Release Notes for Cisco Wireless Control System 5.1.65.4 for Windows or Linux

January 2009

These release notes describe open caveats for the Cisco Wireless Control System 5.1.65.4 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.

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

- High-end server—Supports up to 3,000 Cisco Aironet lightweight access points, 1,250 standalone access points, and 750 Cisco wireless LAN controllers.
  - 3.16-GHz Intel Xeon Quad processor with 8-GB RAM.
  - 80-GB minimum free disk space is needed on your hard drive.
- Standard server—Supports up to 2,000 Cisco Aironet lightweight access points, 1,000 standalone access points, and 150 Cisco wireless LAN controllers.
  - 3.2-GHz Intel Dual Core processor with 4-GB RAM.
  - 40 GB minimum free disk space is needed on your hard drive.

- Low-end server—Supports up to 500 Cisco Aironet lightweight access points, 200 standalone access points, and 125 Cisco wireless LAN controllers.
  - 3.06-GHz Intel processor with 2-GB RAM.
  - 30 GB minimum free disk space is needed on your hard drive.

Note The free disk space listed is a minimum requirement but may be different for your system, depending on the number of backups.

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.

  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 or Internet Explorer 7.0 with the Flash plugin. The Cisco WCS user interface has been tested and verified on a Windows workstation.

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

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 5.1.65.4 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

Location Server, Mesh, and MSE

Cisco WCS 5.1.65.4 supports management for the following location server, mesh, and mobility service engine (MSE) software:

- MSE release 5.1.30.0 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 5.1.30.0* for more information.

- Location server 5.1.35.0

  Location appliances operating with release 4.0 are compatible with Cisco WCS release 5.0. Location appliances operating with release 5.1 are compatible with Cisco WCS release 5.1.

  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, 350 standalone access points, and 100 Cisco wireless LAN controllers. The required processor is a 3-GHz Intel Pentium with 3 GB of RAM and 38 GB of free hard drive space.

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

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

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 an upgrade (shut down WCS, perform a backup, install new version, restore the backup, remove the old WCS version, 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-K9-5.1.X.Y.exe file where 5.1.X.Y is the software build. If you downloaded the installer from Cisco.com, double click the WCS-STANDARD-WB-K9-5-1-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 install 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 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 install. Click **Next** to continue.

Step 6 Choose a folder location to store the shortcuts. It must be a different location than the previous install.

Step 7 Continue to follow the prompts that appear. You are notified of checking for required space, uninstalling of previous versions, backing up files, restoring, and so on. You then see a prompt asking if you are now 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:

a. If you are installing from a CD, switch to the /media/cdrom directory.

b. 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-K9-5.1.X.Y.bin** (for CD users) or **./WCS-STANDARD-LB-K9-5-1-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 install 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 install. Click **Next** to continue.

Step 8 Choose a folder location to store the shortcuts. It must be a different location than the previous install.

Step 9 Continue to follow the prompts that appear. You are notified of checking for required space, uninstalling of previous versions, backing up files, restoring, and so on. You then see a prompt asking if you are now 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.

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
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.

Caveats

This section lists open and resolved caveats in Cisco WCS 5.1.65.4 for Windows and Linux.

Open Caveats

These caveats are open in Cisco WCS 5.1.65.4:

- 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.

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

  Workaround: None.

- 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 a time interval.

  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 an 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.

- CSCsl48483—An access point name is not updated in the main access point page (import access point configuration). It is updated in the access point link, but not in the Configure > Access Point page where all the access points are listed. After a day, the change is applied.

  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 map to display the correct status.

- CSCsl63991—When you use the import config feature, the Tertiary Controller Name is not updated; information regarding this failure does not show up in the status message.

  Workaround: None.

- CSCsl82677—When a hostname is not present for the access point, the MAC address is not replaced in the import status messages.

  Workaround: None required because the status message has no effect on functionality.

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

  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 there are extra or missing standard signatures 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.
- CSCso36847—In the Config Group controller tab, if the controller is selected and then removed, you cannot re-select the controller.

  Workaround: Exit and then return to Config Group to edit it.
- CSCso40295—WCS may show incorrect values when you hover over a connected client device.

  Workaround: None.
- CSCso43619—There are irregular breaks 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.
- CSCso55108—If deletion of a RADIUS Template fails, the failure reason is displayed as "Unable to remove the Radius Auth Server from Controller as it is being used by H-REAP Group."

  Workaround: Remove the RADIUS linkage in the WLAN AAA servers.
- CSCso59323—The PSK ASCII key always displays HEX under controller WLAN and templates.

  Workaround: None.
- CSCso60812—WCS user interface is slow especially when accessed over slow speed connection because the browser must make several connections to retrieve all the page content.

  Workaround: None. You must use a high-speed connection for the WCS Server.
- CSCso61647—The Config group > Country/DCA tab does not list the selected country codes.

Workaround: Select the Update Country/DCA check box to see the selected country codes/channel bandwidth.

