



Release Notes for Cisco Wireless Control System 5.0.72.0 for Windows or Linux

August 2008

These release notes describe open and resolved caveats for the Cisco Wireless Control System 5.0.72.0 for Windows or Linux, which comprises part of the Cisco Unified Wireless Network Solution (Cisco UWN). This software release does not introduce new features; it is an update to release 5.0.56.2 that resolves the defects listed in the [Resolved Caveats](#) section.



Note

Cisco WCS Navigator release 1.2.56.0 is compatible with this release of Cisco WCS. No upgrade from WCS Navigator release 1.2.56.0 is required when you install this release of Cisco WCS.

Contents

These release notes contain the following sections.

- [Cisco Unified Wireless Network Solution Components, page 1](#)
- [Requirements for Cisco WCS, page 2](#)
- [Important Notes, page 5](#)
- [New and Changed Information, page 8](#)
- [Caveats, page 8](#)
- [Troubleshooting, page 27](#)
- [Related Documentation, page 27](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 28](#)

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)



Americas Headquarters:

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

© 2008 Cisco Systems, Inc. All rights reserved.

- Cisco Wireless Control System (Cisco WCS)
- Cisco WCS Navigator
- Cisco 2700 Series Location Appliance
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Catalyst 3750G Wireless LAN Controller Switches
- Cisco Wireless Services Modules (WiSMs) for Cisco Catalyst 6500 Series Switches
- Cisco WLAN Controller Network Modules for Cisco Integrated Services Routers
- Cisco Aironet 1000, 1100, 1130, 1200, 1230, 1240, 1250, 1310, and 1500 Series Lightweight Access Points
- Cisco Aironet 1310 and 1410 Bridges
- Cisco Aironet Access Points running LWAPP

Requirements for Cisco WCS

The following server hardware and software is required to support Cisco WCS for Windows or Linux.

Hardware Requirements for Server

Cisco WCS can be run on a workstation or server, and access points can be distributed unevenly across controllers.

- High-end server—Supports up to 3,000 Cisco Aironet lightweight access points, 1,250 standalone access points, and 750 Cisco wireless LAN controllers.
 - 3.16-GHz Intel 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 5.0 or 5.1 32-bit operating system installations.

Red Hat Linux Enterprise Server 5.0 or 5.1 64-bit operating system installations are not supported.

- Windows 2003 and Redhat Linux version support on VmWare ESX 3.0.1 version and above.

VmWare must be installed on a system with these minimum requirements:

Quad CPU running at 3.16 GHz, 8 GBs RAM, and 200-GB hard drive.

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

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 processors is a 3-GHz Intel Pentium with 3 GB of RAM and 38 GB of free hard drive space.

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

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.

Location Appliance and Mesh Requirements

Cisco WCS 5.0.72.0 supports management for the following location server and Mesh.

- Location server 4.0.38.0

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

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

- WLC running Mesh release 4.1.191.24M and above

Wireless LAN Controller Requirements

Cisco WCS 5.0.72.0 supports management of the following wireless LAN controllers:

- 4.1.171.0
- 4.1.185.0
- 4.2.61.0
- 4.2.99.0
- 4.2.112.0
- 4.2.130.0
- 5.0.148.0
- 5.0.148.2

Finding the Software Release

To find the software release Cisco WCS is running, refer to the *Cisco Wireless Control System Configuration Guide*. If WCS is already installed and connected, verify the software release version by choosing **Help > About the Software**.

Upgrading to a New Software Release

The Cisco WCS release must be the same or more recent than the controller software release. Upgrade the Cisco WCS first to prevent any unexpected problems. Cisco WCS supports database upgrades only from the following official Cisco WCS releases:

- 4.1.83.0
- 4.1.91.0
- 4.2.62.0
- 4.2.62.11
- 5.0.56.0
- 5.0.56.2

Important Notes

This section describes important information about Cisco WCS.

Regulatory Updates

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

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

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

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

- Additional country support—Country codes have been added for these additional countries supported by the controller: Bahrain (BH), Costa Rica (CR), Dominican Republic (DO), Ecuador (EC), 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 AP details a second time, you get an “invalid path / googleArthLradDetails was requested” HTTP status message. This Google Earth problem can be resolved by deleting the first access point details occurrence.

