the backhaul. This issue can also occur if the Adjusted Ease metric (used for parent selection) is such that a parent on the other 2.4-GHz backhaul network is higher than any potential parents on the 5-GHz backhaul network. Workaround: Any of the following four options can mitigate this issue: 1. Use the Global Mode rather than Custom Mode to set the channel. 2. On 1550 APs, use the Cisco CleanAir feature on the 2.4-GHz radio. 3. Ensure that the desired 5-GHz parent AP has a higher Adjusted Ease than the nearby 2.4-GHz backhaul network. 4. Reprovision the 2.4-GHz channel to the desired channel after the reload.
CSCud20593	Symptom: The Cisco TrustSec SXP feature is not supported. Conditions: 7.0.x controller software releases. Workaround: None.

Resolved Caveats

Table 7 lists caveats resolved in controller software release 7.0.116.0.

Table 7 Resolved Caveats

ID Number	Caveat Title
CSCsj33229	Unable to ping APs directly connected to a 2106 controller.
CSCtg73740	AP should default AAA ports to 1812/1813 not 1645/1646.
CSCtg66192	5508 WLC - solid amber alarm light.
CSCtb72660	NEC SIP CAC: Load-based CAC is not working with non-WMM clients.
CSCtl44908	DCA channel lists changes when WLC is upgraded to 6.0/7.0 from 4.2.

Table 7 Resolved Caveats (continued)

ID Number	Caveat Title
CSCtl95978	WLC will not respond to SNMP if its source address is part of a dynamic interface.
CSCtg51544	MSFT: Multiple SSH sessions can cause arrow key failure and password to appear.
CSCtf78029	SNMP traps for 1231 AP also sent for Interface:1(unknown type).
CSCtd21754	Huck Jr "b" radio status moves from disabled to enabled after reboot.
CSCtg44663	WGB: multiple parents created during roaming traffic disrupted.
CSCtg67029	The command **show client tsm** does not display full output.
CSCtg66175	RLDP does not work on CT5500 or WLC2100 + HREAP AP.
CSCtf38802	SIP calls on roaming with CAC failure connects back without B/W reserved.
CSCtg65856	Counters not cleared during intra-controller roaming of SIP calls.
CSCtg74333	Addition of VOICE_CALL_FAILURE_5 Enum to QOS MIB.
CSCtg70271	WEBAUTH_REQD (8) Reached ERROR: occurred from the line 4055 in client debug.
CSCsy18685	Default-group for AP-groups does not contain all SSIDs.
CSCtg84677	AP is deauthenticated with a reason: power capability is unacceptable.
CSCtf27464	Management interface does not use HSRP MAC address when replying.
CSCtf51294	Cannot clear webauth bundle from controller.
CSCtg92171	WLC stops responding to network.
CSCtf62737	Controller URL sanitation issue.
CSCtf90579	With TACACS/RADIUS authentication, lobby admin was unable to edit the guest user role.
CSCtg09589	Duplex mismatch occurs when the 1140 the access point is directly connected to a Cisco 2100 Series Controller.
CSCtg21950	WGB intracontroller roaming must update its clients without an IAPP frame.
CSCtg03203	The access points 1142/1252 recognize 802.11n HT enabled clients as legacy ones.
CSCtg23491	The controller does not process flooded unicast traffic properly.
CSCtg23618	WiSM goes unreachable outside of the Catalyst 6500 Series Switch.
CSCtg30694	Controller webauth client never has to reauthenticate after session timeout.
CSCtg51702	Degraded voice performance occurs on HREAP local switching with TKIP + CCKM.
CSCtg57607	WGB fails to send IAPP updates after roaming.
CSCtg95111	The access point which is not correctly primed, keeps reconnecting with the master.
CSCtk53680	WiSM not able to FTP core dump when running low on memory.
CSCtg55102	HREAP: AssocFailPayload causes payload error in the controller.
CSCsg48089	Controller needs password recovery mechanism without losing configuration.

