Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.2.103.0

First Published: February 6, 2012
OL-26578-01

These release notes describe new features and open and resolved caveats for release 7.2.103.0 for the following hardware platforms:

- Cisco 2500, 5500 Series Controller, Cisco Wireless Services Module 2 (WiSM2), Cisco Flex 7500 Controller.
- Cisco 1040, 1130, 1140, 1240,1250, 1260, 3500, 3500p, Cisco 600 OfficeExtend Access Point, Cisco 3600, 1520, 1550 Access Point, AP801, and AP802.
- Cisco 3310, 3350, 3355, Mobility Services Engine, Virtual Appliance.

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

Contents

These release notes contain the following sections:

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

Cisco Unified Wireless Network Solution Components

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

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

- Cisco IOS Release 12.4(25e)JA
- Cisco Prime Network Control System (NCS) 1.1.0.58
- Mobility services engine software release 7.2.103.0 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 7.2.103.0* for more information.

- Cisco 3350, 3310, 3355 Mobility Services Engines, Virtual Appliance.
- Cisco 2500 Series Wireless LAN Controllers
- Cisco 5500 Series Wireless LAN Controllers
- Cisco Flex 7500 Series Wireless LAN Controllers
- Cisco Wireless Services Module 2 (WiSM2) for Catalyst 6500 Series switches
- Cisco Aironet 1550 (1552) series outdoor 802.11n mesh access points; Cisco Aironet 1520 (1522, 1524) series outdoor mesh access points; Cisco Aironet 1040, 1130, 1140, 1240, 1250, 1260, 3500e, 3500i, 3600e, and 3600i series indoor mesh access points.
- Cisco 1040, 1130, 1140, 1240,1250, 1260, 3500, 3500 P, Cisco 600 OfficeExtend Access Point, Cisco 3600, 1520, 1550, AP801, AP802.

The AP801 and AP802 are integrated access point on the Cisco 800 Series Integrated Services Routers (ISRs). For more information on the SKUs for the access points and the ISRs, refer to the following data sheets:

- AP860:
  - http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78_461543.html
- AP880:

  - http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78_459542_ps380_Products_Data_Sheet.html
  - http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78-613481.html
  - http://www.cisco.com/en/US/prod/collateral/routers/ps380/ps10082/data_sheet_c78_498096.html
  - http://www.cisco.com/en/US/prod/collateral/routers/ps380/ps10082/data_sheet_c78-682548.html
- AP890:

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

  Note The AP802 is an integrated access point on the Next Generation Cisco 880 Series Integrated Services Routers (ISRs).

Controller Platforms Not Supported for 7.2.103.0

The following controller platforms are not supported for the 7.2.103.0 release:

- Cisco 4400 Series Wireless LAN Controller
- Cisco 2100 Series Wireless LAN Controller
- Cisco Catalyst 3750G Integrated Wireless LAN Controller
- Cisco Catalyst 6500 Series/7600 Series Wireless Services Module (WiSM)
- Cisco Wireless LAN Controller Module
- Cisco Wireless Controller on Cisco Services-Ready Engine (SRE) (WLCM2) running on ISM 300, SM 700, SM 710, SM 900, and SM 910

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)

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 (7.0.220.0, 7.0.116.0, 7.0.98.0, 6.0). 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 7.2.103.0.

Scaling and Performance Enhancements for WiSM2

The following table provides details of the scaling and performance enhancements for the WiSM2 Controller.

Table 1-1 Performance and Scaling Enhancements for the WiSM2 Controller

Attribute	Supported Number in 7.0.116.0 Release	Supported Number in 7.2.103.0 Release.
Maximum Number of APs in a controller	500	1,000
Maximum Number of APs in a 6500 chassis	2,100	7,000
Maximum Number of clients in a controller	10,000	15,000
Maximum Number of Clients in a Chassis	70,000	105,000
Throughput	10 Gbps	20 Gbps

Note The minimum software version of the supervisor must be 12.2(33)SXJ2 or 15.0(1)SY1 to support the above features.

Note WiSM2 1000 AP support requires 12.2(33)SXJ2 on Sup720 and 15.0(01)SY1 on Sup2T.

Scaling and Performance Enhancements for the Cisco Flex 7500 Controller

The following table provides details of the scaling and performance enhancements for the Cisco Flex 7500 Controller.

Table 1-2 Performance and Scaling Enhancements for Cisco Flex 7500 Controllers

Attribute	Supported Number in 7.0.116.0 Release	Supported Number in 7.2.103.0 Release.
Maximum number of APs	2,000	3,000
Maximum number of clients	20,000	30,000
Maximum number of Flex Groups	500	1,000
Maximum number of OEAPs	Not Applicable	3,000
Throughput	250 Mbps	1 Gbps
DTLS support for managing OEAP	Not Applicable	Yes

IPv6/Dual Stack Client Support

This section describes new features that have been introduced as part of the IPv6 feature enhancements.

IPv6 Client Mobility

'Intelligent IPv6 Packet Processing enables seamless layer 2 and layer 3 roaming support for both dual stack and IPv6 only client. This feature enables reliable connectivity while roaming.

Note Cisco 2500 Series Controller requires Multicast-Multicast mode to be enabled with a valid Multicast IP address for IPv6 Client Support.

IPv6 Security

First-hop security features, including RA Guard automatically blocks rogue router announcements from the controller and access point. Source guard, DHCPv6 Server guard, and IPv6 Access Control List are supported in controller. This feature enables increased network availability and lower operational costs by proactively blocking known threats.

IPv6 Client Management

IPv6 addresses visibility on a per client basis, system-wide IP version distribution, and trends from NCS. This feature enables network administrators to perform IPv6 troubleshooting, address planning, client traceability, and so on from a common wired and wireless management system.

IPv6 Packet Optimization

Intelligent packet processing through NDP proxy and rate limiting of chatty IPv6 packets. This feature enables increased radio efficiency and reduces CPU utilization in the router.

TrustSec SXP Support

The TrustSec SXP protocol enables security group-based access control, which takes the network topology from the policy and reduces the number of rules to be implemented and managed. This feature enables simplified management and centralized distribution of a policy from a management server.

FlexConnect Enhancements

This section describes the new FlexConnect features.

FlexConnect Rebranding

Starting this release, the Hybrid REAPs (Hybrid Remote Edge Access Points) are referred to as FlexConnect Access Points.

FlexConnect Efficient AP Upgrade

A FlexConnect Efficient AP upgrade feature enables administrators to effectively perform AP upgrades. With this feature, one FlexConnect AP of a particular model per branch office acts as a master and downloads the image from a controller, other APs of the same model in the branch pre-download the AP image from the master.

With this feature you enable local distribution of software images from the master to other APs in a branch which speeds up the upgrade and minimizes traffic over the WAN.

FlexConnect ACLs

You can filter client traffic that is locally switched on the FlexConnect access point which enables protection and integrity of locally switched data traffic at the FlexConnect access point.

FlexConnect AAA Override

This feature allows you to dynamically assign VLANs for locally switched clients on a FlexConnect access point.

FlexConnect-Fast Roaming for Voice Clients in a FlexConnect Group

This feature removes WAN link dependency by handling mobility events at the FlexConnect access points.

FlexConnect Peer-to-Peer Blocking

With this feature, you can block peer-to-peer communication on the WLAN which limits vulnerabilities from insecure peer-to-peer client communication.

Rogue Enhancements

You can now configure a minimum RSSI value for rogue APs, configure rogue reporting intervals, configure transient rogue interval to ignore transient rogue APs, and prevent tracking friendly rogues. This feature includes advanced controls for rogue monitoring, detection, and management

Note This feature is applicable for Rogue APs only. This feature does not apply to adhoc clients.

