Release Notes for Cisco Wireless Control System 3.2.64.0 for Windows or Linux

June 5, 2006

These release notes describe open caveats for the Cisco Wireless Control System 3.2.64.0 for Windows or Linux, which comprises part of the Cisco Unified Wireless Network Solution (Cisco UWN).

The Cisco Wireless Control System is hereafter referred to as *Cisco WCS.*

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

UWN Components

The following components are part of the Cisco UWN:

- Operating system (Wireless LAN Controller and Cisco Aironet Lightweight Access Points)
- 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 Wireless Services Module (WiSMs) for Cisco Catalyst 6500 Series Switch
- Cisco WLAN Controller Network Modules for Cisco Integrated Services Router
- Cisco Aironet 1000 Series Lightweight Access Points
- Cisco Aironet 1130 Series Lightweight Access Points
- Cisco Aironet 1200 Series Lightweight Access Points
- Cisco Aironet 1230 Series Lightweight Access Points
- Cisco Aironet 1240 Series Lightweight Access Points
- Cisco Aironet 1500 Series Lightweight Access Points

Requirements for Cisco WCS

The following server hardware and software is required to support Cisco WCS for Windows or Linux:

- Requirements for Cisco WCS Server – Cisco WCS can be run on a workstation/server class system:
    - For up to 500 Cisco Aironet lightweight access points: 2.4 GHz Pentium processor with 1 GB RAM.
    - For over 500 Cisco Aironet lightweight access points: dual processors (at least 2.4 GHz each) with minimum 2 GB RAM.
    - 20 GB of free space on your hard drive.

    The following operating systems are supported:
    - Windows 2000/SP4 or later, or Windows 2003/SP1 or later with all critical and security Windows updates installed.
    - Red Hat Enterprise Linux ES 3.0.
- Requirements for Cisco WCS User Interface – The Cisco WCS user interface requires Internet Explorer 6.0/SP1 or later, with the Flash plugin. The Cisco WCS user interface has been tested and verified using Internet Explorer 6.0 on a Windows workstation.

Software Information

Cisco WCS 3.2.64.0 is now available. As new releases become available for Cisco WCS, consider upgrading.

Finding the Software Release

To find the software release Cisco WCS is running, refer to the *Cisco Wireless Control System Configuration Guide.* If WCS is already installed and you are connected, verify the software release version in the Help > About the Software option.

Upgrading to New Software

For instructions on installing a new Cisco WCS software release, refer to the instructions in the *Cisco Wireless Control System Configuration Guide.*

New Software Features in Release

Multiple WLANs can use the same WEP key index (referenced as resolved bug CSCsd46973).

Important Notes

This section describes important information about Cisco WCS.

Changing Default Password

To ensure security of the application, you should immediately change the default WCS password.

Cisco WCS Upgrade

Cisco WCS for Linux supports database upgrades only from the following official Cisco WCS releases: 3.0.101.0, 3.0.105.0, 3.1.33.0, 3.2.23.0, 3.2.25.0, 3.2.40.0, and 3.2.51.0.

Compatibility

This release of Cisco WCS for Windows or Linux is compatible with wireless LAN controller and Cisco Aironet lightweight access point operating system 3.0 or later.

Single Cisco WCS per Wireless LAN Controller

The UWN is designed so that one instance of Cisco WCS can be used to configure, monitor, and operate each set of wireless LAN controllers. This design ensures that the wireless LAN controllers are properly represented in Cisco WCS (CSCsc42249).

MCS7800 Servers

Cisco MCS7800 servers are not supported as Cisco WCS servers.

Cisco WCS Physical Location and IP Addresses

Cisco WCS should be run on a robust desktop or rack-mount machine in a server room, but the Cisco WCS user interface can be run on any Windows workstation.

Workaround: If you need to change the IP parameters on the Cisco WCS workstation, such as the IP address or the default gateway, shut down Cisco WCS before making the change, and start Cisco WCS after your IP configuration changes are complete.

Map Rendering

When you have more than 200 tags, clients, or rogues on a maps page, map-page rendering can be slow. The browser may temporarily freeze during the first rendering and when it renders at every refresh interval.

