Release Notes for Cisco Wireless Control System 4.2.62.0 for Windows or Linux

October 25, 2007

These release notes describe open caveats for the Cisco Wireless Control System 4.2.62.0 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.

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

Cisco Unified Wireless Network Solution Components

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

- Operating system (Wireless LAN Controller and Cisco Aironet Lightweight Access Point)
- Cisco Wireless Control System (Cisco WCS) software release 4.2.62.0
- Location appliance software release 3.1.35.0
- Cisco WCS Navigator release 1.1.62.0
- Cisco 2700 Series Location Appliance
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 4100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Catalyst 3750G Wireless LAN Controller Switches
- Cisco Wireless Services Modules (WiSMs) for Cisco Catalyst 6500 Series Switches
- Cisco WLAN Controller Network Modules for Cisco Integrated Services Routers
- Cisco Aironet 1000, 1100, 1130, 1200, 1230, 1240, 1310, and 1500 Series Lightweight Access Points
- Cisco Aironet 1310 and 1410 Bridges
- 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.

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

- High End Server—Supports up to 3,000 Cisco Aironet lightweight access points, 1,250 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. Cisco WCS running Cisco UWN Software Release 4.2 can simultaneously manage controllers running release 4.2.62.0 to support Cisco Aironet lightweight access points and controllers running release 4.1.190.5 to support Cisco Aironet mesh access points. A single Cisco WCS can manage these controllers up to the maximum number of controllers and access points supported by Cisco WCS.

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.
- Windows 2003 and Redhat 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 WCS in VmWare must follow the specifications for the size of WCS you intend to use.

Note Cisco WCS can be installed on Red Hat Linux Enterprise Server 4.0, but it will not be supported in future releases.

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 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 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 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

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

The following new features are available in WCS 4.2.62.0

Note Refer to the *Cisco Wireless Control System Configuration Guide*, Release 4.2 for details and configuration instructions for each of these features.

- 802.11n support—The introduction of the Cisco Aironet 1250 series access point, a business-class access point based on the IEEE 802.11n draft 2.0 standard. The access point offers combined data rates of up to 600 Mbps to meet bandwidth requirements. Cisco WCS display screens include a listing for configuring, managing, and monitoring 802.11n access points and their associated wireless LAN controllers.

- Standalone access point monitoring—Cisco WCS supports standalone access point status and alarm monitoring. Standalone access points can be placed and viewed on Cisco WCS heat maps. Cisco Aironet standalone access points can be monitored in preparation for migrating these access points to run LWAPP and operate with a wireless LAN controller in the unified architecture.
- Migration to the Cisco UWN is simplified with a built-in Cisco WCS tool that simplifies the process of converting Cisco Aironet standalone access points to lightweight access points. Up to ten Cisco Aironet standalone access points of the same model number can be upgraded simultaneously using the tool.
- Workgroup bridge support for standalone access points and wireless bridges—Cisco WCS includes a new workgroup bridge tab that lists the user, IP address, MAC address, and 802.11 state of the workgroup bridge acting as a client. A list of the standalone access points identified as clients operating as workgroup bridges also appears on the Cisco WCS monitor menu. You can select the access points from the list that should operate as workgroup bridges with the unified architecture.
- RF monitoring—Cisco WCS supports adding multiple Cognio Spectrum Expert sensors to monitor interference and includes new Spectrum Expert screens, menu options, and interference search capabilities. A new WCS table displays detected interferer types with severity, impacted channels, affected access points, and affected client devices. Interference information from these sensors can be found through a customized Cisco WCS search and then graphed and integrated with existing Cisco WCS information for more comprehensive reporting. This feature requires a Cisco WCS Spectrum Intelligence license for sensors available as Cisco part number WCS-ADV-SI-Se-10.
- Client troubleshooting enhancements for Cisco Compatible Extensions version 5 client devices—Cisco WCS can collect, save, export, and open debug logs for Cisco Aironet and Cisco Compatible Extensions version 5 client devices. A log analysis tab supports exportation of the debug log to any client device. Frame logs from the client diagnostic tests can be saved and opened in external tools to assist with client troubleshooting.
- Statistical reports for Cisco Compatible Extensions version 5 client devices—Cisco WCS provides real-time and historical statistical reports for Cisco Aironet and Cisco Compatible Extensions version 5 client devices.
- Customizable dashboard—New customizable tabs and focus areas are available on the Cisco WCS dashboard. Users can choose from a predefined list of components and select their order and placement on the home page, tabs, and focus areas.
- Graphics display enhancement—Cisco WCS graphs support interactive graphics and filtering of specific criteria in real time. Data can be displayed charts or tables.
- One click Cisco WCS software upgrade—Cisco WCS software can be upgraded to the latest release using an easy upgrade process.
- AutoCAD map import support—AutoCAD images can be imported into Cisco WCS and used as maps. Users can select the layer of the AutoCAD image to be used as the WCS map when the image is previewed.
- wIDS reporting enhancements—Enhanced intrusion detection system (IDS) reports display rogue devices and ad hoc events. Reports of all rogue ad hoc devices and ad hoc events from specified controllers for a specified duration can be generated and displayed based on the last update received for that rogue device. These new IDS reports provide quick access to critical security information about unauthorized devices and ad hoc events that create potential security breaches in the network.
- Ad hoc client device icon—Client devices operating in ad hoc mode are displayed using a unique ad hoc client icon on the Cisco WCS floor map plan.
- Rogue access point icon enhancements—The rogue access point icon displayed on the floor plan map changes color and differentiates between a variety of states, including alert, pending, contained, threat, contained pending, trusted missing, on network, and off network.

