Release Notes for Cisco Wireless LAN Controllers and Cisco Aironet Lightweight Access Points for Releases 3.2.78.4 and 3.2.78.0

January 26, 2006

These release notes describe open caveats for Release 3.2.78.4 for Cisco Wireless Services Modules and Release 3.2.78.0 for Cisco 2000 Series Wireless LAN Controllers, Cisco 4100 Series Wireless LAN Controllers, Cisco 4400 Series Wireless LAN Controllers, Cisco WLAN Controller Network Modules, Cisco Aironet 1000 Series Lightweight Access Points, Cisco Aironet 1130 Series Lightweight Access Points, Cisco Aironet 1200 Series Lightweight Access Points, Cisco Aironet 1240 Series Lightweight Access Points, and Cisco Aironet 1500 Series Lightweight Outdoor Access Points, which comprise part of the Cisco Unified Wireless Network Solution (Cisco UWN).

The Cisco 2000 Series Wireless LAN Controllers, Cisco 4100 Series Wireless LAN Controllers, Cisco 4400 Series Wireless LAN Controllers, and the controllers on Wireless Services Modules and Controller Network Modules are hereafter collectively referred to as *wireless LAN controllers* (unless noted otherwise), and the Cisco lightweight access points are hereafter collectively referred to as *Cisco lightweight access points.*

Contents

These release notes contain the following sections.

CISCO SYSTEMS

Corporate 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 Unified Wireless Network Solution (Cisco UWN):

- Operating System software 3.2.78.4 [for the Cisco Wireless Services Module (WiSM) for Cisco Catalyst 6500 Series Switches]
- Operating System software 3.2.78.0 [for all Cisco wireless LAN controllers (except those on the WiSM) and Cisco Aironet lightweight access points]
- Cisco Wireless Control System (Cisco WCS)
- Cisco 2700 Series Location Appliances
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 4100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco WLAN Controller Network Module for Cisco Integrated Services Routers
- Cisco Wireless Services Module (WiSM) for Cisco Catalyst 6500 Series Switches
- Cisco Aironet 1000 Series Lightweight Access Points
- Cisco Aironet 1130 Series Lightweight Access Points
- Cisco Aironet 1200 Series Lightweight Access Points
- Cisco Aironet 1240 Series Lightweight Access Points
- Cisco Aironet 1500 Series Lightweight Outdoor Access Points

Requirements for Cisco UWN Components

- Requirements for Web User Interface - Windows XP SP1 or Windows 2000 SP4 running Internet Explorer 6.0.2800.1106.xpsp2.130422-1633 or higher. You also need to load patch KB831167 found at the following location:

  http://www.microsoft.com/downloads/details.aspx?FamilyID=254eb128-5053-48a7-8526-bd38215c74b2&displaylang=en

  Opera, Mozilla, and Netscape are unsupported.
- Requirements for Web Browser when using Web Authentication - Internet Explorer 6.0 with SP1 or Netscape 7.2. Opera is unsupported.

Software Release Information

Operating system software is factory installed on your wireless LAN controller and automatically downloaded to the Cisco lightweight access points after a release upgrade and whenever a Cisco lightweight access point associates with a wireless LAN controller. As new releases become available for the wireless LAN controllers and their associated Cisco lightweight access points, consider upgrading.

Note The Cisco Catalyst 6500 Series Wireless Services Module (WiSM) requires software release SWISMK9-32 or later.

Finding the Software Release

To find the software release running on your wireless LAN controller, look on the Monitor > Summary page on the GUI or enter **show sysinfo** on the controller CLI.

Upgrading to a New Software Release

For instructions on installing the 3.2.78.4 software release on a Cisco Catalyst 6500 Series WiSM or the 3.2.78.0 software release on any other Cisco wireless LAN controller, refer to the *Cisco Wireless LAN Controller Configuration Guide.* Click this link to browse to that document:

http://www.cisco.com/en/US/products/ps6366/tsd_products_support_configure.html

Software Release Support for Access Points

Table 1 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 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	—	4.1.171.0
1100 Series	AIR-LAP1121	4.0.155.0	—
	AIR-LAP1131	3.1.59.24	—
	AIR-LAP1141N	5.2.157.0	—
	AIR-LAP1142N	5.2.157.0	—
1200 Series	AIR-AP1220A	3.1.59.24	—
	AIR-AP1220B	3.1.59.24	—

Table 1 Software Support for Access Points (Continued)

Access Points		First Support	Last Support
1230 Series	AIR-AP1230A	3.1.59.24	—
	AIR-AP1230B	3.1.59.24	—
	AIR-LAP1231G	3.1.59.24	—
	AIR-LAP1232AG	3.1.59.24	—
1240 Series	AIR-LAP1242G	3.1.59.24	—
	AIR-LAP1242AG	3.1.59.24	—
1250 Series	AIR-LAP1250	4.2.61.0	—
	AIR-LAP1252G	4.2.61.0	—
	AIR-LAP1252AG	4.2.61.0	—
1300 Series	AIR-BR1310G	4.0.155.0	—
1400 Series	Standalone Only	N/A	—
1500 Mesh Series	AIR-LAP-1505	3.1.59.24	4.2.176.51M
	AIR-LAP-1510	3.1.59.24	4.2.176.51M
1520 Mesh Series	AIR-LAP1522AG	-A and N: 4.1.190.1 or 5.2 or later[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-LAP1522HZ	-A and N: 4.1.190.1 or 5.2 or later[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-LAP1522PC	-A and N: 4.1.190.1 or 5.2 or later[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-LAP1524SB	-A, C and N: 6.0 or later	—
	AIR-LAP1524PS	-A: 4.1.192.22M or 5.2 or later[1]	—

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

New Features

The following new features are available in the wireless LAN controller 3.2.78.4 and 3.2.78.0 releases:

- Link aggregation (for Cisco 4400 Series Wireless LAN Controller and WiSM)
- QoS enhancements
- Cisco 2000 Series Wireless LAN Controller performance optimizations
- Cisco 2000 Series Wireless LAN Controller guest tunneling
- Cisco WCS backup improvements
- Multicast performance enhancements
- Cisco WCS backup enhancements
- Cisco 2700 Series Location Appliance enhancements
- Cisco Aironet 1500 series lightweight outdoor access point enhancements
- Static and dynamic WEP on the same WLAN
- Regulatory domain updates
- New hardware platform support: Cisco WLAN controller network module for Cisco Integrated Services Routers

Refer to the following location for more information:

http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps6366/prod_bulletin0900aecd80394844.html

Installation Notes

This section contains important information to keep in mind when installing your wireless LAN controllers and Cisco lightweight access points.

Warnings

Warning **This warning means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.**

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

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

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

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

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

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

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

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

Warning **This unit is intended for installation in restricted 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.**

Safety Information

Follow the guidelines in this section to ensure proper operation and safe use of the wireless LAN controllers and Cisco lightweight 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 eqipment. 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

Warning **Do not locate any antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing an 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, refer to national and local codes (e.g. U.S.:NFPA 70, National Electrical Code, Article 810, in Canada: Canadian Electrical Code, Section 54).**

Each year hundreds of people are killed or injured when attempting to install an antenna. In many of these cases, the victim was aware of the danger of electrocution, but did not take adequate steps to avoid the hazard.

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

1. If you are installing an antenna for the first time, for your own safety as well as others, seek professional assistance. Your Cisco sales representative can explain which mounting method to use for the size and type antenna you are about to install.
2. Select your installation site with safety, as well as performance in mind. Remember: 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, 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 complete 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.