Note Only monitor mode APs can be configured with a transient rogue interval.

Wi-Fi Direct Client Management

This feature enables network administrators to allow or block Wi-Fi direct clients from joining a WLAN. This feature can be configured on a per-WLAN basis. This feature enables a flexible architecture that supports and detect Wi-Fi direct clients, thereby preventing enterprises from being vulnerable due to this new technology.

HotSpot 2.0

This feature supports the functionalities described in the IEEE 802.11u "Interworking with External Networks" amendment. The interworking services enables a WLAN to assist mobile clients in automatic network discovery and selection by providing information about the network to the clients prior to the association.

Interworking Services enable equipment manufacturers and operators to provide standardized, interoperable components that simplify connectivity and improve services to Wi-Fi customers within the enterprise, public access, and service provider, including residential for HotSpot access (whether subscription-based or free). This feature lays the groundwork for future Wi-Fi certified passpoint certification.

ISE 1.1 Enhancements

The enhancements for ISE 1.1 for this release include support for Local Web Authentication (LWA) and Central Web Authentication (CWA). This feature enables RADIUS NAC enabled WLAN to support additional configuration using Open Authentication and MAC filtering enabling devices like smart phones and tablets to connect to the corporate wireless network. For local web authentication with RADIUS NAC, web-auth is also supported.

Adder License Without Reboot

You can now apply adder licenses without rebooting the controller.

Fast Roaming Solution With Sticky Keys

In the 7.2.103.0 release, you can configure the controller to provide faster roaming to client models from vendors such as Apple and Motorola (Fusion 3.0) that support WPA2 PKC (SKC) roaming.

Note Apple Wireless client drivers (iOS version 5.0 at the time of writing) support Sticky Key Caching (SKC) but do not support Opportunistic Key Caching (OKC). Motorola wireless client drivers, Fusion version 3.0 and above, support Sticky Key Caching. Opportunistic Key Caching (OKC) is supported in Fusion version 3.40 and above.

KTS-Based CAC Support for NEC

Key Telephone System (KTS)-based CAC is a protocol that is used in NEC MH240 wireless IP telephones. You can configure the controller to support CAC on KTS-based SIP clients to process bandwidth request messages from clients, to allocate the required bandwidth on the AP radio, and to handle other messages that are part of the protocol.

Cisco 600 OEAP Access Point Enhancements

The following new features have been added to the Cisco 600 OEAP Access Points.

Configurable Controller-wide Usage

This release enables network administrators to enable or disable the usage of the Cisco 600 Series OEAP access points using the following command:

config network oeap-600 local-network {**enable** | **disable**}

When enabled, the local SSIDs, local ports are inoperative; and the console is not accessible. When reset, the default restores local access. This configuration does not affect the remote-LAN configuration if configured on the access point.

Configurable Power and Channel Width on 2.4 and 5 GHz

It is now possible to configure the power, channel, and channel width parameters for Cisco 600 OEAP Access Points on both 2.4 GHz and 5 GHz radios.

Dual R-LAN Support

This release provides dual RLAN support on Cisco 600 OfficeExtend Access Points. A new, CLI-only based functionality is added in which the port 3 also functions as a remote LAN port. This configuration is global to the controller and is stored by the AP and the NVRAM variable. When this variable is set, the behavior of the remote LAN is changed. This feature supports different remote LANs per remote LAN port.

The following command is added:

config network oeap-600 dual-rlan-ports {**enable** | **disable**}

If you use an AP group, the mapping to the OEAP-600 ports is determined by the AP-group ordering. To use an AP group, you must first delete all remote-LANs and WLANs from the AP-group leaving it empty. Then add the two remote-LANs to the AP group, adding the port 3 AP remote-LAN first, and the port 4 remote group second, followed by any WLANs. If a group is not used, the remote-LAN configuration with an even RLAN ID control the port 4 on the access point, and remote-LAN configurations with an odd RLAN ID control the port 3.

AP Groups and RF Profiles

This feature enables you to tune groups of APs that share a common coverage zone together and selectively change how RRM operates the APs within that coverage zone.

For example, a university might deploy a high density of APs, in an area where a high number of users will congregate or meet. This situation requires that you manipulate both data rates and power to address the cell density while managing the co-channel interference. While in adjacent areas, normal coverage is provided and such manipulation would result in a loss of coverage.

Using RF profiles and AP groups allow you to optimize the RF settings for AP groups that operate in different environments or coverage zones. RF profiles are created for 802.11b/g/n or 802.11a/n radios. RF profiles are applied to all APs that belong to an AP group, where all APs in that group will have the same profile settings.

The RF profile gives you control over the data rates and power (TPC) values.

Note The application of an RF profile does not change the AP's status in RRM. It is still in global mode configuration controlled by RRM.

Note An AP that has a custom power setting applied for AP power is not in global mode configuration, an RF profile has no effect on this AP. For RF profiling to work; all APs must have their channel and power managed by RRM.

CleanAir Enhancements

As part of the CleanAir Phase 2 Enhancements, the following functionalites are added to the controller software in this release:

- Persistent Device avoidance
  - Minimize use of channels affected by persistence interference.
  - Persistent Device detected by local and monitor mode AP propagated to both CleanAir and non-CleanAir APs.
- Custom Event Driven RRM Threshold—Ability for the radio to change channel in reaction to strong interference reported in form of Air Quality Index.
- Air Quality Unclassified—New alarm triggered by the severity of unclassified category going above a configured threshold.

Enhanced Quality of Service Prioritization

This release offers increased flexibility for QoS priority for unicast and multicast traffic on a per-WLAN basis within the access point.

Video Client Scaling

This release provides enhanced scaling of client devices that stream video, along with mixed voice and data client traffic in the access point.

StadiumVision Multicast

This feature introduces multicast enhancements to increase the scale and overall throughput of multicast sessions supported equating to video streams.

Indoor Wireless Mesh

This release enables Indoor Wireless Mesh support on the Cisco 3600 Access Points.

Ability to Support CAPWAP on Cisco 600 OfficeExtend Access Points

The release supports CAPWAP (secure enterprise access) on a second wired port on a Cisco 600 OfficeExtend access points. Earlier releases supported CAPWAP on a single port.

Online Certificate Status Protocol

The Online Certificate Status Protocol (OCSP) feature provides certificate revocation checking in environments where loading Certificate Revocation Lists (CRL) is not feasible because of the size of the CRL. When a management user accesses the controller GUI using HTTPS, OCSP is used by the controller to get the revocation status of the management user's certificate from an OCSP responder. When OCSP is enabled on the controller, it is mandatory for the management users to have a certificate while accessing the GUI through HTTPS. If a certificate is not present or has been revoked by the Certification Authority, then the management user will not be able to login.

OCSP is supported on the following platforms: Cisco 5508 Controller and WiSM2.

DHCP Option 82

In previous releases, the DHCP Option 82 information was sent in binary format. In this release, DHCP Option 82 information is sent in ASCII format.

802.1X Support in Central Switched Mode

In this release, WLANs that are configured with 802.1X security can work in central switching mode on Cisco Flex 7500 Series Controllers.

VLAN Changes

VLAN Select Feature Changes

The VLAN select feature enables you to use a single WLAN that can support multiple VLANs. Clients can get assigned to one of the configured VLANs. This feature enables you to map a WLAN to a single or multiple interface VLANs using interface groups.

In previous release, wireless clients associated to the WLAN by obtaining an IP address from the pool of subnets using a round-robin algorithm. In this release, the wireless clients that associate to the WLAN get an IP address from a pool of subnets based on the MAC address of the wireless client.

