



Release Notes for Cisco Wireless Control System 5.1.64.0 for Windows or Linux

July 2008

These release notes describe open caveats for the Cisco Wireless Control System 5.1.64.0 for Windows or Linux, which comprises part of the Cisco Unified Wireless Network Solution (Cisco UWN).

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

Contents

These release notes contain the following sections.

- [Cisco Unified Wireless Network Solution Components, page 2](#)
- [Requirements for Cisco WCS, page 2](#)
- [Important Notes, page 5](#)
- [New and Changed Information, page 9](#)
- [Caveats, page 12](#)
- [Troubleshooting, page 30](#)
- [Related Documentation, page 30](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 30](#)



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 5.0 or 5.1 32-bit operating system installations.
Red Hat Linux Enterprise Server 5.0 or 5.1 64-bit operating system installations are not supported.
- Windows 2003 and Redhat Linux version support on VmWare ESX 3.0.1 version and above.
VmWare must be installed on a system with these minimum requirements:
Quad CPU running at 3.16 GHz with 8 GB RAM and a 200-GB hard drive.
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 5.1.64.0 supports management of the following wireless LAN controllers:

- 4.2.61.0
- 4.2.99.0

- 4.2.112.0
- 4.2.130.0
- 4.2.176.0
- 5.0.148.0
- 5.1.151.0

Location Server, Mesh, and MSE

Cisco WCS 5.1.64.0 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 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 5.1.30.0

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

- WLC running Mesh release 4.1.191.24M and above

WCS on WLSE Appliance

Cisco WCS on a WLSE appliance supports up to 1,500 Cisco Aironet lightweight access points, 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 bug CSCsq27887). You must initiate the manual upgrade process to do the upgrade. See the “Upgrading to WCS” section in the *Wireless Control System Configuration Guide*.

- 4.2.97.0
- 5.0.55.0
- 5.0.56.0
- 5.0.56.2

Important Notes

This section describes important information about Cisco WCS.

Configure > Location Sensor

The location sensor option on the WCS GUI is not supported in WCS 5.1.64.0.

Internet Explorer Error

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

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

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

Follow these steps to re-register the DLLs:

-
- Step 1** Open a command-line window in Windows XP (Start > All Programs > Accessories > Command Prompt).
- Step 2** Run these commands one at a time in the following order. After each command has successfully run, you should receive a pop-up message that theDllRegisterServer in_*something*.dll succeeded.
1. regsvr32 msscript.ocx
 2. regsvr32 dispex.dll

3. regsvr32 vbscript.dll
4. regsvr32 scrrun.dll
5. regsvr32 urlmon.dll
6. regsvr32 actxprxy.dll
7. regsvr32 shdocvw.dll

Step 3 Restart the computer.

Cisco WCS Supported on Windows 2003 English and Japanese Operating Systems Only

Cisco WCS is supported only on English or Japanese versions of the Windows 2003 operating system. Display problems sometimes occur when you install and run Cisco WCS on operating systems translated to other languages or with location settings other than English or Japanese.

Regulatory Updates

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

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

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

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

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

Notes about Google Earth

When you launch Google Earth, this message appears:

Google Earth could not write to the current cache or myplaces file location. The values will be set as follows:

My Places Path: "C:\Document and Settings\userid\Application Data\Google\GoogleEarth"

Cache Path: "C:\Documents and Settings\userid\Local Settings\Application Data\Google\GoogleEarth"

This is expected behavior.

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

Refresh Controller Values

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

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

When Audit Mode is Basic

When the audit mode is basic, the following applies:

If you choose *refresh config from controller*, a Refresh Config window opens with two options for "Configuration if present on WCS but not on device, do you wish to:"

- **Retain**—The WCS refreshes the configuration from the controller but does not delete any devices or configurations that no longer exist in the controller configuration. For example, if the WCS database shows an AP1 but that access point is no longer present in the controller configuration, WCS does not delete AP1 from its database.
- **Delete**—WCS deletes the configuration of the controller from its database and retrieves a new configuration from the controller. Delete is the recommended option so that WCS matches the most recent configuration you are refreshing from WLCs.



