Release Notes for Cisco Wireless Control System 5.0.56.0 for Windows or Linux

February 2008

These release notes describe open caveats for the Cisco Wireless Control System 5.0.56.0 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 5.0.56.0
- Location appliance software release 4.0.32.0
- Cisco WCS Navigator release 1.2.55.0
- 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
- 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.
  - 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.
  - 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.
  - 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 supported in wireless LAN controller version 5.0.148.0 will be supported by Cisco WCS 5.0.56.0 and WLC running release 4.1.191.24M to support Cisco Aironet mesh access points.

Operating Systems Requirements

The following operating systems are supported:

- Windows 2003/SP2 or later 32-bit installations with all critical and security Windows updates installed.

  Note Windows 2003/SP2 64-bit installations are not supported.

  Note Windows 2003 32-bit installations provide support for up to 64 GB of RAM provided Physical Address Extension (PAE) is enabled. Refer to Windows documentation for instructions on enabling this mode.

- Red Hat Linux Enterprise Server 5.0 32-bit operating system installations.

  Note Red Hat Linux Enterprise Server 5.0 64-bit operating system installations and Red Hat Linux Enterprise Server 5.1 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.

Supported Browsers

The Cisco WCS user interface requires Internet Explorer 6.0/SP1 or 7.0, with the Flash plugin. The Cisco WCS user interface has been tested and verified 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 768 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. Cisco WCS supports database upgrades only from the following official Cisco WCS releases:

- 4.1.83.0
- 4.1.91.0
- 4.2.62.0
- 4.2.62.11

Important Notes

This section describes important information about Cisco WCS.

Software Version 5.0.55.0 Versus 5.0.56.0

The WCS software version 5.0.55.0 and this software version 5.0.56.0 differ only in terms of the CSCsm73370 bug, which was fixed in version 5.0.56.0.

If you have already upgraded to 5.0.55.0, you can continue using it. The functionality is the same between the two releases, and version 5.0.55.0 is a supported release. However, an upgrade from version 5.0.55.0 to 5.0.56.0 fails. If you have already tried to upgrade from version 5.0.55.0 to 5.0.56.0 and have experienced the failure, you should continue to use version 5.0.55.0.

The 5.0.550 to 5.0.56.0 upgrade related bug will be fixed in an upcoming maintenance release. You can upgrade from any software versions 4.1 or 4.2 directly to 5.0.56.0.

Compatibility

This release of Cisco WCS for Windows or Linux is compatible with wireless LAN controller and Cisco Aironet lightweight access point release 5.0.148.0 or later. Previous releases of Cisco WCS should not be used with the 5.0.148.0 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 4.0.32.0* at this location:

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

Note WCS 5.0.56.0 is not supported for use with the Location Appliance software release 4.0.32.0 due to CSCsm93369. This incompatibility will be addressed in the next release of WCS 5.0.

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

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.

Regulatory Updates

- Japan update—The Japanese government is formally permitting wireless LAN use of the frequencies in the W56 band for 802.11a radios. Table 1 shows the channels, frequencies, and power levels in unit of measure of the W56 band.

Table 1 Channels, Frequencies, and Power Levels for W56 in Japan

Channel	Frequency (MHz)	Maximum Power for AIR-LAP1132AG-Q-K9	Maximum Power for AIR-LAP1242AG-Q-K9
100	5500	17	15
104	5520	17	15
108	5540	17	15
112	5560	17	15
116	5580	17	15
120	5600	17	15
124	5620	17	15
128	5640	17	15
132	5660	17	15
136	5680	17	15
140	5700	17	15

All of the channels in the W56 band require dynamic frequency selection (DFS). In Japan, the W56 band is subject to Japan's DFS regulations. Currently, only the new 1130 and 1240 series access point SKUs support this requirement: AIR-LAP1132AG-Q-K9 and AIR-LAP1242AG-Q-K9.

- Additional country support—Country codes have been added for these additional countries supported by the controller: Bahrain (BH), Costa Rica (CR), Dominican Republic (DO), Ecuador (EC), Kazahkstan (KZ), Kuwait (KW), Oman (OM), Pakistan (PK), Paraguay (PY), Puerto Rico (PR), Vietnam (VN).

