Release Notes for Cisco Wireless Control System 4.0.97.0 for Windows or Linux

April 2, 2007

These release notes describe open caveats for the Cisco Wireless Control System 4.0.97.0 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 Unified Wireless Network Solution Components, page 2
- Requirements for Cisco WCS, page 2
- Important Notes, page 4
- New and Changed Information, page 7
- Caveats, page 7
- Troubleshooting, page 12
- Related Documentation, page 12
- Obtaining Documentation and Submitting a Service Request, page 12

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

Cisco Unified Wireless Network Solution Components

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

- Operating system (Wireless LAN Controller and Cisco Aironet Lightweight Access Point)
- Cisco Wireless Control System (Cisco WCS) software release 4.0.97.0.
- Location appliance software release 2.1.42.0
- Cisco 2700 Series Location Appliance
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 4100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Catalyst 3750G Wireless LAN Controller Switches
- Cisco Wireless Services Modules (WiSMs) for Cisco Catalyst 6500 Series Switches
- Cisco WLAN Controller Network Modules for Cisco Integrated Services Routers
- Cisco Aironet 1000, 1100, 1130, 1200, 1230, 1240, 1310, and 1500 Series Lightweight Access Point
- Cisco Aironet Access Points running LWAPP

Requirements for Cisco WCS

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 750 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

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

- 3.1.20.0
- 3.1.33.0
- 3.2.23.0
- 3.2.25.0
- 3.2.40.0
- 3.2.51.0
- 3.2.64.0
- 4.0.43.0
- 4.0.66.0
- 4.0.81.0
- 4.0.87.0
- 4.0.96.0

Note Scheduled task settings will not be preserved when upgrading from WCS release 4.0 or previous. Make sure to record your settings manually if you wish to retain them or go to Administration > Background Tasks after starting WCS to check or change the settings as necessary.

Note If you upgrade to a WCS software release later than 4.0.87.0 from a release prior to 4.0.87.0, the users, user groups, tasks, and user passwords will not migrate. Upgrading to 4.0.87.0 first before upgrading to a later release allows the migration of the user, user groups, tasks, and user passwords.

Important Notes

This section describes important information about Cisco WCS.

Applying a Combination of Valid L2 Policies with Conditional Redirect

A failure occurs if you apply a combination of valid L2 policies along with conditional web redirect as a L3 policy. The L2 and L3 policies should be set independently. First, set the L2 policy while keeping WLAN disabled, apply the setting to the controller, set the L3 policy to conditional web redirect, and then enable the WLAN.

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

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 4.0.96.0 does not allow you to choose IPSec as a Layer 3 Security option. None and VPN Passthrough are the only available options. If you upgrade to this release from a previous release that supported IPSec as a Layer 3 Security option, any WLANs that are configured for this feature become disabled. If you want to configure IPSec, you must use a version of controller software prior to 3.2 or wait for a future release.

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 4.0.97.0 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).

New and Changed Information

The wildcard character in the search window is a percent mark (%) rather than an asterisk (*).

Caveats

This section lists open and resolved caveats in Cisco WCS 4.0.97.0 for Windows and Linux.

Open Caveats

These caveats are open in Cisco WCS 4.0.97.0:

- CSCsd83836—The resolution of the WCS Map Editor is distorted and barely readable.

  Workaround: None.

- 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.

- CSCsg10906—If you enable IPsec when you are creating a RADIUS server template and then attempt to apply the configuration to the controller, you should receive a message that IPsec is not supported. Instead, applying the configuration to the controller returns a success.

  Workaround: None.

- CSCsg33092—On a Cisco WCS wired network, a minor rogue access point alarm can be designated as critical severity, but the next time the rogue access point task runs, the following error message appears:

  ```
  RogueAP made as Acknowledged AP.
  ```

  Workaround: None.

- CSCsg45499—If the Rogue AP Alarms on Cisco WCS exceeds 20, the No. of Entries field displayed in the last page always exceeds the displayed count by one.

  Workaround: None.

- CSCsg46060—The RADIUS authentication server templates require confirmation fields for shared secret keys.

  Workaround: None.

- CSCsg46139—If you lose your WCS password and have not backed up your database, there is no mechanism to recover the password.

  Workaround: None.

- CSCsg46529—The times displayed when mousing over the elements on a floor map are not accurate. The WCS query is based on the information table times rather than the location table times.

  Workaround: None.

- CSCsg47012—If you change the AP Mode of the associated access point and wait a few seconds before choosing the Refresh link, the ServletException page displays.

  Workaround: None.

- CSCsg50192—When you configure an access point template and choose WLAN override on either the 802.11a or 80.211b radios, only 5 SSIDs display. Of those SSIDs that do appear, not all are WCS SSIDs.

