Release Notes for Cisco Wireless Control System 4.0 for Windows or Linux

June 1, 2006

These release notes describe open caveats for the Cisco Wireless Control System 4.0 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

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.

    – 2.4 GHz Intel processor with 1 GB 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

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 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 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 Features

The following new features are available in the Cisco Wireless Control System (WCS) 4.0 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* 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.

International Characters Not Supported

WCS does not support international characters. You cannot use non-English characters for map names, asset information, and so on.

Changing the Default Password

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

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

The last step in performing an upgrade is restoring the 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 WCS version 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 does not support IPSec. If you upgrade to release 4.0 from a previous release that supported IPSec, any wireless LANs (WLANs) that are configured for this feature become disabled.

Limits to WebAuth Support on Hyrid-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 versions of WCS should not be used with the 4.0 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 the software needs to be reformatted to be used as a Cisco WCS server.

Manually Executing Scheduled Tasks

Manually executing 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

We recommend 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 lower 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).

Caveats

This section lists open caveats in Cisco WCS 4.0 for Windows and Linux.

Open Caveats

These caveats are open in Cisco WCS 4.0:

- CSCsb76160—The rogue and security alarm message for an IDS Signature Attack Alarm indicates "The wireless system is no longer detecting the intrusion,"although "Attack active at" still says alarm is active at one or more access points. The anomaly takes place when an IDS Signature Attack Alarm is no longer detected at one access point but is still detected by other access points. When WCS receives a clear alarm event from one access point, this count is decremented and the alarm is cleared only when the count reaches zero.

    Workaround: Recognize that if "Attack active at" still says the IDS Signature Attack is active at one or more access points, the alarm message applies only to the most recent notification from one of the observer access points.

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

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

- CSCsc39976—The coverage area does not scale when changing the units of measurement from feet to meters in Cisco WCS maps.

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

- CSCsc48752—The location for elements in outdoor areas is improperly displayed when viewing details of an outdoor wireless LAN (WLAN). The Cisco 2700 Series Location appliance functionality is designed for indoor locations. Any location for outdoors will be displayed using best effort but accuracy is not guaranteed.

    Workaround: None.

- CSCsc54046—Heatmaps for mesh access points may not be optimal because they may not be considering certain optimal parameters and may not reflect the exact coverage pattern.

    Workaround: None but some parameters can be tweaked to improve the outdoor mesh heatmaps.

- CSCsc92372—From the Map Editor for an outdoor area, the options listed for Obstacles are all for indoor floors. For example, there are not any obstacles for trees or buildings.

    Workaround: Choose equivalent obstacles from the existing list for outdoor objects, such as trees or buildings. For example, draw a rectangle with thick walls to represent a building.

- CSCsd07119—An *SNMP operation to device failed* message appears when applying a template to a controller that has parameters incompatible with other configuration settings on a controller.

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. Then correct the template or modify the controller settings so the template can be applied without errors.

- CSCsd15481—The mesh link information for an access point shows incorrect links for the mesh parent.

    Workaround: Use the controller CLI command to retreive updated and correct mesh link information for an access point:

    show mesh neigh *Cisco AP name*

    This command shows the mesh link information for an access point including all the neighbors, children, and parent links.

- CSCsd54692—Unable to log into WCS using the default username and password.

    Workaround: Restart the server.

- CSCsd95919—When displaying the Voice TSM report, a graph appears only if data is available but the report title still appears.

    Workaround: None.

- CSCsd85695—If WCS is installed and operating in one of several time zones in Australia, tasks scheduled for a specific time of day will run one hour later than tasks scheduled during the week leading up to daylight savings time. Timestamps on log messages may also be incorrect.

    Workaround: To have scheduled tasks occur on time in the Australian time zones during all weeks, replace the Java Runtime Environment (JRE) zone information directory with an updated version from Sun. Follow these steps to obtain an updated version from Sun Microsystems:

Step 1 From http://www.oracle.com/technetwork/java/index.html, download a JRE 1.5.0_06 or later.

Step 2 Rename the **<wcs>/jre/lib/zi** directory zi.orig.

Step 3 Copy the **jre/lib/zi** tree from the downloaded JRE to <wcs>/jre/lib/zi.

Step 4 Restart the server.

This should update the time zone information and solve the problem.

- CSCsd93796—Email notification time stamps are not accurate because they reflect the time email was sent but not the time of the actual event.

    Workaround: Make sure the mail server does not create delays when receiving alerts from WCS. Common problems are misconfiguration of the IDENT protocol or DNS related delays.

- CSCsd96835—If an invalid or out of range value is entered for a H-REAP native VLAN ID on the access point template, the application returns an invalid attribute error message.

    Workaround: Configure the VLAN ID within the valid range (1 to 4094).

- CSCsd98732—The 802.3x Flow Control Mode option is unavailable on the Configure > Controller System > General configuration pages. This occurs only if the configuration is for a Cisco 2006 wireless LAN controller.

    Workaround: None.

- CSCse12576—During the calibration procedure, a CCX v.2 or later compatible client is recommended to take advantage of the latest features. However, the Aironet information element (IE) option must be enabled on the controller and the wireless LAN to which the client will be communicating. If the Aironet IE option is disabled, the calibration procedure may not generate sufficient data.

   Workaround: Use WCS to enable the Aironet IE option for the controller and the wireless LAN to which the client will communicate. Path: Controller > WLANS > Choose specific WLAN > Check the Enabled box next to Aironet IE entry on the General Properties page that appears.

