Release Notes for Cisco Wireless Control System 4.0.87.0 for Windows or Linux

October 20, 2006

These release notes describe open caveats for the Cisco Wireless Control System 4.0.87.0 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

Cisco Unified Wireless Network Solution Components

The following components are part of the Cisco UWN:

- Operating system (Wireless LAN Controller and Cisco Aironet Lightweight Access Point)
- 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 Catalyst 3750G Integrated Wireless LAN Controller
- Cisco Wireless Services Modules (WiSMs) for Cisco Catalyst 6500 Series Switches
- Cisco WLAN Controller Network Modules for Cisco Integrated Services Routers
- 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 1310 Series Lightweight Access Points
- Cisco Aironet 1500 Series Lightweight Outdoor Access Points
- Cisco Aironet Access Points running LWAPP

Requirements for Cisco WCS

This 4.0.87.0 software release supports WLC versions 3.1.xx to 4.0.0xx. The following server hardware and software is required to support Cisco WCS for Windows or Linux.

Hardware Requirements for Server

Cisco WCS can be run on a workstation or server, and access points can be distributed unevenly across controllers.

- High End Server—Supports up to 3000 Cisco Aironet lightweight access points and 250 Cisco wireless LAN controllers.
  - 3.15-GHz Intel Xeon Quad processor with 8-GB RAM and 200-GB hard drive.
  - 80-GB minimum free disk space is needed on your hard drive.
- Standard Server—Supports up to 2000 Cisco Aironet lightweight access points and 150 Cisco wireless LAN controllers.
  - 3.0-GHz Intel Dual Core processor with 4-GB RAM and 80-GB hard drive.
  - 40-GB minimum free disk space is needed on your hard drive.

- Low End Server—Supports up to 500 Cisco Aironet lightweight access points and 50 Cisco wireless LAN controllers.

    – 3.06-GHz Intel processor with 960-MB RAM and 30-GB hard drive.

    – 20-GB minimum free disk space is needed on your hard drive.

Note The free disk space listed is a minimum requirement but may be different for your system, depending on the number of backups.

Supported Operating Systems

The following operating systems are supported:

– Windows 2003/SP1 or later with all critical and security Windows updates installed. 64-bit operating system installations are not supported.

– Red Hat Linux Enterprise Server 4.0 or Advanced Server 4.0. Only 32-bit operating system installations are supported. 64-bit operating system installations are not supported.

Supported Browsers

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.

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

WCS on WLSE Appliance

Cisco WCS on a WLSE appliance supports up to 1500 Cisco Aironet lightweight access points and 100 Cisco wireless LAN controllers.

Note Windows operating system is not supported with the WCS on the WLSE appliance.

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 connected, verify the software release version by choosing Help > About the Software.

Upgrading to a New Software Release

To install a new Cisco WCS software release, refer to the instructions in the *Cisco Wireless Control System Configuration Guide.*

New Features

The following new features are available in the Cisco WCS 4.0.87.0 release:

- Running Cisco WCS on a CiscoWorks Wireless LAN Solution Engine (WLSE)
- Cisco WCS mobility group templates
- Cisco WCS licensing
- Cisco WCS and Cisco Aironet 1500 Series enhancements
  - Cisco WCS support for third-party antennas on the Cisco Aironet 1500 Series
  - Increased scalability of mesh information on maps
  - Hierarchical view of mesh access point associations
  - Improved heat-map accuracy for outdoor environments
- IDS Event Correlation
- Management Frame Protection (MFP)
- Cisco Compatible Extensions Version 4 (CCX)
- Guest access custom login screen
- Guest access Lobby Ambassador portal
- Hybrid Remote Edge Access Point (H-REAP)
- Unique Device Identifier (UDI)
- Regulatory domain updates

For more information, refer to the *Release Notes for Cisco Wireless LAN Controllers and Cisco Aironet Lightweight Access Points for Software Release 4.0.178.0* and bulletins at the following location:

http://www.cisco.com/en/US/products/ps6305/prod_bulletins_list.html

Important Notes

This section describes important information about Cisco WCS.

Changing the Default Password

The Cisco WCS default root password is *public*. Cisco advises changing the default password after the initial installation. Follow these steps to change the Cisco WCS default password.

Step 1   Log in as **root**.

Step 2   Select **Administration > Accounts**.

Step 3   From the User Name column, click **root**.

Step 4   Enter a new password in the New Password text box and retype the new password in the Confirm New Password text box.

Step 5   Click **Submit**.