  Workaround: None.

- CSCsg51405—You cannot restore a configuration when an ACL with a rule exists. When you try a Restore Config, it displays the following error message:

  ```
  Restore failed for following configuration(s) - Access Control List
  10.50.65.42/testing Failed to create object in device
  ```

  Cisco WCS logs display the following error message:

  ```
  SnmpOperationException: [COMMON-1]: COMMON-1
  ```

  Workaround: None.

- CSCsg51752—If you perform a cold boot on your controller, you observe the cold start trap in the trap logs, but it is not reaching the trap ringer or WCS.

  Workaround: None.

- CSCsg53491—When you try to create a Local Management User with the same name as an existing Local Net User, WCS gives an SNMP error. Instead, it should respond with an error that the username is already used and must be unique.

  Workaround: None.

- CSCsg54554—When you enable Web policy within WCS, you have a choice of authentication or pass through. (You must navigate to Configure > Controllers, choose WLANs >WLANs from the left sidebar menu, and then click Security > Layer 3 to arrive at this parameter.) Enabling wpa1/wpa2 for web policy is not supported on the controller, so a vague error message is generated.

  Workaround: None.

- CSCsg55667—If you install a version of WCS that was installed previously, an error message warns you of the previous install, but the error message reports the wrong version number for the existing version.

  Workaround: None.

- CSCsg55684—During an install, an install path must be specified. The path you specify there is not considered as the default when the final install directory is determined.

  Workaround: None.

- CSCsg57305—The alphabetizing of the “sort by SSID” is not correct.

  Workaround: None.

- CSCsg58340—The method of adding new rules is not functioning as expected. If you choose Configure > Controller Templates > Access Control > Access Control Lists, you can specify rules. When you go to the Select a command drop-down menu and choose Add New Rule, a sequence number 1 is created. When you go to add another rule, you should be warned that rule 1 already exists before proceeding. Instead, rules with sequence 3, 4, 5, and so on are created regardless of whether another exists.

  Workaround: None.

- CSCsg66326—When you create an access point template in WCS, you cannot see all of the WLANs or the scroll down bar for the drop-down list window.

  Workaround: Fully expand the web page.

- CSCsg68269—If a template applied from Cisco WCS attempts to create a WLAN ID greater than 16, the following error message displays:

  ```
  some unexpected  internal error has occurred
  ```

  Workaround: None.

- CSCsg69862—The RADIUS server ping attribute needs a label.

  Workaround: None.

- CSCsg71721—In WCS with location, the heatmap forms a circle aroundthe most likely access point location for a rogue but does not account for the RSSI of neighboring access points.

  Workaround: None.

- CSCsg74466—If you generate a report after navigating to **Monitor** -> **Devices** -> **Access Points** and choosing **Noise**, **Interference, or Coverage** (**RSSI / SNR**) from the Select a report drop-down menu, the legend overlays the chart display area.

  Workaround: None.

- CSCsg75059—WCS has an extra *default* value in the shared key list. The extra value must be removed from the authentication key management PSK list, and only ASCII and hex values should remain.

  Workaround: None.

- CSCsg75349—You cannot log in to WCS with a username that exceeds 15 characters.

  Workaround: None.

- CSCsg81225—After you restore data in preparation for upgrading, WCS fails to start.

  Workaround: Find the highest numbered sol####.log file, where #### is a four-digit number. Delete it and reboot the server. If WCS does not start, repeat for the next highest sol####.log number and so on.

- CSCsg83749—In the map section, the client count number is displayed incorrectly on the access point. Even if you use the drop-down Refresh from Network command and execute a statistics poll to update, the client status and count are not accurately updated.

  Workaround: Manually execute the statistics task to successfully update the map access point client count.

- CSCsg84669—German characters are not displayed correctly when editing the properties of a client or tag (name, category, etc.).

  Workaround: None.

- CSCsg86208—If you enter a blank value for HTTP when installing WCS, the WebServer process does not start.

  Workaround: None.

- CSCsg87636—The AP Sniffer Mode Audit page is not displaying. When you choose Access Point > AP Name and change the access point mode to sniffer, you can then click on the b/g radio, set a channel, and configure a server. If you then click **Audit**, the AP Radio Summary page appears rather than the Audit page.

  Workaround: Set the access point to sniffer mode, save (to reboot the access point), allocate a specific channel, and then the right channel displays.

- CSCsg88347—An error message occurs when you try to modify an existing DHCP scope value (by choosing Configure > Controller > System > DHCP scope).

  Workaround: None.

- CSCsg92286—Adding ad hoc rogues and then disabling the nics results in invalid RSSI values. The rogues go into a containment pending state, and the WCS reports an RSSI value of -140 to -128 with no detecting radios.