Workaround: Cisco recommends that the user limit the number of visible entries to 200 for each asset type (client, tag, rogue access point, rogue client) and then save that as the default view if more than 200 of any asset type are expected on a map.

Background Policies Time Intervals

The default time intervals for scheduled policies give optimal performance when Cisco WCS is monitoring up to 500 Cisco Aironet lightweight access points.

Workaround: When Cisco WCS is monitoring more than 500 Cisco lightweight access points, increase the time intervals to the following values:

- Device Status Policy—12 minutes
- Statistics—30 minutes
- Client Statistics—30 minutes
- Rogue AP—120 minutes

Manually Executing Scheduled Tasks

Manually executed scheduled tasks (device status, client statistics, rogue access point, and statistics) do not run immediately if any of the other tasks are already running. Instead, Cisco WCS queues and executes them as soon as the running tasks are completed.

Workaround: Wait for the manually executed scheduled tasks to complete.

Polling Intervals

The poll interval for Cisco 2700 series location appliances is the time between polls (CSCar15324). When the poll interval is set to 1 second, and the actual poll takes 20 seconds, the start of each poll is 21 seconds apart.

Workaround: Wait for the polling interval to complete.

Slow Imports of FPE Files with More Than 200 Walls

Importing a floor plan editor (FPE) file with more than 200 walls can be slow, and the browser may not report any status or redirect you to any other page.

Workaround: Do not click anywhere on the map page for at least 5 minutes before you try to verify that the file is imported.

Calibrating the Location Model Using Cisco Aironet 802.11a/b/g Wireless Cardbus Adapter Clients

Cisco Aironet 802.11a/b/g Wireless Cardbus Adapter (AIR-CB21AG) clients are not ideal for calibrating the location model (CSCsb52149). The AIR-CB21AG clients do not send the SSID in the probe request when the Broadcast SSID is disabled on the wireless LAN controller.

Workaround: Use an approved wireless client, such as Netgear WAG511.

Restoring an Upgraded Cisco 2700 Series Location Appliance to an Earlier Release

A backup from the latest release of Cisco 2700 series location appliance software cannot be restored on a location appliance running an earlier release (CSCsb54606).

Workaround: Before you upgrade a location appliance to the latest release, Cisco recommends that you create a backup for the earlier release and archive it in case you need to return an upgraded location appliance to an earlier release.

Managing Cisco Wireless Services Modules using Cisco WCS

Unlike other wireless LAN controllers, Cisco Wireless Services Modules (WiSMs) use their service ports to communicate with the Cisco Catalyst 6500 series switch supervisor. The Cisco WCS server uses the WiSM data port to connect to and control the WiSM and its associated Cisco lightweight access points (CSCsb49178).

Using the Cisco WCS Map Editor Tool

Creating a map directly by using a file image from the floor plan editor (FPE) tool is no longer allowed in Cisco WCS. The option to import this type of file is not present in the user interface and attempting to import the file causes Cisco WCS to generate a message indicating that the user needs to enter a valid JPG or PNG image (CSCsb04081). The workaround is to create a map with a regular image and later use the option to edit the floor and reimport the map image with an FPE file. The FPE tool is no longer supported in Cisco WCS. Users are encouraged to use the new Map Editor tool provided within Cisco WCS to draw obstacles, etc.

Using Microsoft Windows 2003 Browsers with Cisco WCS

Browsing on Windows 2003 Cisco WCS servers is not recommended because recommended Windows 2003 security settings cause browsing problems.

Caveats

This section lists open caveats in Cisco WCS 3.2.64.0 for Windows and Linux.

Open Caveats

These caveats are open in Cisco WCS 3.2.64.0.

- CSCar13120—Cisco WCS fails with a null pointer exception because it cannot resolve the name-address of the network DNS server. The Cisco WCS software appears to have conflicts with a DNS name resolution server running on the same Cisco WCS server. The server is configured for DHCP, which receives a name-address resolution from a network server, but Cisco WCS attempts to resolve the name-address locally.

