Release Notes for Cisco Wireless Control System 4.2.62.11 for Windows or Linux

January 25, 2008

These release notes describe open caveats for the Cisco Wireless Control System 4.2.62.11 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
- Compatibility, page 2
- Requirements for Cisco WCS, page 3
- Important Notes, page 5
- New and Changed Information, page 6
- Caveats, page 6
- Troubleshooting, page 18
- Related Documentation, page 18
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page 18

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:

- Cisco Wireless Control System (Cisco WCS) software release 4.2.62.11
- Software release 4.2.99.0 for all Cisco controllers and lightweight access points
- Cisco autonomous to lightweight mode upgrade tool release 3.0
- Location appliance software release 3.1.35.0
- Cisco WCS Navigator release 1.1.62.11
- Cisco 2700 Series Location Appliance
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 2100 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, 1250, 1310, and 1500 Series Lightweight Access Points
- Cisco Aironet 1310 and 1410 Bridges

Compatibility

This release of Cisco WCS for Windows or Linux is compatible with wireless LAN controller and Cisco Aironet lightweight access point release 4.2.96.0. Previous releases of Cisco WCS should not be used with the 4.2.96.0 controller software release.

For compatibility issues with the location server, refer to the Release Notes for Cisco 2700 and 2710 Location Appliances for Software Release 3.1.35.0 at this URL:

http://www.cisco.com/en/US/products/ps6386/prod_release_notes_list.html

Note You may experience compatibility issues if you add a controller with a newer release than the Cisco WCS release. For example, 5.0 controller software release should not be added to Cisco WCS 4.2.

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.

Note AMD processors that are equivalent to the Intel processors listed below are also supported.

- High End Server—Supports up to 3000 Cisco Aironet lightweight access points, 1250 standalone access points, and 750 Cisco wireless LAN controllers.
  - 3.16-GHz Intel Xeon Quad processor with 8-GB RAM and a 200-GB hard drive.
  - 80-GB minimum free disk space is needed on your hard drive.
- Standard Server—Supports up to 2,000 Cisco Aironet lightweight access points, 1,000 standalone access points, and 150 Cisco wireless LAN controllers.
  - 3.2-GHz Intel Dual Core processor with 4-GB RAM and an 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, 200 standalone access points, and 125 Cisco wireless LAN controllers.
  - 3.06-GHz Intel processor with 2-GB RAM and a 30-GB hard drive.
  - 30 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.

Note Cisco WCS can simultaneously manage multiple Cisco wireless LAN controllers running different software versions. The new features in controller software release 4.2.62.0 are supported by Cisco WCS software release 4.2.62.11. WCS release 4.2.62.11 also supports controllers running release 4.1.190.5 to support Cisco Aironet mesh access points.

Supported Operating Systems

The following operating systems are supported:

- Windows 2003/SP2 or later with all critical and security Windows updates installed. 64-bit installations are not supported.
- Red Hat Linux Enterprise Server 4.0 Update 5 or Advanced Server 4.0 Update 5. Only 32-bit operating system installations are supported. 64-bit operating system installations are not supported. Cisco WCS can be installed on Red Hat Linux Enterprise Server 4.0 but it will not be supported in future releases. Please plan on migrating to Red Hat Linux Enterprise Server 5.0.

– Windows 2003 and Red Hat Linux version support on VmWare ESX 3.0.1 version and above.

Note VmWare must be installed on a system with these minimum requirements:
Quad CPU running at 3.16 GHz
8 GBs RAM
200 GB hard drive

Note Individual operating systems running Cisco WCS in VmWare must follow the specifications for the size of Cisco WCS you intend to use.

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 100/375 Cisco wireless LAN controllers. The required processors is a 3-GHz Intel Pentium with 3 GB of RAM and 38 GB of free hard drive space.

Note AMD processors that are equivalent to the Intel processors are also supported.

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

Cisco WCS User Interface

The Cisco WCS user interface requires Internet Explorer 6/0/SP1 or later, with the Flash plug-in. The Cisco WCS user interface has been tested and verified using Internet Explorer 6.0 on a Windows workstation.

Note The screen resolution should be set to 1024 x 76 pixels for both WCS and Navigator.