AAA Override Support for Interface Groups

This release supports AAA override for interface groups.

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

Native VLAN Enhancements

In the controller releases prior to 7.2, the Root Access Point (RAP) native VLAN is forwarded out of Mesh Access Point (MAP) Ethernet ports with Mesh Ethernet Bridging and VLAN Transparent enabled.

In the 7.2 and later controller releases, the Root Access Point (RAP) native VLAN is not forwarded out of Mesh Access Point (MAP) Ethernet ports with Mesh Ethernet Bridging and VLAN Transparent enabled.

This change in behavior increases reliability and minimizes the possibility of forwarding loops on Mesh Backhauls.

Support for Open Security WLAN With EAP Passthrough

In this release, you can configure open security WLAN to pass (or forward) the EAP frames to an external authenticator behind the controller. When this feature is enabled on the WLAN, the controller does not act as authenticator; an external device acts as the authenticator.

RFC 2869 Conformity

The RADIUS accounting has been enhanced to meet the RFC 2869 requirement. The following attributes have been included in the list of AAA attributes:

- Acct-Input-Gigawords
- Acct-Output-Gigawords
- Event-Timestamp

Support for APs behind NAT

In the 7.2.103.0 release, you can deploy up to 3 OfficeExtend access points (OEAPs) behind a NAT device. You can deploy up to 50 FlexConnect access points (with or without Data DTLS) behind a NAT device.

Changes to ClientLink Configuration

With the 7.2 release, it is possible to configure ClientLink (beamforming) only using the controller CLI. It is not possible to configure ClientLink (beamforming) using the controller GUI.

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. We recommend that you install the latest software version available for maximum operational benefit. See "FlexConnect Efficient AP Upgrade" section on page 6.

Guidelines and Limitations

- Cisco 860 ISR is not supported as an access point in a unified wireless deployment.
- If you are using a Cisco 880 ISR, you must use Cisco IOS Release 12.4(20)T or later releases with an advanced IP services license.

- If you are using a Cisco 890 ISR, you must use Cisco IOS Release 12.4(22)YB or later releases. The advanced IP service license is enabled by default on Cisco 890 ISR.

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 7.2.103.0

Before upgrading your controller to software release 7.2.103.0, you must comply with the following rules:

- Make sure that you have a TFTP or FTP server available for the software upgrade. Follow these guidelines when setting up a TFTP or FTP server:
  - Controller software release 7.2.103.0 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 NCS. If you attempt to download the 7.2.103.0 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 NCS because the NCS 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 7.2.103.0. Table 1-3 shows the upgrade path that you must follow before downloading software release 7.2.103.0.
- Before you use an AP802 series lightweight access point with controller software release 7.2.103.0, 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.
- 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 7.2.103.0 software. In large networks, it can take some time to download the software on each access point.
- If you upgrade to the controller software release 7.2.103.0 from an earlier release, you must also upgrade to NCS 1.1.0.58 and MSE to 7.2.103.0.
- Field Upgrade Software (FUS) is a special AES package that contains several system related component upgrades. These include the bootloader, field recovery image, and FPGA/MCU firmware. Installing the FUS image requires special attention because it installs some critical firmware. The FUS image is independent of the runtime image. FUS version 1.7.0.0 can be used for the 7.2.103.0 release. For more information, see the "Installing Field Upgrade Software" section on page 21.

- You cannot upgrade or downgrade a new image if FIPS is enabled.
- 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 intranet IP address of a controller 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 tries to join the non-NAT IP address, fails to join, and tries a rediscovery that fails again. The OEAP can never connect to the controller.

  The issue can be resolved by setting the access point mode to local mode on the controller and let the access point join the controller. On joining, you must disable Least Latency Join option and upgrade to 7.0.116.0 release.
- If you require a downgrade from one release to another, you might lose the configuration from your current release. The workaround is to reload the previous controller configuration files saved on the backup server or to reconfigure the controller.
- Control which address(es) are sent in CAPWAP discovery responses when NAT is enabled on the Management Interface using the following command:

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

  Where:

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

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

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

- You can configure 802.1p tagging by using the **config qos dot1p-tag** {**bronze** | **silver** | **gold** | **platinum**} tag. For the 7.2.103.0 release, if you tag 802.1p packets, the tagging has impact only on wired packets. Wireless packets are impacted only by the maximum priority level set for QoS.

Table 1-3 Upgrade Path to Controller Software Release 7.2.103.0

Current Software Release	Upgrade Path to 7.2.103.0 Software
6.0.182.0 or later 6.0 release	You can upgrade directly to 7.2.103.0
7.0.98.0	You can upgrade directly to 7.2.103.0
7.0.98.218	You can upgrade directly to 7.2.103.0
7.0.116.0	You can upgrade directly to 7.2.103.0
7.0.220.0	You can upgrade directly to 7.2.103.0
7.0.230.0	You can upgrade directly to 7.2.103.0

Table 1-3 Upgrade Path to Controller Software Release 7.2.103.0

Current Software Release	Upgrade Path to 7.2.103.0 Software
7.0.235.0	You can upgrade directly to 7.2.103.0
7.1.91.0	You can upgrade directly to 7.2.103.0

Software Release Support for Access Points

Table 1-4 lists the controller software releases that support specific Cisco access points. The First Support column lists the earliest controller software release that supports the access point. For access points that are not supported in ongoing releases, the Last Support column lists the last release that supports the access point.

Table 1-4 Software Support for Access Points

Access Points		First Support	Last Support
1000 Series	AIR-AP1010	3.0.100.0	4.2.207.0
	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
1130 Series	AIR-LAP1131	3.1.59.24	—
1140 Series	AIR-LAP1141N	5.2.157.0	—
	AIR-LAP1142N	5.2.157.0	—
1220 Series	AIR-AP1220A	3.1.59.24	7.0.x
	AIR-AP1220B	3.1.59.24	7.0.x
1230 Series	AIR-AP1230A	3.1.59.24	7.0.x
	AIR-AP1230B	3.1.59.24	7.0.x
	AIR-LAP1231G	3.1.59.24	7.0.x
	AIR-LAP1232AG	3.1.59.24	7.0.x
1240 Series	AIR-LAP1242G	3.1.59.24	—
	AIR-LAP1242AG	3.1.59.24	—
1250 Series	AIR-LAP1250	4.2.61.0	—
	AIR-LAP1252G	4.2.61.0	—
	AIR-LAP1252AG	4.2.61.0	—
1260 Series	AIR-LAP1261N	7.0.116.0	—
	AIR-LAP1262N	7.0.98.0	—
1300 Series	AIR-BR1310G	4.0.155.0	7.0.x
1400 Series	Standalone Only	N/A	—

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

Access Points		First Support	Last Support
3500 Series	AIR-CAP3501E	7.0.98.0	—
	AIR-CAP3501I	7.0.98.0	—
	AIR-CAP3502E	7.0.98.0	—
	AIR-CAP3502I	7.0.98.0	—
	AIR-CAP3502P	7.0.116.0	—
3600 Series	AIR-CAP3602I-x-K9	7.1.91.0	—
	AIR-CAP3602I-xK910	7.1.91.0	—
	AIR-CAP3602E-x-K9	7.1.91.0	—
	AIR-CAP3602E-xK910	7.1.91.0	—
Note The Cisco 3600 Access Point was introduced in 7.1.91.0. If your network deployment uses Cisco 3600 Access Points with release 7.1.91.0, we highly recommend that you upgrade to 7.2.103.0.			
1500 Mesh Series	AIR-LAP-1505	3.1.59.24	4.2.207.54M
	AIR-LAP-1510	3.1.59.24	4.2.207.54M

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

Access Points		First Support	Last Support
1520 Mesh Series	AIR-LAP1522AG	-A and N: 4.1.190.1 or 5.2 or later[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-LAP1522HZ	-A and N: 4.1.190.1 or 5.2 or later[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-LAP1522PC	-A and N: 4.1.190.1 or 5.2 or later[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-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	—
1552S	AIR-CAP1552SA-x-K9	7.0.220.0	—
	AIR-CAP1552SD-x-K9	7.0.220.0	—

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

Interoperability With Other Clients in 7.2.103.0

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

Table 1-5 describes the configuration used for testing the clients.