- Security search by MAC address of Secure Services Client (SSC)—The MAC address of an SSC is searchable from the Cisco WCS Security-Access Point policy page.
- Unified wired and wireless guest access—Wired user guest access can be enabled from a Cisco wireless LAN controller or a Cisco WCS to deliver a unified guest access solution for both wired and wireless guest users.
- Guest user provisioning templates—Preconfigured provisioning templates are available within Cisco WCS to streamline the process of provisioning guest access. The templates are defined and uploaded by the network administrator.
- Bulk guest user provisioning—Multiple guest users can be provisioned simultaneously by uploading a flat file (csv to text).
- Bandwidth policy controls—Bandwidth limitations and policies can be specified for individual guest users.
- Customizable guest portals per SSID—This feature allows administrators to implement different guest portals based on the access point SSID used by the guest user.
- Provisioning personnel audit trail—Audit trail logs list the name of the provisioning personnel who created, deleted, or modified guest user profiles or guest user credentials. Guest user access reports include information about provisioning personnel activities.
- Customized provisioning personnel views—Cisco WCS screens are available for viewing by provisioning personnel while they are provisioning guest users. You can view a specific wireless LAN controller or access point SSIDs.
- Configurable guest access terms and conditions—The legal disclaimer displayed to guest users can be modified by provisioning personnel or secured to make it uneditable.
- Provisioning personnel authentication to external AAA server—Provisioning personnel can be authenticated against a TACACS or RADIUS AAA server to confirm their identity.
- VoWLAN readiness tool—A new VoWLAN post deployment tool helps validate that the radio coverage requirements for VoWLAN are met. The tool categorizes the radio coverage into three types:
  - Green: Signal strength is within the design guidelines.
  - Yellow: Signal strength is degraded.
  - Red: Signal strength is not within the design guidelines.

  The tool supports input of any signal strength from a Wi-Fi voice device (included non-Cisco devices).
- New outdoor mesh reports—Cisco WCS includes several new reports to simplify outdoor wireless mesh network management, including:
  - Mesh packet queue statistics report that provides, on a per-queue basis, the average number of queued packets, the number of dropped packets, and the number of dropped packets per minute.
  - Stranded mesh access point that provides a list of any mesh access points that may be stranded and are not connected to a WLAN controller.
- Outdoor mesh map enhancements—The Cisco WCS outdoor mesh map displays the value of the link quality for the signal-to-noise ratio (SNR) or packet error rate (PER).
- Signal strength target level for radio resource management (RRM)—Network radio coverage can be optimized for the signal-to-noise ratio and signal strength coverage. Organizations can reduce network maintenance times and deliver an RF signal for applications such as VoWLAN through automatic radio coverage optimization.