Client Requirements

In order for clients to access Cisco WCS, they must have a minimum of 1 GB RAM and a 2-GHz processor. The client device should not be running any CPU or memory-intensive applications.

Finding the Software Release

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

Upgrading to a New Software Release

The Cisco WCS release must be the same or more recent than the controller software release. Upgrade the Cisco WCS first to prevent any unexpected problems.

Note If you upgrade to a Cisco 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 do not migrate. Upgrading to 4.0.87.0 before upgrading to a later release migrates the users, user groups, tasks, and user passwords.

Cisco WCS supports database upgrades only from the following official Cisco WCS releases:

- 4.0.66.0
- 4.0.81.0
- 4.0.87.0
- 4.0.96.0
- 4.0.97.0
- 4.1.83.0
- 4.1.91.0
- 4.2.62.0

Important Notes

This section describes important information about Cisco WCS.

Compatibility

This release of Cisco WCS for Windows or Linux is compatible with wireless LAN controller and Cisco Aironet lightweight access points using version 4.0.66.0 or later.

Cisco WCS Supported on Windows 2003 English and Japanese Operating Systems Only

Cisco WCS is supported only on English or Japanese versions of the Windows 2003 operating system. Display problems sometimes occur when you install and run Cisco WCS on operating systems translated to other languages or with locale settings other than English or Japanese.

New and Changed Information

New Features

There are no new features in Cisco WCS 4.2.62.11.

Changed Information

There is no deployment restriction on the number of hybrid-REAP access points per location. However, the minimum bandwidth restrictions remains at 128 kb/s with the roundtrip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes.

Caveats

This section lists open and resolved caveats in Cisco WCS 4.2.62.11 for Windows and Linux.

Open Caveats

These caveats are open in Cisco WCS 4.2.62.11:

- CSCsb39735—Web authentication certificate details cannot be seen on Cisco WCS.

  Workaround: None at this time.

- CSCse42296 —If a WLAN template already exists in Cisco WCS, it is not updated when you modify the WLAN settings on the controller.

  Workaround: Use Cisco WCS to make changes to the WLAN settings and then apply these changes to all controllers.

- CSCse94732—There is a Cisco WCS and controller template mismatch while configuring CCKM and 802.lx.

  Workaround: When the template is entered, the user will be able to see the CCKM and 8021.x.

- CSCsh43499 —When different users are trying to troubleshoot the same client, Cisco WCS lets the users put the same client on the watchlist at the same time, which Cisco WCS should not allow because the client starts to collect logs from more than one browser. Cisco WCS does not display an appropriate error message.

  Workaround: None at this time.

- CSCsh44930—In the Clients Summary page (Monitor > Clients), typing the MAC address for a mobile client in the Client field and clicking the **Troubleshoot** button does not open up the Client Troubleshooting window.

  Workaround: Search for the client by its MAC address using the Quick Search field and click the link for the returned client to go the Client Details page. On the Client Details page, choose **Troubleshoot** from the Command drop-down list and click **GO**.

- CSCsh47150—Moving a building between campuses or moving a building outside of a campus requires a clean resynchronization with the Location Appliance.

Workaround: After moving a building, go to the Location synchronization page, unassign the Network Designs, submit the synchronization, reassign Network Designs, and resynchronize.

- CSCsh81856—While installing, the password field is only partially encrypted.

  Workaround: Only one or two of the letters show up during installation. Once the password is created and the user clicks **Enter**, the screen proceeds to the next session.

- CSCsh82165—Upon install or uninstall, the following error message sometimes displays: "Command.run( ): process completed before monitors could start."

  Workaround: This message is irrelevant. No workaround is necessary.

- CSCsh95569—During the Web Auth file download, the JSP file is not reflected properly.

  Workaround: None at this time.

- CSCsi14940—When attempting to save an ACL template, an invalid error message displays.

  Workaround: If "Other" is needed for Source or Destination, choose that option only and click **Save** after entering the values.

- CSCsi15088—The local net user mapping to a profile ID is not updated if the profile ID changes on the controller.

  Workaround: Change the profile ID of the local net user using the controller GUI or CLI and refresh the configuration in Cisco WCS to keep the controller and Cisco WCS in sync.