Cisco Lightweight Access Point Installation

Refer to the appropriate Quick Start Guide or Installation and Configuration Guide for instructions on how to install your wireless LAN controllers and Cisco lightweight access points.

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

Personnel installing the wireless LAN controllers and Cisco lightweight access points must understand wireless techniques and grounding methods. The internal-antenna Cisco lightweight access points can be installed by an experienced IT professional.

Important Notes

This section describes important information about the wireless LAN controllers and Cisco lightweight access points.

Important Regulatory Notice

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

Cisco Wireless LAN Controllers Must Run Release 3.2.76.0 or Later to Support -P and -K Regulatory Domains

To support Cisco lightweight access points configured for use in Japan and Korea, you must upgrade the wireless LAN controller software to the 3.2.76.0 or later release. Earlier releases do not support Cisco lightweight access points configured for use in Japan (regulatory domain -P) and Korea (regulatory domain -K).

Voice WLAN Configuration

Cisco recommends that Load Balancing ALWAYS be turned off in any WLAN that is supporting voice, regardless of vendor. When Load Balancing is turned on, voice clients can hear an audible artifact when roaming and the handset is refused at its first reassociation attempt.

Operating Mesh Networks Through Switches and Routers

In mesh networks that operate through low-speed switches and routers, Cisco lightweight access points can disconnect from the wireless LAN controller, which causes the wireless LAN controller to generate traps (CSCsb43906).

Heavily Loaded Cisco Wireless LAN Controllers CPU

When the wireless LAN controller CPU is heavily loaded (for example, when doing file copies or other tasks), it does not have time to process all the ACKs that the NPU sends in response to configuration messages. When this happens, the CPU generates error messages. The error messages do not impact service or functionality (CSCsb48765).

Cisco 7920 Wireless IP Phone Support

When using Cisco 7920 Wireless IP phones with wireless LAN controllers, make sure that the phones and wireless LAN controllers are configured as follows:

- Aggressive Load Balancing on the wireless LAN controllers must be disabled on a per-wireless LAN controller basis. Otherwise, the initial roam attempt by the phone may fail, causing a disruption in the audio path.
- The QoS Basis Service Set (QBSS) information element (IE) must be enabled. The QBSS IE enables the Cisco lightweight access points to communicate its channel usage to wireless devices. Because Cisco lightweight access points with high channel usage might not be able to handle real-time traffic effectively, the 7920 phone uses the QBSS value to determine if they should associate with another Cisco lightweight access point. Use the following instructions to enable the QBSS IE:
  - **>sh wlan summary**
    (use this to determine the WLAN ID No. of the WLAN to which you want to add QBSS support)
  - **>config wlan disable [WLAN ID No.]**
  - **>config wlan 7920-support ap-cac-limit enable [WLAN ID No.]**
  - **>config wlan enable [WLAN ID No.]**
  - **>sh wlan [WLAN ID No.]**
    (use this command to verify that the WLAN is enabled and the field marked “Dot11-Phone Mode (7920)” is in the ‘compat’ mode)
  - **>save config**
- The Dynamic Transmit Power Control (DTPC) information element (IE) must be enabled using the **config 802.11a dtpc enable** and **config 802.11a** commands. The DTPC information element is a beacon and probe information element that allows the Cisco lightweight access point to broadcast information on its transmit power. The Cisco Wireless IP Phone 7920 uses this information to automatically adjust its transmit power to the same level as the Cisco lightweight access point to which it is associated. In this manner, both devices are transmitting at the same level.
- The 7920 phones and the wireless LAN controllers do not currently use compatible fast roaming mechanisms. The phone uses CCKM while the wireless LAN controllers use Proactive Key Caching (PKC). To minimize roaming latency, static WEP is the recommended security mechanism.
- When configuring WEP, there is a difference in nomenclature the wireless LAN controller and the 7920 phone. Configure the wireless LAN controller for 104 bits when using 128-bit WEP for the 7920.

The Upgrade Process

When a wireless LAN controller is upgraded, the code on the associated Cisco lightweight access points is also automatically upgraded. When a Cisco lightweight access point is loading code, each of its lights blinks in succession.

Caution Do not power down the wireless LAN controller or any Cisco lightweight access point during this process, or you might corrupt the software image!

Upgrading a wireless LAN controller with a large number of Cisco lightweight access points can take as long as 30 minutes. The Cisco lightweight access points must remain powered and the wireless LAN controller must not be reset during this time.

Cisco recommends the following sequence when performing an upgrade:

1. Upload your wireless LAN controller configuration files to a server to back them up.
2. Turn off the wireless LAN controller 802.11a and 802.11b networks.
3. Upgrade your wireless LAN controller.
4. Re-enable your 802.11a and 802.11b networks.

Note Cisco Wireless LAN Controllers can be upgraded from one release to another. However, should you require a downgrade from one release to another, you may be unable to use the higher release configuration (CSCsb79383). The workaround is to reload the previous wireless LAN controller configuration files saved on the backup server or to reconfigure the wireless LAN controller.

Exclusion List (Blacklist) Client Feature

If a client is not able to connect, and the security policy for the WLAN and/or client is correct, the client has probably been disabled. From the Web user interface, Monitor page under client summary, you can see the client's status. If they are disabled you can just do a "Remove" operation and the disable is cleared 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 show up on the permanent disable display. This display is only for those MACs that are set as permanently disabled by the administrator.

RADIUS Servers and the Management VLAN

The RADIUS server can be on any subnet as long as it can be reached by the Management VLAN subnet.

The wireless LAN controllers can be managed via the Management VLAN subnet from any other subnet that can reach the Management VLAN subnet.

IPSec Clients Supported in this Release

This operating system release has been tested with the following IPSec clients:

- NetScreen v10.1.1 (build 10)
- Cisco VPN Client v4.6.04
- SSH Sentinel v1.4.1
- Openswan v2.4.0

The Netscreen client does not handle fragmented ICMP packets, does not respond to large ping packets, and does not work with certificates. Other IP fragmented traffic should work correctly.

Maximum MAC Filter Entries

The wireless LAN controller database can contain up to 2048 MAC filter entries for local netusers (CSCar12371).

Client Channel Changes

Cisco lightweight access points are known to go off channel for up to 30 seconds while identifying rogue access point threats. This can cause occasional dropped client connections (CSCar10047).

Cisco Aironet 1030 Remote Edge Lightweight Access Point WPA2-PSK in Standalone Mode

Cisco Aironet 1030 remote edge lightweight access points do not support WPA2-PSK in REAP standalone mode.

XAuth Configuration with NetScreen

Configure XAuth on the wireless LAN controller, and enable extended-authentication on the NetScreen client. The wireless LAN controller initiates the XAuth session.

Rekeys Not Supported with Cisco VPN Client

If a rekey occurs clients must reauthenticate. To mitigate this problem, log into the Web user interface, navigate to the WLANs page, select Edit to display the WLANs > Edit page, choose Advanced Configuration, and change Lifetime (seconds) to a large value, such as 28800 seconds (this is the default), depending upon your security requirements.

RADIUS Servers

This product has been tested with the following RADIUS servers:

- Odyssey Client v1.1 and 2.0 from Funk Software.
- Steel-Belted RADIUS from Funk Software release 4.71.739 and 5.03 Enterprise Edition.
- Microsoft Internet Authentication Service (IAS) release 5.2.3790.1830 on Windows 2003 server.
- CiscoSecure ACS, v3.2.