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.

Customer Found Enhancements Addressed in this Release

The following customer found enhancements have been addressed in 4.2.62.0.

- CSCsj42898—WCS does not start if the hostname contains an underscore.
- CSCsi87932—The building list in the reports should be sorted alphabetically.
- CSCsj63033—The reports should be kept for 100 days.
- CSCsj78949—The lobby ambassador should be allowed to set items per list page.
- CSCsh97662—The Network Audit Report feature requires enhancements.
- CSCsj22572—The ability to search for rogue access points by SSID should be added.
- CSCsj05207—AIR-ANT2414S-R is missing from the external antenna drop-down list.

Caveats

This section lists open and resolved caveats in Cisco WCS 4.2.62.0 for Windows and Linux.

Open Caveats

These caveats are open in Cisco WCS 4.2.62.0:

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

  Workaround: None at this time.
- CSCse42296 —If a WLAN template already exists in WCS, it is not updated when you modify the WLAN settings on the controller.

  Workaround: Use WCS to make changes to the WLAN settings and then apply these changes to all controllers.
- CSCsg75318—There are anomalies with the search feature.

  Workaround: Every search can be created new. If a search is saved, selecting it again and applying the search should help.
- CSCsg83836—While using the Map Editor, the floor plan graphic is distorted. The issue happens when the system compresses a very high resolution image to fit into Macromedia Flash and make it editable in the Map Editor. Because the image is already compressed to fit into Macromedia Flash, compressing the image further distorts it.

  Workaround: Do not use a high-resolution image. Scale down the image to a resolution that can be loaded into a browser and clearly displayed without having to zoom the image. A free image resolution reduction tool can be found at http://www.jhlabs.com/ie/.
- CSCsh04469—The 802.11 state for probing clients displays as dissociated for unique client reports.

Workaround: None at this time.

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

- CSCsh51006—To manage WPA1 or WPA2 WLANs on 3.2 and 4.0 controllers, you will need to create separate profiles in WCS. While CSCse95746 allows the creation of multiple profiles with the same SSID, you will need to create two templates, one for 3.2 controllers and another for 4.0 controllers, which is inconvenient.

  Workaround: Create two profiles. One profile for 3.2 controllers, with WPA or WPA2 L2 security (profile name needs to match the SSID name), and another for 4.0 controllers, with WPA1+WPA2 L2 security. The profile name does not need to match the SSID name for 4.0.206.0 controllers.

- CSCsh71088—When changing the Layer 2 security setting for a WLAN from None to CKIP and applying the changes to the controller, WLAN becomes disabled. This happens only the first time you change the Layer 2 security setting from None to CKIP. There are no problems in subsequent edits.

  Workaround: Change the Layer 2 security setting for the WLAN back to None and then to CKIP again.

- CSCsh73488—When applying a controller template for web authentication with the web authentication type set to External, an SNMP error ("SNMP operation to Device failed") occurs on WCS.

  Workaround: Apply the settings directly on the controller instead of using WCS.

- CSCsh80451 —If by mistake you download a 2006 image to a 2106 controller, WCS does not validate properly and displays a message indicating that there was a failure while storing in Flash. This message is misleading because it appears as a space issue when it is not. The CLI displays the correct message stating that the image version has a mismatch, but both switchweb and WCS mention Flash.

  Workaround: Before downloading an image, make sure that the image and the controller are of same type (same series).

- 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.

- CSCsh83341—While adding access points to maps, the user cannot select multiple access points from different pages.

  Workaround: The user can select a section of access points from within each page rather than access points from all pages.

- CSCsh87109 —The following WCS client troubleshooting error is misleading:

  ```
  QueryCriteria does not exist
  ```

  This error occurs when you start troubleshooting of a client that is not yet registered in WCS.

  Workaround: Interpret this error as follows: WCS cannot locate the client in the controller and the WCS database.

- 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 WCS to keep the controller and WCS in sync.

- CSCsi15731—When you click the **Save** button on the Schedule Guest User page, a time error message appears. This condition happens due to time differences between the system on which WCS is running and the system on which the client browser is running.

  Workaround: To avoid this problem, create the user on the system on which WCS is running.

