Release Notes for Cisco Wireless Control System 5.2.110.0 for Windows or Linux

November 2008

These release notes describe open caveats for the Cisco Wireless Control System 5.2.110.0 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)
- Cisco 3350 Mobility Services Engine
- Cisco WCS Navigator
- 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.

- 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 AMD Xeon Quad processor with 8-GB RAM.
  - Intel AMD Quad core Xeon processor.
  - 200 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 450 Cisco wireless LAN controllers.
  - 3.2-GHz Intel AMD Dual Core processor with 4-GB RAM.
  - 2.13-GHz Intel AMD QC X3210 processor.
  - 2.16-GHz Intel AMD Core2 processor.
  - 80 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 AMD processor with 2-GB RAM.
  - 1.86-GHz Intel AMD Dual core processor.
  - 50 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.

Operating Systems Requirements

The following operating systems are supported:

- Windows 2003/SP2 and Windows 2003 R2/SP2 32-bit installations with all critical and security Windows updates installed.

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

  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 or 5.1 32-bit operating system installations.

  Red Hat Linux Enterprise Server 5.0 or 5.1 64-bit operating system installations are not supported.
- Windows 2003 and Redhat Linux version support on VmWare ESX 3.0.1 version and above.

  VmWare must be installed on a system with these minimum requirements:
  Quad CPU running at 3.16 GHz with 8 GB RAM and a 200-GB hard drive or equivalent.

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

Client Requirements

The Cisco WCS user interface requires Internet Explorer 6.0/SP1, Internet Explorer 7.0 with the Flash plugin, or Mozilla Firefox 2.0.2.11 or later. The Cisco WCS user interface has been tested and verified on a Windows and Mozilla workstation.

Browsing on Windows 2003 Cisco WCS servers is not recommended because recommended Windows 2003 security settings cause browsing problems.

The client running the browser must have a minimum of 1 GB of RAM and a 2-GHz processor. The client device should not be running any CPU or memory-intensive applications.

Note The screen resolution should be set to 1024 x 768 pixels for both WCS and Navigator.

Wireless LAN Controller Requirements

Cisco WCS 5.2.110.0 supports management of the following wireless LAN controllers:

- 4.2.61.0
- 4.2.99.0
- 4.2.112.0
- 4.2.130.0
- 4.2.176.0
- 5.0.148.0
- 5.1.151.0
- 5.2.157.0

Location Server, Mesh, and MSE

Cisco WCS 5.2.110.0 supports management for the following location server, Mesh, and Mobility service engine (MSE) software:

- MSE release 5.2.91.0 and Context Aware Software

  Note Client and tag licenses are required to retrieve contextual (such as location) information within Context Aware Software. See the *Release Notes for Cisco 3350 Mobility Service Engine for Software Release 5.2.91.0* for more information.

- Location server 5.2.91.0

  Location appliances operating with release 4.0 are compatible with Cisco WCS release 5.0. Location appliances operating with release 5.2 are compatible with Cisco WCS release 5.2.

  Location appliance software is backwards compatible with the previous two location appliance releases. Therefore, you can only upgrade two releases forward. For example, you can directly upgrade from release 3.0 or 3.1 to 4.0 but you cannot directly upgrade to release 4.0 from releases 1.1, 1.2, 2.0, or 2.1.

- WLC running Mesh release 4.1.191.24M and above

WCS on WLSE Appliance

Cisco WCS on a WLSE appliance supports up to 1,500 Cisco Aironet lightweight access points and 161 Cisco wireless LAN controllers. The required processor is a 3-GHz Intel AMD Pentium with 3 GB of RAM and 38 GB of free hard drive space.

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

Finding the Software Release

To find the software release Cisco WCS is running, refer to the *Cisco Wireless Control System Configuration Guide.* If WCS is already installed and connected, verify the software release 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:

- 4.2.62.0
- 4.2.62.11
- 4.2.81.0

Note You cannot auto upgrade from 4.2.81.0 to 5.1.64.0 using Red Hat Linux Enterprise Server 5.0 (refer to bug CSCsq27887). You must initiate the manual upgrade process to do the upgrade. See the "Upgrading WCS" section in the *Wireless Control System Configuration Guide*.

- 4.2.97.0
- 4.2.110.0
- 5.0.55.0
- 5.0.56.0
- 5.0.56.2
- 5.1.64.0

Important Notes

This section describes important information about Cisco WCS.