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.

802.1x and Microsoft Windows Zero-Config Supplicant

Clients using Windows Zero-Config and 802.1x MUST use WLANs configured for 40- or 104-bit Key Length. Configuring for 128-bit Key Length results in clients that can associate, but not authenticate.

Cisco Aironet 1030 Remote Edge Lightweight Access Point Default Operation

When a wireless LAN controller reboots, dropped Cisco Aironet 1030 remote edge lightweight access points attempt to associate with any available wireless LAN controller. If the Cisco Aironet 1030 remote edge lightweight access points cannot contact a wireless LAN controller, they continue to offer 802.11a/b/g service on WLAN 1 only.

WEP Keys

This release supports four separate WEP index keys. These keys cannot be duplicated between WLANs. At most four WEP WLANs can be configured on a wireless LAN controller. Each of these WLANs must use a different key index.

Using the Backup Image

The wireless LAN controller bootloader (ppcboot) stores a copy of the active primary and the backup image. If the primary image should become corrupted, you can use the Bootloader to boot with the backup image.

With the backup image stored before rebooting, be sure to use Option 4: Change Active Boot Image from the boot menu to set the backup image as the active boot image. If you do not, then when the wireless LAN controller resets it again boots off the corrupted primary image.

After the wireless LAN controller is booted, the active boot image can be changed to the backup image using the config boot backup CLI command.

Home Page Retains Web Auth Login with IE 5.x

This is a caching issue in the Internet Explorer 5.x browser. Clearing history corrects it, or upgrade your operator workstation to Internet Explorer 6.x.

RLDP Enable/Disable

RLDP Enable/Disable refers to the RLDP protocol which detects rogues on your wired network. When RLDP is enabled, the wireless LAN controller reports a Threat alarm for each rogue detected on the wired network. When RLDP is disabled, rogues detected on the wired network are shown in the Alert state.

Disabling RLDP stops the wireless LAN controller from detecting rogues on the wired network. Rogues can be manually contained by changing the status of the detected rogues. When rogues are being contained, you must manually disable containment for each rogue individually.

Ad-Hoc Rogue Containment

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

Apple iBook

Some Apple Operating Systems require shared key authentication for WEP. Other releases of the Operating System actually do not work with shared key WEP set unless the client saves the key in their key ring. How you should configure your wireless LAN controller is based on the client mix you expect to use. Cisco recommends testing these configurations before deployment.

Features Not Supported on Cisco 2000 Series Wireless LAN Controllers

These hardware features are not supported on 2000 series controllers:

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

These software features are not supported on 2000 series controllers:

- VPN Termination (such as IPSec and L2TP)
- Termination of guest controller tunnels (origination of guest controller tunnels is supported)
- External Web Authentication web server list
- Layer 2 LWAPP
- Spanning tree
- Port mirroring
- Cranite
- Fortress
- AppleTalk
- QoS per user bandwidth contracts
- IPv6 pass-through

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

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

Pinging from Any Network Device to a Dynamic Interface IP Address Not Supported

Clients on the WLAN associated with the interface pass traffic normally.

2006 Image Not Supported for 3504 Series Wireless LAN Controllers

The 2006 wireless LAN controller image is supported for use with only Cisco 2000 Series Wireless LAN Controllers. Do not install the 2006 image on a 3504 Series Wireless LAN Controller. Otherwise, errors may occur. Install only the 3504 image on a 3504 Series Wireless LAN Controller.

Running a 3504 Image on a Cisco 2000 Series Wireless LAN Controller

It is possible to run a 3504 wireless LAN controller image on a Cisco 2000 Series Wireless LAN Controller, but Cisco Aironet 1130 series lightweight access points, Cisco Aironet 1200 series lightweight access points, and Cisco Aironet 1240 series lightweight access points will not be able to connect with the wireless LAN controller.

Cisco Lightweight Access Points Fail to Join Cisco Wireless LAN Controllers

When a Cisco lightweight access point is connected to a terminal server port and reboots because of a join failure or timeout, this sequence repeats forever until the Cisco lightweight access point returns to the boot prompt and stays there. This condition occurs when there is no telnet session to the Cisco lightweight access point console port, and when the wireless LAN controller is not responding to the Cisco lightweight access point join response.

Workaround: Disconnect the Cisco lightweight access point console port from the terminal server. Reprogram the wireless LAN controller to have it respond to the Cisco lightweight access point join request. Power cycle the Cisco lightweight access point to force a restart.

Upgrading External Webauth

When upgrading wireless LAN controllers from operating system release 2.0 or 2.2.127.4 to release 3.0, update the external webauth configuration as follows:

- Instead of using a preauth ACL, the network manager must configure the external web server IP address using the CLI command:

  config custom-web ext-webserver add <IP address>

  (where <IP address> is the address of any web server that performs external web authentication.)

Then, the network manager must use the new login_template which is included below:

```
<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
username is already logged into the system?");
     }
     else if(args.statusCode == 4){
        alert("Wrong username and password. Please try again.");
     }
     else if(args.statusCode == 5){
        alert("The User Name and Password combination you have entered is invalid.
Please try again.");
     }

}

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

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

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

<tr align="center">

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

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

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

Caveats

This section lists open and closed caveats in operating system releases 3.2.78.4 and 3.2.78.0 for wireless LAN controllers and associated Cisco lightweight access points.

Open Caveats

These caveats are open in operating system releases 3.2.78.4 and 3.2.78.0:

- CSCar14535—When configuring a mobility group anchor that is not part of the mobility member list, the wireless LAN controller displays an invalid parameter provided error message.

  Workaround: Make sure that the anchor wireless LAN controller is a mobility group member.
- CSCsa95763—The wireless LAN controller Web UI cannot display more than 80 local net users on the page Security > AAA > Local Net Users.

  Workaround: Use the wireless LAN controller CLI to view all the Local Net User entries.
- CSCsa89818—PDAs are unable to associate with Cisco Aironet 1030 remote edge lightweight access points in REAP mode; local mode works correctly.

  Workaround: None at this time.
- CSCsb01980—When using the web configuration wizard on a wireless LAN controller, when the operator enters incorrect data for the management interface, error messages are shown only at the end of the wizard and therefore the user must return to the management interface page for correction. The data entered in the management interface page, such as the port number, is not validated immediately but at the end of the wizard. As a result any error messages are shown only at the end.

  Workaround: This problem can cause some inconvenience and the user may prefer to use the CLI configuration wizard instead to avoid it.
- CSCsb13548—Cisco lightweight access points frequently reset.

  Workaround: None in this release.
- CSCsb01983—The wireless LAN controller Web Configuration wizard is not reachable after making repeated invalid entries for the management interface port. If an operator connects to the wireless LAN controller Web Configuration wizard on address 192.168.1.1 and enters an invalid

port number on the Management Interface configuration page, the operator is redirected at the end of the wizard to the management interface page to correct the port. If the operator enters an incorrect port and submits, the configuration wizard becomes inaccessible.

Workaround: Reboot the wireless LAN controller through the CLI to access the web wizard again.

- CSCsb15825—Airespace MIBs not submitted to MIB-police nor posted at MIB central.

  Workaround: None in this release.

- CSCsb20269—On the WiSM, when the service VLAN is configured as one of the VLANs on a data port, it does not operate correctly.

  Workaround: Do not configure the service VLAN as one of the VLANs on a data port.

- CSCsb26504—To boot from the backup image when using the Boot Options menu, users need to enter the option twice to boot from the backup image.

  Workaround: When using the Boot Options menu, enter the option twice to boot from the backup image.

- CSCsb34149—Disabling or deleting a wireless LAN on which a large number of clients exists may not result in all clients being deleted. This occurs when several thousand clients are using a wireless LAN when the wireless LAN is disabled or deleted.

  Workaround: Make sure that wireless LANs with a large number of clients associated are not deleted or disabled.

- CSCsb38486—The Cisco Aironet 1500 series lightweight outdoor access point bridge CLI does not accept 10 character bridge group names.

  Workaround: Use 9-character bridge group names.

- CSCsb39522—When a user changes the setting from a static IP address to DHCP and if the DHCP IP address is not available, the supervisor loses keepalive and the WiSM sends a WCP going down trap. Similarly, when a user changes a static IP address and enters an incorrect subnet on the service port, the supervisor detects a loss of WCP keepalive and the WiSM sends a WCP going down trap.

  Workaround: None at this time.

  Note WCP is the protocol running between the Cisco Catalyst 6500 series switch supervisor and the WiSM. The supervisor uses WCP protocol to monitor the health of the WiSM. If you enter the show wism status command or see a WiSM down trap on Cisco WCS, make sure that the WiSM service port and that the supervisor are correctly configured. WCP can fail because of an incorrect configuration.

- CSCsb48197—Multiple authentication requests to the Cisco WCS server.

  Workaround: None in this release.

- CSCsb52557—Cisco Aironet lightweight access points do not connect to the Cisco 4400 Series Wireless LAN Controller if the time is not set first.

  Workaround: Set the time on the Cisco 4400 Series Wireless LAN Controller before allowing the Cisco Aironet lightweight access points to connect to the wireless LAN controller.

- CSCsb53746—A 350 or CB20A client running ACU 6.4 or ACU 6.5 and configured for LEAP authentication with WPAv1 encryption can authenticate to a Cisco Aironet lightweight access point but does not receive an IP address. This problem does not affect clients running ACU 6.3, which does not use WME data frames. To check for this problem enter the following command on the wireless LAN controller:

debug dot1x events enable

In the body of the trace that follows authentication by an affected client, the following messages appear:

```
Fri Jun 3 07:29:59 2005: Received EAPOL-Key from mobile xx:xx:xx:xx:xx:xx
Fri Jun 3 07:29:59 2005: Received EAPOL-key message with invalid version number from
mobile xx:xx:xx:xx:xx:xx
```

Workaround: Configure WME policy to be allowed for the wireless LAN on the wireless LAN controller. To do this on the GUI, browse to the WLANs > Edit page for the appropriate WPAv1 wireless LAN, and in the drop-down menu next to WME policy, select **Allowed** or **Required**. The allowed option means that both WME and non-WME clients can authenticate and receive an IP address; for example, both Aironet ACU 6.4/6.5 and 6.3 clients could authenticate and receive an IP address. The required option means that only WME clients can authenticate; that is, only ACU 6.4/6.5 clients.

- CSCsb55937—VLAN-tagged large ICMP packets that need to be fragmented are not sent by Cisco Aironet 1000 series lightweight access points in direct-connection mode. Ping replies never come back when the Cisco Aironet 1000 series lightweight access point is sending requests to a gateway from a wireless client using large 1500-byte packets, and with RADIUS override configured with any 1p tag. This condition exists for Cisco 4400 Series Wireless LAN Controllers using direct-connect mode, with RADIUS override enabled, the override parameter set to 1p with any VLAN number, and Cisco Aironet 1000 series lightweight access points.

  Workaround: None at this time.

- CSCsb59898—Cisco Aironet 1030 remote edge lightweight access points in REAP mode do not support roaming when configured with a WLAN that is set up for WPA security.

  Workaround: None for this release.

- CSCsb71060—Internal LAG errors when the WiSM management interface is changed from tagged to untagged.

  Workaround: Leave the WiSM management interface as tagged or untagged.

- CSCsb77595—When logging out from Telnet/SSH sessions the session always prompts if you would like to save changes, even when no changes have been made.

  Workaround: Ignore the prompt and exit as usual.

- CSCsb78835—The wireless LAN controllers are not sending all rogue trap information to Cisco WCS.

  Workaround: Run the rogue AP task in Cisco WCS to synchronize Cisco WCS with what the wireless LAN controller is showing.

- CSCsb85113—When users download the code image to a WiSM using the CLI, associated Cisco lightweight access points are sometimes disconnected.

  Workaround: Download new code images to WiSMs at times when there are no clients to be affected.

- CSCsb85582—Cisco 4100 Series Wireless LAN Controllers crash at PES_rqst_exec_again.

  Workaround: None for this release.

- CSCsb88424—Cisco Aironet 1030 remote edge lightweight access points in REAP mode reboot continuously.

  Workaround: Make sure that there are no sub-1500 byte MTU links between the wireless LAN controller and the REAP Cisco Aironet 1030 remote edge lightweight access point.

- CSCsb88588—Incorrect power levels are reported for Cisco lightweight access points when the wireless LAN controller is set to country code SG.

  Workaround: None for this release.

- CSCsb90622—AP impersonation alarms sometimes flood Cisco WCS.

  Workaround: None for this release.

- CSCsb76389—Cannot failover to second instance IP address or port on a RADIUS server.

  Workaround: None for this release.

- CSCsc01221—When downstream test data is sent from the wired endpoint to four wireless clients at different priority levels (voice, video, background, and best effort), the Cisco Aironet 1000 series lightweight access points crash.

  Workaround: None for this release.

- CSCsc02741—In the bootloader mode, users are unable to exit or return to the main prompt. If users make mistakes while entering values, they cannot quit the step and are unable to go back and change existing values.

  Workaround: Reset the system through IOS or power the device off and on if necessary.

- CSCsc02860—When users download the code image to a WiSM for the first time, the WiSM fails to download the new image to flash memory.

  Workaround: Download new code images to WiSMs a second time.

- CSCsc03072—Cisco lightweight access points do not always produce complete logs.

  Workaround: None for this release.

- CSCsc03644—Cisco lightweight access points do not retain location parameter after reboot.

  Workaround: None for this release.

- CSCsc05495—The wireless LAN controllers running 3.0.107 code intermittently send a state attribute 24 in an access-request packet.

  Workaround: Apply the Microsoft KB 883659 patch to IAS. The Microsoft patch may or may not work. There is no workaround on the wireless LAN controller.

- CSCsc06090—For some systems with a large number of Cisco lightweight access points and wireless LAN controllers, the Rogue AP scheduled task can take up to 35 or 45 minutes to complete.

  Workaround: Do the following:

  - Disable Rogue AP from scheduled tasks.
  - Change the settings in the trap control template: disable channel update under Auto RF update and push the modified template to all wireless LAN controllers.
  - Change the RRM threshold: For both 11a and 11b, increase the interference threshold.

- CSCsc11660—The current country screen is not 100% accurate for all deployment scenarios, which may causes confusion in some instances.

  Workaround: None for this release.

- CSCsc14045—VPN passthrough should not be able to combine with web policy.

  Workaround: Do not assign VPN passthrough along with web policy.

- CSCsc15699—In Cisco Aironet 1000 series lightweight access points, the WMM IE (11) is correct, but the QBSS client cac limit (11) is still in its old place.

  Workaround: None for this release.

- CSCsc17827—For Cisco Aironet 1500 series lightweight outdoor access points and Cisco Aironet 1030 remote edge lightweight access points, channel 165 for the 802.11a radio is only available for the -A SKU when the country code is set to USX. Channel 165 is not available for the -N SKU for any of the countries that use this SKU.

  Workaround: In order to set the 802.11a radio to channel 165 when using the -A SKU, set the country code of the wireless LAN controller to USX. For the -N SKU, please select one of the available channels.
- CSCsc20416—ACU site survey disassociates other clients in the LWAPP environment.

  Workaround: Under investigation.
- CSCsc21196—Asymmetrical data rate with A radio on 4012/4024 wireless LAN controllers.

  Workaround: None for this release.
- CSCsc22084—No error message or trap is triggered when a PoE wireless LAN controller with CDP causes Cisco Aironet 1200 series lightweight access points to disable their radios.

  Workaround: Disabling CDP resolves this issue.
- CSCsc22663—Deleting a mobility member mapped to a wireless LAN controller as an anchor removes the anchor's entry as well, but the Auto Anchor knob remains enabled even though only the mobility anchor mapping is deleted.

  Workaround: Before deleting a mobility member, first delete the wireless LAN controller to which it is mapped from the WLAN.
- CSCsc26796—The WiSM web interface does not show correct Cisco lightweight access point SNMP operator status (Registered versus Down).

  Workaround: Use Cisco WCS to view the correct values.
- CSCsc28571—Warning! Task 181 (do_linktest) is taking 4265111% of the CPU.

  Workaround: None for this release.
- CSCsc33769—RRM sets the transmit power to 6 on Cisco Aironet 1000 series lightweight access points.

  Workaround: None for this release.