  Workaround: Run the DNS server on another workstation, fix the name resolution problem on the Cisco WCS server, or remove the local DNS server.

- CSCar13328—Null pointer exception is being logged to the stderr file when starting Cisco WCS on a Linux system with Cisco WCS and a DHCP server running.

  Workaround: Disable DHCP on the Linux system running Cisco WCS.

- CSCar13891—Client search by IP Address takes a long time because rate limiting on the wireless LAN controller starts too quickly, which causes SNMP timeouts.

  Workaround: Change the SNMP timeout values so that SNMP does not timeout during queries. Use 2 seconds and retry 4 for reasonable performance.

- CSCsa93016—While running IE from a Windows 2003 machine, the browser times out when attempting long running tasks like deleting multiple switches from WCS.

- CSCsa93250—Resizing a floorplan using "Edit Floor" does not resize coverage areas.

  Workaround: Use the Map Editor for floor resizing. This is not recommended since it does not maintain aspect ratio. The purpose of the Floor > Edit page is to change image, floor name, or other properties.

- CSCsb15455—Cisco WCS shows timestamps for location server details and history pages based on the Cisco WCS location and not based on the location server timestamp.

  Workaround: If the location server is in one time zone locating objects across multiple time zones, and if a user is in a different time zone accessing the information through Cisco WCS, the time stamps are based on the second Cisco WCS time zone timestamps. The time is correct for all the objects located in the second Cisco WCS time zone.

- CSCsb17095—When you add an invalid IP address as a network route, the IP address is added to WCS but not to the wireless LAN controller.

  Workaround: Do not add invalid IP addresses as network routes.

- CSCsb35470—In the Cisco WCS map editor, zooming is not context specific based on your mouse pointer location.

Workaround: Use the scroll bar to move anywhere on the floor map after zooming.

- CSCsb39611—The uninstaller fails with an error of "unable to locate executable." When you install Cisco WCS, if you place two spaces together in the path name, such as "C:\WCS 31," the install is completed correctly, but the uninstall will fail.

  Workaround: Remove one of the extra spaces in the pathname, and the uninstall should work properly.

- CSCsb41890—Under Monitor > Device > Access Points > (any AP) > 802.11a or 802.11b/g, a table at the bottom of the page is incorrectly titled "Radio MAC Address." It should be titled "Rx Neighbors."

- CSCsb60808—For Windows 2003 users running WCS with an IE client active from a host machine, an IE error can occur. When creating a template under Configure > Templates > Security, a window appears in which templates can be applied to controllers. If Cancel is chosen, an IE error appears. The template is created but does not get applied to controllers, which is the expected behavior.

  Workaround: The procedure actually works, so no workaround is needed. However, browsing on Windows 2003 is not recommended because the recommended security settings for that operating system causes browsing problems.

- CSCsb76160—Rogue and security alarm messages are misleading. A message may read that the alarm is clear and no longer detected. In actuality, the alarm is cleared from the access point name and is still detected by three radios.

- CSCsb98820—Certain security combinations set from Cisco WCS result in SNMP errors, such as Layer 2 802.1x and Layer 3 VPN passthrough with webauth.

  Workaround: These combinations of security settings are not supported. Choose another combination.

- CSCsc07883—On the Network Summary page in the Most Recent Rogue APs table, the SSID is missing.

  Workaround: Click on the MAC Address to see the alarm details, and if the SSID is known, it is listed in the alarm.

- CSCsc22389—The wireless LAN controller system name changes after some time when originally entered from the controller web interface or CLI. This happens only when there is a mismatch between the system name on the controller and in Cisco WCS. When this occurs, Cisco WCS overwrites the system name in the controller.

  Workaround: If the wireless LAN controller is added to Cisco WCS, change only the system name from Cisco WCS. Refresh the configuration from the controller to maintain the same configuration settings on the controller and in Cisco WCS.

- CSCsc23186—Cisco WCS cannot be installed when username contains special characters, such as exclamation marks (!).

  Workaround: Install WCS after logging in as a user with no special characters in your username.