Table 7 Resolved Caveats (continued)

ID Number	Caveat Title
CSCsi27596	Controller lacks support for controlling the group key rotation interval.
CSCso22875	Access points get disconnected during code upgrade.
CSCso60597	AP 1250 fails to configure 40-MHz wide channel for sniffer mode.
CSCsq65895	DHCP proxy option does not validate if DHCP is required on WLAN.
CSCsr10874	Additional client statistics required for autonomous access points.
CSCsw80627	Controller fails to respond on task emWeb in 5.1.151.0.
CSCsx14840	LAG: Management interface change between port BIA and LAG port address.
CSCsx50408	LWAP DOS Attack trap message does not record the source MAC address.
CSCsy28323	Need to improve MFP scalability.
CSCsy30722	Next hop address stored in CAPWAP does not get updated on receiving GRAT ARP.
CSCsy65347	QoS Profiles Per-User Bandwidth Contracts not restricting traffic.
CSCsy71960	1242 AP ignores primary controller to join a wrong controller.
CSCsy96551	Internal WLC-DHCP not sending out NAK.
CSCsz14243	Unable to enable the WLAN while the APs are joining.
CSCsz19203	Controller fails to respond at "SSHpmMainTask".
CSCsz40659	Need to reboot wireless controller for upgrade to work.
CSCsz79621	Inter frame delay causing reassembly issues, breaking EAP-TLS auth.
CSCsz80820	Primary Discovery Request not processed for AP priority scenario.
CSCsz86245	Cisco 5500 Series Controller: Add new usmdb APIs for SNMP optimization.
CSCsz87643	Management interface unreachable via different subnet.
CSCta01750	Controller unresponsive because of a deadlock on spamReceive task.
CSCta03016	Cisco 4404 Series Controller fails to respond in version 5.2.188.0.
CSCta06244	WLAN configuration not same when downloading backup config via TFTP.
CSCta09996	Sometimes LAP cannot join the controller through alternative port in port redundancy.
CSCta28666	Configuration on mesh link test RSSI output is incorrect.
CSCta40160	Controller dropping primary discovery request from an AP that has already joined the controller.
CSCta71448	Request to reduce the severity of the error msg: %APF-1-CHANGE_ORPHAN_PKT_IP
CSCta72642	Access point logging related command does not getting uploaded.
CSCta78236	Request to change min/max rogue RSSI rule values.
CSCta88592	WCS 6.0.132.0 does not show mesh AP Root in map view.
CSCta91358	Hybrid REAP gets locked up due to wedge input queue on radio interface.
CSCtb02136	AP 1252 with AP Groups and hybrid REAP do not broadcast SSID.

Table 7 Resolved Caveats (continued)

ID Number	Caveat Title
CSCtb16583	Static IP LAP cannot join a controller.
CSCtb20125	CCMP errors on key rotation.
CSCtb23682	When logged into Cisco 5500 Series Controller using Telnet, characters are shown multiple times.
CSCtb23924	HREAP: WebAuth user cannot log out after roaming.
CSCtb34971	Controller WiSM loading 3rd party certificate for web-auth disables HTTPS port 443.
CSCtb36010	Lightweight AP responds on port 22 when SSH is disabled.
CSCtb42260	Enabling broadcast forwarding versus multicast forwarding via CLI.
CSCtb45178	Insufficient memory/traceback on AP1130 and AP1232.
CSCtb52563	Controller running 4.2.205.0 is unresponsive at spam_CCM_decrypt+124
CSCtb56664	Remove Over The Air Provisioning (OTAP) in access points.
CSCtb58091	WLC CPU spike with emweb - controller not responding.
CSCtb61628	SNMP trap controls setting is not succeeded on 5.2.
CSCtb63297	File read errors in msglog file.
CSCtb64579	Wired Guest accessUser is not redirected to Webauth page after some time
CSCtb64994	Intermittent webadmin and webauth access on WiSM running 5.2.193.
CSCtb74239	WISM unresponsive on task sshpmMainTask System.
CSCtb82951	Controllers ARP table not updating after receiving gratuitous ARP update.
CSCtb92872	WiSM: System unresponsive - Task "cids-cl Task" taking too much CPU.
CSCtb93729	Authentication trap flag does not get saved on reboot.
CSCtb96750	AP Fallback causes client drop with HREAP.
CSCtc01947	Initial CAWAP Packets are sent to burned-in MAC by controller in HSRP.
CSCtc03575	Controller fails to redirect web authentication to an external server.
CSCtc05478	The packet: deb pm ssh-engine enable does not work.
CSCtc10068	1140 APs trying to join LWAPP controller.
CSCtc13474	Self IP Address displays error message: "No mobility record found for peer".
CSCtc14910	AP 1140 not joining WLC and logging tracebacks.
CSCtc15346	AP1252 fails to retransmit missing AMPDU packet in response to block acknowledgement.
CSCtc32748	Noise/Channel measurements not done on all DCA channels
CSCtc45090	Controller sends wrong MAC in ARP response, can cause mobility flapping
CSCtc49270	Clients can't be deleted from exclusion list if not present in association list.
CSCtc51089	The setting for WLAN security static-wep-key encryption does not get restored.
CSCtc57611	Delay in music on hold on 7925 with HREAP AP.