- CSCso62557—The Access Point report page does not display the exact map location (such as campus, building, floor). It displays only the floor name. It is difficult to determine whether more than one floor has the same name.

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

  Workaround: Ignore the disassociated entries.
- CSCso64074—WCS displays the wrong error message ("Local power constraint is not supported until 5.1.x.x") when the customer tries to enable channel announcement on the 802.11h template and forward the template to controller.

  Workaround: The customer can use WLC to configure the same channel announcement on 802.11h. After a Refresh Config from Controller operation, WCS is able to update the configuration of channel announcement.
- 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.
- CSCso68105—When a map is created (within Monitor > Maps) with more than 33 characters, it is truncated in the Virtual Domain window.

  Workaround: Use the first 33 characters to identify the map.
- 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.
- CSCso75850—After you upgrade WCS from 4.2.81.0 to 5.0.56.2, you cannot remove WLC from WCS.

  Workaround: None.
- CSCso79802—The web auth configuration does not get refreshed from the controller if it is more than 130 characters long.

  Workaround: If you are using 5.0.56.0, delete the web auth configuration from the controller and then forward it to the controller using WCS. If you are using 4.2.62.0 or 4.2.81.0, do one of the following:

  - reduce the message to fewer than 130 characters and then use the WCS to forward the configuration to the controller.
  - configure the message manually on each controller to get it to work. When you view the controller, a blank message appears, even though the configuration and audit are successful.

- 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.
- CSCso94027—WCS does not display the caller or caller ID.

  Workaround: None.
- CSCso98287—The 1130 access point does not allow for modification of the elevation angle.

  Workaround: For advanced features such as Location and Rogue AP detection, Cisco recommends that the installer mount the access point on the ceiling rather than a wall for best RF performance.
- CSCsq02067—The Vocera clients show as unknown on the client monitor pages.

  Workaround: Manually modify the vendorMACs.xml file.
- CSCsq09849—Even if an unlimited guest user account is created, the event history shows no traps for the unlimited guest user.

  Workaround: None.
- CSCsq10734—WCS applies incorrect dBm values for external antenna types.

  Workaround: Set the desired dBM values on each access point individually and save.
- 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.
- CSCsq13073—The Config Group scheduled tasks do not have links for failed tasks. Also, the naming is inconsistent with the access point template scheduled report: one refers to partial success and the other refers to partial failure.

  Workaround: None.
- 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.
- CSCsq17274—After you create a PCI Compliance report, you cannot enable scheduling from the drop-down menu. The schedule shows as expired, and you cannot continue.

  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.

- CSCsq22304—If you create an interface, enable the quarantine option, fill in the details, and save, a script error occurs and prevents the save.

  Workaround: Create a dynamic interface and map the dynamic interface to quarantine.

- 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.

- CSCsq24617—You cannot map ACL to the controller's management interface through WCS.

  Workaround: None.

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

  Workaround: None.

- CSCsq26677—The template name entered during the creation of a trap receiver template has a different range in WCS than in WLC.

  Workaround: None.

- CSCsq27049—The validation for hexadecimal keys is not working as expected for the RADIUS and TACACS+ servers.

  Workaround: None.

  SHOULD CSCsq27887 BE IN RESOLVED?

- 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.

- CSCsq33401—The DSCP value in the ACL template does not match the value in the 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.
- CSCsq34587—WCS planning module is used to predict an access point model. The access point is then placed on the floor map. If any access points are removed after this placement, the new number of access point is incorrectly displayed.

  Workaround: None.
- 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.
- CSCsq38472—The access point template should validate the native VLAN ID and profile VLAN ID mapping.

  Workaround: None.
- 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.
- CSCsq44174—After the completion of an installation, WCS 4.2.91.0 shows that an error occurred.

  Workaround: Remove the following files if no WCS is installed:

  For Linux, /var/.com.zerog.registry.xml
  For windows, Program Files/Zerog Registry/.com.zerog.registry.xml
- 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.

- CSCsq45992—You are unable to remove WLC from WCS after you schedule a guest user.

  Workaround: None.

- CSCsq48059—When you configure WLAN 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.

- CSCsq51180—After you save a search, the Edit option allows you to delete any of the saved searches but not edit them.

  Workaround: None.

- 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.

- CSCsq55580—The session timeout range should be validated and the appropriate pop-up message displayed for each security type.

  Workaround: None.

- CSCsq57840—The WCS reports page does not validate the dates entered by the user.

  Workaround: None.

- CSCsq58142—An "unknown exception" error sometimes occurs when an administrator adds an existing user to other groups or modifies any defaults for users.

  Workaround: Even though the error occurs, the credentials are updated.

- CSCsq59596—When you change the RRM channel list (by browsing to Configure > Controller > 802.11a/n or 802.11b/g/n and choosing an RRM parameter), the WCS audit status value is mismatched with the WLC value.

  Workaround: Perform the Refresh Config from Controller option and delete the WCS configuration.

- CSCsq60358—WCS fails to apply a valid session time-out range for WPA1+WPA2(PSK) to the WLC. An SNMP error message occurs.