Note

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

When Audit Mode is Template Based

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

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

- **Retain**—The WCS refreshes the configuration from the controller but does not delete any devices or configurations that no longer exist in the controller configuration. For example, if the WCS database shows an AP1 but that access point is no longer present in the controller configuration, WCS does not delete AP1 from its database.
- **Delete**—WCS deletes the configuration of the controller from its database and retrieves a new configuration from the controller. Delete is the recommended option so that WCS matches the most recent configuration you are refreshing from WLCs.

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

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

Windows XP Cannot Load CAD Files

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

Take one of the following actions:

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

User Assistant Cannot Configure Controller

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

Deletion of TFTP Server Is Not Updated in the Configuration Backup

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

Conflicting Ports Interrupt WCS Start

WCS fails to start if there is a conflicting port in use. You receive a “Failed to start WCS server” message, but you do not receive a list of conflicting ports. Go to `WCS/webnms/logs/wcs-0-0.log` and view the conflicting ports. Enter the following to get a list of the process IDs associated with each connection:

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

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

In the Task Manager, you see the respective PID and can stop the process using the port that WCS requires.

New and Changed Information

New Features

The following new features are available in WCS 5.1.64.0



Note

Refer to the *Cisco Wireless Control System Configuration Guide*, Release 5.1 for details and configuration instructions for each of these features.

- New Dipole Antenna Support in Cisco WCS—This feature provides support for heat map views of the antenna coverage pattern in Cisco WCS. Supported antennas include:
 - 5 GHz, 3.5 dBi: AIR-ANT5135DW-R, AIR-ANT5135DG-R
 - 2.4 GHz, 2.2 dBi: AIR-ANT2422DW-R, AIR-ANT2422DB-R, AIR-ANT2422DG-R
- Cisco Aironet 1250 Series Support for One or Two Antennas per Radio—With this release, the Cisco Aironet 1250 Series radio module can be configured to operate with only one or two antennas.
- Payment Card Industry (PCI) Assessment and Reporting—WCS PCI Reporting analyzes Cisco Unified Wireless Network (CUWN) security event data, such as rogue and attack events from Wireless IDs, as well as network-wide configurations and audit trails for PCI compliance. Potentially non-compliant events and network configurations are summarized in a WCS PCI report.
- Detailed Client Report—Client information can be viewed from a tabular client report with a customized display. This report tracks up to one year of client history. The clients in the report can be sorted based on variety of criteria, including floor area, controllers, access points, Service Set Identifiers (SSIDs), or client MAC addresses or names.
- RRM Support for 802.11n 40-MHz Channels—With this release, 40-MHz channels can be automatically configured on the Cisco Aironet 1250 Series Access Point using Cisco WCS or the WLAN controller. This feature applies only to 5-GHz radios and is not supported on the 2.4-GHz radios.
- RRM Dashboard in Cisco WCS—The WCS provides troubleshooting and network diagnostics in an easy-to-read, graphical interface. The RRM dashboard includes:
 - Access points with most channel changes
 - Access points running at maximum power
 - Access points with coverage hole events

- Top channel change reasons
- Access Point Failover Priority—Network managers can configure priorities for lightweight access points in the event of a controller failover. In the event a primary controller goes offline and a backup controller is saturated, the higher priority access points are allowed to join the backup controller.
- Cisco WCS Virtual Domains—Cisco WCS virtual domains/partitioning allows individual IT administrators to manage the segment of the wireless network under their responsibility. Cisco WCS virtual domains can be grouped by hierarchical domains. Users can be restricted to discrete infrastructure components or service entities:
 - Infrastructure components include: controllers, lightweight access points, standalone (autonomous) access points, configuration templates, rogue access points, rogue ad hoc access points, summary page, events, alarms, tags, clients, event groups, chokepoints, and spectrum experts.
 - Service entities include guest access and location servers.