- CSCse17963—The Solid database shuts down if the Solid log file is corrupted.

   Workaround: Delete the corrupted Solid log file and restart the server. Also, as part of the workaround, free up some disk space on the WCS server. Solid has a fix for this problem in their next release, which will be included in the next WCS release.

- CSCse18364—When adding a controller, the network route is automatically added based on IP address and netmask. If the network already exists, WCS fails to add a network.

   Workaround: Provide a different subnetmask so that the network falls into a different route that does not already exist in WCS.

- CSCse20068—From a controller running a controller image of version 3.0.0.0 or lower, if the access point is in Layer 3 mode and has a statically configured IP address, clicking Save on the detail page causes the access point to revert to the DHCP option.

   Workaround: The access point configurations for all access points on controllers running controller images of version 3.0.0.0 and lower can be configured using the Web user interface or comand line interface (CLI).

- CSCse22376—The map view is not using the Default Map Protocol View configuration when changing the map views from Monitor > Map and selecting Properties from the drop-down command menu. For example, if the network selection is 802.11 a & b/g, the map view defaults to 802.11b/g.

   Workaround: Manually change the map view.

- CSCse23175—If the WCS server is managing a large network, the database process will sometimes stop or revert to a read-only mode. The system runs out of disk space when large files are backed up.

   Workaround: Turn off the scheduled backup policies or reduce the default number of stored backups.

- CSCse27704—During install for HTTP and HTTPS ports, WCS allows the user to add incorrect values, such as nonnumeric characters. WCS installs but will not start correctly.

   Workaround: Use the default port numbers or specify valid numeric port numbers.

Resolved Caveats

These caveats are resolved in Cisco WCS 4.0:

- CSCar13537—Group permissions for Users belonging to both ConfigManager and SystemMonitoring groups now restrict changing the logging levels and other administrative activities.

- CSCsa93250—Resizing a floorplan using the Edit Floor option correctly resizes the coverage areas.

- CSCsb07534—You can select a backup port during the initial setup of the web interface. When ap-manager interfaces are configured on all ports so that you have equal distribution, no backup port is needed. If the backup port is set up, the ap-manager interface moves to that port, creating two ap-manager interfaces. With release 4.0, the ap-manager interface (both static and dynamic) will not have a backup port.

- CSCsc06090—The performance is no longer slow for systems with a large number of Cisco lighweight access points and wireless LAN controllers attempting to enable a rogue access point policy.

- CSCsc44897—Cisco WCS shows correct antenna orientation when viewing an object.

- CSCsc46598—Items appear in the correct position in the Cisco lightweight access point placement diagram and items in the printed site survey document are correct when performing a Cisco lightweight access point placement planning site survey.

- CSCsc67765—You cannot use hexadecimal when setting preshared keys for WPA in wireless LANs (WLANs). Some phones, for example Vocera, require the key to be hexadecimal. In the 3.2 MR1 release of the controller, you can configure this using the CLI. You cannot configure it with WCS.

- CSCsc71820—The Access Control List can now have the DSCP value set to *any*.

- CSCsc83053—The coverage alarm for backhaul generated for mesh access points is fixed.

- CSCsc90237—The lease time is now accurately displayed in minutes rather than seconds when configuring DHCP on a controller using WCS.

- CSCsd26206—Made adjustments to the temporary directory so that the directory would not appear full and cause the failure of a generate proposal command.

- CSCsd33386—Cisco WCS does not support managing a third party AP, so any third party AP references were removed.

- CSCsd50071—The object now scales correctly with the floor plan changes when using the map editor and saving an object, such as a light wall or heavy door, to the floor plan and changing the horizontal or vertical dimensions to a smaller value.

- CSCsd51049—JRE 1.5.06 can be installed before installing WCS and the server starts without giving a null pointer exception error.

- CSCsd51852—Cisco WCS no longer retains an unused network after a controller is deleted.

- CSCsd54766—Restoring the configuration to the controller does not cause an error and restore is completed.

- CSCsd64228—When selecting and modifying Access Control Lists, you can set the value for DSCP to *any* without receiving an error response.

- CSCsd64641—Static IP addresses can now be configured on access points.

- CSCsd71397—WCS no longer defaults and writes to the root directory if the TFTP path has a space.

- CSCsd82296—Creating an ACL template in WCS and editing a rule with a protocol value of *any* no longer causes an error response stating that the value for this attribute is invalid.

- CSCsd93023—The AP fallback state can be changed without deleting dynamic interfaces on the wireless LAN (WLAN).

- CSCsd95310—Cisco WCS database was not restoring completely when the backup database was larger than 2 GB. This has been corrected and WCS restores and restarts successfully when the backup database is larger than 2 GB.

- CSCsd98962—A report for busiest clients can be run without triggering an unknown exception error.

- CSCsd98976—The mesh tree view correctly accounts for all access points on the floor when viewing maps.

- CSCsd99194—Calibration models are correctly assigned, and heatmaps of added access points display and compute correctly.

- CSCse00886—When saving pico cell mode to the 802.1a parameters on the controller, the system does not give the error "SNMP operation to device failed."

- CSCse14991—The antenna gain is getting set correctly on the controller when changing the antenna pattern on access points from the access point detail page or map position access point page.

- CSCse27134—Upgrading to WCS 4.0, you can save obstacles on current or new maps.

- CSCse30879—The DSCP values are correctly set in the database and controller. When editing rules in the Access Control List, editing the DSCP values are showing the saved value.

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.