Table 1-5 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	7.2.103.0
Controller	Cisco 5500 Series Controller
Access points	1131, 1142, 1242, 1252, AP 3500e and AP3500i, AP3600
Radio	802.11a, 802.11g, 802.11n2, 802.11n5
Security	Open, WEP, PSK (WPA and WPA2), 802.1X (WPA-TKIP and WPA2-AES) (LEAP, PEAP, EAP-FAST, EAP-TLS)
RADIUS	ACS 4.2, ACS 5.2
Types of tests	Connectivity, traffic, and roaming between two access points

Table 1-6 lists the versions of the clients. The traffic tests included data or voice. The clients included laptops, handheld devices, phones, and printers.

Table 1-6 Client Type

Client Type and Name	Version
Laptop	
Intel 3945/4965	11.5.1.15 or 12.4.4.5, v13.4
Intel 5100/5300/6200/6300	v14.3.0.6
Intel 1000/1030/6205	v14.3.0.6
Dell 1395/1397/Broadcom 4312HMG(L)	XP/Vista: 5.60.18.8 Win7: 5.30.21.0
Dell 1501 (Broadcom BCM4313)	v5.60.48.35/v5.60.350.11
Dell 1505/1510/Broadcom 4321MCAG/4322HM	5.60.18.8
Dell 1520/Broadcom 43224HMS	5.60.48.18
Dell 1530 (Broadcom BCM4359)	v5.100.235.12
Cisco CB21	v1.3.0.532
Atheros HB92/HB97	8.0.0.320
Atheros HB95	7.7.0.358
MacBook Pro (Broadcom)	5.10.91.26
Handheld Devices	
Apple iPad	iOS 5.0

Table 1-6 Client Type (continued)

Client Type and Name	Version
Apple iPad2	iOS 5.0
Motorola Xoom	Android 3.1
Intermec CK70	Windows Mobile 6.5 / 2.01.06.0355
Intermec CN50	Windows Mobile 6.1 / 2.01.06.0333
Symbol MC5590	Windows Mobile 6.5 / 3.00.0.0.051R
Symbol MC75	Windows Mobile 6.5 / 3.00.2.0.006R
Phones and Printers	
Cisco 7921G	1.4.1SR1.LOADS
Cisco 7925G	1.4.1SR1.LOADS
Ascom i75	1.8.0
Spectralink 8030	122.023
Spectralink i640/PTX110	110.036/091.047/104.025
Vocera B1000A	4.1.0.2817
Vocera B2000	4.0.0.345
Apple iPhone4	iOS 5.0.1
Ascom i62	2.2.21
HTC Legend	Android 2.2
HTC Sensation	Android 2.3.3
LG Optimus 2X	Android 2.2.2
Motorola Milestone	Android 2.2.1
RIM Blackberry Pearl 9100	WLAN version 4.0
RIM Blackberry Bold 9700	WLAN version 2.7
Samsung Galaxy S II	Android 2.3.3
SpectraLink 8450	3.0.2.6098/5.0.0.8774

Special Rules for Upgrading to Controller Software 7.2.103.0 in Mesh Networks

Before upgrading your controller to software release 7.2.103.0 in a mesh network, you must comply with the following rules.

Upgrade Compatibility Matrix

Table 1-7 outlines the upgrade compatibility of controller mesh and nonmesh releases and indicates the intermediate software releases required as part of the upgrade path.

Table 1-7 Upgrade Compatibility Matrix for Controller Mesh and Nonmesh Releases from 6.0 Release and Later Releases

Upgrade to / Upgrade from	7.2.103.0	7.1.91.0	7.0.230.0	7.0.220.0	7.0.116.0	7.0.98.218	7.0.98.0	6.0.202.0	6.0.199.0	6.0.196.0	6.0.188.0	6.0.182.0
7.2.103.0												
7.1.91.0	Y		N	N	N	N	N	N	N	N	N	N
7.0.230.0	Y	N										
7.0.220.0	Y	N	Y									
7.0.116.0	Y	N	Y	Y								
7.0.98.218	Y	N	Y	Y	Y							
7.0.98.0	Y	N	Y	Y	Y	Y						
6.0.202.0	Y	N	Y	Y	Y	Y	Y					
6.0.199.0	Y	N	Y	Y	Y	Y	Y	Y				
6.0.196.0	Y	N	Y	Y	Y	Y	Y	Y	Y			
6.0.188.0	Y	N	Y	Y	Y	Y	Y	Y	Y	Y		
6.0.182.0	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	

Upgrading to a New Software Release

When you upgrade to the latest software release, the software on the access points associated with the controller is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession.

Guidelines and Limitations

- Predownloading a 7.2.103.0 version on a Cisco Aironet 1240 access point is not supported when upgrading from a controller version prior to 7.2.103.0. If predownloading is attempted to a Cisco Aironet 1240, an AP disconnect will occur momentarily.
- The Cisco 5500 Series Controllers can download the 7.2.103.0 software to 500 access points simultaneously.
- Do not power down the controller or any access point during the upgrade process; otherwise, you might corrupt the software image. Upgrading a controller with a large number of access points can take as long as 30 minutes, depending on the size of your network. However, with the increased number of concurrent access point upgrades supported, the upgrade time should be significantly reduced. The access points must remain powered, and the controller must not be reset during this time.
- If you want to downgrade from the 7.2.103.0 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.
- If you are using the controller software release 7.2.103.0 and if you have configured multicast interfaces, do not use the same configuration file for the 7.0.98.0 release. Using the 7.2.103.0 configuration file with multicast interfaces in the 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 7.2.103.0 controller software:

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

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

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

c. Click **Wireless LAN Controllers**.

   The following options are available:

   - Integrated Controllers and Controller Modules
   - Standalone Controllers

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

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

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

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

g. Click a software release number.

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

i. Click **Download**.

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

k. Save the file to your hard drive.

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

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

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

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

Step 5 Disable any WLANs on the controller.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 19 Reenable the WLANs.

Step 20 For Cisco WiSM2, reenable the controller port channel on the Catalyst switch.

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

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

Step 23 To verify that the 7.2.103.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

Installing Field Upgrade Software

Information About Field Upgrade Software

Field Upgrade Software (FUS) is a special AES package that performs various system-related component upgrades. We recommend that you perform an FUS upgrade (if needed) to upgrade components such as the bootloader, field recovery image, FPGA/MCU, and other firmware to their latest respective versions.

Note On Cisco 5500 Series Controllers, it is observed that the controller sporadically reboots (bug CSCtr39523) and displays the following FPGA error message:

```
fpga: Lost heartbeat from Environment controller, system will reboot in 5 seconds!!!
```

A crash file is not created to debug or troubleshoot the error.)

You can resolve this issue by upgrading to FUS 1.7.0.0 or greater. For more information on the FUS upgrade, see http://www.cisco.com/en/US/docs/wireless/controller/release/notes/fus_rn_1_7_0_0.html

Guidelines and Limitations

Caution Ensure that there are no power outages during the upgrade. Power outages during the upgrade may lead to the controller not being usable.