Common network management features, including searches, reports, role-based access control (RBAC), and RADIUS/TACACS+ have been enhanced to support virtual domains.

- Configuration Auditing—You can audit the configuration of each wireless LAN controller to confirm that its running configuration is identical to the configuration listed in the Cisco WCS database.

Configuration auditing can be performed at three different levels:

- Controller
- Entire network
- Set of templates against current device configuration by Config Group > Audit

In 5.1, the following audit modes are supported:

- Basic audit (the legacy audit: This audit is performed on device configuration in WCS database against current WLC configuration.)
- Template based audit (a new enhancement: This audit is performed against current WLC configuration on applied templates, config group templates which have been selected for background audit, and device configuration objects in the WCS database whose configuration has no corresponding template.)



Note When you apply the audit against the WLC configuration, the network or controller audit enforces WCS values for the discrepancies found if you chose enforcement in the config group template.

The setup for using basic audit and template based auditing requires two independent management tasks.

- Template Usability Enhancements—Organizations can reuse and apply templates to one or all wireless LAN controllers. When attempting to delete any template, you are prompted to indicate whether the template configuration should be removed from controllers as well as Cisco WCS. New templates are identified by their template name. Existing templates are listed on the template drop-down menu.
- Template Scheduling and Status—Access point templates or schedulable configuration groups can be set for a future day or time. The following information about scheduled tasks for Cisco WCS templates is provided:
 - Summary page of scheduled tasks

- History of the success or failure status of scheduled tasks for up to 31 days
- Ease of Use Enhancements—The following Cisco WCS ease-of-use enhancements are included in this release:
 - Customization of column order and display is added to the Client Association Report
 - Flex-based interactive charts are now available for viewing client statistics, including bytes sent and received, signal-to-noise ration (SNR), and received signal strength indication (RSSI).
- Automated Wireless Security Vulnerability assessment—The Cisco WCS audits the security posture of wireless network configurations, including wireless LAN controllers, access points, and management interfaces against wireless security best practices defined by Cisco. WCS provides an at-a-glance security score, a prioritized summary of vulnerabilities, and suggested remedies.
- Enhanced WCS Security Dashboard—WCS delivers a comprehensive security summary status of the entire wireless network with an easy to reference chart. It also provides a real-time summary of network security alarms, attempted attacks, and potential security vulnerabilities. WCS streamlines information by dynamically displaying only current alarms and allowing access to additional details on any event. WCS displays wired network security events, such as wireless client abuse of a wired network, and provides Layer 3 through 7 malware detection reporting from wired network security devices.
- Cisco WCS Integration with Cisco Secure Access Control Server (ACS) View Server 4.0—The Cisco WCS client troubleshooting tool now integrates with Cisco Secure ACS View Server to provide aggregated client status information from multiple Cisco ACS Servers.
 Organizations can poll Cisco Secure ACS View Server through the Cisco Secure ACS tab located on the Cisco WCS client troubleshooting tool user interface. With this tool, you can determine the cause and reason of client authentication failures.
- Rogue Switch-port Tracing and Disable—The WCS verifies the switch port to which a rogue access point on the network is connected and upon identification, disables the port.
- Access Point Wired Port Authentication with 802.1X—WCS authenticates access points plugged into a wired network port using 802.1X to validate credentials. It also provides secure access point provisioning and consistent policy enforcement throughout the network.
- Network Access Control (NAC) Out-of-band Support—The Cisco Unified Wireless Network enables use of the NAC Appliance in out-of-band mode with guest and general WLAN traffic. It also allows for posture assessment and remediation upon authentication and polling of traffic to help ensure that clients connected to the network comply with current security configuration requirements.
- Green Initiative—Improved power management of Cisco Aironet access points to support the Cisco Green initiative. Cisco access points can be turned on or off periodically at scheduled intervals to save power

Changed Information

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

Caveats

This section lists open and resolved caveats in Cisco WCS 5.1.64.0 for Windows and Linux.

