



Release Notes for Cisco Wireless Control System 5.2.130.0 for Windows or Linux

February 2009

These release notes describe open caveats for the Cisco Wireless Control System 5.2.130.0 for Windows or Linux, which comprises part of the Cisco Unified Wireless Network Solution (Cisco UWN).



Note This 5.2.130.0 release replaces 5.2.125.0 which has been deferred. If you installed release 5.2.125.0, you should upgrade to release 5.2.130.0.

The Cisco Wireless Control System is hereafter referred to as *Cisco WCS*.

Contents

These release notes contain the following sections.

- [Cisco Unified Wireless Network Solution Components, page 2](#)
- [Requirements for Cisco WCS, page 2](#)
- [Important Notes, page 8](#)
- [Caveats, page 12](#)
- [Troubleshooting, page 23](#)
- [Related Documentation, page 23](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 23](#)



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

© 2009 Cisco Systems, Inc. All rights reserved.

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 (Lightweight Access Point Protocol (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.X 32-bit operating system installations.

Red Hat Linux Enterprise Server 5.X 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 with Internet Explorer and Firefox on a Windows platform.

Using a web browser running on Windows 2003 to access the WCS web GUI is not recommended because recommended Windows 2003 security settings may 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 5.2.130.0 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
- 5.1.163.0
- 5.2.157.0
- 5.2.178.0

Location Server, Mesh, and MSE

Cisco WCS 5.2.130.0 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 in order 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 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 later.

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 caveat 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
- 5.0.72.0
- 5.1.64.0
- 5.1.65.4
- 5.2.110.0

Upgrading WCS

This section provides instructions for upgrading WCS on either a Windows or Linux server. An automated upgrade is available in software release 4.2 and later. It handles the steps you would normally follow to accomplish a manual upgrade (shut down WCS, perform a backup, remove the old WCS version, install new version, restore the backup, and start WCS). If you choose to use the installer, it searches for any previous WCS versions.



Note You must have software release 4.1.91.0 before you can automatically upgrade to 4.2.

If you choose to use the easy upgrade process, it provides error checking at each step and gives an informative message if an error causing an exit occurs. An upgrade-*version*.log is also produced and provides corrective measures.

**Note**

Scheduled task settings are not preserved when you upgrade from WCS 4.0 or earlier releases. Make sure to record your settings manually if you wish to retain them or go to **Administration > Background Tasks** after starting WCS to check or change the settings as necessary.

**Note**

If you upgrade to a WCS software release later than 4.0.87.0 from a release prior to 4.0.87.0, the users, user groups, tasks, and user passwords do not migrate. Upgrading to 4.0.87.0 before upgrading to a later release migrates the users, user groups, tasks, and user passwords.

Using the Installer to Upgrade WCS for Windows

Follow these steps to upgrade WCS (on a Windows platform) using the automated upgrade:

-
- Step 1** Insert the Windows Cisco WCS CD into the CD-ROM drive and double click the WCS-STANDARD-K9-5.2.X.Y.exe file where 5.2.X.Y is the software build. If you downloaded the installer from Cisco.com, double click the WCS-STANDARD-WB-K9-5-2-X-Y.exe file that you downloaded to your local drive.
- Step 2** The Install Anywhere window appears and prepares the system for installation. After a few seconds, the Introduction window appears, followed by the license agreement window. You must click the “I accept the terms of the License Agreement” option to continue.
- Step 3** At this point, the install wizard detects whether a previous version of WCS is installed and specifies whether the current version is eligible for an automated upgrade. If your most recent WCS version cannot participate in the automated upgrade, you receive such a notice. You must then choose **Install** and must switch to the manual upgrade. (Refer to the *WCS Software Configuration Guide* for manual upgrade instructions.) If your WCS version is eligible for an automated upgrade and the previous qualifying version of WCS is detected, choose **Upgrade** and continue to Step 4. This method is preferred.
- Step 4** Several of the values from the previous installation are retained as part of the upgrade. These include the following:
- the ports
 - the root password
 - the root FTP password
 - the TFTP server file location
 - the FTP server file location
 - the multi-homed server interfaces
- Step 5** Choose a folder in which to install the Cisco WCS at the Choose Install Folder window. It must be a different location than the previous installation. Click **Next** to continue.
- Step 6** Choose a folder location in which to store the shortcuts. It must be a different location than the previous installation.
- Step 7** Continue to follow the prompts that appear. You are notified when the system checks for required space, uninstalls previous versions, backs up files, restores, and so on. A prompt appears asking if you are ready to start WCS as a service. Click **Yes**.