Table 7 Resolved Caveats (continued)

ID Number	Caveat Title
CSCtc85444	Controller locks up on SNMP task when pushing AP Group template from WCS.
CSCtc87690	Clients are mapped to the native VLAN of the H-REAP AP switchport trunk.
CSCtc97144	Fix 1800 second session timeout when H-REAP is in standalone mode.
CSCtd01611	Important TLS/SSL security update required.
CSCtd17116	Emergency image version shows up N/A.
CSCtd19928	WLC TACACS+ accounting sends large amount of white space.
CSCtd23497	1242 AP HREAP Mode unresponsive after %CAPWAP-5-CHANGED state to join.
CSCtd25303	Wrong message on GUI when controller image is upgraded while AP IDs downloading the image.
CSCtd26168	Incorrect source MAC in ARP request when WLC is in LAG mode.
CSCtd33864	WGBs are not shown as clients under Summary page.
CSCtd34312	5508 Web auth breaks with multicast MAC as gateway.
CSCtd46917	CPU ACL and service config priority change required for telnet.
CSCtd49103	AP in static address, uses wrong syslog and LEDs turn off for some seconds.
CSCtd61893	Rogue APs that are classified do not send trap when found missing
CSCtd62937	Show ap summary does not show the access point name.
CSCtd64049	AW:J:FFT: controller unresponsive when upgrading the access point.
CSCtd70053	Guest mobility anchoring fails when the guest roams between controllers.
CSCtd72234	4.2 Mesh MAC auth to external RADIUS has authenticator all zeros.
CSCtd73371	WLC Shared memory allocation failed after web passthrough enabled.
CSCtd74870	Massive DHCP flood/loop with NAC OOB - DHCP Proxy disabled.
CSCtd75094	AP fails to respond when clearing CAPWAP MGIDs for new client.
CSCtd82509	WLC fails to respond when performing findContextInfo+268.
CSCtd84522	Fiber port (gig3) does not create VLAN subinterfaces when bridging.
CSCtd86886	WiSM generates traceback in the msglog occasionally.
CSCtd90304	%MM-3-MEMORY_READ_ERROR: mm_mobile.c:464 Error reading mobility memory.
CSCtd92105	Reaper reset in DHCP task.
CSCtd99602	Wired Guest: DHCP required breaks web auth following session timeout.
CSCtd99659	SNMP Agent inserts nulls during mesh link test.
CSCte08090	AW: TFTP upload broken for packet capture to windows TFTP server.
CSCte18071	Inconsistent use of MAC addresses on controller.
CSCte24079	2106 LAN hangs after high load with duplex mismatch.
CSCte27052	WLC 6.0 - Inconsistency in AAA override feature.

Table 7 Resolved Caveats (continued)