- CSCsc30066—When you uninstall WCS, not all directories are removed.

  Workaround: Manually remove C:\Program Files\WCS32\jre\lib\endorsed, C:\Program Files\WCS32\jre\lib, and C:\Program Files\WCS32\jre.

- CSCsc32975—When the monitor is set for a maximum resolution of 800 x 600 pixels and the browser size is maximized, the information in the Client Summary page overlaps the left-hand menu bar.

  Workaround: Change the monitor resolution to a width of at least 960 pixels.

- 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 745 to 5825 MHz band. 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 3 are supported (in the case of 5500 to 5700 MHz), 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 1, 2, or 3 for all other bands.

- CSCsc39959—When managing a Cisco 2700 series location appliance with software release 1.x using Cisco WCS software release 3.2, a search for specific elements on the location appliance (by MAC address, asset name, group, or category) returns no results, even though the same elements can be seen in the maps and the overall list.

  Workaround: Upgrade your location appliance to software release 2.0. Alternatively, search for the elements in the exact letter case as those originally defined in the MAC, asset name, group, or category (such as if the element was in lowercase, you must search for the value in lowercase).

- CSCsc39976—When you change the units of measurement from feet to meters in Cisco WCS maps, the coverage area does not scale.

  Workaround: Set the units of measurement first and then draw the obstacles and coverage areas.

- CSCsc46598—When you perform a Cisco lightweight access point planning site survey, some items may appear 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 found.

- CSCsc59180—When a rogue access point is detected by WCS and when a user sets the state to *Known - External*, Cisco WCS displays the access point as *Trusted Missing*.

- CSCsc59986—Controller configuration and Cisco WCS are not synchronized after creating a dynamic interface with capital letters in the name.

  Workaround: Create dynamic interface names without capital letters.

- CSCsc61197—An exception error message appears when you click the access point name on the Configure > Access Point window. This message should only appear when the access point is switching from disassociated to associated state on the controller.

  Workaround: Refreshing the erred list page on the browser eliminates the error message. All successive attempts at navigating to the detail page will work.

- CSCsc67765—You cannot use hexadecimal when setting preshared keys for WPA in WLANs. Some phones, like Vocera, require the key to be hexadecimal.

  Workaround: In the 3.2 MR1 release of the controller, you can configure this using the CLI. You cannot configure it with WCS.

- CSCsc90237—When you configure DHCP on a controller using WCS, the lease time is inaccurately displayed in seconds rather than minutes.

- CSCsc92240 - WCS can't delete an interface containing capital letters. When a dynamic VLAN is created on WCS using capital letters, deleting the interface through WCS brings the "SNMP operation to device failed" message.

- CSCsc99816—When you try to add a dynamic interface and set the VLAN ID as 0 (untagged), an *SNMP operation to device failed* error occurs if LAG is enabled on the controller. You can only add one dynamic interface with VLAN ID as 0.

  Workaround: No workaround exists. A warning message that this operation is not allowed will be added to WCS.

- CSCsd05107—When you perform a search using Monitor > Clients and filtering by protocol, 802.11g users are not shown even if they were selected.

  Workaround: If you don't use the filtering option in which you specify certain protocols, all users are displayed.

- CSCsd07119—When you apply a template to a controller that contains parameters incompatible with other configuration settings on a controller, an *SNMP operation to device failed* message appears.

  Workaround: Make the same configuration change on the controller UI. When the controller UI returns a specific error message indicating where the problem occurred, you will know which template parameters are causing the problem. Correct the template or modify the controller settings so the template can be applied without errors.

- CSCsd30763—When a campus or a building without a campus has a name containing an open parenthesis followed by a period, such as San Diego (1st St.), WCS may be unable to synchronize this element with the location server.

  Workaround: Remove the parenthesis from the name. The period can remain. Try to synchronize again.

- CSCsd91001—When a user upgrades from WCS release 2.0.83.0 to 2.2.86.0 using a backup file, the ability to add new users to the 2.2 image was not allowed. An error message appears stating that the user does not have permission to perform this operation and that super users permissions are required.