Client Detail Report

The new client detail report replaces the existing Client Association and Client Detail Report. If you perform an upgrade, Client Association no longer appears in the Reports menu. The data pertaining to these reports migrates successfully, and saved report entries for Client Association and Client Detail reports are migrated. However, the ClientSessionInfo table is not populated with data from the previous reporting period; the table is populated with client-related data that occurred after upgrade. The new client detail report contains the details of association time, disassociation time, and session timeout along with details of VLAN, session length, client location, Megabyte information used, SNR, RSSI, and throughput.

CAPWAP Problems with Firewall

If you have rules set that apply only to LWAPP, the conversion to CAPWAP may cause problems with the firewall, and traffic may not be allowed.

Notifications in Junk Email Folder

If a domain name is not set in the email settings, notifications may end up in the junk email. When the primary device is down, no email notifications are received, but the log message indicates that an email was successfully sent.

Configure > Location Sensor

The location sensor option on the WCS GUI is not supported in WCS 5.2.110.0.

Internet Explorer Error

When you click certain links that call Javascript code, you may get an Internet Explorer error as follows:

Problems with this web page might prevent it from being displayed properly or functioning properly. In the future, you can display this message by double clicking the warning icon displayed in the status bar.

This problem appears if another program has de-registered the DLLs below. Re-registering them corrects the problem.

Follow these steps to re-register the DLLs:

Step 1 Open a command-line window in Windows XP (Start > All Programs > Accessories > Command Prompt).

Step 2 Run these commands one at a time in the following order. After each command has successfully run, you should receive a pop-up message that the DllRegisterServer in_*something*.dll succeeded.

1. regsvr32 msscript.ocx
2. regsvr32 dispex.dll
3. regsvr32 vbscript.dll
4. regsvr32 scrrun.dll
5. regsvr32 urlmon.dll
6. regsvr32 actxprxy.dll
7. regsvr32 shdocvw.dll

Step 3 Restart the computer.

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 location 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 the AP Details window 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 AP Details occurrence.

Refresh Controller Values

If the audit reveals configuration differences (basic or template based), you can either choose restore WCS values on the controller or refresh controller values to synchronize WCS with the controller. Choose **Restore WCS Values to Controller** or **Refresh Config from Controller**.

- *Restore WCS Values to Controller* enforces WCS values to the controller
- *Refresh Config from Controller* actions depends on which audit mode is selected.

When Audit Mode is Basic

When the audit mode is basic, the following applies:

If you choose *refresh config from controller*, a Refresh Config window opens 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 does 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 does 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 that WCS matches the most recent configuration you are refreshing from WLCs.

Note After a Refresh Config from Controller is performed, only the configuration objects for this controller in the WCS database are updated. Upon refresh, the WCS templates are not updated.

When Audit Mode is Template Based

When the audit mode is template based, the following applies:

Templates only get refreshed as a result of a Refresh Config from Controller. If you choose Refresh Config from Controller, a Refresh Config window opens with two options for “Configuration is present on WCS but not on device, do you wish to.”

- Retain—The WCS refreshes the configuration from the controller but does 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 does 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 that WCS matches the most recent configuration you are refreshing from WLCs.

Users are prompted for confirmation to disassociate templates from the configuration objects in the device. If a user chooses to disassociate the templates, the template association for the configuration objects in the device are removed.

After this, the configuration objects in the WCS database are synchronized with the device. When association is removed, the next audit compares configuration objects in the WCS database with the device.

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 present only on Windows Vista.

Take one of the following actions:

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

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 in the group category, log in as that user, and go to Monitor > Controller, you receive a permission denied message as expected behavior.

Deletion of TFTP Server Is Not Updated in the Configuration Backup

To add a TFTP server, 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, enter the name and IP address and click **Save**. If you later delete this TFTP server and back up the configuration (Administration > Background Task > Configuration Backup), the IP address of the TFTP server still appears in the TFTP Server window when only the default server appears.

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. Enter the following to get a list of the process IDs associated with each connection:

In Windows XP and Windows Server 2003, enter **netstat -na0.**

In Linux, enter **netstat -nlp.**

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 5.2.110.0.

Note Refer to the *Cisco Wireless Control System Configuration Guide*, Release 5.2 for details and configuration instructions for each of these features.

- High Availability (HA)—Cisco WCS supports software-based high availability for failover from primary (active) to secondary (standby) servers. Each active server can be backed up a standby server. Automatic and manual failover modes are supported.

  Note Customers with a Cisco WCS license that supports location services must upgrade to software release 5.2 or later in order to enable high availability.

  Note High availability is not supported on a VmWare setup.