Notes about Google Earth

When you launch Google Earth, this message appears:

```
Google Earth could not write to the current cache or myplaces file location. The values
will be set as follows:
My Places Path:"C:\Document and Settings\userid\Application Data\Google\GoogleEarth"
Cache Path: "C:\Documents and Settings\userid\Local Settings\Application
Data\Google\GoogleEarth"
```

This is expected behavior.

Also, if you visit AP details a second time, you get an "invalid path / googleArthLradDetails was requested" HTTP status message. This Google Earth problem can be resolved by deleting the first access point details occurrence.

Refresh Controller Values

If configuration differences are found as a result of the audit, you can either restore WCS values on the controller or refresh controller values to synchronize WCS with the controller. Choose **Restore WCS Values** or **Refresh Controller Values**.

Note If you choose to refresh the controller values, you receive a Refresh Config window with two options for "Configuration if present on WCS but not on device, do you wish to:"

Retain—The WCS refreshes the configuration from the controller but will not delete any devices or configurations that no longer exist in the controller configuration. For example, if the WCS database shows an AP1 but that access point is no longer present in the controller configuration, WCS will not delete AP1 from its database.

Delete—WCS deletes the configuration of the controller from its database and retrieves a new configuration from the controller. Delete is the recommended option so WCS matches the most recent configuration you are refreshing from WLCs.

Note When WCS does a Refresh Config, only the configuration objects for this controller in the WCS database are updated. Upon refresh, the WCS templates are not updated.

Windows XP Cannot Load CAD Files

Internet Explorer 7 running on Windows XP cannot load CAD files because of missing DLLs (C:\Windows\system\DWMAPI.DLL). These DLLs are only present on Windows Vista.

One of the following actions can be taken:

- Uninstall IE7 and install IE6.
- Leave IE7 and install the missing DLLs.

Security Reports Are Not Getting Upgraded

If you are using Windows 2K and upgrading to software release 4.2, the Security report is not getting upgraded. All of the other reports (Audit, Client, Inventory, Mesh, and Performance) are upgrading correctly.

User Assistant Cannot Configure Controller

User assistants cannot configure or monitor controllers. They can only configure LocalNet Users in the controller, but they must access the Configure > Controller path to configure these local net features. If you create a user assistant user under the group category, login as that user, and go to Monitor > Controller, you receive a permission denied message as expected behavior.

Rogue Alarm Discrepency

In the current release of controller, by default, all the alarms are unclassfied unless specifically mentioned. In previous releases of Controller like 4.0.179.11 , when added onto WCS 5.0.55.0 release. all the rogues show up in the dashboard as malicious alarms.

Deletion of TFTP Server Is Not Updated in the Configuration Backup

To add a TFTP server you click **Configure > Controller Templates**, choose **TFTP server** from the left sidebar menu, and choose **Add TFTP Server** from the drop-down menu. To add the TFTP server, you give details of the name and IP address and click **Save**. If you later delete this TFTP server and perform a configuration backup (Administration > Background Task > Configuration Backup), the IP address of the TFTP server still shows in the TFTP Server window when only the default server should be shown.

Conflicting Ports Interrupt WCS Start

WCS fails to start if there is a conflicting port in use. You receive a "Failed to start WCS server" message, but you do not receive a list of conflicting ports. Go to WCS/webnms/logs/wcs-0-0.log and view the conflicting ports. In Windows XP and Windows Server 2003, enter **NETSTAT -0** to get a list of the process ID associated with each connection. In the Task Manager, you see the respective PID and can stop the process using the port that WCS requires.

New and Changed Information

New Features

The following new features are available in WCS 5.0.56.0

Note Refer to the *Cisco Wireless Control System Configuration Guide*, Release 5.0 for details and configuration instructions for each of these features.