- CSCsi18312—The link test option in the Client AP Association History does not work.

  Workaround: Use the link test option on the Client Details page.

- CSCsi18453—The wireless LAN apply fails when the controller does not have the interface associated with the wireless LAN template.

  Workaround: When applying the wireless LAN template on the list of controllers, the user must verify that the associated interface exists on all the controllers.

- CSCsi24635—A Cisco WCS alarm appears on the alarm dashboard when WCS on navigator becomes unreachable. If you click the alarm, you get the alarm details page. When you further click to get the event history, the events page is empty.

  Workaround: None at this time.

- CSCsi26963—The Client Association report does not include any records older than 7 days.

  Workaround: None at this time.

- CSCsi29550—After a restore, Cisco WCS truncates six days worth of data. Only the data from the final day appears.

  Workaround: None at this time.

- CSCsi46344—There are certificate download errors on the Cisco WCS.

  Workaround: Certificates can be downloaded directly to the controller rather than via the Cisco WCS.

- CSCsi86544—The client association history table does not display the same data as the client history graph.

  Workaround: None at this time.

- CSCsi86625—When using average aggregated values, some of the values in reports and interactive graphs may be skewed for dates older than one day. The average value is shown as zero while the max value is not zero.

  Workaround: None at this time.

- CSCsj36970—The Configure > Controller > 802.11 b/g/n page on Cisco WCS does not match the controller user interface RRM changes.

  Workaround: None at this time.

- CSCsj43771—If you enable wireless management on a WiSM through Cisco WCS, an "SNMP operation to device failed error" may result.

  Workaround: Configure wireless management through the controller.

- CSCsj55041—If you enable H-REAP VLAN support and Profile Name VLAN Mappings while creating an access point template, the settings are not saved.

  Workaround: None at this time.

- CSCsj56796—You may receive a "configuration is different on the device" message that may or may not be accurate. Also, when differences between the access point and Cisco WCS do occur, the message may not appear.

  Workaround: Use the audit function to see if there are differences between the access point and Cisco WCS database. All changes made to the access point from Cisco WCS are correctly saved, regardless of the error message.

- CSCsj59749—While the location of the rogue access point icon appears correct on the heatmap, the color map behind it is not centered on the rogue access point.

  Workaround: None at this time.

- CSCsj72272—You cannot enable the Accept Signed Certificate option on the Configure > Controller Template > AP Authorization page.

  Workaround: You can also perform this operation on the Configure > Controller > Security > AP Authorization page with the Edit AP Policies option from the Select a command drop-down menu.

- CSCsj77046—If you add controllers (with comma separation) which are combinations of WiSMs (2000s and 4400s), the status messages makes it appear as if only the WiSMs were added.

  Workaround: On the Configure > Controllers page, you can see a complete list of controllers that were added successfully.

- CSCsj96574—When adding guest user accounts using a CSV file, you may receive an unknown exception error from the import operation.

  Workaround: Make sure you format the file correctly and retry the operation. The correct sequence of fields per row is username, password, lifetime, description, and then disclaimer.

- CSCsj99244—When using Cisco WCS on a Japanese Windows operating system, the location server backup fails.

  Workaround: You can modify the AM and PM values of the backup filename to English before performing the backup.

- CSCsk01665—If you add any template with a negative test case and try to apply the template to the device, the object is not created in the device, even though the Apply To field is incremented.

  Workaround: Confirm if the object is added by logging onto the device and using an audit to check the configuration.

- CSCsk02071—While loading a CAD file in Maps, the following error message is seen: "error in getting data from server. Make sure you have connectivity and server is UP." Check the launch out log file for an error message similar to the following: "java.lang.UnsatisfiedLinkError: C:\Program Files\WCS4.2.44.0\webnms\RFdlls\ax2006dll.dll: Can't find dependent libraries."

  Workaround: Add the dll files in the following locations and restart the Cisco WCS server: c:\windows\system32\msvcp71.dll and c:\windows\system\dwmapi.dll.

- CSCsk08935—When comparing a heatmap to access point radio information, you notice discrepancies within channel utilization.

  Workaround: None at this time.