**Note**

The upgrade log is located in the standard log directory (\webnms\logs) if the automated upgrade completes. If the automated upgrade did not complete, the upgrade log is located in the user home directory.

Using the Installer to Upgrade WCS for Linux

Follow these steps to upgrade WCS (on a Linux platform) using the automated upgrade:

-
- Step 1** Using the command line, perform one of the following:
- If you are installing from a CD, switch to the /media/cdrom directory.
 - If you are installing from Cisco.com, switch to the directory in which the install file was downloaded. For example, if the install file was placed in /root/Desktop, enter **cd /root/Desktop**.
- Step 2** Enter **./WCS-STANDARD-K9-5.2.X.Y.bin** (for CD users) or **./WCS-STANDARD-LB-K9-5-2-X-Y.bin** (for Cisco.com users) to start the install script.
- Step 3** The Install Anywhere message appears and prepares the system for installation. After a few seconds, the Introduction appears, followed by the license agreement statement. You must accept the license agreement to continue.
- Step 4** At this point, the install wizard detects whether a previous version of WCS is installed and specifies whether the current version is eligible for an automated upgrade. You receive a notification whether or not your most recent WCS version is eligible for the automated upgrade.
- Step 5** If you cannot continue to the automated upgrade because your current WCS version is not eligible, choose **Install** and continue to the manual upgrade (refer to the *WCS Configuration Guide* for manual upgrade instructions). You can also choose to do a manual upgrade rather than the recommended automated upgrade by choosing **Install** and continuing to the manual upgrade, but this is not recommended. If your current WCS version is eligible for the recommended automated upgrade, choose **Upgrade** and continue to Step 6.
- Step 6** Several of the values from the previous installation are retained and carried over as part of the upgrade. These include the following:
- the ports
 - the root password
 - the root FTP password
 - the TFTP server file location
 - the FTP server file location
 - the multi-homed server interfaces
- Step 7** Choose a folder in which to install the Cisco WCS. It must be a different location than the previous installation. Click **Next** to continue.
- Step 8** Choose a folder location to store the shortcuts. It must be a different location than the previous installation.
- Step 9** Continue to follow the prompts that appear. You are notified when the system checks for required space, uninstalls previous versions, backs up files, restores, and so on. A prompt appears asking if you are ready to start WCS as a service. Click **Yes**.

**Note**

The upgrade log is located in the standard log directory (\webnms\logs) if the automated upgrade completes. For an incomplete automated upgrade, the upgrade log is located in the user home directory.

Important Notes

This section describes important information about Cisco WCS.

SNMPV3 Stops Working

After a reboot of the controller, SNMPv3 stops working. The controller running SNMPv3 shows as unreachable in WCS once the controller has been rebooted. This issue is a result of caveat CSCsv64590. You must delete and re-add the SNMPv3 users on the controller any time a controller is rebooted.

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 new 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, Megabit information used, SNR, RSSI, and throughput.

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.

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 successfully runs, 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 maximum power levels.

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

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

Channel	Frequency (MHz)	Maximum Power for AIR-LAP1132AG-Q-K9	Maximum Power for AIR-LAP1242AG-Q-K9
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), Kazakhstan (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 and shows the following message: “Configuration if present on WCS but not on device, do you wish to:” Choose one of the options it provides.

- **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 WLC.



Note After you perform the Refresh Config from Controller option, 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 when you choose Refresh Config from Controller. If you choose Refresh Config from Controller, a Refresh Config window opens and shows the following message: “Configuration is present on WCS but not on device, do you wish to.” Choose one of the options provided.

- **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.

You 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 the confirmation, 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.

Caveats

This section lists open and resolved caveats in Cisco WCS 5.2.12120 for Windows and Linux.

Open Caveats

These caveats are open in Cisco WCS 5.2.130.0:

- 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.
 - 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 appear but 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.
 - 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 (which exceed FCC approval) appear for certain channels.

Workaround: None.

- CSCsm75896—When you audit WLC from WCS, the following error message appears after you attempt a restore: “*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.

- 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.

- CSCso67791—A “timeout occurred in contacting server” error message appears when you are choosing multiple country codes from the Config Group > DCA > Country Code tab.

Workaround: Refresh the browser.

- CSCso73532—The Client Detail page has less information than the client page 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 when 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.
- CSCsq34103—On the external Web Auth Server, the server address should be validated and the proper message returned.
Workaround: None.
- 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 a refresh by choosing 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 Link Test drop-down menu 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.