- 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.

- CSCsi24063—Heatmaps do not display properly after a restore.

  Workaround: The user can optimize the floor size. The heatmaps display properly in a larger view.

- CSCsi24635—A 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, 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 WCS.

  Workaround: Certificates can be downloaded directly to the controller rather than via the 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 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 WCS, an "SNMP operation to device failed error" may result.

  Workaround: Configure wireless management through the controller.
- CSCsj50060—If the a radio is disabled, you can still get an access point impersonation alarm listing an 802.11a radio, even though the customer is only using a b or g radio.

  Workaround: None at this time.
- 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 WCS do occur, the message may not appear.

  Workaround: Use the audit function to see if there are differences between the access point and WCS database. All changes made to the access point from 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 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.

- CSCsk01022—Old information appears after a WLC upgrade through WCS. If you follow the refresh configuration steps below, you will see the old information when you afterwards run an access point report:

  a. Refresh configuration from the controller and choose the delete option.

  b. Upgrade WLC through WCS.

  c. Reboot WLC through WCS.

  Workaround: You must do a manual refresh configuration from the controller with the delete option to have WCS show the information correctly.

- CSCsk01099—The status column is not correct if you create guest user accounts in WCS and then view them. For example, an expired account shows as active.

  Workaround: None at this time.

- 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 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 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.

- CSCsk14325—The heatmap for an IOS access point does not compute after converting an IOS access point to LWAPP.

  Workaround: Choose **Recompute RF Prediction** from the drop-down menu on the floor map. The heatmap for IOS access points is recomputed.

- 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.

- 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.

  Workaround: Use the provided calendar to schedule the date.

- CSCsk19339—In the WCS Client Troubleshooting window, under Event Log tab Syslog, you cannot generate or view RSNA logs and Roaming logs.

  Workaround: None at this time.

- 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.

- CSCsk27148—The old backup files are not deleted from WCS.

  Workaround: None at this time.

- 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 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.
- CSCsk31047—The ad hoc rogue SSID name is mismatched in the WCS alarm.

  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 WCS. The configuration displays the current known configuration 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—WCS does not update the Access Point Groups configuration.

  Workaround: Fix the configuration in 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 and CSCsk79065—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 WCS and make changes in the channel and DCA radio channel, 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.
- CSCsk71749—If you search for clients with the *clients detected by* search criteria and restrict it by the 802.11a protocol, the results are incorrect.

  Workaround: When you search for clients, do not restrict the search with the 802.11a protocol.

- CSCsk76444—When you apply the 802.11b/g/n templates to the controller, the changes are not reflected.

  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.

- CSCsk81514—If you configure an ACL name with 32 characters and enable override, the ACL name gets overwritten during roaming.

  Workaround: Create an ACL name with 31 characters or less.

- 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 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 WCS show it as lowercase.

  Workaround: Use lowercase only for known rogues.

- CSCsk93007—If you set up an autonomous access point and set the administration status as down and SNMP as unreachable, an alarm status may show as red. But when you click the status, no alarm actually exists.

  Workaround: None at this time.

- 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.

- CSCsl00148—When the scheduled guest account expires on the controller, the status does not change from Active to Expiry.

  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.

Resolved Caveats

These caveats are resolved in Cisco WCS 4.2.62.0:

- CSCsg88776—The license error, received when trying to upgrade with the incorrect license, needs a better description and a corrective action.
- CSCsh80858 —While modifying an active CPU ACL using WCS, inserting a rule may break the connectivity between WCS and the controller.
- CSCsh89306—WCS generates an SNMP error when transferring a web authentication template to a 4.0.206.0 controller. This happens when transferring a web authentication template with the following parameters:
  - Web Auth Type: Default Internal
  - Logo Display: nothing is checked
  - Web Auth Page Title: Welcome to the Delta Guest Network
  - Web Auth Page Message: Welcome to the Delta Guest Network
  - Custom Redirect URL: empty
- CSCsi04160 —On the All Access Points page, selecting **Copy and Replace AP** from the command drop-down list and clicking **GO** does not copy the AP Static IP and AP Group Name values to the new access point.
- CSCsi12492—Phantom templates are created under Config Groups in WCS due to a synchronization issue between WCS and controllers. These templates cannot be removed from WCS and prevent you from creating new templates with the same name.
- CSCsi14284—Fast roaming mode must be removed from the WCS template.
- CSCsi24972—A user should not be required to enter a tertiary controller.
- CSCsi25491—The CPU ACL for wireless is not applied in 4402 using the web interface.
- CSCsi31142—If you try and create an access point template that has the access point mode set as REAP, along with H-REAP configuration having VLAN support enabled and VLAN assigned, you get a failure message from WCS when attempting to apply the template to the access point.
- CSCsi31186—When you create a WLAN template on WCS that contains a combination of web authentication settings and either WPA PSK or static WEP, the template fails when pushed to a controller, and WCS generates an SNMP error stating that the combination is not supported.