- FUS is applicable only to the following controller platforms:
  - Cisco 5500 Series Wireless LAN Controller
  - Cisco Flex 7500 Controller
  - Cisco Wireless Services Module 2 (WiSM2)
- You do not need to install FUS if you have a Cisco 2500 Series Controller platform.
- You must install FUS only once.
- The controller must be connected to a console during the upgrade.
- After you install FUS for a Cisco Flex 7500 Controller platform, the RAID firmware is also upgraded. During the installation process, the console messages displayed do indicate upgrade of the RAID firmware. However, it is not possible to verify the RAID firmware upgrade either by entering a command or viewing the bootlog.

Downloading Field Upgrade Software

Step 1 Go to the Cisco Software Center at this URL: http://www.cisco.com/cisco/software/navigator.html

Step 2 Choose **Products > Wireless > Wireless LAN Controller**.

Step 3 Choose either of the following depending on the controller platform you use:

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

Step 4 Choose the controller model number or name. The **Download Software** page is displayed.

Step 5 Choose **Wireless LAN Controller Software**.

Step 6 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.

Step 7 Click a software release number. Click the filename (*filename*.aes). The following AES files are available for various controller platforms:

- AIR-CT5500-K9-7-2-103-0-FUS.aes
- AIR-CT5500-LDPE-K9-7-2-103-0-FUS.aes
- AIR-WISM2-K9-7-2-103-0-FUS.aes
- AIR-CT7500-K9-7-2-103-0-FUS.aes

Step 8 Click **Download**.

Step 9 Read Cisco's End User Software License Agreement and then click **Agree**.

Step 10 Save the file to your hard drive.

Step 11 Copy the AES file (*filename*.aes) to the default directory on your TFTP or FTP server.

Installing Field Upgrade Software

Step 1 Enter the following commands on the controller CLI:

a. **transfer download datatype code**
b. **transfer download serverip** *serverip*
c. **transfer download mode** {**tftp** | **ftp**}
d. **transfer download username** *user*
e. **transfer download password** *password*
f. **transfer download filename** *filename.aes*
g. **transfer download path /**
h. **transfer download start**

Step 2 Enter the following command to reboot the controller:

reset system

Information similar to the following appears:

```
WLCNG Boot Loader Version 1.0.1 (Built on Apr 11 2009 at 13:32:33 by cisco)
Board Revision 1.3 (SN: FCW1435L0ES, Type: AIR-CT5508-K9) (G)

Verifying boot loader integrity... OK.

OCTEON CN5645-NSP pass 2.1, Core clock: 600 MHz, DDR clock: 330 MHz (660 Mhz data rate)
FPGA Revision 1.3
Env FW Revision 1.6
USB Console Revision 1.27
DRAM:  1024 MB
Flash: 32 MB
Clearing DRAM........ done
Network: octeth0', octeth1
  ' - Active interface
```

```
  E - Environment MAC address override
CF Bus 0 (IDE): OK
IDE device 0:
 - Model: VM DFC 1GB Firm: 20090819 Ser#: VM1GB       00001925
 - Type: Hard Disk
 - Capacity: 967.6 MB = 0.9 GB (1981728 x 512)


Press <ESC> now to access the Boot Menu...

Loading backup image (Image not found)

** Unable to read "linux.bak.img" from ide 0:2 **
** Launch failure  **

Loading primary image (7.0.120.0)
0%      1%      2%      3%      4%      5%      6%      7%      8%      9%     10%     11%
12%     13%     14%     15%     16%     17%     18%     19%     20%     20%     21%
22%     23%     24%     25%     26%     27%     28%     29%     30%     31%     32%
33%     34%     35%     36%     37%     38%     39%     40%     41%     41%     42%
43%     44%     45%     46%     47%     48%     49%     50%     51%     52%     53%
54%     55%     56%     57%     58%     59%     60%     61%     61%     62%     63%
64%     65%     66%     67%     68%     69%     70%     71%     72%     73%     74%
75%     76%     77%     78%     79%     80%     81%     82%     82%     83%     84%
85%     86%     87%     88%     89%     90%     91%     92%     93%     94%     95%
96%     97%     98%     99%     100%

6012820 bytes read
Launching...
init started: BusyBox v1.6.0 (2010-05-13 17:50:10 EDT) multi-call binary
starting pid 821, tty '': '/etc/init.d/rcS'

Field Upgrade Software

Bundles included in this upgrade:

    - FPGA image
    - Environment Controller (MCU) Image
    - USB Console image

****************************************************************
* Please make sure POWER SUPPLY is always ON during this period. *
* Lost POWER will completely kill this unit and not recoverable. *
* There may be multiple reboot. Please let the program run.      *
****************************************************************
Start soon ...

====================
Checking for FPGA upgrade

FPGA upgrade ...

Upgrading FPGA from rev 1.3 to rev 1.7
****************************************************************
* Upgrade takes about 75 seconds to complete.                  *
* Please make sure POWER SUPPLY is always ON during this period. *
* Lost POWER will completely kill this unit and not recoverable. *
****************************************************************

Are you sure you want to proceed with upgrade (y/N) ? y
```

Step 3 Press **y** to continue.

The controller reboots with the upgraded component.

Step 4 The controller might undergo multiple reboot cycles to upgrade all the components. Press **y** when you are prompted to reboot the controller. After all the components are upgraded, the controller reboots with the existing controller software version.

Verifying the Upgraded Components

On the controller CLI, enter the following command to verify the upgraded components:

show sysinfo

Information similar to the following appears

```
. . . .
. . . .
Firmware Version.............................. FPGA 1.7, Env 1.8, USB console 2.2
. . . .
. . . .
```

Installation Notes

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

Warnings

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

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

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

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

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

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

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

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

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

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

Safety Information

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

FCC Safety Compliance Statement

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

Safety Precautions

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

1. If you are installing an antenna for the first time, for your own safety as well as others, seek professional assistance. Your Cisco sales representative can explain which mounting method to use for the size and type of antenna you are about to install.

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

Installation Instructions

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 installed by experts.

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

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

Using the Controller USB Console Port for Cisco 5500 and WiSM2

The USB console port on the Cisco 5500 Series Controllers and the Cisco WiSM2 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.

You can now remove your console cable and plug it back in again without having to quit the terminal program and restarting it.

USB Console OS Compatibility

The USB console drivers are available for Microsoft Windows (both 32 and 64-bit architectures), Apple Mac OS, and Linux. Please refer to the README PDF files in the USB Console Driver.zip package for installation instructions.

For more information on the versions of the operating systems supported, see http://www.cisco.com/en/US/docs/routers/access/1900/hardware/installation/guide/19cblspc.html#wp1054350.

To download and configure the Cisco Windows USB console driver, follow these steps.

Step 1 Download the driver from the download page:

a. Go to the software download page at:

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

b. Choose **Products > Wireless > Wireless LAN Controller > Standalone Controllers > Cisco 5500 Series Wireless Controllers**

Note The USB Console Port Driver Software is also applicable to the Cisco WiSM2.

c. Click the Download Now button to download the USB Console Port Driver Software.

Step 2 Save the file to your hard drive.

Step 3 Extract the .zip file and install the driver depending on the operating system you are using.

Note Instructions for installing the USB console port software for Apple Mac OS and Linux are provided in the downloadable zip file.

Step 4 Connect the mini Type B connector to the USB console port on the controller.Connect the Type A connector to a USB port on your PC.

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.

