Release Notes for Cisco Wireless Control System 4.2.110.0 for Windows or Linux

September 2008

These release notes describe open caveats for the Cisco Wireless Control System 4.2.110.0 for Windows or Linux, which comprises part of the Cisco Unified Wireless Network Solution (Cisco UWN). The Cisco Wireless Control System is hereafter referred to as *Cisco WCS*.

Contents

These release notes contain the following sections.

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

Cisco Unified Wireless Network Solution Components

The following components are part of the Cisco UWN Solution and are compatible in this release:

- Operating system (Wireless LAN Controller and Cisco Aironet Lightweight Access Point)
- Cisco Wireless Control System (Cisco WCS)
- Cisco WCS Navigator release
- Cisco 2700 Series Location Appliance
- Cisco 2000, 2100, 4100, and 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.

Note Cisco WCS can simultaneously manage multiple Cisco wireless LAN controllers running different software releases. For example, Cisco WCS running 4.2 can simultaneously manage controllers running 4.2.112.0 to support Cisco Aironet Lightweight access points and controllers running 4.1.191.24M to support Cisco Aironet mesh access points. A single Cisco WCS can manage these controllers up to a maximum number of controllers and access points supported by Cisco WCS.

Operating System Requirements

The following operating systems are supported:

- Windows 2003/SP2 or later 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 4.0 or 5.0 32-bit operating system installations.

  Red Hat Linux Enterprise Server 4.0 5.0 64-bit operating system installations and Red Hat Linux Enterprise Server 5.1 and later versions are not supported.

  Note Cisco WCS can be installed on Red Hat Linux Enterprise Server 4.0, but version 4.0 will not be supported in future releases. Plan on migrating to Red Hat Linux Enterprise Server 5.0.
- 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 GBs 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.

Supported Browsers

The Cisco WCS user interface requires Internet Explorer 6.0/SP1 or 7.0 with the Flash plugin. The Cisco WCS user interface has been tested and verified using a Windows workstation.

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

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. A 3-GHz Intel Pentium processor with 3 GB of RAM and 38 GB of free hard drive space is required.

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

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

Cisco WCS User Interface

The Cisco WCS user interface requires Internet Explorer 6.0/SP1 or later with the Flash plug-in. The Cisco WCS user interface has been tested and verified using Internet Explorer 6.0 on a Windows workstation.

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

Client Requirements

In order for clients to access WCS, they must have a minimum of 1 GB RAM and a 2-GHz processor. The client device should not be running any CPU or memory-intensive applications.

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:

- 4.0.66.0
- 4.0.81.0
- 4.0.87.0
- 4.0.96.0
- 4.0.97.0
- 4.0.100.0
- 4.1.83.0
- 4.1.91.0

- 4.2.62.0
- 4.2.62.11
- 4.2.81.0
- 4.2.97.0

Note You cannot auto upgrade from Cisco WCS release 4.2.81.0 to 4.2.110.0 using Red Hat Linux Enterprise Server 5.0 (refer to bug CSCsq27887). You must initiate the manual upgrade process to do the upgrade. See the "Upgrading WCS" section in the *Wireless Control System Configuration Guide*.

Important Notes

This section describes important information about Cisco WCS.

Wireless LAN Controller Requirements

Cisco WCS 4.2.110.0 supports management of the following wireless LAN controllers:

- 4.0.155.5
- 4.0.179.11
- 4.0.217.0
- 4.0.219.0
- 4.1.171.0
- 4.1.185.0
- 4.2.61.0
- 4.2.99.0
- 4.2.112.0
- 4.2.130.0
- 4.2.176.0

Location Server and Mesh

Cisco WCS 4.2.110.0 supports management for the following location server and Mesh software:

- Location server 3.1.42.0

  Location appliances operating with release 3.1.42.0 are compatible with Cisco WCS release 4.2.

  Location appliance software is backwards compatible with the previous two location appliance releases. Therefore, you can only upgrade two releases forward. For example, you can directly upgrade from release 3.0 or 3.1 to 4.0 but you cannot directly upgrade to release 4.0 from releases 1.1, 1.2, 2.0, or 2.1.
- •WLC running Mesh release 4.1.191.24M

Flash Player 9.0.115.0

Flash Player 9.0.115.0 is required for the full WCS benefit.

Refresh Controller Values

If the audit reveals configuration differences, you can either restore WCS values on the controller or refresh controller values to synchronize WCS with the controller. Choose **Restore WCS Values** or **Refresh Controller Values**.