- Cisco WCS Plus license—A Cisco WCS Plus license supports Cisco WCS base license features and the following capabilities:
  - Location services
  - High availability

  A Cisco WCS Plus license is backward compatible to existing Cisco WCS location and enterprise licenses.
- Flexible configuration audit—Cisco WCS supports the ability to selectively audit the configuration parameters of wireless devices. Flexible configuration auditing compares the global audit set configurations against the configurations on individual controllers or across controllers in the entire Cisco Unified Wireless network. A global audit is a set of attributes that can be used to perform selective configuration auditing.
- Template additions and enhancements—Three new template enhancements are now available:
  - Standalone (autonomous) access point configuration template: Cisco Aironet standalone (IOS-based) access points can be configured using the CLI commands template in Cisco WCS. Templates can be applied to selected access points.
  - Controller CLI template: Cisco WLAN controllers can be configured using the CLI command template in Cisco WCS. Templates can be applied to selected controllers.
  - Access point power injector setting in access point template: The access point power injector settings have been added to the access point configuration page and access point templates.
- Enhancements to autonomous to unified migration tool—The embedded Cisco WCS standalone (autonomous to IOS-based) access point to unified (lightweight access point protocol [LWAPP]) access point migration tool is enhanced to support these new features:
  - Analysis of the standalone access points to be migrated to LWAPP.

  - Ability to upgrade the standalone access point to a minimum Cisco IOS software version using a pre-bundled image available with Cisco WCS or an external software image.
  - Ability to upgrade a single-radio autonomous access points to run LWAPP.
- Enhanced client details report—The Cisco WCS client details report is further enhanced to provide information about client session time, session length, session throughput, VLAN, SNR, RSSI, and other information.
- Dual-band platforms (AP1131AG, AP1242AG, AP1250AG, and AP1140) are now sold in Brazil, Argentina, Chile, Puerto Rico, Oman, and Egypt by either defining new regulatory domains or making existing regulatory domains homologous.
- Guest activity logging, reporting, and provisioning audit trail is now consolidated.
- LDAP now supports two types of bind requests: anonymous and authenticated.
- Lightweight access point images are bundled with controller images and managed by the controller. Through Configure > Access Points, you can download images to autonomous access points. The image download is initiated by scheduling an immediate task and is periodically refreshed.

New Features Pertaining to Mesh

The following new features pertaining to Mesh are available in WCS 5.2.110.0.

- Background scanning on Cisco Aironet 1510 access points allows you to actively and continuously monitor neighboring channels for more optimal paths and parents. Because the access points can search on neighboring channels as well as the current channel, the list of optimal alternate paths and parents is greater.
- Ethernet bridging is now available in two mesh network scenarios: point-to-point and point-to-multipoint bridging between MAPs and Ethernet VLAN tagging where specific application traffic is segmented within a wireless mesh network and then forwarded to a wired LAN or bridged to another wireless mesh network.
- You can expand the number of Google Earth Location launch points within Cisco WCS by adding it to the Access Point summary and detail windows.
- The Mesh Nodes and Mesh Link Stats report can now be customized.
- From the Access Points Interfaces tab, you can choose a link under the Protocol heading for direct access.

Changed Information

There is no deployment restriction on the number of hybrid-REAP access points per location. However, the minimum bandwidth restriction 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 5.2.110.0 for Windows and Linux.

Open Caveats

These caveats are open in Cisco WCS 5.2.110.0:

- CSCsh44930—When you enter a client MAC address and click on **Troubleshoot**, client troubleshooting does not start.

  Workaround: Use the search framework to enter the MAC address. When the client is returned, go to the client detail page and choose **Troubleshoot** from the Select a command drop-down menu.

- CSCsh81856—While you install WCS on Linux, the password field is only partially encrypted.

  Workaround: None.

  Note Only one or two of the letters show up during installation. If the partially encrypted password field occurs, it only occurs once while creating the password. After you create the password and click **Enter**, the next installation prompt appears.

- CSCsh82165 —During the installation and uninstallation of WCS or Navigator, the following error message occasionally appears on Linux devices:

  ```
  Command.run(): process completed before monitors could start.
  ```

  Workaround: Because the error message has no effect, a workaround is not required.

- CSCsj36002—When you troubleshoot a client, the generated logs are not truncated into files of 2-MB size.

  Workaround: None. Issue has no adverse effects on functionality.

- CSCsj61673—The event log generated for the client is duplicated after time.

  Workaround: Stop the event log capture by clicking **Stop** when the log has been retrieved.

- CSCsj72272—The WCS does not provide the option to enable the SSC certificate for converted access points from the Configure > Controller Template > AP Authorization menu.

  Workaround: Connect on each WLC and enable the option "Accept Self Signed Certificate."

- CSCsj77046—The controller addition message mentions only WiSMs.

  Workaround: Go to the Configure > Controllers page to see the complete list of successfully added controllers.