- Google Earth Integration—Google Earth can be launched and used, from with Cisco WCS, to correlate the location and define the RF coverage area of a Cisco Aironet lightweight outdoor mesh access point using the Google Earth map feature. Google Earth must be installed to enable this feature.
- Ease-of-use additions—New ease-of-use features have been added that simplify network operations with auto provisioning of WLAN controllers and enhance network monitoring.
- Increased scalability—You can roam across a larger mobility space, thus providing a better user experience for voice and data applications.
- Enhanced WLAN security—With expanded intrusion detection and new rogue classification capabilities, the security on both the wired and wireless networks is increased, false alarms are reduced, and more granular control over detection, policies, and reporting is provided.

- Improved guest user management—You can customize a login failure message and a logout verification message web page. Additionally, you can enhance overall security by introducing guest account creation limits and extending investment protection with the support of LD authentication.
- Enhanced voice over WLAN capabilities— Organizations can improve the quality of voice calls and reduce dropped calls. The new audit tool automates configuration checks by allowing customers to define a set of rules in the WCS to validate the configuration of a group of controllers based on the WoWLAN deployment guide recommendations. Violations of the configuration can be presented in the form of a report and/or alarm.
- Location accuracy—With location accuracy, you can increase visibility to issues impacting location accuracy within the RF environment and simplified location troubleshooting.
- Auto-provisioning of wireless LAN controllers—Cisco WCS can automatically configure a new Cisco wireless LAN controller when it is detected on the wireless network.
- Scheduled shut off of WLAN and access point radios—A scheduled configuration change of the operational mode (on/off) for Cisco Aironet lightweight access points can be set by Cisco WCS.
- Diagnostic channel security enhancements—Cisco Compatible Extensions version 5 client devices can request diagnostic channel association to the unified network to assist with troubleshooting.
- Location Optimized Monitor Mode—Location Optimized Monitor Mode is a new access point configuration that enables the detection of Wi-Fi tags even if a wireless network is not actively deployed. LOMM access points can be easily added exactly where they are needed to provide ideal coverage and location accuracy without disrupting existing network configurations.
- Enhanced coverage hole detection—This feature allows organizations to monitor the RF environment in real time and report the formation of coverage holes based on feedback to the WLAN. The Cisco WCS determines the location and severity of the coverage holes for easy correction by network administrators.
- Automated client troubleshooting—When a Cisco Compatible Extension version 5 client gets associated to the WLAN diagnostic channel on WLC, a diagnostic trap is raised. If you choose to automatically troubleshoot the client, a series of version 5 tests are carried out on the client upon trap arrival, and the client is updated with the test status via pop-up messages. The report is placed in the logs directory. You have the option to export all of the automated troubleshooting logs.

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 5.0.56.0 for Windows and Linux.

Open Caveats

These caveats are open in Cisco WCS 5.0.56.0:

- CSCsg74466—If you choose **Monitor > Devices > Access Points** and select **Noise/Interference/Coverage (RSSI/SNR)** to generate a report, the legend of the report overlays the actual chart display area.

  Workaround: You can instead view the report on the WLC.
- 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**.
- CSCsh81856—While installing, the password field is only partially encrypted.

  Workaround: Only one or two of the letters show up during installation. After 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.
- CSCsi26963—The Client Association report does not include any records older than 7 days.

  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.
- CSCsj16153—You cannot simultaneously troubleshoot two different clients from the same WCS.

  Workaround: None at this time.
- CSCsj18398—When setting up a WLAN from WCS, a WPA or WPA2 choice does not forward to the 4.1 version controller.

  Workaround: You must choose WPA/WPA2 (instead of individual WPA or WPA2) for controller version 4.1 and greater.
- CSCsj36002—The logs that get generated while troubleshooting a client cannot be truncated into 2 MB files.

  Workaround: None at this time. However, this has no adverse effect on functionality.
- CSCsj61673—The event log for the client gets duplicated after some time has passed.

  Workaround: Click **Stop** to terminate the event log capture after the log has been retrieved.
- CSCsj72272—You cannot enable the Accept Signed Certificate option on the Configure > Controller Template > AP Authorization page.

  Workaround: You can 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.

- 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—The following error message occurs when loading a CAD file in maps:

  ```
  Error in getting data from server. Make sure you have connectivity and server is UP.
  ```

  Workaround: Add the .dll files in the following locations and restart the WCS server:

  c:\windows\system32\msvcp71.dll
  c:\windows\system\dwmapi.dll

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

  Workaround: Create a CSV with a valid format.