Refresh Controller Values

If 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 only present on Windows Vista.

One of the following actions can be taken:

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

User Assistant Cannot Configure Controller

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

Deletion of TFTP Server Is Not Updated in the Configuration Backup

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

Conflicting Ports Interrupt WCS Start

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

New and Changed Information

New Features

This release does not include new features.

Changed Information

There is no deployment restriction on the number of hybrid-REAP access points per location. However, the minimum bandwidth restrictions remains at 128 kb/s with the roundtrip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes.

Caveats

This section lists [Resolved Caveats](#) and [Open Caveats](#) in Cisco WCS 5.0.72.0 for Windows and Linux.

Resolved Caveats

These caveats are resolved in software release 5.0.72.0:

- CSCsk39485—When you make modifications to an existing HREAP AP group template and save them, the changes are now reflected correctly.
- CSCsl41999—An exception failure no longer occurs when you apply an SNMP template.
- CSCsl43880—Lobby ambassadors can now log into WCS using their configured username and password credentials.
- CSCsl53877—You can now search for an access point by floor area on an access point template page.
- CSCsl85843—The Cisco Compatible Extensions version 5 client statistics task now runs in an acceptable amount of time and no longer blocks other scheduled tasks from running.
- CSCsm17395—WCS location access point rogue information is no longer inaccurate.
- CSCsm74066—WCS 5.0 now provides a proper error message and prevents installation when a user tries to install WCS or Navigator on a server running Red Hat Linux Enterprise Server 5.1.
- CSCsm78993—WCS now correctly restores the database when you upgrade to WCS 5.0.56.
- CSCsm91474—The client count graph now displays the correct clients in a weekly display.
- CSCsm99967—When you enter Primary and Secondary controller names for access points, WCS no longer requires you to enter a tertiary controller.
- CSCso23848—You can now configure more than three WLANs for local switching.
- CSCso29306—When you upload a CAD file to WCS as a floor map, WCS now successfully pushes the map to the location server during synchronization.
- CSCso33201—For some outdoor access points (including 1510 access points), the heatmap calculation is no longer incomplete with missing values. The cases in a heatmap where low signal strength areas are displayed between high signal strength areas is limited.

- CSCso38611—WCS no longer indicates a partial failure when pushing out a simple access point template to update the primary and secondary controllers.
- CSCso39180—A standalone SE demo License now enables the SE feature.
- CSCso39483—WCS can now authenticate users against TACACS or RADIUS servers.
- CSCso58983—When you create two templates with the same name on different radios, you can now tell which template is for a specific radio.
- CSCso59303—WCS no longer displays an erroneous error message for pre-shared keys created through the controller GUI.
- CSCso60394—The ConfigGroup Apply Template no longer gets stuck during auto-provisioning.
- CSCso63312—The search for authenticated clients now yields results.
- CSCso64503—When you configure PSK with WPA on the controller and then change the key management in a WCS template to CCKM or 802.1x, WCS now successfully pushes the new key management type to the controller.
- CSCso64971—WCS now supports conversion of the 3201 Wireless Mobility Interface Card (WMIC) to LWAPP.
- CSCso66270—The reason code that appears on WLANs when you use WPA2+802.1x authentication has been appropriately remapped.
- CSCso68005—The Tx power level on the 802.11n radio shows accurately rather than with only a 0 value.
- CSCso68232—Java errors no longer appear in WCS logs after you take action to contain a rogue access point or mark it as friendly.
- CSCso70728—The WCS error message, “Error in geting data from server. Make sure you have connectivity and the server is UP;” no longer contains the typo *geting*.
- CSCso71881—WCS no longer allows you to enter an access point name that contains a space.
- CSCso97982—WCS now correctly reports rogue access points as being on the wired network.
- CSCso99445—When you attempt to refresh a configuration from the controller, you no longer receive an unknown error.
- CSCsq04319—You can now access WCS pages (even from non-IE browsers) without getting the "error in getting data from server. Make sure you have connectivity and the server is UP" message.
- CSCsq05159—You can now delete rogue alarms in WCS.
- CSCsq10744—WCS now retains the configured scheduled reporting period for the last period of a report.
- CSCsq10750—You can now specify the destination for the output file for a scheduled backup.
- CSCsq10758—WCS now performs data cleanup on temp directories.
- CSCsq41209—You can now use SNMPv3 to add a controller to WCS.
- CSCsq53174—The count of rogue access points and rogue adhoc reported on the WCS home page now matches the same counts on the Security Summary page.
- CSCsq58382—When an access point group name contains the maximum limit of 32 characters, the access point group name template is now forwarded to the access point.
- CSCsq72345—The WCS solid database no longer shuts down when the size exceeds 13 GB.