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

  Workaround: Confirm the correct information by logging onto the device, or use the audit from the configuration side to confirm.

- CSCsk17031—When you view the location history of a tag or a client, the history page loads slowly.

  Workaround: Under Location Server > Administration > History Parameters, make sure the history interval for client, tags, rogue clients, and access points is not too excessive. Make sure data pruning happens more frequently.

- CSCsk31174—After an access point is migrated from autonomous to unified, the location information of the autonomous access point is not migrated if device status polling and wireless polling are disabled. The access point is discovered, but the location information previously entered as an autonomous access point is not carried over. The information must be re-entered.

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

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

  Workaround: None.
- CSCsk45607—When an SNMPv3 user with privacy and an authentication password enters an AES cipher with less than 12 characters, an error should be returned.

  Workaround: No functionality problems exist because of this missing error message.
- CSCsk78181—Frame Logs file(cap) does not contain frames data in the file.

  Workaround: None.
- CSCsk79095—On the client detail page for WGB clients, some tabs and commands appears that are not applied to a WGB client. Selecting one of these commands may cause WCS errors.

  Workaround: None required. Avoid using one of these commands.
- CSCsk81958—WCS shows wireless clients connected to autonomous access points as rogue clients.

  Workaround: None.
- CSCsl12804—The Link Test fails on some authenticated clients.

  Workaround: None.
- CSCsl42250—When multiple WCS users try to concurrently log in as “root,” several pages take a long time to load.

  Workaround: None.
- CSCsl53950—The Alarm Status on the access point icon for single radios displays incorrectly in maps. For example, if you select protocol 802.11a/n, the access point icon for b/g radios displays as green instead of gray.

  Workaround: Re-launch the map to display the correct status.
- CSCsl82286—WCS TFTP uploads may fail when running 4.2.62.x.

  Workaround: Configure WCS with the TFTP server on the same partition of the hard disk as the WCS installation.
- CSCsm13536—The channel bandwidth is listed differently for the 20-MHz and 40-MHz range of an 802.11n access point.

  Workaround: None.
- CSCsm14307—When you create a new config group, add two 4404 controllers, select a few templates (such as WLAN, NTP, Telnet, TrapReceiver, and so on), and perform an audit, WCS displays both controllers and all templates as out of synch. In actuality, the controllers have the proper configuration, but that message is not being conveyed.

  Workaround: None.
- CSCsm35824—The restore operation fails after consecutive restores.

  Workaround: Attempt the restore operation a second time.
- CSCsm58636—On the WCS Configure > Access Point page, incorrect maximum power values appear for certain channels that exceed FCC approval for that channel.

  Workaround: None.

- CSCsm75896—When you audit WLC from WCS, the following error message appears after you attempt a Restore Config: "*Restore Config Report Restore failed for following configuration(s) Name Error "StdSignaturePattern <IP address/ID> - MIB access failed.*" This error occurs if extra or missing standard signatures exist on WLC compared to what WCS has in its database for that WLC.

  Workaround: None; restoring WCS signatures is not possible on WCS.
- CSCsm80253— DHCP failure in client troubleshooting provides unclear messages.

  Workaround: None.
- CSCsm99598—A blank page appears when the ID certificate is downloaded from Configure > Controller > Security > ID Certificate. The certificate download is unsuccessful.

  Workaround: Download the ID certificate from the controller GUI.
- CSCsm99662—The Network Access Control Security Template accepts invalid server IP addresses without displaying warning messages.

  Workaround: Do not configure NAC templates with invalid IP addresses.
- CSCso07969—A DECT phone will not show as an interferer with an SAgE2 card.

  Workaround: Include another interferer besides a DECT phone or use an SAgE1 card.
- CSCso43619—Irregular breaks occur in some of the client monitoring graphs.

  Workaround: None.
- CSCso43754—The AP801 is not shown in the access point list during the conversion process.

  Workaround: Use the "Select CSV File" option and provide the .csv file name.
- CSCso49557—The Tools > Voice Audit page takes a long time to load when a report was previously created.

  Workaround: None.
- CSCso53785—When you search rogue access points using a MAC address, the rogues recently retrieved from the controllers do not appear. The rogue access point trap gets disabled from WCS.

  Workaround: Enable the rogue access point trap.
- CSCso59323—The PSK ASCII key always displays HEX under controller WLAN and templates.

  Workaround: None.
- CSCso63900—When you search clients from WCS, the list may contain multiple entries for the same client.

  Workaround: Ignore the disassociated entries.
- CSCso64095—Duplicate entries appear in the client association report.

  Workaround: None.
- CSCso67339—If you apply legacy syslog templates between controller upgrades, an error message occurs when you try to later delete the templates.