- 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, 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—Cisco WCS might experience slower refresh and rendering times (in Location > Synchronization) when managing large controller networks (200 or more) because of increased page synchronization requirements. Additionally, the CPU use for the web browser increases substantially and the browser might be unresponsive for a short period of time.

  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.

- CSCsk28639—The restore configuration system command is not working.

  Workaround: Restore the templates individually or access the controller to make the changes there.

- 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.

- CSCsk31842—WLC fails to join WCS if a NAT/PAT is in place.

  Workaround: Downgrade to 3.2.195.13.

- CSCsk39485—If you make modifications to an existing HREAP AP group template and save them, the changes are not reflected.

Workaround: None at this time.

- CSCsk41869—If you apply a template and then reapply the same template, the sort process returns an exception.

  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.

- CSCsk45607—An error should appear when a snmpv3 user enters less than 12 characters for an AES cipher authentication password.

  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.

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

  Workaround: None at this time.

- 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.

- CSCsk72193—When you perform a refresh config from the controller, you are given the option to retain or delete if the configuration is present in WCS but not on the device. The differences between the options is unclear to the user.

  Workaround: None at this time.

- CSCsk78181—The Automatic Client Troubleshooting Logs or CCXv5 Test Analysis generates a frame log .cap file, but the file does not contain any frames data.

  Workaround: None at this time.

- CSCsk79095—On the client detail page for WGB clients (Monitor > WGB), the drop-down menu contains options which are not relevant to the WGB clients. If you choose radio measurements, V5 statistics, operation parameters, and so on, a misleading message appears.

  Workaround: None at this time. Commands related to the radio do not apply to WGB clients.

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

  Workaround: None at this time.

- CSCsk87607—When a location accuracy test is tracking a large number of elements and it is left in the enabled state for a number of days, large log files might fill the logs directory. A subsequent download of a given log file might timeout given the size of the file.

  Workaround: Log into the location server via SSH and move or remove log files of the following format: rf-*MAC-address*.log (rf-00-oc-5c-07-18.log) from the `/opt/locserver/logs` directory.

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

  Workaround: None at this time.

- CSCsk91931—Even if rogue entries are made into the WCS template with uppercase MAC addresses, the WLC and WCS always show them as lowercase. This results in an audit error.

  Workaround: Use only lowercase for known rogues.

- CSCsl08696—If you establish an RF calibration model under WCS > Monitor > Maps > RF Calibration Model, you cannot change the name. This occurs in WCSs running version 4.1.91.0 and 4.2.62.0.

  Workaround: None at this time.

- CSCsl11236—If you try to change the 802.11b/g configuration by checking or unchecking parameters, you may see a servlet exception error.

  Workaround: None at this time.

- CSCsl12804—When you test the link between the controller and the client using Link Test, the ping results or RSSIs fail for some authenticated clients and voice clients. An error message that appears says the connection requires an associated client when in actuality it requires authenticated clients.

  Workaround: None at this time.

- CSCsl38408—When you press the Exit or Save button, the map editor does not exit.

  Workaround: You can close the window by pressing X on the right-hand side of the browser.

- CSCsl38717—After a guest user template is created and applied, some of the attributes are represented incorrectly when the template is revisited. For example, the status of the user account may show as expired rather than active.

  Workaround: Delete the existing template and create and apply a new one.

- CSCsl40179—The CSV file contains a typo. It should read *csv-telnetpassword.jpeg* instead of *csv-tenetpassword.jpeg*.

  Workaround: None at this time.

- CSCsl41999—An exception failure occurs when applying an SNMP template.

  Workaround: None at this time.

- CSCsl42250—When running concurrent user sessions on WCS, some access pages take a very long time to display.

  Workaround: None at this time.

- CSCsl42358—In a quick search, the substring matching function returns more data than the matched strings.

  Workaround: None at this time

- CSCsl44156—When using Cisco WCS, attempts to login to Monitor Lite are denied after upgrading from release 4.0 to 5.0. A window displays stating that you do not have privileges for the requested operation.