ID Number	Caveat Title
CSCte38645	RADIUS Attribute NAS-Port(5) not included in Access-Request for Web-Auth.
CSCte39477	Web GUI: External Web Servers field needs to always be displayed.
CSCte43374	The WGB connection breaks under EAPoL logoff attack.
CSCte43508	The Cisco 5508 Series Controller DP unresponsive: buffer leak due to ARP storm.
CSCte45826	AP drops packets with SIP Based CAC- WPA2/AES or tcp-adjust-mss/WPA/TKIP.
CSCte55370	Controller unresponsive during ping of virtual interface.
CSCte55458	Web authentication: Web page takes a long time to display under heavy load.
CSCte64350	Cisco 5500 Series Controller encounters an internal membuffer system error.
CSCte73125	APs unable to join WiSM.
CSCte89891	Radio may stop transmitting beacons periodically.
CSCte92365	The fix for auto immune attacks does not cover for incorrectly formatted association request. Does not cover missing IE.
CSCte92886	4.2 Mesh controller memory leak in EAP framework.
CSCtf08553	Syslog not sent to server that is on same subnet as dynamic interface.
CSCtf11461	CPU ACL check for Outbound ICMP traffic should be removed on Cisco 5500 Series Controller.
CSCtf14098	Controller unresponsive at task sshpmMainTask under high web-auth load conditions.
CSCtf18016	WiSM hung unable to HTTP, HTTPs, Telnet or SSH. Only ping responded.
CSCtf23682	Cisco 5508 Series Controller- AP cannot join with Multicast MAC as gateway (checkpoint).
CSCtf27779	The command **show tech** from CAPWAP AP does not include CAPWAP information.
CSCtf28217	AP Unexpectedly joins the controller in bridge mode instead of local or H-REAP mode.
CSCtf34858	Client cannot transmit traffic if it reassociates to an AP within 20 seconds.
CSCtf36053	Any CPU ACL blocks service port DHCP offer.
CSCtf38685	Need source MAC in mentioned msglogs.
CSCtf39285	Cisco 5500 Series controller accepts a 4400 4.2.x.x image.
CSCtf39550	Traceback messages are seen on console logs for instruction *osapiReaper.
CSCtf51287	The command **show exclusionlist** does not display excluded clients it only displays disabled clients.
CSCtf53010	Controller unresponsive when 12 or more handsets associate to it.
CSCtf53344	LWAP DOS attack trap message does not record the source MAC address.
CSCtf55495	AP may crash during rate shift operation.
CSCtf57349	Controller only allows 47 access points to join on single port.

Table 7 Resolved Caveats (continued)

ID Number	Caveat Title
CSCtf69598	Memory leak in access point on CCKM failure.
CSCtf81266	APF-1-ROGUE_CLIENT_UPDATE_FAILED filling up syslog.
CSCtf91342	LDAP server does not respond for 15 minutes when an incorrect UN is used.
CSCtf94589	Access point MAC address discrepancy in aggressive load balancing packets.
CSCtf94857	OEAP does not respond to probes on 2.4 radio.
CSCtg09393	RRM TPC - Minimum power level assignment not working for levels below 4.
CSCtg14532	Controller PMKID debug output indicates "No valid PMKID" but PMKID works.
CSCtg19722	MFP - Cisco 4400 Series Controller running 6.0 version detects an MFP error of 5500 running 7.0.
CSCtg23396	The command **show dhcp stats** does not display when DHCP proxy is enabled.
CSCtg35661	XML error - while netusers configured.
CSCtg42627	CLI Allows "+" (Plus Sign) In AP Group Name Breaking WLC Config via GUI.
CSCtg42711	SANITY:5500 DP unresponsive: Hardware deadlock - all Packet Buffers in use
CSCtg45014	CT5508 - CAPWAP Control traffic has incorrect DSCP marking.
CSCtg52300	CPU Hog due to tight loop in case socket() or bind() fails.
CSCtg71658	AP power level reset to 0 when upgrading from 5.0 to 6.0.196.158.
CSCtg80756	Wrong BSSID in reassociation response during intracontroller roaming if CAC/CCKM fails.
CSCtg89404	Association response is sent with AID 0.
CSCtg94715	WLC unresponsive in dtlARPTask task.
CSCth11041	The command **show cdp neighbors detail** does not display correct duplex type.
CSCth12513	LAG fail-over does not work on CT5508.
CSCth19326	Country is not lexicographically ordered.
CSCth19362	The instruction cLApEntPhysicalIndex returns 2 always.
CSCth24422	Cisco Flex 7500 Series Controller-AP "TCP Adjust MSS" value changed to 21253 in WEB GUI.
CSCth25811	Mobility anchor configuration is not displayed on GUI after config upload.
CSCth26279	Controller unresponsive when accessing 0xfefefefc while logging.
CSCth27809	Running the CLI command renders the controller unresponsive.
CSCth27835	Bootloader output on console port is incorrect.
CSCth28860	Clarify support for third party chained certificates.
CSCth30456	Need to prevent from enabling VLAN support for OEAP.