Open Caveats

These caveats are open in Cisco WCS 5.0.72.0:

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

Workaround: You can instead view the report on the WLC.
- CSCsh44930—In the Clients Summary page (Monitor > Clients), typing the MAC address for a mobile client in the Client field and clicking the **Troubleshoot** button does not open up the Client Troubleshooting window.

Workaround: Search for the client by its MAC address using the Quick Search field and click the link for the returned client to go the Client Details page. On the Client Details page, choose **Troubleshoot** from the Command drop-down list and click **GO**.
- CSCsh81856—While installing, the password field is only partially encrypted.

Workaround: Only one or two of the letters show up during installation. After the password is created and the user clicks **Enter**, the screen proceeds to the next session.
- CSCsh82165—Upon install or uninstall, the following error message sometimes displays: “Command.run(): process completed before monitors could start.”

Workaround: This message is irrelevant. No workaround is necessary.
- CSCsi26963—The Client Association report does not include any records older than 7 days.

Workaround: None at this time.
- CSCsj16153—You cannot simultaneously troubleshoot two different clients from the same WCS.

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

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

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

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

Workaround: You can perform this operation on the Configure > Controller > Security > AP Authorization page with the Edit AP Policies option from the Select a command drop-down menu.
- CSCsj77046—If you add controllers (with comma separation) which are combinations of WiSMs (2000s and 4400s), the status messages makes it appear as if only the WiSMs were added.

Workaround: On the Configure > Controllers page, you can see a complete list of controllers that were added successfully.

- CSCsj96574—When adding guest user accounts using a CSV file, you may receive an unknown exception error from the import operation.
Workaround: Make sure you format the file correctly and retry the operation. The correct sequence of fields per row is username, password, lifetime, description, and then disclaimer.
- CSCsk01665—If you add any template with a negative test case and try to apply the template to the device, the object is not created in the device, even though the Apply To field is incremented.
Workaround: Confirm if the object is added by logging onto the device and using an audit to check the configuration.
- CSCsk02071—The following error message occurs when loading a CAD file in maps:
`Error in getting data from server. Make sure you have connectivity and server is UP.`
Workaround: Add the .dll files in the following locations and restart the WCS server:
c:\windows\system32\msvc71.dll
c:\windows\system\dwmapi.dll
- CSCsk12424—An invalid CSV file results in an unknown exception on the migration template.
Workaround: Create a CSV with a valid format.
- CSCsk17031—The history page loads slow when trying to view the location history of a tag or client.
Workaround: Make sure the history interval for client, tags, rogue clients, and access points is not significantly high on the Location Server > Administration > History Parameters page. You can also frequently purge the data.
- CSCsk18826—Cisco WCS might experience slower refresh and rendering times (in Location > Synchronization) when managing large controller networks (200 or more) because of increased page synchronization requirements. Additionally, the CPU use for the web browser increases substantially and the browser might be unresponsive for a short period of time.
Workaround: Wait for the page to load completely.
- CSCsk25417—All clients are displayed if you click any header to resort WGB clients.
Workaround: Choose **Monitor >WGB** to reset the list of WGB clients.
- CSCsk28639—The restore configuration system command is not working.
Workaround: Restore the templates individually or access the controller to make the changes there.
- CSCsk28942—While omnidirectional antennas' radiation pattern may have some asymmetry, they generally radiate in all directions. This causes confusion trying to set antenna orientation and position access points in WCS. When Cisco omnidirectional antenna products are chosen, the setting for omni products should be disabled since the specifications of the antenna are known. The following Cisco products should have omnidirectional patterns considered: AIR-ANT5959, AIR-ANT4941, AIR-ANT2422DW-R, AIR-ANT1728, AIR-ANT2506, AIR-ANT3213, AIR-ANT24120, integrated AP1120 antenna, integrated RM21A antenna, AIR-ANT5135D-R, AIR-ANT5135DW-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT58G9VOA-N, AIR-ANT5175V-N, AIR-ANT2455V-N, and integrated AP1130AG antennas.
Workaround: Set the antenna orientation value to 0.
- CSCsk31842—WLC fails to join WCS if a NAT/PAT is in place.
Workaround: Downgrade to 3.2.195.13.