  Workaround: Perform the upgrade without using the 2.0 backup file.

- CSCsd93796—Traps are sent by the controller and are processed by WCS sequentially. Events are created and put in a queue, and alarms are updated when the event is taken off the queue. If the alarm meets certain criteria, an email is sent. Timestamps shown in the email reflect the time the email was sent but not the time of the actual event.

  Workaround: There should be a delay between when the event is created and when the mail is sent if there are many events in the queue. Make sure the mail server does not create delays when receiving alerts from WCS. Ensure that the identification protocol and DNS-related delays are set appropriately.

- CSCsd95144—Location data for a client is collected periodically from the network and stored in the location history table. The state of clients that have already been disconnected may incorrectly appear as Associated in the location history table.

- CSCsd98732—The 2000 series controller does not have 802.3 flow control configuration.

- CSCse00886—If you enable the Pico Cell Mode check box, an error message displays. It states that the SNMP operation to device failed. (You access the Pico Cell Mode check box by choosing Configure > Controllers. Click to select a controller from the IP address column and then choose 802.11a > Parameters from the left sidebar menu.)

- CSCse04117—You cannot create a template in WCS that has the same name as one created on the controller.

  Workaround: Remove the duplicate template. Go to Configure > Controller Templates > Management > Trap Receivers to find the template.

- CSCse04554—You may see an alert that an impersonation is detected by an authenticated access point, but the source MAC address isn't given so that you can determine the hardware that caused the issue.

- CSCse11202—Wireless clients running TKIP are reported in the WCS logs as having an incorrect WEP key.

- CSCse20068—Using WCS 3.2, an access point's statically assigned IP address can be overwritten when making changes (such as name, primary controller, etc.) on controllers older than 3.0.

- CSCse21104—An access point always shows the default antenna in planning mode, even if a different type is selected and saved. The correct antenna type shows on the map.

- CSCse21649—The trap logs state that an attack occurs on a 802.11b/g radio (Slot ID 0), but WCS incorrectly reports the attack on the 802.11a radio, which the access point does not even have installed.

Resolved Caveats

These caveats are resolved in Cisco WCS 3.2.64.0:

- CSCar13919—The problem of wireless LAN controllers being lost after reboot has been fixed. When any change in the Cisco WCS database is quickly followed by an abnormal termination of Cisco WCS (such as a hard reboot of the system), the newly changed information is retained upon a Cisco WCS restart.

- CSCsb90622—The false alarms in the access point impersonation detection have been repaired.

- CSCsc44897—WCS now correctly shows antenna orientation while viewing an object.

- CSCsc54952—A calibration performs as expected even if all RSSIs of the first calibration point are outside of the -80 to -40 dBm range. The correct process is to calculate each time a calibration point is added. The measurements are filtered to remove RSSIs that are too high or too low (outside the -80 to -40 dBM range), with a second filter to remove too small or too large of distances (outside the 10 to 100 ft range).

- CSCsc71820—When you configure an access control list (ACL) template and apply it to the controller, the DSCP value can be set to *any* or a DSCP specific value between 0 and 63.

- CSCsc90227—You can now configure DHCP on a controller using WCS without triggering an error.

- CSCsd05834—On a 1240 series access point, enabling WLAN override allows you to choose a power level of 8 without it being reported as invalid.

- CSCsd07433—When you create a trap receiver template in WCS, make an edit to the IP address created in this template, save it, and apply it to the controller, you get a successful message in WCS. On the controller side, this change was not reflected. You can now edit only the administrative status of the trap receiver template within WCS, and IP address and template name are read only.

- CSCsd15951—Database passwords are written with clear text on the program folders (c:\program files\WCS32\bin) rather than being hidden.

- CSCsd18053—You can now poll for client statistics and get new data from the location appliance (on the WCS Monitor > Devices > Client page). The controllers on WCS must be assigned to the location server for the graphs and values to appear correctly.

- CSCsd18463—A warning message was added to state that a connection status may change to non-responsive even though a download was actually successful. This warning message appears when performing a configuration download to the controller. (Choose Configure > Controller. Click to choose a controller and then choose System > Commands from the left sidebar menu. Select Upload/Download Commands > Download Config and click GO.) After the download is complete, the controller reboots.