- CSCsk12424—An invalid CSV file results in an unknown exception on the migration template.

  Workaround: Create a CSV with a valid format.

- CSCsk14288—The Cisco WCS conversion of an autonomous access point to LWAPP occurs only if one of the supported radios for conversion is found. Both radios are not being checked.

  Workaround: None at this time.

- CSCsk15266—The IP address is displayed incorrectly in the CDP neighbor tab under Monitor > AP. If the IP address of the access point is A.B.C.D, it is shown as D.C.B.A.

  Workaround: None at this time.

- CSCsk16498—Because the reports were designed mostly for wireless clients, new capabilities need to be added so that reports such as Client Count and Client Association can show wired clients as well.

  Workaround: None at this time.

- CSCsk17031—The history page loads slow when trying to view the location history of a tag or client.

  Workaround: Make sure the history interval for client, tags, and rogue clients and access points is not significantly high on the Location Server > Administration > History Parameters page. You can also frequently purge the data.

- CSCsk17038—If more than 1000 elements (clients and tags) are tracked by the location server on a single floor, the performance for maps on that floor is affected.

  Workaround: Turn off the client and tags layer on the map so you can see the access points and other information on the map. Viewing over a thousand items on a single map is not practical. You should use the search option on the Monitor > Clients or Monitor > Tags page to look at the clients.

- CSCsk18826—The Location > Synchronization page takes awhile to load if several hundred controllers are being loaded.

  Workaround: Wait for the page to load completely.

- CSCsk25417—All clients are displayed if you click any header to resort WGB clients.

  Workaround: Choose Monitor >WGB to reset the list of WGB clients.

- CSCsk26658—An error occurs if you click on link test for a wired client.

  Workaround: No workaround. A link test is not supported for wired clients. It applies only to wireless clients.

- CSCsk27242—If you draw thick walls on a floor with smaller dimensions (such as 100 ft by 50 ft), you see a heatmap shift of around 4 to 8 feet.

  Workaround: None at this time.

- CSCsk28942—While omnidirectional antennas' radiation pattern may have some asymmetry, they generally radiate in all directions. This causes confusion trying to set antenna orientation and position access points in Cisco WCS. When Cisco omnidirectional antenna products are chosen, the setting for omni products should be disabled since the specifications of the antenna are known. The following Cisco products should have omnidirectional patterns considered: AIR-ANT5959, AIR-ANT4941, AIR-ANT2422DW-R, AIR-ANT1728, AIR-ANT2506, AIR-ANT3213, AIR-ANT24120, integrated AP1120 antenna, integrated RM21A antenna, AIR-ANT5135D-R, AIR-ANT5135DW-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT58G9VOA-N, AIR-ANT5175V-N, AIR-ANT2455V-N, and integrated AP1130AG antennas.

  Workaround: Set the antenna orientation value to 0.

- CSCsk30371—Options in the drop-down menu of the search network include controllers which have not been added.

  Workaround: None at this time.

- CSCsk31174—When device status polling and wireless polling are disabled, location information from an access point converted from autonomous to unified does not migrate.

  Workaround: Do not disable device status and wireless status polling.

- CSCsk32874—The Wired LAN parameter should be changed to Guest LAN.

  Workaround: None at this time.

- CSCsk32881—For a guest LAN interface, the creation page should not have the following fields: IP address, Mask, Gateway, Primary DHCP, and Secondary DHCP.

  Workaround: None at this time.

- CSCsk41183—If you upgrade to release 4.1, ghost templates appear that were not present in the earlier version.

  Workaround: None at this time.

- CSCsk45060—Within access point templates, the WLAN profiles in the WLAN override list are retained even when profiles are no longer used on any controllers.

  Workaround: None at this time.

- CSCsk46429—The SSID report keeps repeating the same entry.

  Workaround: None at this time.

- CSCsk46615—The WLAN template settings using WPA1+WPA2 with PSK and default setting cannot be forwarded for pre-shared key.

  Workaround: Choose either hexadecimal or ASCII for pre-shared key, and the pre-shared key forwards completely.

- CSCsk47555—On the monitor list page, the access point is shown as local when it should be bridging mode.