Base Licensing

Starting 7.2.103.0 release, the controller software does not require base licensing to work. All features are included in active state along with the software image.

One-Time Password (OTP) Support

One Time Passwords (OTPs) 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 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.

Disable Options That Require Network for A and G

Listing options that require network for A and G needs to be disabled before configuring any of these parameters: Country code, QoS profile, enabling/disabling channels from DCA, coverage, DTPC, channel width, 802.11h global parameters, EDCA profile, media config—media, voice, video, and CAC.

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.

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 2500 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 2500 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

Learn more about inter-release controller mobility compatibility across releases at this URL

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

RLDP Limitations

The Rogue Location Discovery Protocol (RLDP) is a controller feature that detects the presence of rogue access points that are connected to your wired network. 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, RLDP works when the managed access point is a monitor mode AP on a DFS channel.

Internal DHCP Server

When clients use the internal DHCP server of the controller, 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 See 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.

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 connect to an access point but cannot pass traffic. When you configure the controller for 802.11g traffic only, you must mark 11g rates as mandatory.

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 external web authentication redirects to HTTPS (HTTP over SSL) servers.

Note For Cisco 5500 Series Controllers, Cisco 2500 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 Cisco Aironet 1250 Series Access Points

The 1250 series access points might 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)
```

Issues with APs That Transmit Multicast Frames at Highest Configured Basic Rate and Management Frames with Lowest Basic Rates

Access points running recent Cisco IOS versions transmit multicast frames at the highest configured basic rate and management frames at the lowest basic mandatory rates, 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 might fail to be received.

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

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

- 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, 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, you can 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 release, 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 –1 dBm to 30 dBm.

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 controllers forwarding (multicast or otherwise) and multicast replication is 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 releases 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 enables 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 that use MAC filtering do not need to obtain an IP address through DHCP to be added to the controller's client table.

Controller software releases 7.0.116.0 provide the passive client feature for Cisco 2500 and 5500 Series Controllers that enable devices like printers connected to WGB to hear ARP requests, answer and move to run state. That is a dynamic alternative that replaces the MAC filter.

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 correctly. Set the current date and time on the controller before allowing the access points to connect to it.

Synchronizing the Controller and Location Appliance

If a location appliance (release 3.1 or later release) 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 7.2,* for instructions for setting the time and date on the controller.

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

FCC DFS Support on 1130 Series Access Points

Federal Communications Commission (FCC) dynamic frequency selection (DFS) is supported only on 1130 series access points in the United States, Canada, and the Philippines that have a new FCC ID. Access points use DFS to detect radar signals such as military and weather sources and then switch channels to avoid interfering with them. 1130 series access points with FCC DFS support have an FCC ID *LDK102054E* sticker. 1130 series access points without FCC DFS support have an *LDK102054* (no

E suffix) sticker. 1130 series access points that are operating in the United States, Canada, or the Philippines; have an FCC ID *E* sticker; and are running the 6.0 software release or later can use channels 100 through 140 in the UNII-2 band.

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-W switch with Power over Ethernet (PoE) by entering this command:

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

A Cisco prestandard 15-W switch does not support intelligent power management (IPM) but does have sufficient power for a standard access point. The following Cisco prestandard 15-W 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-W 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-W 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 for the changes to take effect:

- Enable or disable link aggregation (LAG)
- Enable a feature that is dependent on certificates (such as HTTPS and web authentication)

- Changes made to the virtual IP Interface address
- Changes made to the controller settings for web authentication.

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

ICMP pings to the management interface either from a wireless client or a wired host is supported. 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 might 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 by 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 7.0.220.0 is compatible with the Gateway Load Balancing Protocol (GLBP).

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 must ensure that only authorized clients gain access to the management network through proper CPU ACLs, 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, if 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 are 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, see *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. If you use RADIUS interface override (using the command **config wlan radius_server overwrite-interface**), you can connect to the dynamic interface to the server.

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 might 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, We strongly advise that you change these values. See the *Cisco Wireless LAN Controller Configuration Guide, Release 7.2,* for configuration instructions.

Changing the Default Values for SNMP v3 Users

The controller uses a default value of "default" for the username, authentication password, and privacy password for SNMP v3 users. Using these standard values presents a security risk. Therefore, we strongly advise that you change these values. See the *Cisco Wireless LAN Controller Configuration Guide, Release 7.2,* for configuration instructions.

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

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.

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

Note Directly connected APs are supported only in Local mode.

Features Not Supported on WiSM2 and Cisco 5500 Series Controllers

These software features are not supported on Cisco 5500 Series Controllers:

- Static AP-manager interface

  Note For Cisco 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)

Features Not Supported on Cisco Flex 7500 Controller

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
- TrustSec SXP
- IPv6/Dual Stack client Support
- WGB
- HotSpot2.0 (802.11u)
- Client rate limiting for centrally switched clients
- Access points in local mode
- Internal DHCP server

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

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

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

In a crowded RF environment, clients might 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.

Upgrading External Web Authentication

1. For Cisco 5500 Series Controllers, 2500 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. The network manager must use the new `login_template` shown here as follows:

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>
```

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 FlexConnect mode works only with the following authentication or key management combinations:

- WPA2+AES
- WPA+TKIP

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

- WPA+AES
- WPA2+TKIP

Errors When Using AAA with an 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 a fallback, which might be dropped by the RADIUS Server. The controller cannot send accounting information with the session ID because during the fallback the controller does not have the context of the client. Some RADIUS Servers like ISE might report errors for accounting probes that are sent to ISE. If your Authentication and Accounting servers are the same, ignore the errors that are logged in ISE.

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 the dynamic AP management interface. This situation is applicable only for Cisco 5500 Series Controllers. NAT 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.

Enforce a minimum configured data rate

24Mbps is always enabled even if you select OFDM rates that are less than 24Mbps.

Important Notes for Controllers and Mesh Access Points

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

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

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

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

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

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

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

Open Caveats

Table 1-8 lists open caveats in controller software release 7.2.103.0.

Table 1-8 Open Caveats

ID Number	Description

CSCua43558	Controller does not respond during a task with IPv6 traffic.
	Symptom: Controller might unexpectedly reboot with crash information that is similar to the following:
	`Analysis of Failure:`
	`Software was stopped for the following reason:`
	`pmalloc detected memory corruption`
	`---`
	`pmalloc memory corruption type: ++PMALLOC_POISONED_AREA_CORRUPTION`
	`- Corruption detected at pmalloc entry address: (1cd15914)`
	`- Corrupt entry: entryMagic_0(0xbe90be90), entryMagic_1(0xbe91be91), trailer(0xead0ead0),poison(0xcc00ffed)`
	Conditions: Controller is handling IPv6 traffic.
	Workaround: None.

CSCtx64420	Error message appears when Cisco 2500 Wireless Controller and Cisco Flex 7500 Controller are unconfigured for the first time. `"FP0.00:(54)[cmdAddMcastRgTun:5037]failed to create mcast rg tun 0 ifTun=3130 NO TUNNEL FOUND"` **Symptom**: The following error message appears on the console when a Cisco 2500 Wireless Controller and Cisco Flex 7500 Controller is unconfigured for the first time: `"FP0.00:(54)[cmdAddMcastRgTun:5037]failed to create mcast rg tun 0 ifTun=3130 NO TUNNEL FOUND"` **Condition**: This message appears only once when the controller is unconfigured using the **clear config** command. This error message may appear when the default multicast mode is mulitcast-multicast. On a Cisco 5500 Series Controller and WiSM2 this message does not occur because the default multicast mode is unicast. This message appears only when the controller boots for the first time after the **clear config** command is used and when the management IP is not configured. **Workaround**: This error does not affect the normal functionality of the controller. This message disappears when the controller is configured using the GUI configuration wizard.