- CSCsc34060—IPSec clients enter the run state but do not communicate.

  Workaround: Under inversigation.pole-top
- CSCsc34713—The wireless LAN controllers crash when there are heavier traffic loads (about 200 clients and 30 Cisco lightweight access points) associated with them.

  Workaround: Turn off aggressive load balancing.
- CSCsc35784—The transmit power control adjustment levels 3, 4 and 5 are not supported on Cisco Aironet 1500 series lightweight outdoor access points in the band from 5745 to 5825 MHz. The transmit power control adjustment levels 4 and 5 are not supported on Cisco Aironet 1500 series lightweight outdoor access points which operate in the 5500 to 5700 MHz band and at 2.4 GHz.

  These levels correspond to -6, -9, and (in the case of 5500 to 5700 MHz) -12 dB from the maximum power, respectively. Power levels 1, 2, and (in the case of 5500 to 5700 MHz) 3 are supported, which correspond to maximum power for the particular data rate and channel, and -3 dB relative to this maximum, at which these adjustment levels provide little or no further reduction in transmit power output.

  Workaround: Set the transmit power level to either 1 or 2 for 5745 to 5825 MHz. Set the transmit power level to either 1, 2, or 3 for all other bands.

- CSCsc38093—Poor performance for wireless clients associated with a Cisco 4400 Series Wireless LAN Controller.

  Workaround: Under investigation.

- CSCsc40648—The rooftop access points are displayed in the web interface as pole-top access points for more than four minutes which does not allow them to be configured.

  Workaround: Configure the Cisco lightweight access point as a rooftop AP using the CLI.

- CSCsc41313—The Cisco Aironet 1500 series lightweight outdoor access points are configured by default to allow old bridges. When this is enabled, the shared secret key set on the wireless LAN controller is not passed on to the Cisco lightweight access points. So a few Cisco lightweight access points might be running on the old key. If these Cisco lightweight access points reset or there are new Cisco lightweight access points waiting to join the running network, they may take a very long time to connect to the network or might not join at all.

  Workaround: Configure the wireless LAN controller as follows: **config network allow-old-bridge-aps disable**.

- CSCsc42923—A 32-character SSID does not allow Cisco lightweight access points to join wireless LAN controllers.

  Workaround: Use a 31- or shorter character SSID.

- CSCsc43587—The wireless LAN controllers crash in the apfReceiveTask software.

  Workaround: None for this release.

- CSCsc44897—Cisco WCS shows incorrect antenna orientation while viewing an object.

  Workaround: None. This is a cosmetic issue only, and does not impair or alter performance.

- CSCsc46598—When performing a Cisco lightweight access point placement preplanning site survey, some items may show up in the wrong position in the Cisco lightweight access point placement diagram and various items in the printed site survey document may be incorrect.

  Workaround: Click Apply All Changes to save the layout to the Cisco WCS database before printing out a site survey document. Some discrepancies may still appear.

- CSCsc53452—When a Cisco WCS user attempts to retrieve the association history of a client that was formerly associated with a replaced Cisco lightweight access point, the association history cannot be retrieved. Cisco WCS shows an error message with the MAC address of the replaced Cisco lightweight access point saying that it cannot be located.

  Workaround: None.

- (NEW CAVEAT)—Over the temperature extremes of the product specification, primarily at the hot temperature extreme of 55 degrees Celsius, the Cisco Aironet 1500 series lightweight outdoor access point may not meet the IEEE 802.11a/b/g transmitter linearity parameter of error vector magnitude (EVM) of the 54Mb and 48Mb product specification.

Resolved Caveats

These caveats are resolved in operating system releases 3.2.78.4 and 3.2.78.0:

- CSCar11327—Cisco lightweight access points no longer crash when idling.
- CSCar12979—The show run-config commands now show the complete configuration.
- CSCar13154—The show debug command now shows the debug pm commands.

- CSCar13192—In Cisco 2000 Series Wireless LAN Controllers, the trap message for SNMP authentication failure no longer contains reversed IP addresses.
- CSCar13259—Clients are no longer excluded on Cisco Aironet 1030 remote edge lightweight access points in REAP mode.
- CSCar13330—The Cisco 2000 Series Wireless LAN Controller web configuration wizard no longer returns the error message "Error in enabling the server."
- CSCar13544—The IPv6 option is now removed from the Cisco 2000 Series Wireless LAN Controller WLAN configuration.
- CSCar13951—The show run-config command no longer returns incomplete results.
- CSCar14253—Uploading a new weblogo for WebAuth no longer resets the custom web title to the default title.
- CSCar14254—Cisco lightweight access points no longer send primary discovery requests even when primary wireless LAN controllers are not configured.
- CSCar14549—Added warning messages when a dynamic AP manager is enabled or disabled.
- CSCar15151—Users can now ping wireless clients from and to wired personal computers on the same subnet.
- CSCej11552—The Cisco WLAN controller network module configuration wizard now prompts the user to confirm the configuration. If not, the wizard prompts the user to re-enter the NTP server configuration.
- CSCej18903—RTOS exception messages are no longer displayed by the wireless LAN controller during shutdown.
- CSCej26232—Reboot option 4 now correctly changes the active boot image.
- CSCsa47748—RLDP protocol is now supported in Cisco Aironet 1130 series lightweight access points, Cisco Aironet 1200 series lightweight access points, and Cisco Aironet 1240 series lightweight access points.
- CSCsa96223—Legitimate Cisco lightweight access points that are part of the mobility group are no longer considered to be interference.
- CSCsa96930—All SSID characters are now displayed.
- CSCsa98683—L2TP client handoffs now work properly.
- CSCsa99899—Added static link aggregation group support.
- CSCsb00116—In Cisco WCS users are now able to create RF domain names less that 8 characters long.
- CSCsb00680—New sessions are only deleted from the VPN/ESM module when the control path receives a response from the data path.
- CSCsb01323—Now able to set zero-config bridging through the wireless LAN controller CLI.
- CSCsb02011—Users can now use the wireless LAN controller CLI to create the maximum number of interfaces.
- CSCsb02820—Checked in code for the DFS implementation.
- CSCsb03900—Cisco 2000 Series Wireless LAN Controllers can now load code images without running out of space.
- CSCsb06108—Cisco lightweight access point MAC address is now consistent with that shown on the Monitor > Summary > Cisco APs > Detail page.
- CSCsb08660—Cisco lightweight access points no longer crash after downloading a new image.

- CSCsb09353—Multicast is now working in inter-NPU deployments.
- CSCsb10749—Intra-Cisco 2000 Series Wireless LAN Controller handoffs now works properly for WPA2 with AAA override.
- CSCsb11342—When an ARP storm occurs on the network and when the wireless LAN controller receive multicast queue fills up, the wireless LAN controller no longer generates a “Receive Multicast Queue Full” trap for each new packet.