- 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.

- CSCsq72787—A rescheduling for the guest template does not always work.

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.

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

Workaround: None.

- CSCsr41614—Only a1:b2:c3:d4:e5:f6 is accepted as a format for entering MAC addresses.

Workaround: You can use built-in Microsoft Excel functions to convert MAC addresses into a format accepted by WCS.

- 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.

- CSCsr68574—If WCS shows a mismatch of values between WLC and WCS and the Restore WCS Values to Controller option is chosen, the stored configuration does not successfully pass to the controller.

Workaround None.

- CSCsu29867—When you check the client statistics page for a radio measurement, an error exception occurs.

Workaround: The same device should not use more than one browser to check the client statistics.

- CSCsu30166—The roam reason is not displayed for some clients.

Workaround: None.

- CSCsu39828—Even if activity for an infrastructure client is no longer occurring, the client still remains on the WCS map.

Workaround: None.

- CSCsu68600—When a location changes, the map does not quickly adjust with the new location.

Workaround: None.

- 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.

- CSCsu79969—WCS should check the MSE/LBS version (after you add, remove, or add back to a campus) and perform a function to fix any discrepancies.

Workaround: None.

- CSCsu84793—During statistics polling, the log contains several Null objects.

Workaround: None.

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

Workaround: None.

- CSCsv00394—After a secondary device restores because of the high availability function, the re-registration fails on the primary servers.

Workaround: Disable high availability and then re-enable it again for the primary device where re-registration initially failed.

- 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.

- 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 about an unreachable controller is returned. 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 you attempt 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 the WLC details page.

Workaround: None.

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

Workaround: None.

- CSCsv11632—If you create a floor for an access point and then create a scheduled guest user using 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.
- 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.
- 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.
- CSCsv29428—TFTP servers are showing up under FTP server selections.
Workaround: None.
- CSCsv62174—When you use the client troubleshooting feature on WCS, the 802.11 association test fails for connected clients.
Workaround: None.
- CSCsv66623—The Ethernet interfaces do now show for all of the mesh access points.
Workaround: None.
- CSCsv83390—If you add new access points to a floor map, the heatmap cannot redraw.
Workaround: None.
- CSCsv92855—On the client detail window, the values for AP Name and Client MAC Address are reversed.
Workaround: None.
- 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.

- CSCsw23291—The scheduled audit report is only correctly generated the first time it runs. On subsequent attempts, it just re-generates the same report regardless of the actual status.
Workaround: None.
- CSCsw29095—If a 4.2 location server has no campus established on a 5.1 WCS, synchronization fails.
Workaround: None.
- CSCsw37398—A warning about an unrecognized, illegal, or deprecated entry appears in the log messages.
Workaround: None.
- CSCsw44695—Clients on a guest network receive a base AP not found error.
Workaround: None.
- CSCsw47811—CSV files obtained under a specific environment include multiple entries for a given time.
Workaround: None.
- CSCsw49711—The 11n AP windows on WCS show both legacy diversity configs as well as 3 antenna 11n diversity configs. Both cannot exist in the configuration for a single access point.
Workaround: None.
- CSCsw68048—After you upgrade WCS, you receive a permission denied message when attempting to access guest reports.
Workaround: None.
- CSCsw69355—A client which is associated on the controller shows as disassociated when you mouse over.
Workaround: None.
- CSCsw71297—The client detailed information on WCS does not show the IP address, username, or correct state.
Workaround: All of this client information is correct in the detailed report.
- CSCsw78373—When you mouse over a client on the map, the text box shows client information without the username.
Workaround: You can directly poll the anchor WLC for this information.
- CSCsw84928—The MAC filter templates from the controller show SSID as the profileName.
Workaround: None.
- CSCsw85352—In earlier versions of WCS, the scroll bar stayed in a fixed position on the bottom right of the browser even when you scrolled in and out. In 5.2.110.0, the scroll bar is not visible even if you choose to resize based on available browser space.
Workaround: Use the browser scroll bars to get to the map editor scroll bars.
- CSCsw88127—Any AP authentication list templates created in all uppercase and sent to WLC in all uppercase will have limitations in WLC because mixed case is not supported.
Workaround: None.