Table 7 Resolved Caveats (continued)

ID Number	Caveat Title
CSCth31542	CT5508 7.0.98.0 - **show ap crash-file** does not include a timestamp.
CSCth31652	Image predownload breaks HREAP standalone.
CSCth31837	WLC as DHCP server for AP: CoS value incorrectly processed as a VLAN.
CSCth32078	Release note for WLC 7.0.98.0 references wrong WCS version.
CSCth36045	SNMP OID is not increasing in clcrRoamReasonReport table.
CSCth38520	OfficeExtend Docs Need to Remove the WPLUS License Requirement for 7.0.
CSCth41876	AMAC: MFP - Invalid MIC error due to held beacons on the radio.
CSCth42489	Multicast traffic stops after fast roaming - incorrect AP client count.
CSCth43373	5508 running 7.0 shows Field recovery images version as N/a
CSCth51156	Extracting custom web authentication tar package may fail on 5500 WLC
CSCth54834	Update WLC dot1x message logs to provide more useful information
CSCth56224	Clients with a static IP address may get stuck in DHCP_REQD state.
CSCth59030	The AP1140 fails for radio status check task.
CSCth60816	Mesh: A MAP fails to join the WLC again if the MAP switches a RAP.
CSCth66643	Docs need to specify that after successful web auth CPU ACL's apply.
CSCth67671	AP fallback IP is not displaying in GUI
CSCth68265	Key size support for third party certificates
CSCth68708	Clients are unable to get a DHCP offer from WLC internal DHCP scope
CSCth71298	*spamApTask4: %OSAPI-5-OSAPI_INVALID_TIMER: timerlib.c:543 Failed to return.
CSCth84839	Need to document that WGB does not support DirectStream feature.
CSCth90250	WLC does not bridge DHCP NAK to station and puts it into the RUN state.
CSCth90962	Document QoS 802.1p tagging blocks traffic on untagged interfaces.
CSCth93062	WLC may hang due to kernel Oops exception.
CSCth93134	Add additional Country vs. Regulatory Domain mappings.
CSCth93785	5508WLC generate duplicate ip add message & cause connectivity issue.
CSCth95130	Release notes for upgrade path on 7.0.98.0.
CSCth95827	QoS bandwidth limiting not supported on HREAP locally switch WLANs
CSCth95889	Web GUI Help: Session & DHCP Corrections to WLANs > Edit > Advanced Page.
CSCth96194	WLC kernel hang followed by flash issue; WLC not rebooting.
CSCth96617	Native VLAN configuration is not consistent in HREAP
CSCth97629	Wrong WLC version to support for 1260/3500 series APs.
CSCth97638	Mounting bracket information references 3500 instead of 1260 AP
CSCth97643	DHCP option 60 information is incorrect for 1260 series APs.
CSCth98074	Instruction clMeshNodeBatteryChargingState OID always returns '1'.

Table 7 Resolved Caveats (continued)