If you choose to refresh the controller values, a Refresh Config window appears displaying the following message: "Configuration is present on WCS but not on device, do you wish to:" Choose one of the following options:

- **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 On the Refresh Config window, only the configuration objects for this controller in the WCS database are updated. Upon refresh, the WCS templates are not updated.

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 the Windows Vista operating system.

Take one of the following actions:

- Uninstall Internet Explorer 7 and install Internet Explorer 6.
- Leave Internet Explorer 7 and install the missing DLLs.

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 locale settings other than English or Japanese.

Report Name Change

If you are upgrading to 4.2, the Rogue Detected by AP report is renamed to Rogue AP Events. All other reports (Audit, Client, Inventory, Mesh, and Performance) are upgraded with the same name.

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.

Changed Information

There is no restriction on the number of hybrid-REAP access points deployed 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 Caveats and Resolved Caveats in Cisco WCS 4.2.110.0 for Windows and Linux.

Open Caveats

These caveats are open in Cisco WCS 4.2.110.0:

- CSCsb39735—Web authentication certificate details cannot be seen on Cisco WCS.

  Workaround: None.
- CSCsg74466—If you choose Noise > Interference > Coverage (RSSI/SNR) to generate a report on the Monitor > Devices > Access Point page, the report displays a chart with the legend overlaying the display area.

  Workaround: You can view the graph on the WLC.
- CSCsh43499—When multiple users are trying to troubleshoot one client, Cisco WCS lets them put the same client on the watchlist at the same time, which Cisco WCS should not allow because the client starts to collect logs from more than one browser. Cisco WCS does not display an appropriate error message.

  Workaround: None.
- 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 Select a command drop-down menu and click GO.
- CSCsh47150—Moving a building between campuses or moving a building outside of a campus requires a clean resynchronization with the Location Appliance.

  Workaround: After moving a building, go to the Location synchronization page, unassign the Network Designs, submit the synchronization, reassign Network Designs, and resynchronize.
- CSCsh81856—During installation, 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 you click Enter, the screen proceeds to the next session.

- CSCsh82165—Upon install or uninstall, the following error message sometimes appears: "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.

- CSCsi15088—The local net user mapping to a profile ID is not updated if the profile ID changes on the controller.

  Workaround: Change the profile ID of the local net user using the controller GUI or CLI and refresh the configuration in Cisco WCS to keep the controller and Cisco WCS in sync.

- CSCsi18312—The link test option in the Client AP Association History does not work.

  Workaround: Use the link test option on the Client Details page.

- CSCsi26963—The Client Association report does not include any records older than 7 days.

  Workaround: None.

- CSCsj36002—The logs generated while troubleshooting a client are not truncated into 2-MB files.

  Workaround: None.

- CSCsj61673—The event log generated for the client gets duplicated after a time interval.

  Workaround: Stop the capture of the event log by clicking Stop when 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) that 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.

- CSCsj79103—WCS release 4.0.81.0 allows installation on a 64-bit operating system. WCS is tested only on a 32-bit operating system, and installation on a 64-bit operating system should be prevented.

  Workaround: Uninstall WCS from the 64-bit operating system device and install it on a 32-bit device.

- CSCsj99244—When using Cisco WCS on a Japanese Windows operating system, the location server backup fails.

  Workaround: You can modify the AM and PM values of the backup filename to English before performing the backup.

- 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 that the object is added by logging onto the device and using an audit to check the configuration.

- CSCsk17031—The history page loads slowly 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—The Location > Synchronization page takes awhile to load if several hundred controllers are being loaded.

  Workaround: Wait for the page to load completely.

- CSCsk26658—An error occurs if you click on link test for a wired client.

  Workaround: No workaround. A link test is not supported for wired clients. It applies only to wireless clients.

- CSCsk28942—While omnidirectional antennas' radiation patterns may have some asymmetry, they generally radiate in all directions. This causes confusion for the user setting antenna orientation and positioning access points in Cisco WCS. Choose the Cisco omnidirectional antenna products and disable it 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.

- CSCsk30371—Options in the drop-down menu of the search network include controllers that have not been added.

  Workaround: None.

- CSCsk31174—Location information of an autonomous access point does not migrate to the lightweight access point when status polling and wireless polling are disabled.

  Workaround: Ensure that device status and wireless status polling is not disabled.

- 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.

- CSCsk47555—On the monitor list page, the access point is shown as local when it should be bridging mode.