  Workaround: None at this time.

- CSCsl47529—When WCS is upgraded from 4.1.83.0, the lobby ambassador cannot view the password of guest users created in this version.

  Workaround: None at this time.

- CSCsl48403—When you import an access point configuration, you get an unwanted WCS prefix before the access point names in the status message.

  Workaround: None at this time.

- CSCsl48483—The access point name gets updated in the access point link but not in the Config > Access Point page where all the access points are listed.

  Workaround: None at this time.

- CSCsl51188—WCS does not update the friendly internal state for a rogue access point when the same MAC is present on two WLCs.

  Workaround: None at this time.

- CSCsl53127—The operation status in Config > AP does not show the correct information. The admin status of the radios differ from the operational status, and they should be the same.

  Workaround: None at this time.

- CSCsl53478—The access point goes into pending state while searching for access points using Monitor > AP and does not retrieve the results.

  Workaround: Search for access points from a different page, such as the Monitor page.

- CSCsl53595—When the controller information on the access point is imported through the Import AP Config feature, the access point gets updated but the error message returns that it was not updated.

  Workaround: None at this time.

- CSCsl53612—The first and last information which appears for rogue access points on maps does not appear.

  Workaround: None at this time.

- CSCsl53877—The access point cannot be searched by floor area on an access point template page. Without this, an admin may not be able to apply an access point template to a particular access point.

  Workaround: Use the Search for AP based on Controller(s) option instead of floor areas and then apply the templates on the access point.

- CSCsl53950—The icon for single radios appears incorrectly on the floor map. For example, if you choose 802.11a/n, the 802.11b/g radio shows as green when it should be gray. When the map is initially launched, the status shows correct, but when you change the protocol, the status is wrong until the map is launched again.

  Workaround: None at this time.

- CSCsl54522—The port number that displays in the pop-up when you mouse over a client icon map might differ from the port number that displays in the client general properties panel when you click on the client icon on the map. These port values should be the same.

  Workaround: Use the port value that displays on the client general properties panel.

- CSCsl57064—When an administrator tries to create a wired guest user within WCS, an error message appears.

  Workaround: The wired guest user interface can be created on the controller instead of WCS. The created wired guest user interface can then be pushed to WCS through the refresh config from a controller command.

- CSCsl57546—When WCS is displaying a rogue device, it sometimes shows the detecting access point's MAC address instead of its name depending on the detection method used. If WCS discovers the rogue through a poll, it uses the MAC address of the access point for a name. If WCS discovers the rogue by a trap from a WLC, it uses the name.

  Workaround: None at this time.

- CSCsl63991—The status message does not display tertiary controller information after you do a Config > AP > Import.

Workaround: None at this time.

- CSCsl64048—If you try to update more than two access point host names, the update does not occur.

  Workaround: None at this time.

- CSCsl64243—The status of the tertiary controller does not show up in the log.

  Workaround: None at this time.

- CSCsl68504—When you create a guest user whose limited life spans the end of the month, WCS incorrectly throws an “end data cannot be older than start date” error.

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

- CSCsl73139—The channel utilization for mesh access point for backhaul interface does not match that of regular maps and Google Earth maps.

  Workaround: None at this time.

- CSCsl73205—When a rogue is detected as friendly on one controller, the rogue state is not always updated from malicious to alert to friendly.

  Workaround: If you execute the rogue access point background task multiple times, the rogue state on the controller is updated.

- CSCsl75176—In some cases the access point heatmap is displayed in the upper left-hand corner instead of where the access point is placed.

  Workaround: None at this time.

- CSCsl75617—The interference alarm is detected by the spectrum expert but shows no location information on the Location Server when the alarm is generated.

  Workaround: Synchronize your location server.

- CSCsl76192—If you use the Apply button when in planning mode, a servletException error appears.

  Workaround: None at this time.

- CSCsl77797—The Location Accuracy Tool (Tools > Location Accuracy Tool) does not generate a spatial image when the map is not imported as a GIF file.

  Workaround: Import maps as JPEG files.

- CSCsl79802—When importing a file, the primary and secondary controller entries cannot be blank.