  Workaround: Synchronize the controller configuration with Cisco WCS. The configuration displays the current known configuration Cisco WCS has maintained in the database until it is synchronized.

- CSCsk48245—The title for Client SNR History on the CCXV5 Statistics tab shows an incorrect unit. The title should read Client SNR History (dBm) instead of Client SNR History (dB).

  Workaround: None at this time.

- CSCsk48985—If you change template parameters of an existing template and then apply it to a different number of controllers, the window shows the template as applied to the original number of controllers.

  Workaround: If you need to change parameters in a template, create a new template.

- CSCsk49569—After you apply access point templates for specific WLANS under access point radio WLAN override, WLAN SSIDs and profiles are mismatched.

  Workaround: None at this time.

- CSCsk51302—When you click on Client Troubleshooting in Monitor > Clients, an “object *switch* does not exist” error displays.

  Workaround: None at this time.

- CSCsk51549—The Cisco Compatible Extensions Version 5 client radio receiver sensitivity data rate is incorrect when performing a search for associated clients with Monitor > Clients.

  Workaround: None at this time.

- CSCsk52999—The severity of affected access point displays as -1.

  Workaround: None at this time.

- CSCsk53564—When you apply a WLAN template to multiple controllers running different software versions (such as 4.0 and 4.1), the session timeout validation does not consider the different ranges for the WLC versions.

  Workaround: Set the session timeout in the range of 300-65535.

- CSCsk55160—If you switch between perimeter and rectangle in the planning mode tool, the total coverage area does not change, and the message above the radio buttons does not update.

  Workaround: Adjust the size of the rectangle to approximately cover the perimeter area. Generate the report in either perimeter or rectangle mode.

- CSCsk55422—If an invalid port is entered and then corrected during installation, the installer reports that an error occurred during installation.

  Workaround: None at this point.

- CSCsk63878—Cisco WCS does not update the Access Point Groups configuration.

  Workaround: Fix the configuration in Cisco WCS so that it matches the controller.

- CSCsk65190—If you try to create a guest user with the same name as a local net user, an SNMP commit fail error is returned.

  Workaround: Use a unique name while creating a guest user.

- CSCsk65520—If you perform a client search, the returned client list shows the profile name for all probing clients as mesh profile. This profile name does not exist.

  Workaround: None at this time.

- CSCsk70003—When guest user credentials are emailed, default "WCS AdminTeam" signature text is added to the mail message.

  Workaround: None at this time.

- CSCsk70270—Cisco WCS has no AAA (TACACS or RADIUS) debugs.

  Workaround: Decrypt the sniffer trace.

- CSCsk70368—When you choose Monitor > Security and then click the Reserved Management link in the Signature Attack column, no results appear.

  Workaround: None at this time.

- CSCsk70905—If you create a configuration group on Cisco WCS and make changes in the channel and DCA radio channel, Cisco WCS gives you an error that the radio settings cannot be applied.

  Workaround: None at this time.

- CSCsk71342—If you perform a sort by controller or profile name on the Client Detail page, no clients are returned.

  Workaround: None at this time.

- CSCsk76677—The Top 5 Access Point section on the Network Summary page should display the 5 busiest access points in the network. Instead it shows 5 access points associated to the first controller on the Configure > Controllers page.

  Workaround: None at this time.

- CSCsk81958—Clients that are connected to autonomous access points are showing as rogue clients.

  Workaround: None at this time.

- CSCsk83657—When you choose AAA > Users and edit the password for an existing user and then later click on "Click here for current pswd policies," an empty pop-up box is shown.

  Workaround: None at this time.

- CSCsk87368—The 802.11a/n coverage in the access point profile status displays as Fail regardless of how it is reported by the controller.

  Workaround: None at this time.

- CSCsk88821—When creating maps, the floor information for a building is not retained, and Cisco WCS displays an error.

  Workaround: None at this time.

- CSCsk91931—If a known rogue entry is entered with uppercase MAC addresses on the template pages, WLC and Cisco WCS show it as lowercase.

  Workaround: Use lowercase only for known rogues.

- CSCsk97963—If you import an access point placement file immediately after exporting it without making changes, an error results.

  Workaround: None at this time.