  Workaround: None.
- CSCso67791—A "timeout occurred in contacting server" error message occurs when you are choosing multiple country codes from the Config Group > DCA > Country Code tab.

  Workaround: Refresh the browser.
- CSCso68860—The Add option in HREAP Groups does not include a 1250 hybrid REAP access point.

  Workaround: Manually configure the 1250 hybrid REAP access point on the controller.

- CSCso73532—The Client Detail page has less information than the client page shown when you do a search for clients and pick from the list.

  Workaround: The information is available when the client gets associated again. You can use the information in the list.

- CSCso83838—The message that indicates that the current load on the radio is exceeded fails to specify which access point name or radio MAC has exceeded the load.

  Workaround: None.

- CSCsq09849—Even if an unlimited guest user account is created, the event history shows no traps for the unlimited guest user.

  Workaround: None.

- CSCsq12690—The device type is not shown for the detecting phone on the interferer list.

  Workaround: Look at the device category.

- CSCsq12721—Under Monitor > Spectrum Expert, the affected channel is now shown in the alarm.

  Workaround: Get the data from the interferer summary.

- CSCsq14066—The field length of the Local Power Constraint parameter is different in WCS and WLC.

  Workaround: None.

- CSCsq15741—The Mesh controllers in the WCS logs contain some exceptions.

  Workaround: None.

- CSCsq17846—An error is received if you download software on a WLC using WCS regardless of whether you use FTP, TFTP, or the GUI. This error occurs only if the access point is already downloading software from the WLC.

  Workaround: None.

- CSCsq18339—WCS generates a new event for every polling cycle rather than just updating the same event with the latest timestamp.

  Workaround: None.

- CSCsq21753—The network access control template is not supported until WLC release 4.0.219.0. In releases prior to 4.0.219.0, the GUI should either state the non-support or the template should be removed.

  Workaround: None.

- CSCsq22287—The WCS graph shows the access point uptime even though the access point is not running.

  Workaround: None.

- CSCsq22319—WCS allows the deletion of a WLAN even if the guest LAN is mapped to it.

  Workaround: None.

- CSCsq23147—If you create a floor map and place autonomous access points with a critical radio status on the map, the status icon on the Monitor > Maps menu shows as green rather than red. An LWAPP access point does not have this problem.

  Workaround: None.

- CSCsq24634—The refresh and hold time interval of CDP shows the wrong range values.

  Workaround: None.

- CSCsq29204—When you create an LDAP server template and apply it to controllers, the 4.0.219.0 and 4.1.185 controllers are not properly applied.

  Workaround: None.

- CSCsq31648—The EAP-FAST parameters template cannot be applied to the controller without generating an error.

  Workaround: None.

- CSCsq31683—When you choose Monitor > Client, the MAC address is not validated.

  Workaround: None.

- CSCsq31986—Not all controllers appear in the list when you forward a WCS 4.2.86.0 WLAN template to a controller.

  Workaround: None.

- CSCsq34103—On the external Web Auth Server, the server address should be validated and the proper message returned.

  Workaround: None.

- CSCsq34380—In the client operating parameters, the IP address shows in reverse order.

  Workaround: You can reference the WLC because it shows the IP address correctly.

- CSCsq34416—On the access point association history graph, WCS shows errors for any commands.

  Workaround: None.

- CSCsq34438—WCS shows wrong values for channel and client profiles with OFDM.

  Workaround: You can reference the WLC because it shows the values correctly.

- CSCsq36098—In the access point template, you can save an invalid value in the Stats Collections Interval field.

  Workaround: After you save the template, go back to the access point parameter tab and check the input value.

- CSCsq38486—The profile VLAN mapping is not updated correctly on the access point, even though the native VLAN is applied correctly.

  Workaround: Configure the hybrid REAP configuration with native VLAN and forward it to the access point. The native VLAN is correctly applied. Change the profile name on the same native VLAN and forward the mapping to the access point. The profile name VLAN mapping is correctly applied.

- CSCsq38650—Fortress and Cranite security is unsupported; however, WCS successfully applies these securities to a WLC 4.2.112.0 and later.

  Workaround: None.

- CSCsq40098—WCS has a maximum limit of 16 WLANs per WLC; however, it will apply the 17th wireless WLAN to WLC.

  Workaround: WLC does not allow the 17th WLAN and produces the appropriate error message. Perform the Refresh Config from Controller option.

- CSCsq44178—Access point information for the 802.11a/n radio does not appear on the map page.

  Workaround: Manually click **Load** or wait for the next refresh (which is 5 minutes by default).