Cisco WCS Upgrade

In order to be compatible, the Cisco WCS release must be the same or a more recent than the release on the controller. If an upgrade is planned, upgrade the Cisco WCS first to eliminate any unexpected issues. Cisco WCS for Linux supports database upgrades only from the following official Cisco WCS releases:

- 3.1.33.0
- 3.2.23.0
- 3.2.25.0
- 3.2.40.0
- 3.2.51.0
- 3.2.64.0
- 4.0.66.0
- 4.0.81.0

The last step in performing an upgrade is restoring the Cisco WCS database. The steps previously recorded on page 10-6 of the *Wireless Control System Configuration Guide* did not include those users restoring from a WCS version prior to 3.2 The following note was added to this section.

Note If you are restoring from a Cisco WCS release prior to 3.2, you must enter a directory rather than a backup file because tar/gzip did not exist prior to 3.2. Enter **DBAdmin restore** *directory*, where *directory* is the backup directory that you created.

IPSec Not Supported

Software release 4.0.87.0 does not support IPSec. If you upgrade to release 4.0.87.0 from a previous release that supported IPSec, any wireless LANs (WLANs) that are configured for this feature become disabled.

Limits to WebAuth Support on Hybrid-REAP Access Points

Access points in Hybrid-REAP mode support WebAuth only with Open Authentication if the wireless LAN (WLAN) has local switching enabled.

Compatibility

This release of Cisco WCS for Windows or Linux is compatible with wireless LAN controller and Cisco Aironet lightweight access point operating system 3.1 or later. Previous releases of Cisco WCS should not be used with the 4.0.87.0 controller software release.

Cisco WCS IP Addresses

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.

MCS7800 Servers

The Cisco MCS7800 server hardware is supported, but you must reformat the software so that it can be used as a Cisco WCS server.

Manually Executing Scheduled Tasks

Manually executed scheduled tasks (such as 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. Wait for the manually executed scheduled tasks 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 recommends using a Cisco Aironet 802.11a/b/g Wireless Cardbus Adapter (AIR-CB21AG) with the latest drivers. When using a card for calibrating, make sure it is CCX compatible and Version 2 or later. If the card is earlier than version 2 then it is not ideal for calibration.

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).

Losing WPA Encryption

When you create a WLAN template with Cisco WCS 4.0, you can choose to apply a WPA security policy. If you choose WPA or WPA2 security, save the template, and then apply the template to controllers running release 4.0, you receive a message that the template security was successfully applied. However, the WPA encryption actually gets removed from SSID configuration when the template is applied to the controller. This results in the SSID being left unencrypted.

Workaround: Create a template with WPA1+WPA2 security (or WEP), save the template, and then apply the template to the release 4.0 controllers. You can also configure all WPA encryption on the controller itself and not copy the templates to WCS.

Caveats

This section lists open caveats in Cisco WCS 4.0.87.0 for Windows and Linux.

Open Caveats

These caveats are open in Cisco WCS 4.0.87.0:

- CSCsc39959—No results are returned when searching for specific elements by MAC address, asset name, group, or category using WCS 3.2 to manage a 1.x location server. Even those elements visible in the maps and overall list may not appear.

  Workaround: Upgrade your location server to 2.0.0.

- CSCse04554—When the WCS server displays an access point impersonation alert, the source MAC address is not shown (as in the controller alert). This makes troubleshooting difficult.

  Workaround: None.

- CSCse47027—The poll stats policy sometimes fails when Mesh links are updated.

  Workaround: None.

- CSCse79012—After the WiSM controller is added to WCS, the Configure > Controller and Monitor > Controller pages sometimes show slot 0 port 0 under the Type column.

  Workaround: None.

- CSCse81548—The RADIUS template is incorrect when the information was copied from the controller configuration.

  Workaround: None

- CSCse87571—If a network state change trap is received for 802.11a or 802.11b, an alarm is created; however, the network, radio, access point, and map objects do not reflect the change.

  Workaround: None, although the situation eventually resolves itself if status polling is enabled. If you run status polling manually, you get the current status of the network, radio, access point, and map.

- CSCse88835—If you choose Configure > Controller, select a specific controller, change any properties, and click the Save button, the controller status becomes unreachable.

  Workaround: Do not change the controller properties from the base controller properties page. You can manually run the status poll if the controller status is wrong.

- CSCse90024— Clients cannot connect to access points if 128 WEP encryption is set.

  Workaround: If you are using 1200 or 1130 access points, do not choose 128 WEP encryption.

- CSCse95746—You should be able to configure WPA1 or WPA2 (on controller 3.2) and WPA1+WPA2 (on controller 4.0) with the same SSID.

  Workaround: None.

- CSCsf01292—The network route address should be in the same subnet as the management interface.

  Workaround: None:

- CSCsf09775—If you try to enable Fortress or Cranite as a Layer 2 security with WLAN, nothing happens.

  Workaround: None.

- CSCsf12509—A separate trap must be added in case the RADIUS server is not responding to a client.