- CSCsk41869—If you apply a template and then reapply the same template, the sort process returns an exception.
Workaround: None at this time.
- CSCsk45060—Within access point templates, the WLAN profiles in the WLAN override list are retained even when profiles are no longer used on any controllers.
Workaround: None at this time.
- CSCsk45607—An error should appear when a snmpv3 user enters less than 12 characters for an AES cipher authentication password.
Workaround: None at this time.
- CSCsk48985—If you change template parameters of an existing template and then apply it to a different number of controllers, the window shows the template as applied to the original number of controllers.
Workaround: If you need to change parameters in a template, create a new template.
- CSCsk51302—When you click on Client Troubleshooting in Monitor > Clients, an “object *switch* does not exist” error displays.
Workaround: None at this time.
- CSCsk55160—If you switch between perimeter and rectangle in the planning mode tool, the total coverage area does not change, and the message above the radio buttons does not update.
Workaround: Adjust the size of the rectangle to approximately cover the perimeter area. Generate the report in either perimeter or rectangle mode.
- CSCsk78181—The Automatic Client Troubleshooting Logs or CCXv5 Test Analysis generates a frame log .cap file, but the file does not contain any frames data.
Workaround: None at this time.
- CSCsk79095—On the client detail page for WGB clients (Monitor > WGB), the drop-down menu contains options which are not relevant to the WGB clients. If you choose radio measurements, V5 statistics, operation parameters, and so on, a misleading message appears.
Workaround: None at this time. Commands related to the radio do not apply to WGB clients.
- CSCsk81958—Clients that are connected to autonomous access points are showing as rogue clients.
Workaround: None at this time.
- CSCsk87607—When a location accuracy test is tracking a large number of elements and it is left in the enabled state for a number of days, large log files might fill the logs directory. A subsequent download of a given log file might timeout given the size of the file.
Workaround: Log into the location server via SSH and move or remove log files of the following format: rf-MAC-address.log (rf-00-oc-5c-07-18.log) from the `/opt/locserver/logs` directory.
- CSCsk88821—When creating maps, the floor information for a building is not retained, and WCS displays an error.
Workaround: None at this time.
- CSCsk91931—Even if rogue entries are made into the WCS template with uppercase MAC addresses, the WLC and WCS always show them as lowercase. This results in an audit error.
Workaround: Use only lowercase for known rogues.