- CSCsk99218—The single input filter is not handled properly. When you go to the Client Association Report creation window and specify an SSID and a valid client MAC address, the generated reports contains information for all clients within that SSID rather than just the specified client.

  Workaround: None at this time.

- CSCsl03053—Client utilization in the station information table should consider wired as well as 11n clients.

  Workaround: None at this time.

- CSCsl04475—Configuration group templates will fail to be applied to Wireless LAN Controllers.

  Workaround: Keep applying the configuration group template until all dependencies are fulfilled or apply each template separately from the configuration group template in the correct order of dependency.

- CSCsl08696—Cisco WCS does not allow a name change for RF Calibration Model under WCS > Monitor > Maps > RF Calibration Model.

  Workaround: None at this time.

- CSCsl11236—Servlet exception error occurs when changing some 802.11b/g parameters.

  Workaround: None at this time.

- CSCsl30099 and CSCsk31447—An administrator error is displayed when an administrator cancels an access point audit.

  Workaround: None at this time.

- CSCsl32786—Guest accounts are lost after a controller reboot.

  Workaround: None at this time.

- CSCsl34472—Cisco WCS removes the last 2 digits that are entered in the lifetime field when adding guest users from a CSV file.

  Workaround: Add 2 trailing digits, for example: For the value 8400 seconds, add two extra zeros to make 840000. This creates a guest user with a value of 8400 seconds on the controller.

- CSCsl34500—Adding Guest users with a CSV file fails with an exception message. When adding a guest user with a CSV file the disclaimer field is mandatory.

  For example: If a user is added with the syntax: *Username*, *Password*, *30023*, *description* the addition of the user fails with an exception error.

  Workaround: Use this format when adding users from a CSV file:

  Username, *Password*, *30023*, *description*,

  Using the trailing comma causes the default disclaimer to be used.

- CSCsl37290—Unable to troubleshoot clients associated to a wireless LAN controller running Release 4.1 software, an Unknown Exception Occurred error is displayed.

  Workaround: On WCC, click **Monitor > Clients > New Search** (on the left side).

  When that window displays, check **Search on Controllers Now**.

  The page displays all clients attached to the wireless LAN controller that is being monitored by Cisco WCS.

  Click on the desired client, then choose **Troubleshoot** in the drop-down on the upper right side of the page. The client troubleshooting information displays.

- CSCsl37451—Cisco WCS documentation does not list all the required ports.

  Workaround: None at this time.

- CSCsl13793—When adding a Cisco 1310 access point with an internal antenna to a Cisco WCS map, an error message displays concerning the setting of antenna gain for the external antenna.

  Workaround: None at this time.

- CSCsl33346 and CSCsj11609—Issues deleting guest users on Cisco WCS Release 4.2.62. When a guest user (created using a guest user template) is deleted, and error message is sometimes displayed. The error reads “Batch update returned row count from update[0]; actual count 0; expected:1” .

  Workaround: None at this time.

- CSCsl38408—After resizing a map, the Map Editor does not exit.

  Workaround: None at this time.

- CSCsl38435—When editing the AAA mode in Cisco WCS, the option *Fallback on Local* option is always checked for RADIUS and TACACS+ modes, even when it has just been configured as not checked.

  Workaround: None at this time. This is only a GUI issue. The backend is not affected when the *Fallback on Local* option is not checked.

- CSCsl39335—Cisco WCS fails to start. When there is a conflicting port in use, Cisco WCS fails to start and just displays the error message *Failed to start WCS Server*. Cisco WCS should display the list of conflicting ports as a reason for failure.

  Workaround: Go to WCS/webnms/logs/wcs-0-0.log on your hardisk and look for the conflicting ports.

  In Windows XP and Windows Server 2003, you can type **NETSTAT -O** to get a list of all the owning process IDs associated with each connection.

  Look Task Manager for the respective PID and stop the process using the required port.

- CSCsl40179—On the Cisco WCS GUI, *Tenet_password* is misspelled for the CSV file under Add autonomous access points.

  Workaround: None at this time.

- CSCsl42358—Quick search on Cisco WCS does not work with partial entries.

  Workaround: None at this time.