ID Number	Caveat Title
CSCti00211	Association fails on hybrid REAP access point when client changes SSID.
CSCti00488	ARP entry cannot be deleted permanently in controller.
CSCti02734	Radius CallStationIdType show undefined for ap-macaddr-ssid.
CSCti04259	Intermittent webauth page with HREAP local switching.
CSCti06406	Controller GUI does note have channel bandwidth selection for sniffer mode.
CSCti06835	Multicast packets stuck on radio after WLAN changes.
CSCti08253	Controller displays IP address 0.0.0.0 when it receives packets from console.
CSCti21621	Switch CAM table not updated after L2 roam.
CSCti23852	Downstream traffic degraded with OPEN environment.
CSCti26237	Mesh AP sends all primary discovery simultaneously; causes drops.
CSCti28117	Internal DHCP in a specific case returns "wrong IP address".
CSCti34667	Cisco 5508 controller drops TCP UDP packets.
CSCti35617	Management interface does not use HSRP MAC address when replying.
CSCti36424	7925 CCKM WPA2 failure: CCKM: Failed to validate REASSOC REQ IE.
CSCti36685	The value of ifSpeed in SNMP is incorrect in Cisco 5508 Controller.
CSCti40371	CSCtg96879 is not applicable to 7.0, remove from open caveats in RN.
CSCti41854	Controller 5500 does not use LAG_MAC when LAG is enabled.
CSCti44550	Low throughput when using block ACK with low MCS rates.
CSCti45379	Cisco 5508 Controller crashes when trying to shut the data ports one by one.
CSCti45717	PMK cache must be cleared upon reception of EAP-Failure.
CSCti50119	Controller running release 5.2 and higher releases config guides need to note about CISCO CAPWAP controller.
CSCti52933	When configuring Hybrid REAP with WLAN local switching, the static IP address bypasses 'DHCP required.'
CSCti53131	Controller unresponsive while executing the **debug hreap aaa event** command.
CSCti56136	Client stuck in DHCP required state if roaming with AAA override enabled.
CSCti58705	3500 series AP unresponsive - process CAPWAP client due to a memory error.
CSCti59414	Cisco 2500 Series Controller unable to add 72 mobility group member.
CSCti69852	Controller displays XML error if ACL is changed to “none” on WLAN.
CSCti75313	TKIP MIC errors on clients connected to AP3500 due to Raw 802.3 packets.
CSCti77984	LAG failover not working on Cisco 5508 Controller for FTP traffic.
CSCti78035	Request to fix a pop up error message when handling web authentication.
CSCti79172	Security baseline violation: backup restore on unit replacement.
CSCti81590	Controller time displays one hour offset from NTP server time.

Table 7 Resolved Caveats (continued)

ID Number	Caveat Title
CSCti83830	Passive clients are unable to pass traffic on Cisco 5500 Controller. This works fine on Cisco 4400 Series Controllers.
CSCti86618	AP3500 in local mode stops servicing allowed WLANs on 2.4 GHz.
CSCti89937	Containment of rogue access point and Rogue clients is ineffective.
CSCti91044	EAP state not cleared on RADIUS failover.
CSCti91944	Unified access points remove clients on maximum retries.
CSCtj02084	Cisco Flex 7500 Series Controller unresponsive on task emWeb when a running stress test.
CSCtj05569	WLC is not releasing the BIND for the first LDAP, the next user fails authentication.
CSCtj16960	Controller with of web authentication users may go unreachable or fail to redirect client.
CSCtj20267	Clients on service port VLAN cannot reach management interface.
CSCtj20996	Controller unresponsive when using a Bluetooth console serial adapter.
CSCtj21321	AP error due to process_execute; unexpected exception to CPUvector.
CSCtj21464	WLC data plane core fails to respond due to memory corruption.
CSCtj28483	C1130 core dump: Radio command cmd 21 (FF50,0,0) status 7F17.
CSCtj33453	Controller displays the error emWeb when running 6.0.199 in disabled client page.
CSCtj39193	Controller does not allow some rogue commands via TACACS+.
CSCtj45963	Controller RADIUS accounting stop packets are sent to the wrong AAA server.
CSCtj47041	AP unresponsive and core dumps due to low memory.
CSCtj47495	Cisco 5508 Controller forwards traffic on incorrect VLAN in AP group setup.
CSCtj53304	Wrong DTIM counter value.
CSCtj55556	AP names that contain spaces are lost in upgrade from 5.2 to 7.0.
CSCtj57012	When event driven RRM works, it changes global to custom channel set.
CSCtj57086	Persistent device avoidance does not work.
CSCtj57703	Subinterface not getting an IP address leads to high CPU and incorrect configuration.
CSCtj58064	CAPWAP encap ICMP reply packet from management interface uses burned-in MAC in HSRP.
CSCtj61260	11r IE should be removed from open auth reassociation response.
CSCtj61997	Controller unresponsive while running the command **show ap eventlog**.
CSCtj71342	Controller may fail to allow incoming traffic on ingress guest LAN interface.
CSCtj72131	Controller configuration for "avoid persistent non-wifi interference" missing.
CSCtj72400	Controller SNMP entPhysicalTable not returning all devices.