- CSCs108696—If you establish an RF calibration model under WCS > Monitor > Maps > RF Calibration Model, you cannot change the name. This occurs in WCSs running version 4.1.91.0 and 4.2.62.0.
Workaround: None at this time.
- CSCs112804—When you test the link between the controller and the client using Link Test, the ping results or RSSIs fail for some authenticated clients and voice clients. An error message that appears says the connection requires an associated client when in actuality it requires authenticated clients.
Workaround: None at this time.
- CSCs138408—When you press the Exit or Save button, the map editor does not exit.
Workaround: You can close the window by pressing X on the right-hand side of the browser.
- CSCs138717—After a guest user template is created and applied, some of the attributes are represented incorrectly when the template is revisited. For example, the status of the user account may show as expired rather than active.
Workaround: Delete the existing template and create and apply a new one.
- CSCs140179—The CSV file contains a typo. It should read *csv-telnetpassword.jpeg* instead of *csv-tenetpassword.jpeg*.
Workaround: None at this time.
- CSCs142250—When running concurrent user sessions on WCS, some access pages take a very long time to display.
Workaround: None at this time.
- CSCs142358—In a quick search, the substring matching function returns more data than the matched strings.
Workaround: None at this time
- CSCs148403—When you import an access point configuration, you get an unwanted WCS prefix before the access point names in the status message.
Workaround: None at this time.
- CSCs148483—The access point name gets updated in the access point link but not in the Config > Access Point page where all the access points are listed.
Workaround: None at this time.
- CSCs151188—WCS does not update the friendly internal state for a rogue access point when the same MAC is present on two WLCs.
Workaround: None at this time.
- CSCs153478—The access point goes into pending state while searching for access points using Monitor > AP and does not retrieve the results.
Workaround: Search for access points from a different page, such as the Monitor page.
- CSCs153595—When the controller information on the access point is imported through the Import AP Config feature, the access point gets updated but the error message returns that it was not updated.
Workaround: None at this time.
- CSCs153612—The first and last information which appears for rogue access points on maps does not appear.
Workaround: None at this time.

- CSCsI53950—The icon for single radios appears incorrectly on the floor map. For example, if you choose 802.11a/n, the 802.11b/g radio shows as green when it should be gray. When the map is initially launched, the status shows correct, but when you change the protocol, the status is wrong until the map is launched again.
Workaround: None at this time.
- CSCsI54522—The port number that displays in the pop-up when you mouse over a client icon map might differ from the port number that displays in the client general properties panel when you click on the client icon on the map. These port values should be the same.
Workaround: Use the port value that displays on the client general properties panel.
- CSCsI57064—When an administrator tries to create a wired guest user within WCS, an error message appears.
Workaround: The wired guest user interface can be created on the controller instead of WCS. The created wired guest user interface can then be pushed to WCS through the refresh config from a controller command.
- CSCsI57546—When WCS is displaying a rogue device, it sometimes shows the detecting access point's MAC address instead of its name depending on the detection method used. If WCS discovers the rogue through a poll, it uses the MAC address of the access point for a name. If WCS discovers the rogue by a trap from a WLC, it uses the name.
Workaround: None at this time.
- CSCsI63991—The status message does not display tertiary controller information after you do a Config > AP > Import.
Workaround: None at this time.
- CSCsI64243—The status of the tertiary controller does not show up in the log.
Workaround: None at this time.
- CSCsI73139—The channel utilization for mesh access point for backhaul interface does not match that of regular maps and Google Earth maps.
Workaround: None at this time.
- CSCsI73205—When a rogue is detected as friendly on one controller, the rogue state is not always updated from malicious to alert to friendly.
Workaround: If you execute the rogue access point background task multiple times, the rogue state on the controller is updated.
- CSCsI75176—In some cases the access point heatmap is displayed in the upper left-hand corner instead of where the access point is placed.
Workaround: None at this time.
- CSCsI76192—If you use the Apply button when in planning mode, a ServletException error appears.
Workaround: None at this time.
- CSCsI77797—The Location Accuracy Tool (Tools > Location Accuracy Tool) does not generate a spatial image when the map is not imported as a GIF file.
Workaround: Import maps as JPEG files.
- CSCsI79802—When importing a file, the primary and secondary controller entries cannot be blank.
Workaround: None at this time.

- CSCs180359—Although the task scheduler may show guest users as expired, the Guest User template shows them as scheduled.
Workaround: None at this time.
- CSCs182286—A WCS TFTP upload may fail when running software version 4.2.62.x. This occurs if the TFTP directory for WCS is on a drive other than the one in which WCS is installed.
Workaround: Configure WCS to have the TFTP server on the same partition of the hard disk as the WCS installation.
- CSCs182677—The Config > AP > Import Config page needs to have a column for the access point name (or MAC address if the access point name is not known). Without a host name, nothing is displayed in the import status messages.
Workaround: None at this time.
- CSCs189809—If you audit a WLC and then choose **Restore WCS Values**, you get the following error:

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


Workaround: None at this time.
- CSCs195415—In some cases, the Network Configuration Audit Report (Reports > Audit Report) might display blank lines in the results table.
Workaround: None at this time.
- CSCs198668—The New Rogue AP Count report (Reports > Security Reports) might graph a bar that covers the entire chart when the selected reporting period is *the last 6 hours* and only one record is collected and graphed for that time period. However, the number that displays on the Y axis of the chart represents the accurate number of New Rogue APs records.
Workaround: None at this time.
- CSCsm00991—It takes awhile for client troubleshooting to appear.
Workaround: None at this time.
- CSCsm03250—The location appliance logs contained within the downloaded WCS logs are outdated.
Workaround: Download the logs manually from the location appliance.
- CSCsm04809—The radio utilization report shows accurate information, but the rest of the reports are skewed. The 802.11 counters and Tx power reports show information for Tx but none for Rx.
Workaround: None at this time.
- CSCsm13536—The supported channel bandwidths are different depending on whether 20-MHz or 40-MHz range is used. The controller lists them differently for an 802.11n access point, but WCS lists them the same in both ranges.
Workaround: None at this time.
- CSCsm14363—When you create a config group and then perform an audit, the Attribute Differences page does not have a Close button.
Workaround: None at this time.
- CSCsm20294—When the primary and secondary controllers are not configured in the access point, an import fails. The following error message appears: “AP4 primaryMwar and secondaryMwar entries 10.20.10.5 Maz40 are not configured in WCS.”
Workaround: None at this time.

- CSCsm30661—If you choose all templates from a controller and then add them to the config group with Apply, the number of templates in the report does not add up to the total number of templates in the config group.
Workaround: Choose each applicable template individually to add to the config group.
- CSCsm33619—In WCS 4.2.62.0 under Monitor > Clients, the client search does not show the location server information for the client when doing a quick or new search. If you go to the maps where the client's access point is located, the client shows on the map as *located* by the location server.
Workaround: Go to the map where the client's access point is located.
- CSCsm35824—The restore operation fails after two consecutive restores.
Workaround: Restart the server. The restore operation is not successful for the second attempt. If you restore it again, it is successful.
- CSCsm48775—Some copy and paste errors occurred in the upgrade from 4.2 to 5.0 for the LradXxxStats table. Sometimes the wrong sequence is dropped, but the wrong sequence may also be used in migration, and the table is not getting populated.
Workaround: None at this time.
- CSCsm50334—If the template application or any other such templates for the guest users fails, the message shows up as limited. The error may occur because of a lack of DB space, but the error message needs to explain the cause.
Workaround: None at this time.
- CSCsm56708—Even if you set the Last Detected Within setting to a minimal amount (such as 15 minutes), all clients detected even many months prior appear in the Monitor > Security > Rogue Clients menu. Also, the rogue access point MAC addresses are all zeroes.
Workaround: None at this time.
- CSCsm60523—The PoE status for the 1250 access point shows as *not applicable* on the Monitor > Access Points window.
Workaround: None at this time.
- CSCsm60843—The copyright information shown when logging onto WCS should show 2008.
Workaround: None at this time.
- CSCsm61279—The client throughput on the Client tab of the WCS Home page should display the traffic values in Mbps rather than Kbps.
Workaround: None at this time.
- 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.

- CSCsm80303—When an administrator tries to troubleshoot a client with 802.1x security settings and has the wrong credentials, WCS shows the status as green instead of red. A message is returned that states 802.1x authentication failure, which is correct, but the status icon should be red.
Workaround: None.
- CSCsm89434—When a virtual domain is created or updated with a large number of controllers or access points, it may take several minutes.
Workaround: None.
- CSCsm96761—When you run a Client Report > Client Association, duplicate lines for every event such as associate or disassociate are reported.
Workaround: None.
- CSCsm98662—In Monitor > Clients, the client statistics values display zero in the table.
Workaround: None.
- CSCsm98667—Saving a client search sometimes creates two copies of the same search or creates one copy and displays the following error: "Search with this name already exists."
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.
- CSCso13473—In WCS 5.0.56.0, the error message contains the Airespace product name ACS instead of WCS when MAPs are missing for a client location.
Workaround: None.
- CSCso29564—The Administration > Settings > Report window displays an incorrect repository path.
Workaround: After WCS is restored, go to Administration > Settings > Reports and update the repository path.
- CSCso35098—A "Could not execute JDBC batch update" error message appears when you try to create a guest user.
Workaround: Not applicable.
- 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.