  Workaround: Create a WLAN template with WPA1+WPA2(PSK) and a default session timeout value and apply it to the controller. Set the session timeout value within range and forward it to the WLC.

- CSCsq61215—The serial number of the location server is not visible under Location > Location Server > Advanced parameter.

  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.

- CSCsq62951—If hybrid REAP switching is selected, WCS should allow peer-to-peer blocking. Currently, the option is disabled.

  Workaround: Configure hybrid REAP with peer-to-per blocking on WLC. Perform the Refresh Config from Controller option.

- CSCsq63018—An unreachable autonomous access point appears as green in the Alarm Status column.

  Workaround: None.

- CSCsq63056—An unknown exception error is returned when you give an invalid port number or character on the FTP server download.

  Workaround: Provide a valid port number for the FTP operation.

- CSCsq64288—A KML file cannot be imported to a Google Earth map if the file contains an access point name that is present on multiple access points.

  Workaround: Remove duplicate access point names from WCS.

- CSCsq66346—The channel utilization is the same for both radios when you hover over any access point on the 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.

- CSCsq71288—Client statistics under Location History are blank.

  Workaround: Use the statistics under Monitor > Clients.

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

  Workaround: None.

- CSCsr00359—A super user cannot access the Import Civic Information window.

  Workaround: Access the page as a root user rather than a super user.

- CSCsr27204—Rx neighbor information is missing from the Monitor > Access Point window when you choose an active access point and click on either radio.

  Workaround: The Rx neighbor and other similar information is available from the Maps page. If you hover over the access point in Maps for each radio tab, an Rx neighbor link shows the complete information.

- CSCsv50287—If an AP template is created with HREAP VLAN support and profile name VLAN mappings enabled, the settings are not saved on the template.

  Workaround: Manually configure the access point with WLC instead.
- CSCsv63553—When you run the client count report (Reports > Client Reports > Client Count), the option to export the report into CSV format does not exist.

  Workaround: If you instead schedule a report, you have the option to save or email the report in CSV format.
- CSCsv78303—When you search access points by floor name, a “failed to contact server” error message appears.

  Workaround: Log in as a root user.
- CSCsv83390—When you add new access points to a floor map, the heat map does not draw.

  Workaround: None.
- CSCsv95793— Using config groups to audit the controller results in an audit mismatch for the switching template.

  Workaround: None.
- CSCsw19979—The asterisk which indicates when WLC must be rebooted for settings to apply no longer applies. This asterisk seen when configuring 802.11b/g parameters in WCS implies a reboot for short preamble settings.

  Workaround: A reboot of WLC is not required.
- CSCsw35154—Even if you use scheduled tasks to establish a path for backups, WCS checks for free space in the default backup location only.

  Workaround: None.
- CSCsw47811—CSV files can contain multiple time entries when they are obtained under specific environments. Only one time entry should be allowed.

  Workaround: None.
- CSCsw71297—The client detailed information on WCS does not show the IP address, username, or correct state.

  Workaround: In the detailed report, this information is correct.
- CSCsw90711—While a backup is performed (either manually or as part of the automatic upgrade), an error can result if you select Yes to the save the backup during auto upgrade prompt.

  Workaround: Initiate the backup again.

Resolved Caveats

These caveats are resolved in Cisco WCS 5.1.65.4:

- CSCsl82286—This caveat was resolved by adding documentation to the installation chapter of the software configuration guide.
- CSCsm89434—This caveat was resolved by adding the following note to the *Modifying a Virtual Domain* section in the documentation:

  Note: Because all maps, controllers, and access points are included in the partition tree, you should expect it to take several minutes to load. This time is increased even more if you have a system with a significant number of controllers and access points.

- CSCso70155—This caveat was resolved by adding the following note to the software configuration guide:

  Note: Once an access point is converted to LWAPP, the previous status or configuration of the access point is not retained.
- CSCsq54142—This caveat was resolved with additional documentation in the online help and configuration guide.
- CSCsr20910—The slow down during heavily stressed calibration conditions has been corrected.
- CSCsr83155—AP templates can now be forwarded when the password override option is checked.
- CSCsr96094—The guest information in the Detailed Clients Report is no longer missing.
- CSCsu03989—When a rogue AP is detected on the network by WLC, the trap sent to WCS now upgrades the level of the rogue AP to critical.
- CSCsu46050—The map editor now launches even if obstacles resulting from migration or corrupted data exist.
- CSCsu46832—Reports with large outputs can now be run without an out-of-memory error.
- CSCsu48429—When an ACL template is created, all of the rules received from the controller now appear as well.
- CSCsu50193—If an error occurs when you add MSE to or delete it from WCS, an exception trace is now printed to the logs.
- CSCsu62576—Now when you create a guest user, the end date matches the date and time in the email window.
- CSCsu67431—If an ACL template is created and a rule is added, no error occurs.
- CSCsu76621—The Security Summary page now displays as expected.
- CSCsv55732—WCS continues to process SNMP traps and to generate or clear new alarms even if the SNMP trap listener is turned off.

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