  Workaround: Synchronize the controller configuration with Cisco WCS. The current known configuration that Cisco WCS has maintained in the database is displayed until it is synchronized.

- 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.

- CSCsk55422—If an invalid port is entered and then corrected during installation, the installer reports that an error occurred during installation.

  Workaround: None.

- CSCsk79095—The client detail page for WGB clients shows some tabs and commands that are not applied to the WGB client.

  Workaround: None.

- CSCsk81958—Clients that are connected to autonomous access points show as rogue clients.

  Workaround: None.

- CSCsk87607—When you try to download logs from the location server, it times out, and an error is displayed.

  Workaround: Log into the location server via SSH and move or remove the accuracy test debug log files that start with rf-<mac-address>xxx from the /opt/locserver/logs directory.

- CSCsk88821—When you create maps, the floor information for a building is not retained, and Cisco WCS displays an error.

  Workaround: None.

- CSCsl08696—Cisco WCS does not allow a name change for the RF Calibration Model under WCS > Monitor > Maps > RF Calibration Model.

  Workaround: None.

- CSCsl12105—WCS fails to upgrade the location server from 3.0.42.0 to 3.1.35.0.

  Workaround: None.

- CSCsl39335—Cisco WCS fails to start. When a conflicting port is in use, Cisco WCS fails to start and displays the error message Failed to start WCS Server. Cisco WCS should display the list of conflicting ports as a reason for failure.

  Workaround: Go to WCS/webnms/logs/wcs-0-0.log on your hard disk and look for the conflicting ports.

  In Windows XP and Windows Server 2003, you can type **NETSTAT -0** to get a list of all the owning process IDs associated with each connection.

  Look in the Task Manager for the respective PID and stop the process using the required port.

- CSCsl57546—When Cisco WCS displays a rogue device, the detecting access point is displayed by IP address or name depending on how the rogue was detected.

  If Cisco WCS discovers the rogue during a poll, it uses the MAC address of the access point for the access point name. If Cisco WCS learns about the rogue from a trap received from a wireless LAN controller, it uses the real access point name instead.

  Workaround: None.

- CSCsl59647—LAG Mode on next reboot and Broadcast Forwarding options are missing in Cisco WCS.

  Workaround: Configure these options from the controller directly.

- CSCsl74361—Cisco WCS cannot restore StdSignaturePattern (Standard Signatures) on the wireless LAN controller.

  Workaround: Restore Standard Signatures manually on the wireless LAN controller.

- CSCsl79599—When you add access lists or WLANs in Cisco WCS, unfounded messages are produced.

  Workaround: Contact Cisco support to determine which database queries can fix the entries.

- CSCsl80359—The guest user account template status does not show correctly.

  Workaround: Check WLC and WCS to see if the account status is the same. If not, reapply the template.

- CSCsl89809—A UDI Common-1 error is displayed when you click Restore WCS Values after auditing a controller.

  Workaround: None.

- CSCsm03250—Location logs are not updated when you download logs from Cisco WCS.

  Workaround: Download the location logs manually from the location appliance using the Cisco WCS GUI.

- CSCsm04809—The Cisco WCS radio utilization report shows zero values or incorrect information.

  Workaround: None.

- CSCsm17395—Cisco WCS access point rogue location information/report is not accurate. When you look at rogue clients through Cisco WCS, the access points that detected the rogue client might not be indicated.

  Workaround: Check the rogue clients listed directly on the controllers by clicking Monitor > Security > Rogue Clients and search using Cisco WCS Controllers. To determine which access points detected the rogue, click on the rogue access point in the list. If the rogue client was detected by a location server, the rogue client's location is indicated.

- CSCsm30661—The Config Group Apply report shows an incorrect number of templates in the config group.

  Workaround: Choose each applicable template individually to add to the config group.

- CSCsm33619—When you perform a quick search or new search, the location information for the client does not appear in WCS release 4.2.62.0 under Monitor > Clients.

  Workaround: Go to the map where the client's access point is located, and the client shows as located by the location server.

- CSCsm50334—If a guest user template (or any other template) fails, the error message is too limited. The failure may be lack of space, but you cannot determine this from the error message.

  Workaround: None.

- CSCsm66780—If you create a WLAN with an ACL but no rules added, an SNMP error occurs.

  Workaround: None.

- CSCsm75896—When you audit WLC from WCS, you get an error message after attempting a restore configuration, if extra or missing standard signatures exist on the WLC that are not in the WCS database.

  Workaround: None.