- CSCsq44188—The wrong error message is displayed when an IPSEC Layer 3 WLAN template is forwarded to the 4.2.x.x. WLC. The error message should read “IPSEC not supported.”

  Workaround: None.

- CSCsq44968—When you select WISM WLC to perform a software download using FTP, WCS shows an undefined error.

  Workaround: The FTP operation can be successfully performed after you click **OK** to the error message.

- CSCsq45098—You have the option to add a WiSM with no peers, and this operation should not be allowed.

  Workaround: None.

- CSCsq48059—When you configure WLANs with IPv6 plus Layer 2 security, an error results.

  Workaround: Manually perform the configuration on the WLC.

- CSCsq49368—If you choose link test from the AP Association History Graph, a page error is returned.

  Workaround: Use the drop-down menu Link Test option from the Client Details page.

- CSCsq51230—None of the packets shown by the DHCP Message filter (found by navigating to Monitor > Clients > [pick one] > Troubleshoot > GO) are related to DHCP. The expected DHCP messages are found under the PEM filter instead.

  Workaround: None.

- CSCsq51717—The Aggregation Frequency graph does not have the proper units.

  Workaround: None.

- CSCsq61851—If FTP was last used on WLC, you cannot back up the configuration from the controller.

  Workaround: Save the controller configuration using Configure > Controllers > System > Command > Upload file.

- CSCsq62389—The results returned from the Network Configuration Audit Report Details are not discernible.

  Workaround: None.

- CSCsq62761—WCS should provide a map location link only when an access point is placed on a map.

  Workaround: None.

- CSCsq67659—When you choose Configure > Access Points, and then choose an access point from the AP Name column, the password field appears with hashed and dotted values. The confirmed access point password is empty. When you attempt to edit the parameters and save, WCS displays a mismatch error between the password and confirmed password.

  Workaround: None.

- CSCsq71540—If multiple errors occur when you add a new interface, clicking **Cancel** will not redirect you to the interface list.

  Workaround: None.

- CSCsr04276—When you add a controller, a “failed to add device to WCS Reason: Object not found in device” message may appear. The message could be more detailed, explain that WCS failed to find the SNMP attribute, and give the customers more information about what do to.

  Workaround: None.

- CSCsr23785—

- CSCsr40503—On the discovered SNMP template, the netmask is in reverse IP address order from the perform discover templates on the WLC.

Workaround: None.

- CSCsr59335—If you upgrade to 5.0.70.0 using the Linux operating system, you can no longer login to WCS.

  Workaround: None.

- CSCsr71910—The access point template returns an error when you try to enable the OfficeExtend and Encryption option.

  Workaround: You can use the Configure > AP menu option and enable the OfficeExtend and Encryption option on the AP Detail page.

- CSCsu71562—The CLI template does not work for the show run-config command.

  Workaround: None.

- CSCsu76333—The results of an all client search on Monitor > Clients > New Search return N/A for some values.

  Workaround: None.

- CSCsu80805—If the Administration > Settings > Mail Server configuration contains a "&" special character, the email is not sent.

  Workaround: None.

- CSCsu84224—An error occurs when performing client troubleshooting, even though the client is associated to the controller.

  Workaround: None.

- CSCsr91548—If you change an SNMP community in WLC, the community actually gets deleted.

  Workaround: Do not change the community used to manage controllers.

- CSCsu39828—Even if there is no client activity, an infrastructure client stays on the WCS map.

  Workaround: None.

- CSCsu47979—When you add more than one controller with different authentication priorities, WCS incorrectly populates the template for Authentication Priority List.

  Workaround: None.

- CSCsu88908—When checking the primary host name, the secondary host name points to its IP. The email notifications refer to the IP address of the secondary rather than its host name.

  Workaround: None.

- CSCsu95625—E-mails are not sent to the modified SMTP host.

  Workaround: After you modify the SMTP host, choose update on high availability configuration again to receive e-mail notifications with the new SMTP host.

- CSCsu95903—The wrong antenna options are displaying for the AP801 AGN-A-K9.

  Workaround: None.

- CSCsv01994—You should not be given the option to install 5.2.84 over 5.2.84.

  Workaround: None.

- CSCsv02000—Users should not be given the option to install 5.1.64.0 if they already have 5.2.84.0 installed, unless they are first instructed to uninstall 5.2.84.0.

  Workaround: None.

- CSCsv03326—Newly created virtual domains are not showing in the top right of the Administration > AAA > User > Virtual Domain window. No warning is issued to the user.

Workaround: None.

- CSCsv03331—After a root domain is removed, you cannot save Virtual Domains.

  Workaround: None.