Table 7 Resolved Caveats (continued)

ID Number	Caveat Title
CSCtj73291	U-APSD state machine is stuck in "active mode" - trigger frames ignored.
CSCtj79172	WMM non-compliant U-APSD client does not "trigger" without TIM.
CSCtj82323	AP 1500 Global channel setting is changed to custom after reboot.
CSCtj84836	MC2UC (Directstream) stream stops due to IGMP query timeout.
CSCtj87294	RRM Start-Up mode is invoked under unknown conditions.
CSCtj88253	Cisco 5508 Series Controller does not allow RIPv2 updates.
CSCtj94377	Various access points unresponsive from block overrun or red zone corruption.
CSCtj97821	WLC does not use a consistent MAC address for forwarding traffic.
CSCtk05220	EAPoL key timer expires incorrectly.
CSCtk12832	ARP poisoning attack from wireless client on dynamic interface.
CSCtk17467	TACACS Authorization not allowing specific user roles full privileges.
CSCtk32374	AP unresponsive on CheckAdjustTransmitRate due to packet retries of WGB.
CSCtk34586	Anchor gateway failover breaks guest client traffic.
CSCtk34829	Some incomplete commands may cause the controller to be unresponsive.
CSCtk34919	IF-MIB::ifDescr changed in release 5.2 and later.
CSCtk53570	DP crash file contains incomplete backtrace.
CSCtk60177	Cisco 4402 Series Controller running version 7.0.98.0 is unresponsive with "Out of Memory" and "mwar_exit.crash".
CSCtk60361	Default CleanAir state is wrong if 11g is disabled.
CSCtk62719	Controller msglog shows Invalid ACL ID while debugging.
CSCtk83586	Controller unresponsive when executing task dtlArpTask.
CSCtk95891	ARP poisoning on 4400 platform using static IP address.
CSCtk99624	Cisco 5500 Series controller unresponsive- Software Failed while accessing the data located at :0x59.
CSCtl04377	DHCP flooded with redundant anchors and proxy disabled.
CSCtl07274	Web auth redirect fails with Hybrid REAP local switching.
CSCtl09302	Enabling password cleartext does not display some passwords in configuration file.
CSCtl22466	WLAN anchor information does not get saved correctly in configuration file.
CSCtl41344	Hybrid REAP access point rejects reassociation request without 802.11 authentication (Status 13).
CSCtl41711	Standalone hybrid REAP does not provide 11n access.
CSCtl46842	Client LEAR IP Address and L3 policies do not work together.
CSCtl50432	Controller is unresponsive at spectrumDataTask Reason: Reaper Reset.
CSCtl67176	WiSM unresponsive reaper reset: Task "dtlDataLowTask" missed software watchdog.

Table 7 Resolved Caveats (continued)

ID Number	Caveat Title
CSCtl71583	Memory leak sshpm, on sshencode line 252.
CSCtl74406	Controller forwards traffic to the wrong VLAN for the wired WGB clients.
CSCtn02943	Controller learns an incorrect MAC for Default Gateway of management VLAN.
CSCtn03174	The command **clear arp** does not clear all ARP entries in kernel.
CSCtn04253	Radio stops transmitting for several seconds under a high load.
CSCtn14126	ARP client protection breaks DHCP address reuse.
CSCtn16281	Mesh unresponsive on BVI restart by DHCP.
CSCtn17576	VLAN jumping is possible with WGB VLAN client support feature.
CSCtn26578	Cisco 5500 Series Controller unresponsive due to memory corruption.
CSCtn27632	H-REAP access point sends incorrect RADIUS service-type to backup server.
CSCtn37462	The **command show net user summary** Does Not Show Users Past 256 Entries.
CSCtn52948	HREAP - Reached max limit on the association ID for AP.
CSCtn54009	RLDP not restoring the serving channel causes the AP to reboot.
CSCtn73474	Memory corruption with SIP inspection enabled. Crash in PMALLOC_TRAILER.
CSCtn94220	Correct configuration guides concerning service-port IP addressing.
CSCtn99092	AP1130 unresponsive - IO memory corruption caused by bad 802.11 RX frames.
CSCto08803	Controller leaking unencrypted frames for WGB clients.
CSCtj81930	AP1140 reboot by Reason: Radio Not Beaconing for too long

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*

You can access these documents from this link:

http://www.cisco.com/cisco/web/support/index.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.