- CSCsd23865—Calibration had been performing too slowly when using large numbers of measurements. Adjustments have been made so that the performance is no longer slow.

- CSCsd27755—In the Proposed AP Placement portion of the WLAN proposal, the access point direction and orientation now correctly show as one arrow at a time (802.11a and 802.11b/g are considered separately).

- CSCsd36639—An access point correctly shows an appropriately shaped heatmap when you import a floor map into WCS version 3.2.40.0.

- CSCsd42730—Even though the location appliance contained all the information about the maps, access point positions, and angles, the angles were not correctly transferred when adding this location information into a clean WCS install. This problem has been fixed.

- CSCsd46973—Multiple WLANs can use the same WEP key index.

- CSCsd49848—Regulatory support for Venezuela, Columbia, Peru, and Chile has been added.

- CSCsd54489—When you restart Cisco WCS after a database upgrade and restore from version 2.2, the StartWCS command no longer times out or causes an error response.

- CSCsd55773—When you went to Monitor > Maps, clicked on Properties, and chose Use Walls from the Calibration drop-down menu, an unknown exception occurred. Modifications were made to the Properties page so an exception no longer occurs.

- CSCsd66221—The default of the Network audit policy has been changed from enabled to disabled.

- CSCsd71397—If the TFTP path given during installation contained spaces, the path was not recognized by the TFTP server. This resulted in the root directory being used. The TFTP directory will now be kept even if extra spaces are included.

- CSCsd93023—When you attempt to change the AP Fallback state (or other settings on the Config > Controller > System > General page), a newly added warning message states that a WLAN is connected to a dynamic interface. This prevents an inadvertent deletion of WLANs and dynamic interfaces when you change the fallback state.

- CSCsd95310—When a backup file was greater than 2 GB, it was split into multiple .db* files, and the restore would appear unsuccessful. Now during a restore, the multiple source database files are consolidated into one file, and then migration is continued.

- CSCsd95890—When running WCS 3.2 and 3.2.5.1 on Windows, the database could overflow into a second database file if it was larger than 10GB. This caused the restore function to not operate properly. The database is now reconsolidated into one file so that the restore function performs correctly.

- CSCsd96213—Known rogue template entries will no longer be lost after you upgrade to a newer WCS software version.

- CSCse02292—You can add access point MAC addresses and access point templates even if the same MAC address already exists in the rogue alarms.

- CSCse03150—The correct event notification (for a campus, building, or floor) now appears for in/out campus events. The alert message is correctly stated.

- CSCse03184—The recompute prediction function in the map editor works properly after a software upgrade.

- CSCse05155—Choosing Configure > Controllers > 802.11a > General no longer responds in an error.

- CSCse14991—When the antenna pattern is changed, the antenna gain is now set correctly on the controller.

- CSCse15753—WCS may lock up when you add a controller with configured mobility anchors. This problem occurs because the controller returns mobility anchors in the order in which they were added rather than in numerical order. Eventually this problem can deplete JAVA virtual memory, thereby leaving WCS unable to perform any functions.

- CSCse20068—Any statically assigned IP addresses on 2.x controllers were overridden when changes were made to the access point (such as name, primary controller, etc.) on WCS version 3.2. This problem has been corrected.

- CSCse20372—The maximum value of service domains has been readjusted so that large customers can potentially add several new buildings or floors.

- CSCse22071—When you add both 802.11a and 802.11b/g access points and attempt to calibrate them, the calibration is successful.

- CSCse28098—An incorrect antenna gain warning has been removed. Previously, if an 1131 access point was added to a floor map and positioned, you received an error message that the antenna gain failed to update and that the antenna type should be set to external. An 1131 access point has only an internal antenna.

- CSCse30879—The function of adding an access control list and then editing a rule was not functioning as desired. A specific value could be added to DSCP and shown on the ACL template, but when the rule was later selected, the DSCP value was not preserved. These DSCP values are now retained.

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:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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