- CSCsv03403—On MSE > System > Trap destinations, MSE IP addresses should not be added as a trap destination to MSE.

  Workaround: None.

- CSCsv05911—If you select two controllers (one that is reachable and another that is unreachable), and then select Save Config to Flash, an error is returned about an unreachable controller. No mention is made of the reachable controller.

  Workaround: None.

- CSCsv06447—One MSE cannot be managed by multiple WCSs, but no warning message is given when a user attempts to add an MSE to WCS.

  Workaround: None.

- CSCsv09820—If you create a scheduled guest user with an unlimited time frame and then Save, WCS fails to show the scheduled guest user on WLC details page.

  Workaround: None.

- CSCsv11228—The WCS login is taking longer than 20 minutes if the wIPs alarms are large (like around 700k and 7 GB).

  Workaround: None

- CSCsv11632—If you create a floor for an access point, and then create a scheduled guest user but use a profile name that does not exist on the access point, WCS does not check the profile name and does not recognize that it is invalid.

  Workaround: None.

- CSCsv11915—If you create a csv file with Lifetime set to greater than 35 weeks, WCS fails to validate the lifetime.

  Workaround: None.

- CSCsv12274—If you choose an invalid file with the Download Image selection, you get a bad header message rather than an "invalid file" message.

  Workaround: None.

- CSCsv12374—An SNMP error occurs on the WCS after choosing Configure > Controller > 802.11 > General and changing the authentication timeout value, but the value gets set on the WLC.

  Workaround: None.

- CSCsv13564—An error message is not displayed for "other" antenna types attached to an access point.

  Workaround: None.

- CSCsv13610—If you go to Monitor > Client and go to the Client Detail page, some extraneous characters appear on the screen.

  Workaround: None.

- CSCsv15779—The controller audit returns a null error on the secondary failover device.

  Workaround: None.

- CSCsv17866—When you select the client detail report, the wrong alignment is shown.

Workaround: None.

- CSCsv19289—Even if an 802.11a/b/n radio is chosen for an access point on a map, the details for only an 802.11a/n radio show when you click on the access point.

  Workaround: Navigate to the 802.11a/b/n radio page instead of using the map.

- CSCsv19291—In version 5.0.56.0 and later, WCS reports the AP interface as down during configuration.

  Workaround: None.

- CSCsv19369—When you go to the Monitor > AP and Alarms page, the TDD phone displays as a generic periodic fixed frequency. On the Maps pages, it comes up correctly.

  Workaround: None.

- CSCsv20762—The Association History page shows invalid location details.

  Workaround: None.

- CSCsv21253—The WLAN template and AP template list duplicate values.

  Workaround: None.

- CSCsv24277—When you configure a WiSM from Controller > Configure Controllers, the page results in an error. The error does not appear unless javascript debugging is enabled in Internet Explorer.

  Workaround: Use a template from Configure > Controller Templates to apply the settings.

- CSCsv28326—When you use a preauthentication ACL in a WLAN template, the template is forwarded to the controller successfully, but the preauthentication ACL value does not reflect the desired change. If a value exists on the controller before the template was received, the value is overwritten with None.

  Workaround: None. The change can be made on the WLC.

- CSCsv29199—If you are using FTP to transport an image to the MSE, and the FTP interface is either down or otherwise unreachable, an unrelated error message is returned.

  Workaround: None.

- CSCsv29428—TFTP servers are showing up under FTP server selections.

  Workaround: None.

- CSCsv84229—After you import WLSE data of a large size and then add an access point to the map, an error occurs in the map.

  Workaround: Restart WCS.

- CSCsv94031—It may take a long time for alarm summary to load after a restore.

  Workaround: After the data cleanup task is over, stop the WCS. Start only the database (with dbadmin start) and wait until the merge is complete. When the last row and last column show all zeros, the merge is over. Restart WCS.

Resolved Caveats

These caveats are resolved in Cisco WCS 5.2.110.0:

- CSCsi26963—The Client Association report now includes records older than seven days.
- CSCsj50060—The AP Impersonation alarm now shows the correct radio even when 802.11a radios are disabled.