- CSCsm79472—WCS does not back up prior to an auto upgrade.

  Workaround: Manually back up the database.

- CSCsm80253—If client troubleshooting encounters a DHCP failure, the error message is not clear.

  Workaround: None.

- CSCsm99598—When you choose Download ID Certificate from the Configure > Controller > Security > ID Certificate window, a blank page is given. The certificate download does not occur.

  Workaround: The ID certificate can be downloaded from the controller.

- CSCsm99662—If you choose Network Access Control (under Controller Template > Security), you can enter an invalid server IP without getting a warning message.

  Workaround: None.

- CSCso40295—When hovering over the menu on a map, WCS may incorrectly show the Auth value as Yes and the Status value as Disassociated.

  Workaround: None.

- CSCso83838—The exceeded load message that reads “current load on the radio of this AP is exceeded hence ignoring the request from this client” should include the name or radio MAC of the access point in error.

  Workaround: None.
- CSCsq09849—Even if you create an unlimited guest user account, the trap within the event history shows no 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.
- CSCsq17846—If the WLC is busy because access points are downloading software, WCS gives a confusing error message when you try to download software to a WLC.

  Workaround: If you use the WLC GUI instead, a more explanatory message is provided.
- CSCsq21753—Network access control template is not supported until WCS release 4.0.219.0. A pop-up message should be added to address this non-support or the template should be removed.

  Workaround: None.
- CSCsq34380—The client operating parameter shows the IP addresses in reverse order.

  Workaround: If you instead look at the CLI of WLC, the IP addresses show correctly.
- CSCsq34438—The CCXv5 client profiles with OFDM show the wrong channel values.

  Workaround: WLC shows the correct values in the GUI and CLI.
- CSCsq38486—In the access point template, H-REAP configuration receives an unexpected error message when you apply the profile name VLAN mapping.

  Workaround: None.
- CSCsq38650—WCS successfully applies unsupported Fortress and Cranite securities to WLC 4.2.112.0 and higher.

  Workaround: None.
- CSCsq40098—WCS incorrectly applies the 17th wireless WLAN to WLC even though the maximum limit is 16.

  Workaround: The 17th WLAN cannot be configured on WLC, and the proper error message shows. Perform a refresh config from WLC to WCS after configuration is complete.
- CSCsq44178—The map page shows access point information for the 802.11a/n radio as not present, even when it is.

  Workaround: Click Load or wait for the next refresh, which is 5 minutes by default.
- CSCsq44188—An incorrect error message is shown when an IPSEC layer 3 WLAN template is pushed to 4.2.x.x WLC. The message should state that IPSEC is not supported.

  Workaround: None.
- CSCsq62389—The Audit Report details in network configuration could be more descriptive.

  Workaround: Use the Audit Now feature under Configure > Controllers to get the differences between WCS and the controller.
- CSCsq62761—When the access points are placed on maps and a search for clients is performed, the Map location results show a root area link. When this link is clicked, the root area floor map with all of the access points is not positioned.

  Workaround: None.

- CSCsu29541—If you add guest users from an import file and select Controller List, any attempt to update the remaining controllers generates a “no new guest accounts in list” error message.

  Workaround: If you apply only a few of the controllers in the list when adding guest users, it will work. Or delete the accounts from WCS and re-import the CSV with the new configuration attributes.

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

  Workaround: Make sure the same device only uses one browser to check the client statistics.

- CSCsu30166—The roam reason is not displayed for a particular client.

  Workaround: None.

- CSCsu47979—The template for the authentication priority list populates incorrectly.

  Workaround: None.

- CSCsu62576—The email end date and times on the guest user creation page is mismatched between the GUI and the email page.
- CSCsr23785—When an access point joins a controller in the same mobility group that has the same WLAN profile and SSID but a different WLAN ID number, the information that appears in the access-point WLAN override list is wrong.

  Workaround: None.

- CSCsr68574—WCS cannot forward stored configurations onto the controller after a mismatch is detected from an audit.

  Workaround: None.