- CSCsl54419—When importing map floors from WLSE to Cisco WCS, the floor index and floor numbers are reverse. WLSE ver2.15 maps are in sequence. WLSE maps are then exported and then imported into Cisco WCS. Cisco WCS transposes the floor number with the floor index. For example floor 4 in WLSE would be showing index 4 floor 1 in Cisco WCS.

  Workaround: None at this time.

- CSCsl57317—Cisco WCS template does not hold the sort value when advancing screens. When using Cisco WCS to view a MAC address filter template in a sorted order, advancing to the next screen of MAC addresses causes the sorting order to be lost.

- CSCsl57546—When Cisco WCS displays a rogue device, the detecting access point is displayed by IP address or name depending on how the rogue was detected.

  If Cisco WCS discovers the rogue via a poll, it uses the MAC address of the access point for the access point name. If Cisco WCS learns about the rogue from a trap received from a wireless lan controller, it uses the real access point name instead.

  Workaround: None at this time.

- CSCsl59647—LAG Mode on next reboot and Broadcast Forwarding options are missing in Cisco WCS.

  Workaround: Configure these options from the controller directly.

- CSCsl63740 and CSCsl42358—A quick search for access points displays invalid results.

  Workaround: None at this time.

- CSCsl67268—Access point filter with 802.11a/g/n causes the heapmap to display as unavailable for access points without an 802.11a radio.

  Workaround: Use an access point filter with 802.11b/g/n rather than 802.11a/g/n to display the 802.11b/g clients.

- CSCsl68504—Cisco WCS ignores Starting Month when creating guest user with limited life. When creating a guest user whose limited life spans the end of a month, Cisco WCS incorrectly displays an error: *End date cannot be older than start date*. For example, a guest user whose life starts December 28th and ends January 3rd.

  Workaround: Create the guest user from the start date until the end of the month, then create a second user from the first of the month until the end date.

- CSCsl74361—Cisco WCS cannot restore StdSignaturePattern (Standard Signatures) on the wireless LAN controller.

  Workaround: Restore Standard Signatures manually on the wireless LAN controller.

- CSCsl75176—Access point heat map might not be properly generated and displayed. In some cases, the access point heat map is displayed in the upper left-hand corner instead of where access point is placed.

- CSCsl76595—Wrong alarm displayed on security page after deletion.

  Workaround: None at this time.

- CSCsl76604—In the Cisco WCS Linux version, importing a CAD file using the Map Import Floor feature introduces artifacts not shown in the original CAD drawing.

  Workaround: None at this time.

- CSCsl79599—When adding access-lists or wlans in Cisco WCS, there are bogus messages produced.

  Workaround: Contact Cisco support to determine the database queries that can be run to fix the entries.

- CSCsl76945—Cisco WCS does not apply a MAC filter template to a controller when the interface is set to none.

  Workaround: Do not set the interface to none, specify an interface already created in the controller.

- CSCsl77656—Cisco WCS displays two instances of the same controller after pushing out a template.

  Workaround: None at this time.

- CSCsl79809—The Cisco WCS RRM template turns off the automatic transmit power setting.

  Workaround: Re-enable the RRM settings either through Cisco WCS or directly on the controller.

- CSCsl82286—TFTP transfers fail when the TFTP server is not located on the same drive as Cisco WCS.

  Workaround: None at this time.

- CSCsl82335—When the Cisco WCS communicates with a controller using SNMP version 1, the client statistics of the clients associated to that particular controller show a value of zero.

  Workaround: None at this time.

- CSCsl85320—Cisco WCS email alerts do not contain the controller name for the TRAP message.

  Workaround: None at this time. Look on Cisco WCS to see which device logged the message.

- CSCsl85479—Client troubleshooting on Cisco WCS does not work for clients on wireless LAN controller release 4.1.185.0.

  Workaround: None at this time.

- CSCsl86349—Applying the access point template should only provision the specified values.

  Workaround: Reset the controller configuration.

- CSCsl89809—A UDI Common-1 error is displayed when clicking Restore WCS Values after auditing a controller.

  Workaround: None at this time.

- CSCsl90553—Cisco WCS renaming of CPU ACL templates sometimes fail. When changing the name of a controller CPU ACL template on Cisco WCS, an error message might appear about a missing name attribute even though a name was entered.