- CSCsk77484—If the controller to which the access point is associated has more than 15 SSC access points, the migration time is now as expected.
- CSCsl08696—If you establish an RF calibration model under WCS > Monitor > Maps > RF Calibration Model, you can now change the name.
- CSCsl32412—You can now save a map in the Map Editor even if the floor name contains a special character.
- CSCsl48483—An access point name is now updated in the main access point page (import access point configuration from the Configure > Access Point page).
- CSCsm20294—The import process of the access point is successful even when the primary controller and secondary controller are not configured in the access point.
- CSCsm66516—You can delete a RADIUS server from the controller using WCS without getting an error.
- CSCso05664—Location appliance is now reachable from WCS.
- CSCso11659—To avoid confusion, the Administration > Background Tasks have been switched to Controller Configuration Backup, Location Server Backup, and WCS Server Backup.
- CSCso14397—The chokepoint range no longer expands as the number of tags and client size increases.
- CSCso27008—A quick search within WCS now produces valid results.
- CSCso33201—The heatmap calculation for an AP1510 no longer contains missing values. These missing values lead to incomplete heatmaps or unusual shapes.
- CSCso40295—WCS now shows correct values when you hover over a connected client device.
- CSCso73789—The imported asset information from WCS (Location > Location Servers > *server name* > Administration > Import Asset Information) reports all the clients in the map without any problems. You no longer see the clients in the map as “not set” after time passes.
- CSCso75850—After you upgrade WCS from 4.2.81.0 to 5.0.56.2, you can now remove WLC from WCS.
- CSCso79802—The web auth configuration now gets refreshed from the controller when it is more than 130 characters long.
- CSCso92492—The text box size to enter the primary, secondary, and tertiary controller has been increased.
- CSCsq10734—WCS now applies the correct dBm values for external antenna types.
- CSCsq16412—The conversion process from autonomous to LWAPP no longer fails if the login prompt on the access point is changed from its defaults.
- CSCsq22292—When you use the map editor, the imported image is no longer truncated on the bottom and right-hand side.
- CSCsq48999—An access point username password template no longer gets created with a blank name.
- CSCsq61215—The serial number of the location server is now visible under Location > Location Server > Advanced parameter.
- CSCsq63724—Some display widgets now display the entire length of the contained selection.
- CSCsq65153—When you specify management user authentication order, WCS 5.0.56.0 now allows TACACS or RADIUS servers as a priority over local.
- CSCsq71288—Client statistics under Location History are no longer blank.

- CSCsq85678—The client count is now accurate on the Monitor > Access Points and Monitor > Maps window. The client count on the maps window had been showing as 0 even though clients were associated with the access point.
- CSCsq88025—The java.exe process no longer consumes 100% CPU usage when a configuration sync background test is run.
- CSCsr02317—The random "system error: wrong alarm type rogueUnclassifiedMinor" message no longer appears after upgrading WCS.
- CSCsr20910—The slow performance issues seen during calibration have been fixed.
- CSCsr27204—Rx neighbor information is no longer missing from the Monitor > Access Point window when you choose an active access point and click on either radio.
- CSCsr65578—You no longer receive a "permission denied" error when logging into WCS with a Monitor Lite account.
- CSCsr68838—Changes made to the ACL Template on WCS are now propagated to the WLC.
- CSCsr83155—Even with Override Global User Password checked, you can now apply an access point template without receiving the "timeout occurred in contacting server" error message.
- CSCsr84358—The Busiest AP Report now uses more than channel utilization for calculation so that it accurately reflects the Tx and Rx utilization within WCS.
- CSCsr85688—When a WLAN using WEP encryption is edited and then applied to a controller using a template, the Probe Response packets from that WLAN contain a Challenge Text field (used for WEP Shared Key Authentication), and the shared key authentication is now enabled on that WLAN.
- CSCsu07868—The Configure > Controller > System > General configuration page can now be submitted without error.
- CSCsu29541—When you use an import file to add guest users and then select Controller List, attempts to update the controllers no longer generates a "no new guest accounts in list" error message.
- CSCsu42445—WCS no longer shows an audit mismatch with the controller on the syslog configuration.
- CSCsu44721—Heatmaps are now being created for 1300/1400 IOS and LWAPP mode bridges.
- CSCsu46050—The Map Editor/Planning tool now launches as expected.
- CSCsu46832—You can now run reports with large output without receiving an out of memory error and without impacting the Java heap space.
- CSCsu52246—You can now reboot an access point with the Configure AP task checked.
- CSCsu52638—After several minutes running 5.1.64.0, the controllers intermittently become unreachable, and a Java heap error appears in the logs.
- CSCsu54835—You can now successfully add a controller to WCS without a "some records dropped" error message. Likewise, if you perform an audit, the device is now reachable.
- CSCsu58337—The rogue containment mismatch between WLC and WCS has been corrected.
- CSCsu63880—The map hierarchy now reflects any changes made to the campus name.
- CSCsu76621—The Monitor > Security > Summary window not appears as expected.
- CSCsu78331—After an upgrade from 4.0.97.0 to 4.2.97.0, the heat map now shows access points with mesh links.
- CSCsv03304—The mouse over tooltip works properly in the Voice Audit report.

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