Release Notes for Cisco Wireless Control System 4.0.81.0 for Windows or Linux

September 19, 2006

These release notes describe open caveats for the Cisco Wireless Control System 4.0.81.0 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.

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.
  - 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

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) 4.0.81.0 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

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

In order to be compatible, the WCS version must be the same or a newer revision than that of the software version installed on the controller. If an upgrade is planned, it is strongly recommended to upgrade the WCS first to avoid running into 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

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 4.0.81.0 does not support IPSec. If you upgrade to release 4.0.81.0 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 versions of WCS should not be used with the 4.0.81.0 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).

Losing WPA Encryption

When you create a WLAN template with 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 version 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 4.0 controllers. You can also configure all WPA encryption on the controller itself and not push the templates down to WCS.

Caveats

This section lists open caveats in Cisco WCS 4.0.81.0 for Windows and Linux.

Open Caveats

These caveats are open in Cisco WCS 4.0.81.0:

- CSCsb76160—The rogue and security alarm message for an IDS Signature Attack Alarm indicates that the wireless system is no longer detecting an intrusion, even though “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.

- 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—When certain optimal parameters are not taken into account, backhaul heatmaps for mesh access points are not accurately reflected in the exact coverage pattern. Local access heatmaps are operating correctly.

  Workaround: None; however, some parameters can be adjusted to improve the outdoor mesh heatmaps.

- CSCsc59986—The controller configuration and Cisco WCS are not synchronized if you create a dynamic interface with capital letters in the name.

  Workaround: Create dynamic interface names without capital letters.

- CSCsc92372—From the Map Editor of an outdoor area, the options listed for obstacles are all for indoor floors. For example, you cannot choose a tree or another building as an obstacle.

  Workaround: Choose equivalent obstacles from the existing list for outdoor objects. 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.

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

  Workaround: Restart the server.

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

  Workaround: None.

- CSCsd93796—Email notification time stamps are not accurate because they reflect the time an 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).

- 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

- 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, clear some disk space on the WCS server. Solid has a fix for this problem which will be included in the next WCS release.

- CSCse18364—When you add 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.

- 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 installation for HTTP and HTTPS ports, WCS allows you to add incorrect values, such as nonnumeric characters. WCS installs but does not start correctly.

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

- CSCse34650—When you perform a calibration with CCX on a floor that is served by access points connected to multiple controllers, some measurements may be lost, and the calibration quality inspection may show regions having less accuracy.

  Workaround: None. If the calibrated floor is served by access points attached within the same controller, the lost measurements may not be observed.

- CSCse47530—When you choose Monitor > Devices > Access Points and choose the Voice TSM table, the table is generated only for the first access point selected. Although it is by design to allow the selection of only one access point, a reminder against choosing multiple access points could be added by Cisco.

  Workaround: None.

- 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.

  Workaround: None.

- CSCse56442—An error message sometimes appears if a WLAN template with either WPA-PSK or WPA2-PSK security is created (locally or by using WCS) and is then modified. If the WLAN template contained either static WEP or dynamic WEP (802.1X), an "SNMP operation to device failed" message may appear.

  Workaround: Set the security to WEP shared key in the template and reapply.

- CSCse60657—A campus with many buildings (around 60) having multiple floors may experience synchronization problems with the location server. Because the location server imposes a limit of 32 MB for message transfer, a synchronization error may occur because of the large amounts of data being transferred.

  Workaround: None.

- CSCse62608—Traps from an undiscovered controller or other unknown device are handled inefficiently. WCS should check the trap sender's IP address before processing the trap.

  Workaround: None.

- 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.

  Workaround: Add any new rules to the end of the ACL and modify previous rules.

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

  Workaround: None.

- 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.

  Workaround: Manually perform the placement based on the recommended outdoor guidelines.

- CSCse83586—When a WLAN ID 9-16 is created on the controller and then added to WCS, the template fails. Provisioning of WLANs with IDs from 1 to 8 only are allowed on the 4.0 version of the controller.

  Workaround: None.

- CSCse88985—When you create a WLAN template with 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 version 4.0, you receive a message that the template security was successfully applied. However, the WLAN is actually applied on the controller with no security policy. A refresh of the configuration from the controller still doesn't apply the template security properly.

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

- CSCsf06408—An SNMP error occurs when the WLAN template is configured with WPA2+WPA2 PSK. If you set PSK, select ASCII, and apply the template to the controller, the error results. The appropriate PSK keys may get distributed from WCS, but the controller doesn't allow clients to associate.

  Workaround: Use an ASCII PSK key with a length longer than eight characters.