Table 1-8 Open Caveats (continued)

ID Number	Description
CSCtr70376	Access Point Group Profile when uploaded using the TFTP does not contain the RF Profile information. **Symptom**: The AP group profile configuration upload does not contain RF profile information. **Conditions**: RF profile information is unavailable when the user uploads the configuration. **Workaround**: Use the XML configuration file to upload the configuration. The RF profile information is in this file. The missing commands in the configuration file can also be manually entered from the command prompt or configured from the user interface.
CSCtw65316	LAG with CDP does not show all the physical ports correctly. **Symptom**: CDP neighbors on the switch do not display correct port information. **Conditions**: LAG is enabled on the controller and CDP is enabled on both sides. **Workaround**: None.
CSCtx27591	Duplex or Speed settings are lost on reload if AP has static IP address. **Symptom**: The AP cannot be configured with static speed or duplex settings. The interface settings are lost on a reload. **Conditions**: This issue is seen when the access point has a static IP address. **Workaround**: Use DHCP.

CSCts50317	Idle status is displayed when you run the **show client ap 802.11b** *AP Name* remains permanently
	Symptom: An access point displays the idle status until an AP reboot.
	`(Cisco Controller) >show client ap 802.11b <AP Name>`
	`MAC Address  AP Id  Status  WLAN Id  Authenticated`
	`xx:xx:xx:xx:xx:xx  XXX  Idle  N/A  No`
	`yy:yy:yy:yy:yy:yy  XXX  Idle  N/A  No`
	Also:
	• When you view the client summary using the **show client summary** command, the controller does not indicate the client.
	• When you view the CAPWAP command **show capwap client mn** and **show controllers d0/1** on the access point, the status does not indicate the client association entry.
	Conditions: Unknown.
	Workaround: Reboot the access point.

Table 1-8 Open Caveats (continued)

ID Number	Description
CSCtt15179	Foreign controller does not rehome the client after it roams to an AP in the same AP group. **Symptom**: Wireless clients cannot communicate with each other when they are associated to APs on the same controller. **Conditions**: This issue is seen with L3 roam within the controllers. Consider the following scenario: • A client associates with an access point on WLC1 in VLAN1. • When the client roams to an AP in an AP group in VLAN2 on WLC2–now anchored to WLC1. • A client now roams to an AP on WLC2 but in an AP group in VLAN1. WLC2 should rehome client to be local to WLC2 in his home VLAN, but client remains anchored to WLC1. **Workaround**: Do not use AP groups for the WLAN.
CSCtu33597	Clients may fail to roam when CCKM and WPA 2 is turned on. **Symptom**: CCKM MIC fails during roaming when clients sends reassociation requests. Clients are unable to reassociate successfully during roaming. **Conditions**: The WLAN is configured with WPA2/802.1X CCKM. **Workaround**: Change WLAN security to WPA1/802.1x CCKM.
CSCtx03556	TACACS user login failure on Cisco 5508 Wireless Controller running 7.0.116.0. **Symptom**: A login failure is observed when a TACACS user tries to login to a Cisco 5508 Wireless Controller running version 7.0.116.0. The following error message is observed: `aaaQueueReader: Oct 11 20:14:45.909: TPLUS Transmission Queue Full` **Conditions**: This issue is seen when a Cisco 5508 Wireless Controller running a 7.0.116.0 image is used. **Workaround**: Use the local user account on the controller.

Table 1-8 Open Caveats (continued)

ID Number	Description
CSCtu36088	MAP key error on failover recovery scenario between RAPs. **Symptom**: A map can be stuck on decrypt errors for long time and fail to recover when joining from the secondary to the primary controller. After a failure of the primary controller, it may need to reboot to recover. **Conditions**: This issue has been reproduced consistently in a lab environment under the following conditions: • Two controllers, one primary, one backup. • Two RAPs, two MAPs. All mesh APs are associated to the primary controller. • Mesh tree is R-M1, R2-M2 for example. • Primary WLC is disconnected from the network. • All APs join into WLC2, same mesh tree. • After a few minutes, the WLC1 is brought back online, and fallback is enabled. • APs will move back to primary. • Map1 tries to join RAP2, instead of RAP1. • Map1 authenticates and starts the join/discovery process but decrypt errors at MAP are seen and reported in traps at controller. **Workaround**: Disable AP fallback and if a failure occurs, the recovery can be done in phases.
CSCtw87226	Cisco 5508 Wireless Controller does not respond to SNMP sets. **Symptom**: WCS is unable to push any changes to a Cisco 5508 Controller using SNMP v2 read-write community in 7.0.220.0 release. The read functionality works with the same community and the controller responds to get requests. However, when a set request is sent, no response is seen on the controller debugging or returned in the packet capture. **Conditions**: The issue is seen on a Cisco 5508 Wireless Controller using version 7.0.220.0. **Workaround**: Make the configuration change directly to the controller and then refresh the configuration to synchronize with NCS which is the supported controller in this release.
CSCtx02515	The task webJavaTask may cause high CPU if the traffic is allowed by the CPU ACL. **Symptom**: High CPU cycles are observed on webJavaTask. **Conditions**: A library used for controller web pages may cause high CPU if the CPU ACL allows traffic to TCP port 4242, which is blocked by default. The port may be opened due to a "permit any any" ACL rule. **Workaround**: Modify the CPU ACL so this port is not opened by error.

Table 1-8 Open Caveats (continued)

ID Number	Description

CSCtx27358	Controller does not reply to SNMP after some time.
	
	Symptom: Controllers are unreachable from the network management application (WCS in 7.0 or earlier releases, and NCS in 7.1 and later releases) after some time. The controller is fully operational and reachable except through SNMP. An snmpwalk on them fails. The controller reports the following information through debugs:
	
	`*SNMPTask: Dec 22 10:00:53.076: Authentication failure, bad community string`
	`*SNMPTask: Dec 22 10:00:53.076: Bad Community name`
	`*SNMPTask: Dec 22 10:00:53.076: SNMPD: Failed to get result Pdu.`
	
	This issue occurs even when the community name is correctly specified. The controller configuration backup shows that the same community exists on the controller. Deleting and adding the community to the controller solves the problem temporarily.
	
	Conditions: Unknown.
	
	Workaround: Re-create the community on the controller.

CSCtx17373	Lightweight Access Point syslog level setting cannot be saved. **Symptom**: The lightweight access point syslog level setting cannot be saved **Conditions**: This issue is seen when the controller uses version 7.0.220.0 under the following conditions: 1. A LAP joins to a controller. 2. Execute the following command: **config ap logging syslog level emergencies all** from the controller. 3. The syslog level has changed to emergencies on the LAP indicating the logging of the traps. 4. Reload the LAP. 5. After the LAP rejoins the LAP syslog logs a trap error. **Workaround**: Reconfigure syslog setting after the LAP is reload.
CSCtu19860	Cisco 5508 Wireless controller does not set 802.1p marking for downstream CAPWAP packets. **Symptom**: The Cisco 5508 Wireless Controller does not set the configured 802.1p marking for downstream CAPWAP packets. The controller only sets the 802.1p marking for unencapsulated packets that go out to the wired network. When trusting CoS on the controller port this issue causes the switch CoS to DSCP map to remark the packet to 0, when the AP receives the packet and sends it over the air, the 802.11e UP value is 0 which causes a one-way QoS. **Conditions**: Configure WLAN for platinum QoS and configure the platinum QoS profile for an 802.1p value of 6. **Workaround**: Trust DSCP on the switchport connecting to the WLC instead of trusting CoS.