Open Caveats

These caveats are open in Cisco WCS 5.1.64.0:

- CSCsg74466—On the Monitor > Devices > Access Points page, when **Noise / Interference / Coverage (RSSI / SNR)** is selected and a report is generated, the report displays a chart that has the legend overlaying the chart display area.

Workaround: None. The chart can also be viewed on the WLC user interface.

- 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.

- CSCsk15266—The IP address shown in the CDP Neighbor tab in Monitor > AP is incorrect. For example, if the IP address is A.B.C.D, it is shown as D.C.B.A.

Workaround: None.

- CSCsk17031—When you try to view the location history of a tag or a client, the history page loads slowly.
Workaround: Under Location Server > Administration > History Parameters, make sure the history interval for client, tags, rogue clients, and access points is not too excessive. Make sure data pruning happens more frequently.
- CSCsk31174—After an access point is migrated from autonomous to unified, the location information of 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.
- CSCsk77484—If the controller to which the access point is associated has more than 15 SSC access points, migration takes longer than expected.
Workaround: Set the session timeout value on the controller to 1.
- 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.
- CSCsl47529—When WCS is upgraded from 4.1.83.0, the lobby ambassador cannot view passwords of guest users created in WCS 4.1.83.0.
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.
- CSCsl82286—WCS TFTP uploads may fail when running 4.2.62.x.
Workaround: Configure WCS to have the TFTP server on the same partition of the hard disk as the WCS installation.
- 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.
- CSCsm13536—The channel bandwidth is listed differently for the 20-MHz and 40-MHz range of an 802.11n access point.
Workaround: None.
- 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.
- 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.
- 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.
- CSCsq58382—When an access point group name contains the maximum limit of 32 characters, the access point group name template is not forwarded to the access point.
Workaround: Assign an access point group name with less than 18 characters.
- 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-peer 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.

- 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.

- 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.

Resolved Caveats

These caveats are resolved in Cisco WCS 5.1.64.0:

- CSCse91247—Events will now create the related alert objects.
- CSCsi87610—The installation program now ensures that minimum WCS server requirements are met before installation so that WCS runs at expected speed.

- CSCsj18398—When you set up a WLAN from WCS, a WPA or WPA2 choice is now forwarded to the 4.1 controller.
- CSCsj32075—The solid database no longer has a memory leak. The “out of central memory” fatal error has been corrected.
- CSCsj56796—The “configuration is different on the device” error message that appeared randomly now appears only if differences between the access point and WCS truly exist.
- CSCsj79103—Installation onto a 64-bit operating system is now prevented. Because WCS is tested only on a 32-bit operating system, it should not have allowed installation onto a 64-bit operating system.
- CSCsj96574—When you add guest user accounts using a CSV file, you no longer receive an unknown exception error from the import operation.
- CSCsk28942—When Cisco omnidirectional antenna products are chosen, the setting for omni products is now disabled because the specifications of the antenna are known. The following Cisco products now 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.
- CSCsk39485—If you make modifications to an existing hybrid REAP AP group template and save them, the changes are now reflected.
- CSCsk72169—The audit controller options have been changed to *Restore WCS values to controller* and *Refresh config from controller*. The Restore WCS Values and Refresh Controller Values were too ambiguous and confusing to the user.
- 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 is successful.
- CSCsk88821—When you create maps, the floor information for a building is now retained.
- CSCsl08696—If you establish an RF calibration model under WCS > Monitor > Maps > RF Calibration Model, you can now change the name.
- CSCsl35056—Access to cgi-bin URLs has been removed.
- CSCsl38408—When you press **Exit** or **Save**, the map editor now exits.
- CSCsl39335—WCS starts even when a conflicting port is in use.
- CSCsl41999—You can now apply SNMP templates as RW or RO.