- CSCsb12041—In the Cisco 2000 Series Wireless LAN Controller web interface, change the Cisco lightweight access point mode from local to sniffer and reboot, and the Cisco lightweight access point restarts in sniffer mode.
- CSCsb12899—The AP Detail page now shows the full IOS version.
- CSCsb12925—When a Cisco lightweight access point has an unequipped radio, the radio is no longer reported to the wireless LAN controller web interface or Cisco WCS.
- CSCsb14045—Made sure that auto RF works properly on 802.11b/g on Cisco lightweight access points.
- CSCsb14366—Adding the third wireless LAN controller to a mobility group no longer to affects pings.
- CSCsb14635—IPSec Clients are now able to complete Phase-1 IKE.
- CSCsb15051—The wireless LAN controller now displays the correct message when setting a channel on which radar has been detected.
- CSCsb15201—The wireless LAN controller internal DHCP default router no longer displays incorrect IP addresses after an update.
- CSCsb15725—When users assign static IP addresses to Cisco lightweight access points, the wireless LAN controller no longer displays an IP mask error message.
- CSCsb16026—During auto-anchor mobility clients now receive DHCP IP assignments correctly after moving to a foreign wireless LAN controller.
- CSCsb16430—The wireless LAN controllers now use the correct log file location for new processes in Microsoft Windows.
- CSCsb16496—The debug aaa all enable command no longer displays client names and passwords in clear text.
- CSCsb16502—Corrected a memory corruption caused by the remote debug feature.
- CSCsb16891—The rogue client detail page now lists all detecting radios.
- CSCsb16902—Cisco lightweight access points now operate correctly on channels 12, 13, and 100-140.
- CSCsb17013—Corrected a MAC address issue that disabled the SSC feature.
- CSCsb17508—The wireless LAN controller web interface has been updated to display the complete local management user name.
- CSCsb17573—Unnecessary IKE deletion messages are no longer sent to clients during roaming.
- CSCsb18037—There is now a backup port configured on the interface where WLAN is mapped, and when port 1 and 3 are trunked with multicast enabled on the wireless LAN controller and ports.
- CSCsb18644—The wireless LAN controller now generates a trap when a Cisco Aironet 1130 series lightweight access point or Cisco Aironet 1200 series lightweight access point joins the wireless LAN controller.

- CSCsb18651—Created a Cisco 2000 Series Wireless LAN Controller bundle without the Cisco Aironet 1130 series lightweight access point or Cisco Aironet 1200 series lightweight access point images.
- CSCsb18653—Added a TFTP memory core dump function in the wireless LAN controller.
- CSCsb19427—The wireless LAN controller now allows an empty TFTP path in the web interface and CLI.
- CSCsb19841—The devshell spamdisablecrypto command now works correctly for SSC.
- CSCsb20026—The AP Details page now correctly displays the regulatory domain details.
- CSCsb20027—Compact flash ISR checks now correct the CPLD offset for IO ready.
- CSCsb20284—Added support for new Cisco Certificate Authorities.
- CSCsb21470—The Cisco 4100 Series Wireless LAN Controller interface no longer fails after 30 seconds if the link is down for 2 seconds.
- CSCsb22698—Added SNMP QBSS and DTPC support for IP phones.
- CSCsb23290—The wireless LAN controller no longer responds to WMM queries when WMM is not enabled.
- CSCsb23609—The wireless LAN controller no longer degrades the hash key table for some Cisco lightweight access points upon upgrade.
- CSCsb23689—Changed the AP Type to AP Model in the show ap summary.
- CSCsb25566—The wireless LAN controller now displays the configured Cisco lightweight access point static IP address bytes in the correct order.
- CSCsb26299—The wireless LAN controller no longer fails because of a MAC Table NPU failure.
- CSCsb26328—Added extended Cisco 7920 IP phone support.
- CSCsb26335—Added DTPC support.
- CSCsb26682—Transmit power now changes correctly when RRM is enabled.
- CSCsb26788—Updated the regulatory domain information in the Country page.
- CSCsb26858—In the WiSM, the AP interface type now lists all 802.11 radios.
- CSCsb27097—In the WiSM when the user configures an AP manager interface on four ports, and when one of the data port GigE link is administratively disabled on the supervisor side or when the supervisor side GigE port is down, the Cisco lightweight access points now associate with the WiSM.
- CSCsb27142—Channel assignments no longer fail on the wireless LAN controller web interface.
- CSCsb27153—802.1X no longer fails after a Cisco lightweight access point is switched to a static IP address.
- CSCsb27283—Updated CWMIN and CWMAX to 3 for affected beacons.
- CSCsb27470—Enabled level2 optimization for the application module.
- CSCsb27605—Cisco lightweight access points now join the wireless LAN controller, and no longer time out waiting for a join reply.
- CSCsb27702—Added a warning message in the CLI when a user enters a system name with spaces.
- CSCsb27765—The wireless LAN controllers no longer crash when auth lists are added without hash value when using the CLI.
- CSCsb27911—Made miscellaneous changes to the 802.11h parameters page.

- CSCsb28029—During basic traffic flows, Cisco Aironet 1500 series lightweight outdoor access point rooftop or pole-top access points no longer have this assert occur.
- CSCsb28644—Corrected a crash in Cisco 2000 Series Wireless LAN Controllers when retrieving the channel list.
- CSCsb28875—Discovery requests are now only accepted over the management interface.
- CSCsb28881—Cisco lightweight access points no longer send ARP requests with unknown IP addresses.
- CSCsb29726—Removed extra log messages when a wireless LAN controller attempts multiple roots to verify Cisco lightweight access points.
- CSCsb30070—Added web interface support for 7920 IP phone QBSS and DTPC on the WLANs > Detail page.
- CSCsb30211—Cisco Aironet lightweight access points no longer continue rebooting when WMM mode is enabled.
- CSCsb30688—The Cisco lightweight access point RF channel assignment web interface page now shows correct values in the drop-down boxes.
- CSCsb30945—The ESC boot prompt now appears at all 115200 baud rates.
- CSCsb31596—Cisco Aironet 1000 series lightweight access points no longer crash when they have only one radio.
- CSCsb31686—Cisco lightweight access points now join a wireless LAN controller using the IP address discovered via DNS.
- CSCsb32061—The wireless LAN controller CLI now allows users to configure a Bridge Group Name for bridge access points.
- CSCsb32107—Corrected a crash when viewing bridging information from the AP list page.
- CSCsb32275—All wireless LAN controller user interface locations referring to the access point MAC addresses now clarify whether they are the Ethernet or BSS MAC addresses.
- CSCsb32630—Cisco Aironet 1500 series lightweight outdoor access points no longer crash after joining a wireless LAN controller.
- CSCsb32669—Corrected the Cisco lightweight access point code to not send any deauth frames to the wireless LAN controller.
- CSCsb33161—XAUTH IPsec WLAN now passes traffic when AAA override is enabled.
- CSCsb33499—RADIUS Auth failure trap is now generated upon auth failure.
- CSCsb33946—WiSMs no longer crash with 150 associated Cisco lightweight access points.
- CSCsb34222—Setting the Cisco lightweight access point 802.11a transmit power level to 8 no longer fails when the wireless LAN controller is in UK mode.