Resolved Caveats

These caveats are resolved in Cisco WCS 4.0.81.0:

- CSCsc39976—The coverage area now scales correctly when the units of measurement are changed from feet to meters in Cisco WCS maps.
- CSCsd05107—When you search for clients in the location server and filter them by protocol, both the 802.11b and 802.11g clients are now visible. Prior to 4.0.76.0, only 802.11b clients were visible.
- CSCsd95144—In the Location History table and Client Details window, the 802.11 state of already disconnected clients is now correctly portrayed as disassociated.
- CSCsd98732—On a Cisco 2006 wireless LAN controller, the 802.3x Flow Control Mode option is now available on the Configure > Controller System > General configuration pages.
- CSCse12576—The calibration of a CCX v.2 or later compatible client now performs as expected.
- CSCse20068—A controller running version 3.0.0.0 or lower operates as expected when you click **Save** on the Detail page. The access point does not revert to the DHCP address even if it is in Layer 3 mode and has a statically configured IP address.
- CSCse21649—A large NAV field alarm for an 802.11 radio no longer occurs with an AP1231G when WLC trap logs are generated. A NAV is a network allocation vector which accompanies every packet being sent and operates like a timer. But if you continuously sent packets with a large NAV, other stations on the network would have to wait to transmit.
- CSCse22079—Datapoints added during the calibration procedure can now be deleted. The progress bar and the points tally accurately reflect the deletion.
- CSCse35840—The login for WCS and the method for loading maps was changed so that it takes less time.
- CSCse36067—When you added WLC 2006 to a recently installed WCS and then tried to add maps, a failure occurred. After positioning the access points onto their floors and restoring WLC, an "SNMP operation to device failed: attempting to set conflicting attribute value" error message resulted. This failure has been corrected.
- CSCse54546—The management frame protection is now mapped correctly for all event types, and the help message for the events/alarms page is now based on the event type.
- CSCse59277—When you logged in as monitor lite (for asset monitoring purposes), a list of tags was returned. Upon attempting to sort them by MAC address, an HTTP status 400 error was returned. The sorting process no longer returns the invalid path message.
- CSCse63087—When you view the Tag Properties page, the controller IP address information is hidden. After creating a user with Location User and logging in as that user, you can no longer see the controller IP address when clicking on the MAC address of any tag.
- CSCse66523—Controller objects no longer get discarded after a data migration from a pre-4.0 release. This occurred only when a controller object had an improper parent network object set in the WCS database.
- CSCse66859—In WCS 3.2 code, the day-of-the-week input was not recorded properly and therefore was not sent to location-based services (LBS) appropriately. This input is now corrected so that you can choose between none, all 7 days, some of the 7 days, or all of the time. LBS version 2.1.39 correctly receives this data and makes notifications as appropriate.
- CSCse67010—An error message no longer appears when you log onto WCS as a location user group member and choose Monitor Lite > Tags from the Summary page.
- CSCse67752—When you view an enlarged version of the floor map from the Tag/Client Details window, the access points are not present on the map. When you search for tags or clients, click the check box to enable debug for a particular one, and then click to expand on the tag of interest, the map opens. When you enlarge the map, the tags are visible but the access points on the floor are not.

- CSCse68019—An error message was added to alert you that an antenna name cannot be *missing* or *null* if heatmaps were entered for calibration. Whenever a *missing* or *null* antenna name existed on the Maps window, you saw an "RF prediction engine could not retrieve coverage heatmaps from the database" error message when you attempted the Add Data Points function. The heatmaps were not created or retrieved, and calibration was halted. The new error message alerts the user to the probable cause and suggests a solution so that calibration can proceed.
- CSCse72286—The ability to search for tags on controllers has been added.
- CSCse77999—A null pointer exception no longer appears when you choose Configure > Controller > WLANs.
- CSCse80321—After you perform a code upgrade, the access point height correctly defaults to 10.
- CSCse80700—WCS 4.0 was not polling the detecting access point table for rogue access point alarms seen by pre-4.0 controllers. The table is polled if the RSSI information is not already set in an existing alarm. To ensure that you always have the latest RSSI, upgrade your controller to 4.0.
- CSCse83815—WCS was not creating heatmaps for access points added after an upgrade from 3.2 to 4.0, and a "failed to create heat map for MAC: xx:xx:xx:xx:xx:xx" message was received. The heat maps are now visible.
- CSCse88211—WCS was reconfigured so that one configuration can have multiple matching templates. If there is more than one matching template, WCS arbitrarily picks one rather than failing. Prior to this fix, two RADIUS server templates created with the same IP address caused a failure.
- CSCse88374—You can now add and save a cubicle wall in WCS 4.0 map editor without receiving the "Error:\nInvalid enum value for attentuationType" message. The enum value was correctly reset to 4.
- CSC88985—If you used a security other than WEP or Layer 2, an SSID was left unencrypted upon sending any SSID configuration from a WCS (running 4.0.66.0) to a controller (running 4.0.x.x or 3.2.x.x). This security breach has been corrected.
- CSCse92285—The network audit failed whether running on schedule or running manually. The audit attribute length was adjusted upward so the network audit functions as expected.
- CSCse95557—The WLAN template was not functioning as expected when PSKs were retrieved from client devices. The template now works even when you choose WPA1+WPA2, WPA1, TKIP, PSK, or ASCII and type in an ASCII string.
- CSCse99453—When you plan access point coverage on a map (using planning mode), a Java servlet error was returned when the Add APs button was chosen. Even though the modifications were made successfully, the planning mode window had to be closed and data had to be re-entered to continue working. This problem has been corrected.
- CSCsf00932—Logic was added to the data migration code so that a matching planned access point can be found for each heat map. Data migration previously failed to preserve the association, and a matching planned access point could not be found for a heat map.

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.