  Workaround: None at this time.

- CSCsl80359—Although the task scheduler may show guest users as expired, the Guest User template shows them as scheduled.

  Workaround: None at this time.

- CSCsl82286—A WCS TFTP upload may fail when running software version 4.2.62.x. This occurs if the TFTP directory for WCS is on a drive other than the one in which WCS is installed.

  Workaround: Configure WCS to have the TFTP server on the same partition of the hard disk as the WCS installation.

- CSCsl82677—The Config > AP > Import Config page needs to have a column for the access point name (or MAC address if the access point name is not known). Without a host name, nothing is displayed in the import status messages.

  Workaround: None at this time.

- CSCsl83378—If you use the Firefox browser to open up the Monitor > Clients page, the graphs and white space around it are not proportioned.

Workaround: None at this time.

- CSCsl84309—If a lobby ambassador creates a guest user using a CSV file, the end time and account expiration does not appear correctly.

  Workaround: You can create a guest user account without using CSV files.

- CSCsl85843—The Cisco Compatible Extensions version 5 client statistics task takes many hours to complete and blocks the other scheduled tasks from running.

  Workaround: None at this time.

- CSCsl87541—If you choose Monitor > AP and click **Edit View**, the search results show multiple listings of the client count.

  Workaround: None at this time.

- CSCsl89809—If you audit a WLC and then choose **Restore WCS Values**, you get the following error:

  ```
  Udi <ipaddress>/<number>COMMON-1: Some unexpected internal error has occurred. If the
  problem persists, please report to the Tech Support.
  ```

  Workaround: None at this time.

- CSCsl95415—In some cases, the Network Configuration Audit Report (Reports > Audit Report) might display blank lines in the results table.

  Workaround: None at this time.

- CSCsl98668—The New Rogue AP Count report (Reports > Security Reports) might graph a bar that covers the entire chart when the selected reporting period is *the last 6 hours* and only one record is collected and graphed for that time period. However, the number that displays on the Y axis of the chart represents the accurate number of New Rogue APs records.

  Workaround: None at this time.

- CSCsm00991—It takes awhile for client troubleshooting to appear.

  Workaround: None at this time.

- CSCsm03250—The location appliance logs contained within the downloaded WCS logs are outdated.

  Workaround: Download the logs manually from the location appliance.

- CSCsm04809—The radio utilization report shows accurate information, but the rest of the reports are skewed. The 802.11 counters and Tx power reports show information for Tx but none for Rx.

  Workaround: None at this time.

- CSCsm09162—In the Monitor > Event page, if you generate a pre-coverage hole by phones in the calling state, the pre-coverage hole report shows data clients rather than voice clients.

  Workaround: None at this time.

- CSCsm13536—The supported channel bandwidths are different depending on whether 20-MHz or 40-MHz range is used. The controller lists them differently for an 802.11n access point, but WCS lists them the same in both ranges.

  Workaround: None at this time.

- CSCsm14363—When you create a config group and then perform an audit, the Attribute Differences page does not have a Close button.

  Workaround: None at this time.

- CSCsm17395—WCS location access point rogue information is inaccurate. When looking at the rogue clients through WCS, the "APs that detected this rogue client" value is blank.

  Workaround: Change the Search In value to *WCS Controllers* on the Monitor > Security > Rogue Clients page. You can also search for rogue clients directly on the controller. From those clients that result, you see detecting access points as well as the location if the rogue client was detected by a location server.

- CSCsm20294—When the primary and secondary controllers are not configured in the access point, an import fails. The following error message appears: "AP4 primaryMwar and secondaryMwar entries 10.20.10.5 Maz40 are not configured in WCS."

  Workaround: None at this time.

- CSCsm30661—If you choose all templates from a controller and then add them to the config group with Apply, the number of templates in the report does not add up to the total number of templates in the config group.

  Workaround: Choose each applicable template individually to add to the config group.

- CSCsm33619—In WCS 4.2.62.0 under Monitor > Clients, the client search does not show the location server information for the client when doing a quick or new search. If you go to the maps where the client's access point is located, the client shows on the map as *located* by the location server.

  Workaround: Go to the map where the client's access point is located.