Table 1-8 Open Caveats (continued)

ID Number	Description
CSCtw89776	Controller accepts registration of invalid IP addresses for clients. **Symptom:** The controller accepts address registrations for source addresses from clients that are invalid per RFC. **Condition**: The controller should reject registrations of invalid IP addresses, and treat them as "IP theft" as they are addresses that can never be used as source address. **Workaround**: None.
CSCtw67184	Cisco 7500 Flex Controller: System loses RAID after a power outage. **Symptom**: While booting the controller, an error message appears on the attached monitor or on the serial console displaying the following error: `All the disks from your previous configuration are gone. If this is an unexpected message, then please power off your system and check your system and check your cables to ensure all disks are present. Press any key to continue or C to load the configuration utility.` When any key is pressed, the system fails to boot from the disk. **Conditions**: This issue occurs because the controller went through an accidental power interruption (that is, the power plug was pulled while the system was operational). Upon reboot, the RAID card fails to locate its configuration in the flash memory and fails to boot. **Workaround**: Use the RAID management tool - WebBIOS. You can use either the GUI or the CLI. To use the CLI: 1. Pres Ctrl Y key after the above error message. 2. Enter the following command: `-CfgForeign -Import -a0` 3. Reboot the server.
CSCtw75830	Controller accounting wrong CLI command. **Symptom**: The controller sends wrong information to the accounting server when the command **802.11a cac voice sip enable**. **Conditions**: This issue is seen every time the **802.11a cac voice sip enable** command is entered. **Workaround**: None.

Table 1-8 Open Caveats (continued)

ID Number	Description
CSCtx27591	Duplex or Speed settings are lost on reload if AP has static IP address. **Symptom**: AP cannot be configured with static speed or duplex settings. The interface settings are lost on reload. **Conditions**: This issue is seen when the access point has static IP address. **Workaround**: Use DHCP.
CSCtz07676	Controller cannot establish SXP connection with a Cisco Nexus 7000 Series switch. **Symptom**: An SXP connection from the controller to the Cisco Nexus 7000 Series switch reports the On state on the controller side while the switch reports the Waiting for Response state. **Conditions**: Establishing SXP connection between the controller and ASA. **Workaround**: Add an intermediate device that supports SXPv2 between the controller and the Cisco Nexus 7000 Series switch.

Resolved Caveats

Table 1-9 lists caveats resolved in controller software release 7.2.103.0.

Table 1-9 Resolved Caveats

ID Number	Caveat Title
CSCtr80528	When entering the primary/secondary/tertiary controller on an access point, an address ending with 255 is not accepted, even when it is not a broadcast address.
CSCti74871	Cisco 5500 Series Controller does not send SNMP traps through dynamic interface.
CSCtq46316	Some rogue classifications are not retained after reboot.
CSCsg32646	When LAG is enabled, CDP does not display proper port information.
CSCto06303	Controller does not learn client IP from BOOTP.
CSCts52998	Cisco 2504 Wireless Controller does not respond to discover requests with Public AP manager IP.
CSCto35511	Cisco 5508 Wireless Controller displays traceback errors.
CSCti97823	Controller uses wrong source MAC while sending DHCP request to DHCP server.
CSCtn16347	Controller does not rewrite DHCP acknowledge packets correctly for DHCP Information.
CSCto25030	AP hostname displays 31 characters after upgrading to 6.0 on controller.
CSCtj91693	Cisco 5508 Wireless Controller–GARP on management interface forwarded to clients on a different VLAN.
CSCtu44208	Unable to Telnet or SSH to a controller. Error indicates that the maximum number of connections are reached, but no connections are in use.

Table 1-9 Resolved Caveats (continued)

ID Number	Caveat Title
CSCtn95179	No DSCP marking when CAPWAP data encryption enabled.
CSCtu24889	AP 'DOT11-2-RADIO_RX_BUF' Crash upon receipt of WPA packet with length 0.
CSCtl98942	CleanAir Trap types go back to default after configuration restored.
CSCtw81357	Add customer control for aggregation scheduler parameters.
CSCto11157	Controller does not send association response.
CSCtn20944	Supported CLI to disable fastpath.
CSCsg87862	WLC Console/Telnet/SSH/HTTP/HTTPS unresponsive when AAA server is unresponsive.
CSCtw90269	RADIUS server fallback account requests are sent with missing AcctSessionId.
CSCsu54884	Adhoc rogues not shown anywhere on the controller once made internal.
CSCtl80242	The Controller must use UTC (GMT) when performing certificate date validity check.
CSCth65648	WLANs disabled after power outage.
CSCtt94100	Association request from a client having stale entry in WLC is dropped.
CSCtw78616	APs not sending the ELM flag when reporting wIPS traffic.
CSCtt70290	PMK cache entry for a CCKM client after a valid fast roam is set to zero.
CSCtn74703	With load balancing enabled, clients doing passive scan can't associate.
CSCtn92381	Cisco 600 Series OEAP: Remote LAN commands get uploaded as WLAN.
CSCtg42711	Cisco 5500 Wireless Controller: DP CRASH: Hardware deadlock - all Packet Buffers in use.
CSCtn04229	Signal strength increase for a while though TxPower is static.
CSCtu24652	Mesh: MAPs not honoring data rate updates from the controller.
CSCtw69785	DCA list corrupt with 16 or more country codes configured.
CSCtb78072	SNMPv3 communication breaks with NAC Appliance CAM.
CSCtt02432	Cisco Flex 7510 Wireless Controller fails to respond due to stack corruption.
CSCtu74944	DNS hostname in the virtual interface is broken.
CSCtu42966	Webauth does not redirect when IE opens to default URL.
CSCtw66600	Controller fails to respond while processing login.html.
CSCto06251	AP sends DHCP renew before discovery with fast heartbeat enabled.
CSCtw56233	Controller fails to respond when on `process_one_tx_packet` for 1130.
CSCtw68649	SIP: Preferred Call does not work when calling from ST450 softphone.
CSCto33804	Extra bytes as part of IP data packet length create wrong IE Association packet.
CSCud20593	The Cisco TrustSec SXP feature was not supported.

Table 1-9 Resolved Caveats (continued)

ID Number	Caveat Title
CSCtr49064	The Secure Shell (SSH) server implementation in Cisco IOS Software and Cisco IOS XE Software contains a denial of service (DoS) vulnerability in the SSH version 2 (SSHv2) feature. An unauthenticated, remote attacker could exploit this vulnerability by attempting a reverse SSH login with a crafted username. Successful exploitation of this vulnerability could allow an attacker to create a DoS condition by causing the device to reload. Repeated exploits could create a sustained DoS condition. The SSH server in Cisco IOS Software and Cisco IOS XE Software is an optional service, but its use is highly recommended as a security best practice for the management of Cisco IOS devices. Devices that are not configured to accept SSHv2 connections are not affected by this vulnerability. Cisco has released free software updates that address this vulnerability. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ssh
CSCtr91106	A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device. Products that are not running Cisco IOS Software are not vulnerable. Cisco has released free software updates that address these vulnerabilities. The HTTP server may be disabled as a workaround for the vulnerability described in this advisory. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai
CSCto90842	Rogue ignore list enhancements.

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, see 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.

Related Documentation

For additional information on the Cisco controllers and lightweight access points, see these documents:

- The quick start guide or installation guide for your particular controller or access point
- *Cisco Wireless LAN Controller Configuration Guide*
- *Cisco Wireless LAN Controller Command Reference*
- *Cisco Prime Network Control System Configuration Guide*
- *Cisco Prime Network Control System Command Reference*

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.