  Workaround: Use the RSSI from the initial alert.

- CSCsg94421—The shortcut icons are not displaying in the Quick Launch Bar after a successful installation and a reboot.

  Workaround: None.

- CSCsg94509—WCS sometimes fails to apply a WLAN template to 4400 and 2000 series controllers when the WLAN is configured for static WEP and 802.1x. WCS displays this message:

  ```
  SNMP operation to Device failed: Unspecified error / Session timeout range invalid -
  for 802.1x(300-86400) f or others(0-65535)
  ```

  Workaround: None.

- CSCsg94525—The setting for the current LWAPP operating mode (found when choosing Configure > Controller IP > System > General) is not retaining its value after an audit is performed.

  Workaround: None.

- CSCsg97505—The error message that may appear when editing a DHCP scope needs to be more descriptive.

  Workaround: None.

- CSCsg98415—When you delete templates from WCS, the "failure" message that displays for unreachable WLCs could be more descriptive.

  Workaround: None.

- CSCsh05313—When you restore data in preparation for updating to a later WCS version, the restore does not complete.

  Workaround: None.

- CSCsh13721—The Edit AP Assignment option in the AP Groups VLANs shows all access points as assigned to the first group, even if the access point has been correctly configured before. The problem is related only to showing the current values. If a change is made, it is correctly saved.

  Workaround: None.

- CSCsh17858—While performing a WCS assisted site survery, you may get an error message that an unknown error has occurred.

  Workaround: None.

- CSCsh22237—If tags are associating and disassociating at a very high rate, a "Getting more than x disassociate messages in 30 seconds" alert appears.

  Workaround: None.

- CSCsh24961—An SNMP error occurs if you try to apply a controller template for web authentication with Web Auth Type set to *external*. Choose Configure > Controller Templates > Security > Web Auth Configuration > Add Template and when filling out the template information, select **External** for Web Auth Type and specify External Redirect URL. When you save this configuration and apply it to controllers, the error occurs.

  Workaround: Apply settings directly on WLC instead of using WCS.

- CSCsh25458—The access points on the client location debug are displayed slightly off (down and right) of their actual locations on the map.

  Workaround: None.

- CSCsh26050—The first time after a migration from a previous release, WCS sometimes fails to start. This occurs only for access points whose antenna name was empty in the earlier release. A "Failed to start WCS server" message appears.

  Workaround: If you browse to the server a couple of hours later, you will see the server is up, even though you may have received the failure to start message.

Resolved Caveats

These caveats are resolved in Cisco WCS 4.0.97.0:

- CSCsg28181—In 4.0.96.0, a ServletExceptions occurs when applying an access point group VLANs configuration.
- CSCsg34904—WCS (running version 3.2.64 or 4.0.81) is not updating NTP templates after a controller (running version 3.2.x.x) refreshes.
- CSCsg61618—Licensings was updated to support quantity concept.
- CSCsg72068—MFP is not being synched between what WCS reports and what WLC is set to.
- CSCsg76801—Need to allow multiple WLSE features in a license.
- CSCsg77364—Upon editing a WLAN template, the web policy can be set to both web authentication and web passthrough, which is an invalid security policy combination.
- CSCsg78455—Unable to disable client from WCS.
- CSCsg82961—When you restore data in preparation for updating to WCS version 4.0.96.0, a Java VM crash occurs, and the restore does not complete.
- CSCsg94455—The protection type value does not remain consistent after an audit is performed. You set protection type by choosing Configure > Controller IP > Security > AP Authentication and MFP, choose **protection type** as the access point authentication, and click **Save**.
- CSCsg99514—After a guest WLAN template with a mobility anchor has been created, you get operation failures or error messages when you try to delete them from Controller Templates > WLAN.
- CSCsh06926—On the radio configuration page, the antenna gain is reported as the default value for every antenna type rather than the actual configured gain in the access point. If an access point is initially configured with a specific antenna gain and then later the value is changed directly in the controller, WCS reports the antenna type value and not the actual value, even after a refresh.
- CSCsh23930—An exception occurs in wrapper.log.
- CSCsh44651—WCS is not handling bad input. It should attempt to add statistics for a given client only once, even if it is a duplicate entry.
- CSCsh47911—In 4.0.96.0, the table, transmit power, and channel has only 12 scales.
- CSCsh57153—WCS specific search for excluded clients is blank.
- CSCsh73300—Adding a controller fails if access point configuration values exceed the WCS maximum length.
- CSCsh73617— UDI table should be retained after restore on 4.0.97.0.
- CSCsh74810—WCS backup archives get corrupted if database is greater than 8 GB.
- CSCsh75099—The groupvlanname in lrad metadata has an incorrect length.

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.