  Workaround: None at a this time.

- CSCsl91585—Monitor > Alarms does not eliminate any alarms when doing a quick search

  Workaround: None at this time

- CSCsl94720—The Retransmit timeout setting is not the same on Cisco WCS and the controllers.

  Workaround: Configure the retransmit timeout manually on the controllers.

- CSCsl95529—The Cisco WCS heat map displays inconsistent reporting of the access point state.

  Workaround: None at this time.

- CSCsm03250—Location logs are not updated when downloading logs from Cisco WCS.

  Workaround: Download the location logs manually from location appliance using the Cisco WCS GUI.

- CSCsm04809—The Cisco WCS radio utilization report shows zero values or incorrect information.

  Workaround: None at this time.

- CSCsm13333—Commas are not allowed in the Cisco WCS keyadmin.bat file.

  Workaround: Do not use commas in the keyadmin.bat file.

- CSCsm15535—Unable to add an autonomous access point to a Cisco WCS when the access point's configuration includes an snmp-server location string with more than 80 characters.

  Workaround: Reduce the string to 80 characters or less.

- CSCsm16356—Apply and delete multiple templates - System/General

  Workaround: None at this time.

- CSCsm17395—Cisco WCS access point rogue location information/report is not accurate. When looking at rogue clients through Cisco WCS, the access points that detected the rogue client might not be indicated.

  Workaround: Check the rogue clients listed directly on the controllers by clicking **Monitor > Security > Rogue Clients** and searching using Cisco WCS Controllers. To determine the access points that detected the rogue, click on the rogue access point in the list. If the rogue client was detected by a location server, the rogue client's location is indicated.

- CSCsm18894—Cisco WCS cannot refresh the controller configuration. When trying to refresh the controller configuration, an error in listed in the Cisco WCS logs.

  Workaround: None at this time.

- CSCsm30661—Templates are missing in the report after applying a configuration group. If you select all templates from a controller and add to a configuration group, when you apply the configuration group, the number of templates in the report does not equal the number of templates in the config group.

  Workaround: Select each applicable template individually to add to configuration group.

Resolved Caveats

These caveats are resolved in Cisco WCS 4.2.62.11:

- CSCsk01099 and CSCSl00148—The status column is not correct if you create guest user accounts in Cisco WCS and then view them. For example, an expired account shows as active.
- CSCsk56441—WCS configuration changes to controllers and access points are now updated in the database.
- CSCsk85166—Cisco WCS allows user to create guest accounts greater than 30 days.
- CSCsl30932—Scheduling a guest user fails with an Unknown Exception Occurred error when configured with Indoor Area and All Floors.
- CSCsl35056—CGI-bin needs to be disabled.
- CSCsl52023—Guest user life time is displayed incorrectly when created using the import option.
- CSCsl52184— Error while creating guest using import without optional fields.
- CSCsl52626—Unable to import .dwg files without a CAD application installed.
- CSCsl38764—Guest user creation sometimes produces an error message.
- CSCsl61875—Unable to change the start time for a scheduled guest user
- CSCsm01769—A database restore produces errors in the ROGUEAPTRENDDATA table.

- CSCsk01022—Old information appears after a WLC upgrade through Cisco WCS.
- CSCsk19035—You cannot modify the time manually when scheduling a guest user. If you do not use the calendar to enter time and instead use the text box, an error message occurs, and you cannot proceed with the operation.
- CSCsk27148—The old backup files are not deleted from Cisco WCS.
- CSCsl23771—When you set up a guest user in Cisco WCS without an expiration date, the email sent to the guest user erroneously shows the expiration is one month hence.

If You Need More Information

If you need information about a specific caveat that does not appear in these release notes, you can use the Cisco Bug Toolkit to find caveats of any severity. Click this URL to browse to the Bug Toolkit:

http://tools.cisco.com/Support/BugToolKit/

(If you request a defect that cannot be displayed, the defect number might not exist, the defect might not yet have a customer-visible description, or the defect might be marked Cisco Confidential.)

Troubleshooting

For the most up-to-date troubleshooting information, refer to the Cisco TAC website at the following location:

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

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, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.