- CSCsl43880—A lobby ambassador with username and password credentials can now log into WCS without a privilege error.
- CSCsl48403—When you import an access point configuration, you no longer get an unwanted WCS prefix before the access point names in the status message.
- CSCsl53478—The access point no longer goes into pending state while searching for access points using Monitor > AP, and results are retrieved.
- CSCsl53612—The first and last information for rogue access points now appears on the map.
- CSCsl53877—The access point can now be searched by floor area on an access point template page. With this, an administrator can now apply an access point template to a particular access point.
- CSCsl57064—An error message no longer appears when an administrator creates a wired guest user within WCS.
- CSCsl57546—When WCS is displaying a rogue device, the detecting access point's name now appears regardless of the detection method used (whether the rogue is discovered through a poll or by a trap from a WLC).
- CSCsl64243—The status of the tertiary controller now appears in the log.
- CSCsl66326—The default sort order for alarms was oldest to newest. It has now been reversed to newest to oldest.
- CSCsl76192—The servletException error no longer appears when you use the Apply button in planning mode.
- CSCsl77797—The Location Accuracy Tool (Tools > Location Accuracy Tool) now generates a spatial image when the map is not imported as a GIF file.
- CSCsl79599—In WCS 4.2.62, you can now add access lists or WLANs without getting unwarranted messages.
- CSCsl79802—When importing a file, the primary and secondary controller entries can now be blank.
- CSCsl80359—The task scheduler and guest user template both show guest users in the same form (expired or scheduled).
- CSCsl85479—Client troubleshooting on the Client Summary page works for clients associated to controllers running 4.1.185.
- CSCsl85843—The Cisco Compatible Extensions version 5 client statistics task completes without blocking the other scheduled tasks that are running.
- CSCsl86349—You can apply selected attributes of an access point template to devices as expected.
- CSCsl89670—You can now choose Synchronize with Deployment in planning mode without an error resulting.
- CSCsl89809—If you audit a WLC and then choose Restore WCS Values, you no longer 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.`
- CSCsl92801—When info object is null, use location object to populate Tag form.
- CSCsl95415—The Network Configuration Audit Report (Reports > Audit Report) does not display blank lines in the results table.
- CSCsl98668—The New Rogue AP Count report (Reports > Security Reports) displays the appropriate graphs.

- CSCsm03250—The location appliance logs contained within the downloaded WCS logs are now current.
- CSCsm04809—The 802.11 counters and Tx power reports now show information for both Tx and Rx.
- CSCsm14363—When you create a Config Group and then perform an audit, the Attribute Differences page now has a Close button.
- CSCsl88958—The issues with the radio templates have been addressed. The classes was changed from mesh to subband naming conventions. The template now configures power and channel values independently and includes a parameter to configure Admin Mode and WLAN profile settings.
- CSCsm30661—The Config Group Apply Report shows the correct total number of templates.
- CSCsm33619—In WCS 4.2.62.0 under Monitor > Clients, the client search now shows the location server information for the client when doing a quick or new search.
- CSCsm50334—If the template application or any other such templates for the guest users fails, the the error message explains the cause.
- CSCsm60523—The PoE status for the 1250 access point displays on the Monitor > Access Points window.
- CSCsm60843—The copyright information shown when you log onto WCS is now 2008.
- CSCsm66516—You can delete a RADIUS server from the controller using WCS without getting an error.
- CSCsm79472—Prior to an auto-upgrade, WCS now performs a backup.
- CSCsm91474—The Client Count graph displays the correct clients for the weekly display.
- CSCsm93369—When you assign a location server to the network design and choose Synchronize, WCS now shows the design as assigned.
- CSCsm95941—WCS correctly reports the access point client count from the number of clients displayed on the access point in a map.
- CSCsm96146—The Coverage Threshold alerts in WCS now show the appropriate values for Total Clients, Failing Client, and Coverage Threshold.
- CSCsm99538—The error message generated when you apply an access point template to an access point no longer occurs.
- CSCso05664—Location appliance is now reachable from WCS.
- CSCso07819—When you make a configuration change on an access point, the erratic “changes to static IP configurations may momentarily disrupt clients connected to this AP” message no longer appears.
- CSCso19108—The Coverage Threshold Template now operates as expected.
- CSCso27008—A quick search within WCS now produces valid results.
- CSCso29306—AutoCAD images imported for a floor map are now forwarded to the location server during synchronization.
- CSCso32170—You can now delete a RADIUS server template from WCS or WLC without a failure.
- CSCso35894—You can now log into WCS with TACACS+ management enabled (using wildcard NAS definition) without failure.
- CSCso38149—WCS now applies a DHCP required template to WLC when the DHCP server is not defined.
- CSCso39180—With the standalone spectrum expert demo you can now enable spectrum expert.