- CSCso58483—WCS alerts for access point impersonation report the wrong radio band (802.11a) for slot 0.

Workaround: None.

- 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.

- CSCso63362—The Monitor Client and the Client Details pages have different results for probing clients.

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.

- CSCso64801—The SSID field in the WLAN Override section may be dimmed or unchecked when the WLAN override feature has been invoked.

Workaround: Use the CLI to configure the WLAN override with the following command:

```
<cmdEnv>config ap wlan add {802.11a | 802.11b}<wlan_id><ap_name></CmdEnv>
```

- 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.
- CSCso68457—You cannot configure an external web auth server on 5.0 and 4.1 controllers with a WCS template.
Workaround: Manually configure the external web auth server on the controller.
- CSCso68860—The Add option in HREAP Groups does not include a 1250 hybrid REAP access point.
Workaround: Manually configure the 1250 hybrid REAP access point on the controller.
- CSCso70155—After an autonomous access point migrates and joins the controller, the access point is missing from the current partition. This occurs only when the partition was created with autonomous access points.
Workaround: Move the access point to the appropriate partition.
- 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.
- CSCso84517—A lobby ambassador cannot change the guest user lifetime from limited to unlimited.
Workaround: Change the guest user from limited to unlimited from the controller side and perform the Refresh Config from Controller option.
- CSCso94027—WCS does not display the caller or caller ID.

Workaround: None.

- CSCso98274—The TFTP log messages should be more descriptive.

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.

- CSCsq16412—The conversion process from autonomous to LWAPP fails if the login prompt on the access point is changed from its defaults.

Workaround: Use the default prompt. It asks for user access verification.

- 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.

- CSCsq21602—The Traffic Steam Metrics Report gives incomplete results. If the reporting period is greater than one day, far less information is generated than if the reporting period was only one day.

Workaround: Run the reports for 1 day or less to retrieve full information. If you are scheduling a report, choose the last day rather than giving a value for date and time as a reporting period.

- 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.

- CSCsq22292—When you use the map editor, the imported image is truncated on the bottom and right-hand side.

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.

- CSCsq25753—After an upgrade, the Network Audit Report may not show any data. The results depend on when the original report was expired. The blank Network Audit Report occurs if the expired report was modified to run as a scheduled report before the next Network Audit polling cycle.

Workaround: Choose **Administration > Background Tasks > Network Audit**. Create a new Network Audit report with scheduling instead of using the expired one.

- CSCsq26062—The wrong IP address is shown for anchor controllers.

Workaround: If you click on the client, the correct IP address is shown for the anchor controller.

- 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.

- CSCsq27887—WCS fails to start after an automatic upgrade from 4.2.81.0.

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.
- CSCsq29265—If you try to add an ID certificate through WCS, a blank page appears.
Workaround: Manually configure the ID certificate on the controller.
- CSCsq29917—WCS reports an unknown exception error when multiple config groups have been created or selected.
Workaround: None.
- CSCsq30438—The client count on the maps is not showing correctly when the map is initially launched.
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.
- CSCsq35823—When you perform radio measurement for various parameters in the CCXv5 client, some SNMP operations fail.
Workaround: You can reference the WLC because it shows the radio measurements 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.