- CSCsm35824—The restore operation fails after two consecutive restores.

  Workaround: Restart the server. The restore operation is not successful for the second attempt. If you restore it again, it is successful.

- CSCsm48775—Some copy and paste errors occurred in the upgrade from 4.2 to 5.0 for the LradXxxStats table. Sometimes the wrong sequence is dropped, but the wrong sequence may also be used in migration, and the table is not getting populated.

  Workaround: None at this time.

- CSCsm50334—If the template application or any other such templates for the guest users fails, the message shows up as limited. The error may occur because of a lack of DB space, but the error message needs to explain the cause.

  Workaround: None at this time.

- CSCsm53129—The 1310 access point with a 2506 antenna shows an incorrect heatmap on the large outdoor map. The map may show approximately 700 feet, and the customer site survey information indicates that -50dBm extends 300 feet from the access point, but the heatmap does not reflect that.

  Workaround: None at this time.

- CSCsm56708—Even if you set the Last Detected Within setting to a minimal amount (such as 15 minutes), all clients detected even many months prior appear in the Monitor > Security > Rogue Clients menu. Also, the rogue access point MAC addresses are all zeroes.

  Workaround: None at this time.

- CSCsm57470—When you are adding an outdoor area to a map and change the zoom level, the newly added outdoor areas do not scale to the selected zoom level. The zoom level stays at 100%.

  Workaround: After changing the zoom value, click **Place** after it scales the new area.

- CSCsm60523—The PoE status for the 1250 access point shows as *not applicable* on the Monitor > Access Points window.

  Workaround: None at this time.

- CSCsm60843—The copyright information shown when logging onto WCS should show 2008.

  Workaround: None at this time.
- CSCsm61279—The client throughput on the Client tab of the WCS Home page should display the traffic values in Mbps rather than Kbps.

  Workaround: None at this time.
- CSCsm74066—WCS 5.0 should provide a proper error message and prevent installation when a user tries to install WCS or Navigator on a server running Red Hat Linux Enterprise Server 5.1.

Resolved Caveats

These caveats are resolved in Cisco WCS 5.0:

- CSCsh80858—On the Access Control List Template, inserting a rule into the current CPU breaks traffic to the WLC.
- CSCsi84233—When you modify the WLAN template on 4.1.83.0 but do not change the session timeout, you receive an error that the session timeout must be within the range of 300 to 86400 seconds.
- CSCsi86544—The client association history table does not display the same data as the client history graph.
- CSCsi88303—Some WCS operations may fail after completing a restore.
- CSCsi99517—WCS 4.1.83.0 shows an accumulative value rather than the actual value in the performance report (Report > Performance Reports > 802.11 Counters).
- CSCsj11792—When access points are not placed on the maps, the WCS does not update the client count of the top 5 access points under Network Summary and Monitor > Client page.
- CSCsj32075—The solid database has a memory leak. It keeps consuming memory over a period of time and shuts down with an “out of memory” fatal error when there is no more RAM to consume.
- CSCsj43771—If you try to enable wireless management through WCS on a WiSM, you get an SNMP operation failure message.
- 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.
- CSCsj59749—Even though the location of the rogue access point icon appears to be correct on the heatmap, the likelihood color map is not centered on the rogue access point.
- CSCsk01099—When you view a guest user account that you created, the status column is not correct. For example, an expired account shows as active.
- CSCsk05450—Calibration aborts with the following Matlab error:

  ```
  Matlab Exception: All matrices on a row in the bracketed expression must have the same
  number of rows.
  ```
- CSCsk08823—If you have four profiles tied to one WLAN ID but with four different MAC addresses, the profile name gets changed to 0 when you apply the MAC filtering template.
- CSCsk09265—If an invalid MAC address is entered in client troubleshooting (Monitor > Clients), the message that appears is misleading. The error message states that the client is not currently associated rather than that the MAC address is invalid for troubleshooting.