Resolved Caveats

These caveats are resolved in Cisco WCS 4.2.110.0:

- CSCsj50060—When an access point has the a radio disabled, the WCS AP Impersonation alarm shows the wrong radio.
- CSCsk16619—The 11n radio is no longer listed as an 11g radio on autonomous 1250 access points.
- CSCsk27242—If you draw thick walls on a floor with smaller dimensions (such as 100 ft by 50 ft), you no longer see a heatmap shift of around 4 to 8 feet.
- CSCsk64802—When you run the Mesh Stranded APs report (Reports > Mesh Reports), values are now reported in the “first time seen” and “last time seen” columns for those access points identified as “none detected but previously associated stranded APs” in the State column.
- CSCsl38717—After you create and apply a guest user template, the attributes are now retained when you revisit the guest user template and make modifications.
- CSCsm70525—When you add new access points to a map or change the position of access points on a map, the map no longer shrinks.
- CSCsm87034—WCS 4.2.62.11 no longer displays a square cut-off heatmap for a mesh deployment consisting of the 1522 access point for an outdoor environment.
- CSCsm93352—The validity date range for PAC upload using FTP is now synchronized with the WLC validity dates.
- CSCso16846—Internet Explorer no longer displays a page error when you create a guest LAN template.

- CSCsq10758—When WCS shuts down, it now removes the files previously left in the webnms/Temp directory.
- CSCsq14066—The field length of the Local Power Constraint parameter is now the same in both Cisco WCS and on the controller.
- CSCsq23147—When 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 now shows red.
- CSCsq24634—The refresh and hold time interval of CDP now shows the correct range values.
- CSCsq27049—The validation for hexadecimal keys now works as expected for RADIUS and TACACS+ servers.
- CSCsq29204—When you create an LDAP server template and apply it to controllers, the template is now properly applied on controllers running software release 4.0.219.0 and 4.1.185.
- CSCsq31683—When you choose Monitor > Client, the MAC address is now validated.
- CSCsq34103—On the external Web Auth Server, Cisco WCS now validates the server address and returns the proper message.
- CSCsq37850—When you log in and try to authenticate and authorize a TACACS user, a “login failed” message no longer appears.
- CSCsq38472—The access point template now validates the native VLAN ID and profile VLAN ID mapping.
- CSCsq44174—After the completion of an installation, WCS 4.2.91.0 no longer shows that an error occurred.
- CSCsq44188—The error message that is displayed when an IPSEC Layer 3 WLAN template is forwarded to a controller running software release 4.2.x.x. now reads “IPSEC not supported.”
- CSCsq44968—When you select WISM WLC to perform a software download using FTP, WCS no longer shows an undefined error.
- CSCsq49368—A page error no longer appears when you choose link test from the AP Association History Graph.
- 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.
- CSCsq51230—Packets shown by the DHCP Message filter are now related to DHCP.
- CSCsq51717—The Aggregation Frequency graph now displays the proper units.
- CSCsq58142—An “unknown exception” error no longer occurs when an administrator adds an existing user to other groups or modifies any defaults for users.
- 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.
- CSCsq61851—WCS can now complete a configuration backup when the last download or upload operation on the controller was through FTP.
- CSCsq63724—Display widgets now display the entire length of the contained selection.
- CSCsq73540—When you create a “throughput by controller” or a “throughput by floor” report in WCS under the Reports/802.11n Scaling menu, the output now references the controllers and access points by name.
- CSCsq84439—Cisco WCS no longer incorrectly shows guest users as expired when they are still active on the controller.
- CSCsq84583—Scheduled Guest user does not get created by WCS when using Config Groups.

- CSCsq85678—The number of associated client devices reported on the Monitor > Maps page now matches the number of associated clients reported on the Monitor > Access Points page.
- CSCsq88025—A java.exe process no longer consumes 100% of CPU time when you run a configuration sync background task.
- CSCsu00545—Email end times are now accurately reflected when a guest user imports a file.
- CSCsu36326—If you perform a restore using WCS release 4.2.81, you can start 4.2.97 without failure.
- CSCsu42445—WCS no longer shows an audit mismatch in the syslog configuration when a clean controller is added.
- CSCsr08964—Access points now successfully rejoin the controller when you apply an access point template through Cisco WCS.
- CSCsr20910—WCS no longer runs slowly under heavy calibration loads.
- CSCsr37282—You can now export the Client Association report at Monitor > Client > Client > AP Association History Table in CSV format.
- CSCsr46720—WCS data cleanup jobs no longer increase the database size when they fail to complete.
- CSCsr60853—Unexpected errors are no longer observed during the Audit Status and Restore Config Report.
- CSCsr66296—WCS no longer creates an incorrect ACL when you add new lines to an existing ACL Template.
- CSCsr68838—Changes made to the ACL Template on WCS are now propagated to the controller.
- CSCsu52893—You no longer receive an “out of memory” error when running reports in WCS with large outputs.

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