  The following combinations are supported encryption web authentication methods:
  - Static WEPS
  - WPA using PSK

  You should be able to create a template that supports this combination on WCS and push it to a controller. You can create the WLAN template on WCS but will be unable to push it to a controller.
- CSCsi31278—The WCS Trap Control template has a typo in the WEP Decrypt Errors template.
- CSCsi34248—WCS and location notification test fires do not work.
- CSCsi62468—The WCS client user count intermittently drops.
- CSCsi64956—A shared key of more than 33 characters cannot be entered on the WLAN templates page.
- CSCsi66950—The TSM data between 20ms and 40ms is missing from the WCS reports.
- CSCsi71278—The SSIDs of rogue access points do not display in the alarms of WCS.

- CSCsi73823—The summary page incorrectly displays the number of access point radios.
- CSCsi75121—The title bar of the Configure > Access Points window is incorrectly displayed as “Configure Controllers.”
- CSCsi77521—The 7920 CAC check boxes on the WLAN Templates window are not retaining the desired option after a Save.
- CSCsi79768—TACACS+ users without WCS permission should not be allowed to login and get to the Network Summary page.
- CSCsi84233—A session timeout out-of-range error occurs when you edit a WLAN configuration.
- CSCsi85514—A scripting error occurs while configuring a mesh 4.0 access point.
- CSCsi85688—The client exclusion timeout value on the WLAN Template window is not saved.
- CSCsi85697—An incorrect number of access points is reported in the message section for rogue alarms.
- CSCsi88303—An error is received when logging in to WCS after restoring data from the 4.1 software release.
- CSCsi89307 and CSCsk14150—The access point link on the Configure > Access Point page goes to the wrong place.
- CSCsi93345—The installer provides no progress messages when upgrading Linux.
- CSCsi95289—The number of guest users is displayed incorrectly on the Lobby Ambassador page. Also, the guest user cannot be found in WCS after being created.
- CSCsj01432—Quick search is using the wrong search string for rogue access points.
- CSCsj01835—When a map displays in Firefox, most building labels are incorrect.
- CSCsj09208 and CSCsj96182—The wrong left-hand panel appears instead of the search panel.
- CSCsj11792—The busiest access point feature does not work unless access points are placed on maps.
- CSCsj12626—On the WCS > Controller page, the correct IP address is not accepted if the IP address was entered incorrectly the first time.
- CSCsj13963—The default number of elements to display is 20 and does not change even if you set it to a different value.
- CSCsj16506—When a controller running 4.1.171.0 has an existing TACACS configuration and that controller is added to WCS 4.1.83.0, the TACACS template shows it as applied to the same controller multiple times.
- CSCsj17482—A quick search on the Monitor > APs window returns a 400 bad request page.
- CSCsj17507—On WCS with TACACS enabled, a caller ID field of dummytest is returned instead of the IP address.
- CSCsj19626—Guest user creation fails after a merge with software release 4.1.
- CSCsj27469—The quick search alarm count should display both active and inactive alarms, but the list shows only those that are active.
- CSCsj29057—WCS authentication to FreeRadius, Steel Belted Radius, and IAS fails.
- CSCsj29720—An enhancement is required to rewrite the client and AP counts in WCS so that the counts are more accurate.
- CSCsj30700—A failure occurs when applying a new RADIUS template.