   Workaround: None.

- CSCsf12520—WCS logs an incorrect WEP key error when a wireless client is running TKIP.

   Workaround: None.

- CSCsf14934—A WPA1 + WPA2 WLAN cannot be created if web authentication is enabled.

   Workaround: None.

- CSCsf24719—If the WCS configuration file has the TraceDisplay option set to true, any login attempts to WCS fail. Neither the default user credentials (root/public) nor any user-defined credentials will work to access WCS.

   Workaround: None.

- CSCsg09390—The 2106 controller .gif image only displays 4 ports rather than the actual 8 that exist.

   Workaround: None.

- CSCsg10769—In WCS release 4.0.81.0 or controller release 4.0.184.0, the device type for a 2106 controller is incorrectly shown as a 2000 controller.

   Workaround: None.

- CSCsg10990—If SNMP returned null pointer for the numberOfClients, WCS returned an exception.

   Workaround: None.

- CSCsg12197—Upon applying a configuration with WPA1+WPA2 security policy to a 2106 controller from WCS, the controller user interface incorrectly displays the security policy as "]."

   Workaround: None.

- CSCsg14182—If WLAN is enabled on WCS build 4.0.81.1 or controller build 4.0.188.0, you cannot apply a web redirect configuration. However, if the WLAN is disabled when the configuration is processed, the configuration is correctly updated on the controller.

   Workaround: None.

- CSCsg14229—The base WLAN definition is missing a multiset disable attribute or value. This multiset disable value was removed when the WLAN profileName was changed to metadata.

   Workaround: None.

- CSCsg17263—When you apply the system template to controller 2106, it fails. The template also cannot be deleted.

   Workaround: None.

- CSCsg20154—WCS will not start if the system timezone has been recently changed.

   Workaround: Use the **DBAdmin checkschema** command to reset the schema timestamp.

- CSCsg21266—The access point radio state changes to an unintended mode when you use the 802.11a template to change RF power levels of MESH radios.

   Workaround: None.

- CSCsg22177—RADIUS server configuration applied from WCS (build 4.0.81.1) is not updated on the controller when the controller (build 4.0.188.0) already has a related configuration on it.

   Workaround: None.

- CSCsg22262—The access point template should remember which access point the template was last applied to.

  Workaround: None.

- CSCsg22970—In WCS planning mode, a generated proposal, saved as HTML and viewed in a browser, does not display in the floor plan image.

  Workaround: Manually edit the HTML file and add the relative path to the floor plan image file.

  1. Using a text editor, open the html file as it was saved in the generated proposal.

  2. Search for the **/webacs/images/domainmaps** string and replace it with the path to where the image is stored.

- CSCsg23864—The shared secret key is displayed in clear text when configuring RADIUS authentication servers on WCS. This key needs to be masked with asterisks (*).

  Workaround: None

- CSCsg25368—Access points are incorrectly appearing as Acknowledged on the Minor Alarms list.

  Workaround: None.

- CSCsg28181—A ServletException appears if you apply an access point group VLAN configuration with a profile or WLAN ID which does not exist on the controller. These exceptions need to be detected and mapped to an error message which tells the user that the profile, WLAN, or SSID does not exist.

  Workaround: None.

- CSCsg28418—With WCS build 4.0.81.2 or controller build 4.0.189.0, an error message appears when you select the Apply to Controllers buttons on the RADIUS template screen. This error is specific to the 2006, 2106, and Boxer controllers.

  Workaround: None.

- CSCsg31725—A PartialOperationExceptions appears if you apply guest user configurations for certain lifetimes.

  Workaround: None.

- CSCsg32063—The VLAN profile count in the access point group is not being updated upon associating with an interface and a profile.

  Workaround: None.

- CSCsg32069—The WLAN template is not retaining its values. The security parameters based on Layer 2 and Layer 3 are displayed as static web pages with parameters such as CKIP, WPA, WPA2, 802.1x, etc. When you input values for these parameter and click Save, the template is not saved. Instead, it takes you to a new WLAN template page.

  Workaround: None

- CSCsg33092—A minor rogue access point may me labeled critical, but the next time the rogue access point task runs, the status is changed. The severity remains critical, but the message changes to "RogueAP made as Acknowledged AP."

  Workaround: None.

- CSCsg36206—When you set up a WLAN template, configure it with WPA1+WPA1, set a PSK, and select hexadecimal, you must assign a key. The key can only contain valid hexadecimal characters and can only be 64 hexadecimal characters long. However, if you enter more than 64 characters, no warning message is given.

  Workaround: None.

- CSCsg36501—The user assistant group does not have read-only access to alarms and events.

Resolved Caveats

These caveats are resolved in Cisco WCS 4.0.87.0:

- CSCar11402—The inconsistencies with the antenna diversity verbiage between WCS and the controller have been resolved.