- CSCso39483—WCS can now authenticate users against TACACS+ or RADIUS servers.
- CSCso39789—Clarification changes were made to the X and Y axis labels on the access point 802.11 counters report.
- CSCso43362—Corrected the access point status to correspond with the WLC status. Prior to this fix, some down alarms were appearing within WCS that were not appearing as down in WLC.
- CSCso44817—A guest user can now be created with an unlimited lifetime.
- CSCso58983—When you navigate to Configure > Config Groups, you can now distinguish between 802.11a/n and 802.11b/g/n voice parameter templates.
- CSCso60394—The apply report action within a Config Group sometimes showed an indefinite progress bar after provisioning the controller. The status never reached 100% so that the Apply tab turned active. This template has been corrected.
- CSCso63312—A search for authenticated clients now yields results.
- CSCso64503—After you configure PSK along with WPA for a WLAN template, save the template, and forward it to a WLC, the adjustments are now reflected when you change the key management from PSK to CCKM or 802.1x and save the template again.
- CSCso64971—The “migration process failure” error that occurred when 3201 WMIC is applied has been corrected.
- CSCso66270—The mapping of the reason code is now correct.
- CSCso67334—The Syslog Configuration message now reads “Syslog Template is applicable only until controller version 4.2” rather than a specific 4.2 version.
- CSCso73789—The imported asset information from WCS (Location > Location Servers > *server name* > Administration > Import Asset Information) reports all the clients in the map without any problems. You no longer see the clients in the map as “not set” after time passes.
- CSCso77051—An unclassified access point was added in the alarm summary. It shows the number of unclassified rogue access points.
- CSCso76667—Guest user creation now works as expected.
- CSCso97850—The Location Accuracy tool now runs as expected with appropriate results.
- CSCso97982—A rogue access point is now reported when it is detected on a wired network.
- CSCso99445—The refresh configuration from controller operation no longer fails.
- CSCsq04319—The random “error in getting data from server” message that appeared when you opened various WCS pages with a non-Internet Explorer browser has been eliminated.
- CSCsq05606—The campus map at 100% zoom now shows the complete layout.
- CSCsq09463—When you create the lobby user, the disclaimer now retains the description after a save.
- CSCsq10744—After a scheduled Client Association or Detailed report is run, the correct time is shown.
- CSCsq10758—When WCS shuts down, it now removes the files previously left in the webnms/Temp directory.
- CSCsq34307—The WCS alerts now correctly portray the radio type.
- CSCsq41209—You can now add a controller with SNMPv3 and the right credentials.
- CSCsq41209—When you do a quick search, the results returned are now specific to the MAC address entered rather than a full set of results and events that are unassociated with MAC address.

- CSCsq48999—An access point username password template no longer gets created with a blank name.
- CSCsq50205—When you perform a quick search using a MAC address, the search now returns results for the specified MAC address rather than the full set of events.
- CSCsq53174—The count of rogue access points and rogue adhoc now displays correctly on the WCS home page.
- CSCsq72345—The solid database is no longer corrupted when you run 4.5.0134 for Linux or perform other database upgrades.
- CSCsq72787—If you enter a guest user with a lifetime greater than 30 days, the scheduled task now executes as expected.

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)