- CSCsj32075—The solid database server may run out of memory and stop if several hundred controllers are running several thousand access points.
- CSCsj33491—The guest user template needs a disclaimer that the message cannot exceed 255 characters.
- CSCsj34936—If a non-default port is chosen, WCS does not install properly.
- CSCsj37671—If the wrong antenna elevation is provided, a heatmap is not created.
- CSCsj39020—The AP Group VLAN cannot be removed from the AP Template page.
- CSCsj43197—The variables as part of the rogue error message are not displayed.
- CSCsj43228—If you upgrade from 4.0 to 4.1, WCS shows 2106 as the network module controller.
- CSCsj43332—The rogue list values differ on WCS and WLC.
- CSCsj47265—When you choose Monitor > Security, the Security Summary page displays. Under the AP Threats and Attacks heading, you can click one of the alarms to see how many are active. If you click the link to the active one(s), you see the alarm page but no alarms appear. The alarms appear incorrectly for signature attacks, client security related attacks, and access point threats and attacks.
- CSCsj47754—In a Linux environment, a WLA script error occurs when trying to pull up maps.
- CSCsj60008—A search of access points by floor area shows the wrong results.
- CSCsj62403—A Javascript error occurs during scheduling of a guest user.
- CSCsj64392—On the Web Auth Template page, the verification for the maximum size of the message is not done.
- CSCsj64785—The access point alarms are not clearing after a hibernation.
- CSCsj66354—You cannot add WLC to WCS using SNMPv3 Privacy Protocol set to None.
- CSCsj66950—bitlist_count needs to be replaced with bitlist_anybit_set( ).
- CSCsj66992—The alarm summary does not show the major rogue access point alarm count when the severity is changed from minor to major.
- CSCsj68444—An import asset into the location server fails.
- CSCsj72570—The client access point association history table does not work.
- CSCsj73965—If WCS has a WLAN ACL configured in the template, it will not push the ACL to the controller running 4.0.
- CSCsj76540—The WCS floors need a default value for the RF calibration model.
- CSCsj79103—When an installation on a 64-bit operating system is attempted, the installer should abort.
- CSCsj80544—WCS should not allow chokepoints with duplicate MAC addresses.
- CSCsj92176—The client count on the building map displays incorrectly.
- CSCsj98722—You cannot add MAC filters using MAC filtering on the WEB GUI.
- CSCsk08823—The MAC filtering template corrupts the WLAN profile ID on WLC.
- CSCsk09265—If an invalid MAC address is entered in client troubleshooting, the message in the pop-up window is misleading.
- CSCsk15926—WCS users without superuser or root permissions cannot search access points by floor area or outdoor area.

- CSCsk17497—After the successful scheduling of a guest account, the detail page of the created account does not show expiration time details.
- CSCsk18191—A vulnerability in Apache Tomcat (the servlet container for JavaServlet and JavaServer Pages web applications) may result in remote code execution attacks.
- CSCsk26825—Outdoor areas are not listed on the access point tab of the access point templates.
- CSCsk29765—If multiple AAA servers are configured, WCS does not allow failover to the second server if the first AAA server is not running RADIUS or does not exist.
- CSCsk36954—Some unique violations occur on the Client Association table.
- CSCsk46429—The SSID report keeps repeating the same entry.
- CSCsk46615—The default setting for PSK is default. The pre-configured pre-shared key value of hexadecimal or ASCII is not applied. The default selection should be removed so that hexadecimal or ASCII is the default.
- CSCsk56441—If you change an access point IP address, it is not updated in the WCS database until WLC refreshes.
- CSCsk56546—WCS modifies WLC when it executes a background configuration backup.
- CSCsk63878—WCS does not refresh the access point group configuration.
- CSCsk66298—The configuration of 4.1 WLCs cannot refresh on WCS.
- CSCsk70077—A trap message states that “traffic on that channel was suspended.” This message is incorrect.
- CSCsk81016—A permission denied error occurs when editing VLANs for HREAP access points.
- CSCsk91931—If a known rogue entry is entered with an uppercase MAC address in the template, the WLC and WCS shows it as lowercase, and an audit error is generated.

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, detailed troubleshooting information, refer to the Cisco TAC website at the following location:

http://www.cisco.com/tac

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, 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