- CSCsk15266—The IP address in the CDP neighbor tab within Monitor > AP is incorrect. If the correct IP address of the access point is A.B.C.D, it is shown as D.C.B.A.
- CSCsk19035—You cannot manually modify the time 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—Old backup files are not deleted when you run a backup through a scheduled task.
- CSCsk27242—If you draw thick walls on a floor with small dimensions like 100 feet by 50 feet, the heatmap is shifted 4 to 8 feet from the wall.
- CSCsk49569—After you apply access point templates for specific WLANS under access point radio WLAN override, WLAN SSIDs and profiles are mismatched.
- CSCsk56441—After configuration changes to the controller and access points are made from WCS, the WCS database does not update and reflect the changes. The controller and access points take configuration changes successfully, and the changes can be viewed from the controller.
- CSCsk70003—When guest user credentials are e-mailed, a default signature text of "WCS AdminTeam" is added to the mail message.
- CSCsk70270—No debug commands display for AAA TACACS or RADIUS.
- CSCsk81016—When you log in as root user or any other user and then click **Edit Link** on any WLAN under the Locally switched VLANs set for H-REAP, a permission denied message appears.
- CSCsk85166—When WCS is running release 4.1.91 and the controller is running release 4.1.185, adding guest users from WCS sometimes fails.
- CSCsl00148—The status for scheduled guest user accounts is not updated properly.
- CSCsl21249—Importing CAD files (.dxf or .dwg files) with WCS fails when the client browser contains the CAD plugin.
- CSCsl23771—When a guest user with no expiration is set on WCS running release 4.2.62, an e-mail is sent that states when guest-user access expires.
- CSCsl24843—On the planning tool, changes made to the access point power level for 802.11a are not reflected in the planning tool heatmaps. For example, even if you drop the power level for 802.11a from 15 dBm to 1 dBm, the heatmap for the access point looks the same after the planning tool changes are complete. Also, if power levels are changed for 802.11b/g, the new 802.11b/g levels are not reflected in the 802.11a heatmaps.
- CSCsl28412—Even when a critical alarm is marked as known, WCS continues to send e-mail notices that the alarm status is being changed. This e-mail is generated every 30 minutes by default.
- CSCsl30932—The Schedule Guest User feature fails with an unknown exception when configured with "Indoor Area" and "All Floors." With this configuration, this error message appears:

  ```
  Error(s): You must correct the following error(s) before proceeding:
  Error: Unknown Exception Occurred. If the problem persists please send logs to the
  Tech Support.
  ```

- CSCsl35383—If the HREAP location authentication is enabled and the template is applied to the controller, reselecting the template does not show this config being enabled.
- CSCsl36016—When a Guest User template is applied from a WCS that is running release 4.2.62 to a controller that is running either release 4.2.61 or release 4.1.185, the following message appears, even though the profile is configured correctly on the controller and web-auth is enabled:

  ```
  Please verify selected profile exist on controller.Please verify selected profile has
  web-auth enabled.
  ```

- CSCsl39335—WCS failed to start when conflicting port were present. It now displays the list of conflicting ports as a reason for the failure.
- CSCsl42051—When a user sets the CSM-S SSL daughter card with stopbits 1 under line con 0, upgrade of the SW version fails.
- CSCsl51342—When you are logged in as a Super User, and attempt to access the Location Presence page (Edit Location Presence Info option from the Select a command menu) from a specific map, permission is denied. This does not affect any other users.
- CSCsl79599—In WCS 4.2.62, the "Selected combination is already defined" error when adding access lists or "Error: The Controller is already configured with "256" WLANs, which is the maximum limit that can support" error when adding WLANs is no longer appearing.
- CSCsl84817—When you go to Configure > Controller > Management > Trap Receiver and choose to add a default trap receiver, you receive a check box with an option to delete the trap receiver. If you add another trap receiver and delete the initial trap receiver, the Delete option disappears.
- CSCsm13643—If the zoom size is changed when viewing a scheduled task in Accuracy Tool, devices are decoupled from the initial actual location while the floor map is adjusted in size.
- CSCsm19910—If you try to add a user on the Administration > AAA > Users page, you see a javascript error.
- CSCsm73370—If you upgrade WCS from version 4.2.62.11 (or earlier) to 5.0.55.0, the TFTP root folder is deleted, and a new empty TFTP folder is created.

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