- CSCsa97002—If a coverage hole is encountered during polling, the generated message provides more information than the original "unknown" alarm message.

- CSCsd85695—WCS was updated with the appropriate version of the JRE so that timezone information for Australia is now correct.

- CSCse02213—The RF Network Name field is now retained even after an upgrade from WCS release 2.2 to 3.2.

- CSCse22376—The Default Map Protocol View setting was removed from the Map > Properties page.

- CSCse49764—On the radio detail page, the access point name in Rx-Neighbor appears the same as the access point name of the radio. It should provide the access point name of the neighbor radio. Also, clicking on the access point name does not go to the access point detail page as desired.

- CSCse52851—The valid range for the DSCP Field is 0 to 255. If you enter a value outside of that range, an error warns you of the range.

- CSCse66255—When you add a rule to an ACL in the WCS template, you cannot add a rule number that already exists or insert a rule in the beginning or middle of an existing list. You will receive an error, and an exception will be generated on the logs.

- CSCse69855—The email address field on Monitor > Alarms > Email Notifications is limited to 56 characters.

- CSCse69904—The Maps page always sorts by the type (campus, building, or floor area).

- CSCse71841—If more than one campus exists and one is an outdoor area, the buildings to select from are accurately depicted and reflect the appropriate area.

- CSCse72323—In planning mode, automatic placement for Mesh access points (1500, 1505) is not accurate for outdoor areas. If you are using planning mode for an outdoor area and chose AP1500, the calculation of automatic placement is based on the indoor calculation.

- CSCse79377—If the licensed count of an access point is exceeded, the alarm that is generated is now complete, listing the severity level, giving a timestamp, and reporting complete information on the alert.

- CSCse89000—Access point group VLANs can now have commas in any part of the name. Prior to this fix, VLANs containing commas could not be sent to the WCS server.

- CSCse89225—While saving a template, the value for Local Power Constraint defaults to 1, accepts only values between 1 and 30, and displays an error dialog box if outside of the acceptable range.

- CSCse90043—Because H-REAP local switching is not allowed on WLAN IDs 9 to 16, the H-REAP local switching setting is now hidden.

- CSCse91247—Under certain circumstances, some events did not create or update relevant alerts. The root cause was orphaned entries in the database tables that slowed performance. The performance is now as expected.

- CSCse96812—The rogue client counts are now accurately represented.

- CSCse96819—The Web Policy check box status is maintained when opening the WLAN for editing.

- CSCse97619—WCS can now search for clients per building on all floors and receive accurate results.

- CSCse98623—When a general template was forwarded from WCS to WiSM, the DHCP configuration in the controller became corrupted. This is now fixed.

- CSCsf01767—If a user was assigned to any group and then a lobby ambassador group was added, the lobby ambassador privileges would overwrite all others. An error message now appears to warn against a lobby ambassador account being combined with any other group.

- CSCsf07475—The incorrect information shown on decrypt error traps has been addressed.

- CSCsf11953—The missing entry for WCP Peer Info caused an exception. The code has been adjusted to address this.

- CSCsf17545—The information for rogue clients is now provided.

- CSCsf19291—The heat map incorrectly showed coverage areas as squares rather than circular. The coverage areas are now represented appropriately.

- CSCsf23427—If a user tried to access alarms or events, they often received a message that they didn't have appropriate permissions. However, when clicking on OK, the alarms and events displayed anyway. The user assistant permissions have been corrected.

- CSCsf25102—When you added controllers that were part of WiSM, it caused an exception. Although the MIB variable names got changed, these changes were not making it to WCS. This exception no longer appears.

- CSCsg02389—Clicking on a map location inside the rogue detecting access point screen resulted in a servlet exception. You should be able to go to a rogue detail page and choose Detecting APs from the drop-down menu. Then click the map link for any detecting access points to go to the map floor view. All map location links in the rogue detecting access point list now direct you to the respective map page.

- CSCsg03907—If you attempted to remove an unassociated access point from the All APs page, an alert appeared and removal did not occur. This has been corrected.

- CSCsg05190—Additional server side authorization steps have been taken to monitor ambassador accounts: 1) a lobby ambassador user can only access 3 to 4 allowed URLs; 2) the Admin > Accounts menu and its related URLs can only be accessed by a user who has permissions for user administration; and 3) after logging in, a user is redirected to the welcome page for lobby ambassadors if they type in https://server_addr.

- CSCsg12596—The new daylight savings time rules have been incorporated into the code to reflect the changes made by the Energy Policy Act of 2005.

- CSCsg20819—The WCS performance degraded over time on a large network. This performance is tied into the AdventNet event table, and it has been scaled for improvement.

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.