- CSCsw89208—An AP config import from a CSV file fails, and a switchKeyNotSet error is recorded in the logs.
Workaround: Remove all unassociated access points from WCS.
- CSCsw90711—During a backup (either manual or as part of an automatic upgrade), an error results if you choose Yes at the “Save the backup” prompt. The backup is unsuccessful.
Workaround: Re-initiate the backup.
- CSCsw90720—When you import CAD files, the floor plan displays them as a red x.
Workaround: Restart WCS and try to import the failed file again. You can also import JPG files instead.
- CSCsw92604—You cannot delete an AP rogue rule unless a corresponding template exists.
Workaround: None.
- CSCsw98587—An upgrade takes more than 9 hours to complete.
Workaround: None.
- CSCsx02076—The bootloader should identify the ER version so that it is possible to verify that an emergency image upgrade was successful.
Workaround: None.
- CSCsx10316—The network design and controller out-of-synch alarms are not cleared after the designs and controllers are manually or automatically synched from WCS.
Workaround: Manually clear the alerts.
- CSCsx11411—WCS applies a session timeout of 1800 to WLANs.
Workaround: None.
- CSCsx13908—The scheduled reports are showing with the wrong last run time value.
Workaround: None.
- CSCsx17095—If WCS is installed on a VmWare ESX device, the WCS service stops when you log off from Windows using the VM console. This problem is not specific to VmWare management software but instead is reflective of how the Apache that WCS uses is started.
Workaround: Use RDP to manage you device instead of the VM console.
- CSCsx21972—When you use Windows 2003 with R2 and WCS 5.2.110.0 with DameWare Remote Control 6.5.0.1 or 6.8.x, the apache.exe process terminates prematurely when you log out of Windows.
Workaround: Use Windows RDP client instead of Dameware.
- CSCsx61055—If you have diagnostic WLAN enabled, an error is reported when you try to apply WLAN templates.
Workaround: Remove the diagnostic WLAN.
- CSCsx68894—Non-root users cannot log in to WCS after AAA mode is set to RADIUS and fall back to local is enabled.
Workaround: None.
- CSCsx81224—After you apply the AP group template to an access point, the OK button does not work.
Workaround: None.

Resolved Caveats

These caveats are resolved in Cisco WCS 5.2.130.0:

- CSCsw20262—In a wireless network with thousands of clients, Internet Explorer no longer appears inactive if you try to run a client association by client MAC address report.
- CSCsw35154—An alternate path configured in scheduled tasks as a backup can now be used rather than using the default TFTP directory.
- CSCsw36163—The lobby administrator can now log in to WCS when using TACACS authentication.
- CSCsw42942—A super user can now see guest users created by an administrator.
- CSCsw45414—The audit mismatch (for parameters such as Pre-Standard State, overrideCapable, selectedCountryCode, apPwd, Cisco Discovery Protocol, and enablePwd), which occurred when a new access point registered to WLC 5.2, has been corrected. The parameters for the newly joined access point are now correctly retrieved by WCS.
- CSCsw52617—You can now upgrade a large database (of more than 100,000 client records) without receiving an out of memory exception error.
- CSCsw77819—All applicable controllers are now listed on the apply template page for the WLAN template.
- CSCsw79725—You can now trace the switch port of a non-root user without failure.
- CSCsw89208—When you import an access point configuration for an access point associated with the controller, you no longer receive a SwitchKeyNotSet error.
- CSCsw91194—The audit mismatch, shown when an access point was configured for DHCP, has been corrected. WCS no longer audits static IP fields when an access point is using DHCP.
- CSCsw91189—The null pointer exception shown in the Message column of the Wireless Status Background Task has been corrected.
- CSCsx01811—The WLAN override selections are now stored in the AP Template.
- CSCsx11385—The Lightweight AP Templates window now displays the last applied AP list information.
- CSCsx18358—The maximum access point name length is now the same as the length in WLC.
- CSCsx22488—The heatmap is now computed even when antenna type is set to other.
- CSCsx27179—The Client Count report run by SSID no longer returns too many records to display.
- CSCsx27373—The rails and regions feature is no longer missing from the map editor.
- CSCsx39615—When you create a WLAN template with admin status enabled and apply it to the controller, the WLAN shows up in the access point group on both the WLC and WCS GUI.
- CSCsx46189—When a WLAN is deleted, it is now removed from the ap-group. Also, when a WLAN with an ID greater than 16 is added, the associated AP group mappings are returned.
- CSCsx46479—The IP address of the access point no longer changes after applying a template. The access point can therefore rejoin WLC.
- CSCsx65413—The 1000 series and 1500 series access points can now be discovered by WCS and no longer show as unassociated.

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>

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive,

HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)