- CSCsb34766—The wireless LAN controllers no longer crash when configuring the internal DHCP server on a foreign wireless LAN controller.
- CSCsb35674—Enabling or disabling the 802.11b/g global RF network no longer causes an error.
- CSCsb35799—The wireless LAN controllers no longer crash when deleting the RADIUS accounting server.
- CSCsb36093—When the country code is set to DE, 802.11b/g channels 12 and 13 are now available.
- CSCsb36379—Users can now enter a 64-character shared secret.
- CSCsb37006—The timestamp on the DFS scan message when a Cisco lightweight access point boots up is now accurate.

- CSCsb37836—Users can now edit the local net user to change access back to any WLAN.
- CSCsb37979—All 802.11a channels are now available in the -S channel set.
- CSCsb38416—Users can perform an administrative shutdown on the GigE supervisor interface and the show port summary command on the wireless LAN controller now displays the link down.
- CSCsb39203—Cisco Aironet 1000 series lightweight access points no longer reset when the ethernet link is disconnected.
- CSCsb39464—Cisco Aironet 1500 series lightweight outdoor access point wireless clients associated to a pole-top Cisco lightweight access point can now ping the gateway.
- CSCsb39891—The hapiMmcTimerTick task no longer crashes on the wireless LAN controller.
- CSCsb40376—Cisco Aironet 1000 series lightweight access points no longer crash when detecting radar.
- CSCsb41433—Client exclusion on authentication failure is now working correctly.
- CSCsb41543—Cisco Aironet 1000 series lightweight access points are now using the correct value for CWMIN and CWMAX for various data queues.
- CSCsb42133—When editing a WLAN, on entering an invalid value for session timeout, the correct range is now shown to the user in the error message.
- CSCsb43843—The Symbol 9060g scanner now authenticates using LEAP.
- CSCsb43919—The service port now receives an IP address when DHCP is disabled and enabled.
- CSCsb46318—The internal DHCP server is now working correctly.
- CSCsb46987—REAP Cisco Aironet 1130 series lightweight access points now change channels after reconnecting with the wireless LAN controller.
- CSCsb47135—Users can now remove a mobility anchor from a WLAN using the web interface without first disabling the WLAN.
- CSCsb50067—Corrected a typographical error in the IDS signature file for Wellenreiter detection.
- CSCsb50431—L2TP termination via IPSec now works with NAT-T packets.
- CSCsb51395—In the Preview page users no longer receive runtime error messages.
- CSCsb53803—The internal DHCP server no longer fails when the last byte of the network address is non-zero.
- CSCsb55516—Symbol handheld running Windows Mobile 2003 can now connect to the wireless LAN controller using L2TP/IPsec.
- CSCsb57027—The wireless LAN controllers no longer crash because of IPsec-related mobility events with many clients.
- CSCsb57305—Cisco Aironet lightweight access points no longer transmit beacons after the associated wireless LAN is deleted from the wireless LAN controller.
- CSCsb58091—Made changes in LWAPP code so that it remains portable.
- CSCsb59664—Config erase now clears AP-Group VLAN configurations.
- CSCsb59724—Custom-web config no longer lost when upgrading code.
- CSCsb61049—LAG configuration support now available through the wireless LAN controller web interface.
- CSCsb62289—The transmit power values for Cisco Aironet 1500 series lightweight outdoor access points are now correct in the wireless LAN controller web interface and in Cisco WCS.

- CSCsb62833—Added support to the Cisco 2000 Series Wireless LAN Controller for the foreign side of the auto-anchor (guest WLAN) feature.
- CSCsb63479—Clicking the Refresh link on the Cisco APs page no longer results in a Page Not Found error.
- CSCsb64519—Added four new PEAP-GTC CLI config advanced eap commands (identity-request-timeout, identity-request-retries, request-timeout, and request-retries) to support authenticating via a one-time password to a token server.
- CSCsb65096—The Cisco lightweight access point security key no longer loses synchronization with the wireless LAN controller, thereby allowing the Cisco lightweight access point to connect using LWAPP to the wireless LAN controller.
- CSCsb65658—The wireless LAN controllers no longer crash when handling WEP+ cache timeouts.
- CSCsb65731—Added a fix for initializing the bridge group key before setting it.
- CSCsb66875—IPSec WLANs no longer stop working because of memory leaks.
- CSCsb67400—Sometimes REAP Cisco Aironet 1130 series lightweight access point clients lose network connectivity, while the REAP is still seen by Cisco WCS and while the client is still associated. Resetting the REAP recovers the client network connectivity.
- CSCsb70361—Cisco lightweight access points no longer disassociate when port admin mode is disabled.
- CSCsb70966—Corrected a mistake in bitwise manipulation on a bootup notification change.
- CSCsb71400—Now able to change the VLAN ID for dynamic interfaces using the web interface.
- CSCsb72480—Updated the country code table to the latest values.
- CSCsb72663—Modified the procedure to install Cisco device certificates for WiSMs.
- CSCsb72697—In L3 LWAPP, UDP packets with more than two fragments are forwarded instead of being dropped.
- CSCsb73853—Added support for static and dynamic WEP on the same WLAN.
- CSCsb74034—Added the following non-LAG to LAG events: (1) Disable all WLANs and map them to the management interface. (2) Delete all dynamic AP manager interfaces. (3) Delete all untagged dynamic interfaces. (4) When enabling the LAG interface, display the following confirmation message: “Note - Enabling LAG will map your current interface configuration to LAG interface, all dynamic AP manager interfaces and untagged interfaces will be deleted. All WLANs will be deleted and mapped to management interfaces. Are you sure want to continue?”

  LAG to non-LAG events: All interfaces are mapped to port 1.

  When disabling the LAG interface, the following confirmation message appears: “Disabling LAG will map all existing interfaces to port 1. Are you sure want to continue?”
- CSCsb74041—The SSC hash key is now displayed correctly for Cisco Aironet 1130 series lightweight access points.
- CSCsb74528—Corrected processing of association request frames at the wireless LAN controller.
- CSCsb74844—Added WiSM code to disable PCI, Rapid IO and FE in the devdisr register.
- CSCsb75121—Generated crash file now includes NPU 0 and 1 in dual-NPU wireless LAN controllers.
- CSCsb752843—Corrected the WiSM GUI Monitor page to remove the incorrect model type displayed for WiSM.
- CSCsb76113—The SRAM UPM timing was corrected.

- CSCsb76240—The phone support variable is now initialized before doing ‘or’ and ‘and’ operations.
- CSCsb76710—The correct QBSS value is reported for element 11 / length 4 and element 221.
- CSCsb77161—The Cisco Aironet 1500 series lightweight outdoor access point receiver saturation performance has been improved to comply with the IEEE 802.11 maximum receiver saturation specification. Cisco Aironet 1500 series lightweight outdoor access points can now be placed as close as 33 feet apart without experiencing increased packet error rate and without turning down the transmitter power.
- CSCsb77410—Corrected the show interface detailed command response to display LAG and 29 when a LAG is enabled.
- CSCsb77487—Updated LAG debug messages.
- CSCsb77493—Corrected the message log so that when the service port is disconnected, the wireless LAN controller no longer detects network loop messages.