- CSCsq37850—When you log in and try to authenticate and authorize a TACACS user, a “login failed” message appears.
Workaround: Disable the secondary ACS server.
- 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.
- CSCsq45095—You cannot modify a local management template after you have created one.
Workaround: None.
- 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.
- CSCsq48048—The webauth security check box gets unchecked if IPv6 is enabled for the same WLAN.
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.
- CSCsq50504—The WPA1+WPA2(802.1x+CCKM) security WLAN cannot be forwarded to WLC 4.1.185.0. An “invalid security combination” error occurs.
Workaround: Configure the same security on the WLC and perform the Refresh Config from Controller option.
- CSCsq50523—The session timeout is not updated on WLC 4.2.112.0 for WPA1+WPA2(CCKM+802.1) security WLANs.
Workaround: Configure the session timeout for the same security on the WLC and perform the Refresh Config from Controller option.
- 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.
- CSCsq52192—An audit of WLC shows WCS and WLC as identical, but after the access point authorization template is forwarded from WCS to WLC, the access points (or location appliances) with self signed certificates can no longer join the WLC.
Workaround: Enter the command **debug pm pki enable** to see if mismatched SSC key hash exists.
- CSCsq52236—An unknown exception occurs when you navigate to Monitor > Maps.
- CSCsq54142—The importing of an autocad floor map fails because of CSCsk02071, and no information is present in the logs.
Workaround: None.
- CSCsq54706—The values you enter for session timeout on the WLAN configuration are not validated by WCS.
Workaround: Provide valid values for the session timeout.
- CSCsq55384—If you do an advanced client search, the search results show the location server column as *unknown*.
Workaround: Edit the search view window and remove the location server column.
- CSCsq55580—The session timeout range should be validated and the appropriate pop-up message displayed for each security type.
Workaround: None.
- CSCsq55793—When you change the local management user password, it is not reflected in the audit.
Workaround: Delete the existing user and create a new user with the required password.

- 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.
- CSCsq60716—A WCS system error page appears when WISM controllers are added individually and then chosen to be added to WCS.
Workaround: Click **Cancel** when you are adding existing WLCs on a WISM.
- 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.
- CSCsq63724—Some display widgets may not display the entire length of the contained selection.
Workaround: None.

- CSCsq63954—You cannot add a controller running 4.2.130.0 to WCS running 5.0.x.x. An object not found error results.
Workaround: On the controller, enter the **transfer download mode tftp** command.
- 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.
- CSCsq65153—When you specify management user authentication order, WCS 5.0.56.0 does not allow TACACS or RADIUS servers as a priority over local.
Workaround: None.
- CSCsq66346—The channel utilization is the same for both radios when you hover over any access point on the map.
Workaround: None.
- CSCsq67143—On a 1510 access point, Google Earth shows an unrelated alarm color.
Workaround: None.
- CSCsq67460—When you look at a building view in WCS, you see an overview of all floor maps (in the form of minimaps). The access point status is misrepresented in its red, yellow, or green circles.
Workaround: Click the floor map to show the correct status.
- 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.
- CSCsq71792—The process of synchronizing mobility service engines and location servers encounters problems.
Workaround: None.
- CSCsq74792—If you upgrade from 5.0 to 5.1, the following error appears:

```
system error:wrong alarm type rogue alarm unclassified
```


Workaround: Navigate to another page.
- CSCsr00359—A super user cannot access the Import Civic Information window.
Workaround: Access the page as a root user rather than a super user.
- CSCsr06419—You cannot delete multiple rules from the ACL page. If you create an ACL from the Security page, click the Add button to add one or more rules, and then try to delete more than one rule, the records are not deleted.
Workaround: Choose the record that shows in the ACL page and delete the rule.
- CSCsr10714—If you create an authentication priority from management, choose the second option, select RADIUS/TACACS server, and click Save, an SNMP error occurs.

Workaround: Choose the first option, select the RADIUS server, and then choose the second option. You should then see the TACACS server if the priorities are set accordingly for RADIUS and TACACS.

- CSCsr15110—After you upgrade from 5.0, users other than root cannot launch Reports > Compliance Assistance Reports.

Workaround: Log in as root and enable the task list under Administration > AAA > Groups < *respective group* > Reports > Compliance Assistance Reports.

- CSCsr22132—The scheduled guest user is not activated when you upgrade from 4.1 to 5.0.56.

Workaround: Reapply the guest user account in the upgraded WCS.

- 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.

- CSCsr27851—In the controller template, if you create a WLAN profile with a diagnostics channel and forward it to the controller, an SNMP error occurs.

Workaround: Add the record to the controller even though the SNMP error message appears.

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 Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, 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, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, 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. (0807R)

© 2008 Cisco Systems, Inc. All rights reserved.