- CSCsb77761—No longer receiving frame length out of bounds error messages on the CLI console.
- CSCsb77881—The idle timeout now works on REAP Cisco lightweight access points.
- CSCsb78726—Corrected the code so L2TP debugs no longer show passwords in clear text.
- CSCsb79228—Multicast is now working on the second Cisco 4400 Series Wireless LAN Controller NPU.
- CSCsb79267—The LAG option can no longer be disabled for those platforms, such as the WiSM, in which the LAG is not optional.
- CSCsb79282—The show lag port hash output now matches the actual port numbering.
- CSCsb79395—The LAG function no longer experiences an interface initialization error.
- CSCsb80402—Cisco 2000 Series Wireless LAN Controllers now prompt with an error message when running the install script.
- CSCsb80561—Cisco lightweight access points now join a wireless LAN controller after they reset.
- CSCsb81759—Made changes to the WiSM dynamic SDRAM configuration to support future memory modules.
- CSCsb82767—Updated the session timeout to work correctly with webauth.
- CSCsb8286—During bootup the WiSM no longer generates a bad CRC error.
- CSCsb83130—Cisco 2000 Series Wireless LAN Controllers no longer send web auth client DNS queries out over the management port instead of over the client's dynamic interface before client authentication.
- CSCsb83539—The Controller > General web interface page configuration entries can now be changed.
- CSCsb83552—The web interface now shows the mobility anchor IP addresses in the WLAN Mobility Anchors page.
- CSCsb84030—The wireless LAN controllers no longer display VLAN modify error messages when booting.
- CSCsb84451—Users are now able to configure the Cisco 4400 Series Wireless LAN Controller management IP address using the configuration wizard.
- CSCsb85034—When users enable WME or WMM on wireless LAN controllers, the TXOP values are now transmitted in the correct format.
- CSCsb85116—The bsnTemperatureAlarmHighLimit & bsnTemperatureAlarmLowLimit functions now work correctly.

- CSCsb85978—Cisco lightweight access point radios can no longer be activated when set to disabled.
- CSCsb86060—Added a fix for the top WLAN link on the Monitor Summary page.
- CSCsb87107—Cisco lightweight access points no longer crash because they receive incorrect information in the LWAPP header.
- CSCsb87766—Show AP summary now reports the correct ports for associated Cisco lightweight access points.
- CSCsb88572—Editing a WLAN using the web interface no longer disables its auto anchor status.
- CSCsb89184—ARP responses from multiple AP managers to a Cisco lightweight access point are no longer sent out via the wrong ports.
- CSCsb89779—Overrides are now applied to the export anchor.
- CSCsb90244—The web interface MAC filtering screen is now more usable.
- CSCsb9084—Added new -P access points, which use country code JP2. The system fully supports both the UNII 1 and UNII 2 changes in the new frequency plan as well as the normal 2.4 GHz channels.
- CSCsb91061—IPSec clients can now pass traffic when connected with a Cisco 4400 Series Wireless LAN Controller equipped with a VPN Termination Module.
- CSCsb92188—In Cisco Aironet 1500 series lightweight outdoor access points, the interaction between auto scan and BMK is now working correctly.
- CSCsb92303—In the web interface, the session timeout (seconds): 0 is a correct value.
- CSCsb92724—When the number of clients is greater than the number of key cache entries, and the clients connect using WPA and TKIP, packets are no longer dropped.
- CSCsb93202—Cisco lightweight access points no longer crash with spam tasks named in the AP log.
- CSCsb93624—Made the error message that appears when the key length is misconfigured more meaningful.
- CSCsb93817—The wireless LAN controllers no longer crash without a crash file output.
- CSCsb94179—In WiSMs, corrected the Cisco lightweight access point certificate operation.
- CSCsb95006—When connected to Cisco 4100 Series Wireless LAN Controllers, REAP Cisco Aironet 1030 remote edge lightweight access points no longer spontaneously reboot.
- CSCsb95888—When the IP address of a Cisco lightweight access point changes (from DHCP, for instance), clients now receive an updated IP address when the lease times out and it completes a DHCP discover.
- CSCsb96680—Corrected the multicast configuration in Cisco 2000 Series Wireless LAN Controllers and WiSMs.
- CSCsb96850—Made changes to combine FPGA bitfiles and to remove the SVC-WXSM string as name.
- CSCsb98031—In Cisco Aironet 1500 series lightweight outdoor access points, prevented locking or unlocking the backhaul device to prevent the backhaul link to repeat a DFS scan.
- CSCsb98097—In the Taiwan regulatory domain the maximum power for channels is now displayed correctly.
- CSCsb98172—The WEP and 802.1x configuration now works correctly.

- CSCsb98213—When Cisco Aironet 1030 remote edge lightweight access points and Cisco Aironet 1500 series lightweight outdoor access points in bridging mode are to be used as pole-top access points, they no longer need to be configured as pole-top access points before they are deployed in the network.
- CSCsb98376—WEP and 802.1x clients are now able to authenticate.
- CSCsc04140—In the -CH country code ETSI domain, the wireless LAN controller correctly displays the maximum power for the 5 GHz radio as 14.5 dBm.
- CSCsc05054—When setting the enhanced multicast address, there is no show command that tells the multicast address to which the AP will join. The web GUI always shows 255.255.255.255. We need this to see the multicast address which the AP will join.
- CSCsc05207—The TooManyUnsuccessLoginAttempt trap was not working, so that anyone logging in via Telnet, HTTP, HTTPS, or the console port with an incorrect password more than three times did not generate any trap information in the trap logs.
- CSCsc07648—The wireless LAN controller fanFailureTrap and powerSupplyChange traps now work as expected.
- CSCsc08130—RRM in large RF groups no longer causes Cisco Aironet lightweight access points to restart LWAPP connections because of ECHO timeouts.
- CSCsc12019—The wireless LAN controllers no longer crash because of packets of invalid length.
- CSCsc13711—The wireless LAN controllers now accept IPSec authentications from clients.
- CSCsc14331—Cisco 4100 Series Wireless LAN Controllers no longer crash with the emWeb task.
- CSCsc14801—DHCP Option 43 now works on Cisco Aironet 1000 series lightweight access points and Cisco Aironet 1200 series lightweight access points when using the vendor.id option.
- CSCsc19717—Re-authentication is no longer being triggered in groups. In addition, the granularity of re-authentication timers has been changed to 25 seconds.
- CSCsc22899—Cisco lightweight access points no longer crash.
- CSCsc24609—The DSCP value is now set correctly by Cisco lightweight access points.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at the following location:

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

Click **Technology Support**, select **Wireless** from the menu on the left, and click **Wireless LAN**.

Related Documentation

For information on the Cisco Unified Wireless Network Solution and for instructions on how to configure and use the Cisco UWN, refer to the *Cisco Wireless Control System Configuration Guide* and the *Cisco Wireless LAN Controller Configuration Guide.*

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.