



Release Notes for Cisco Wireless Control System 4.2.97.0 for Windows or Linux

May 2008

These release notes describe open caveats for the Cisco Wireless Control System 4.2.97.0 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](#)
- [Changed Information, page 7](#)
- [Caveats, page 8](#)
- [Troubleshooting, page 16](#)
- [Related Documentation, page 16](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 16](#)



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) software release 4.2.97.0
- Location appliance software release 3.1.38.0
- Cisco WCS Navigator release 1.1.97.0
- Cisco 2000, 2100, 4100, and 4400 Series Wireless LAN Controllers running software release 4.2.130.0
- 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



Note You cannot auto upgrade from 4.2.81.0 to 4.2.97.0 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 4.2.97.0 supports management of the following wireless LAN controllers:

- 4.0.155
- 4.0.179.8
- 4.0.179.11
- 4.0.206.0
- 4.0.216.0
- 4.1.171.0
- 4.1.185.0
- 4.2.61.0
- 4.2.99.0
- 4.2.112.0
- 4.2.130.0
- 4.2.172.0

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 location 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 and resolved caveats in Cisco WCS 4.2.97.0 for Windows and Linux.

Open Caveats

These caveats are open in Cisco WCS 4.2.97.0:

- 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.

- CSCsi18453—Applying the wireless LAN fails when the controller does not have the interface associated with the wireless LAN template.
Workaround: When applying the wireless LAN template on the list of controllers, you must verify that the associated interface exists on all the controllers.
- 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.
- CSCsk16619—The 11n radio is shown as an 11g radio on the autonomous 1250 access point.
Workaround: None.
- 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.

- CSCsk27242—If you draw thick walls on a floor with smaller dimensions (such as 100 ft by 50 ft), you see a heatmap shift of around 4 to 8 feet.

Workaround: None.

- 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.

- 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—If there are no maps in WCS and the user continues to create calibration models by clicking Next without selecting a floor and building, WCS returns an error message.

Workaround: Create a map and continue calibration by selecting that map.

- CSCsk91931—If a known rogue entry is entered with uppercase MAC addresses on the template pages, WLC and Cisco WCS show it as lowercase.

Workaround: Use lowercase only for known rogues.

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

Workaround: None.

- CSCsl11236—When you change some 802.11b/g parameters, aservlet exception error occurs.

Workaround: None.

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

Workaround: None.

- CSCsl38717—After you create and apply a guest user template, the attributes may not be retained when you revisit the guest user template and making modifications. Your account may show a status of expired instead of active.

Workaround: Delete the existing template and create and apply a new one.

- 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 -O** 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.

- CSCsl61808—After SNMP settings between WLC and WCS are changed from V2 to V3, an SNMP authentication failure message appears on the WLC for location server. The SNMP v3 settings are not synchronized with the location server from WCS. WCS should be able to inform you of SNMP changes automatically.

Workaround: Remove the location server and add it back.

- 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.

- CSCsl82286—TFTP transfers fail when the TFTP server is not located on the same drive as Cisco WCS.
Workaround: None.
- 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.
- CSCsm70525—When you add new access points to a map or change the position of access points on a map, the map shrinks so much that it no longer matches the access points that are already in place. You then cannot place new access points or reposition them because the map does not reflect the actual arrangement.
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.

- CSCsm80303—The Summary page of the Client Troubleshooting window shows all stages in green, even if 802.1x authentication failed. If 802.1x authentication failed, it should appear as red while the other stages remain gray.
Workaround: None.
- CSCsm87034—WCS 4.2.62.11 displays a square cut-off heatmap for a mesh deployment consisting of the 1522 access point for an outdoor environment.
Workaround: If you modify the bin size in the default outdoor calibration model, you may see a slight improvement, but the coverage may still be inadequate.
- CSCsm93352—The validity date range for PAC upload using FTP is not synchronized with the WLC validity dates.
Workaround: None.
- CSCsm96761—The Client Association report shows every record twice.
Workaround: None.
- CSCsm98667—Two copies of the same search are sometimes created.
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.
- CSCso16846—After you create a guest LAN template, Internet Explorer displays a page error.
Workaround: Click **OK** to close the error. It does not affect functionality so it can be ignored.
- 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.
- CSCso98274—The TFTP log messages should be redone so that the troubleshooting of TFTP problems is easier.
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.
- CSCsq38486—In the access point template, H-REAP configuration receives an unexpected error message when you apply the profile name *VLAN mapping*.
Workaround: None.
- CSCsq44178—The map page shows access point information for the 802.11 a/n radio as not present, even when it is.
Workaround: Click **Load** or wait for the next refresh, which is 5 minutes by default.

- CSCsq44968—When WISM WLC is selected to perform a software download using FTP, WCS shows an undefined error.

Workaround: The FTP operation can be successfully performed after clicking OK to the error message.

Resolved Caveats

These caveats are resolved in Cisco WCS 4.2.97.0:

- CSCsj56796—The random “configuration is different on the device” error message no longer appears when you use the audit function.
- CSCsk25417—The option to resort WGB clients is now operating as expected.
- CSCsl38408—After you resize a map, the Map Editor can now exit.
- CSCsl40179—On the Cisco WCS GUI, the *Tenet_password* misspelling for the CSV file under Add autonomous access points has been corrected.
- CSCsl53478—When you choose Monitor > AP and choose a specific access point, the search results are no longer in a pending state.
- CSCsm04906—If you specify certain search options and save them, the saved options are now retained when the search is revisited.
- CSCsm91474—The hourly aggregation task is now running as expected.
- CSCsm95941—WCS now reports the correct access point client count in a map. When you navigate to the individual access point, the number of active users now matches the number shown on the access point.
- CSCsm96146—The coverage threshold alerts in WCS now display correctly.
- CSCso16220—When you download WLC software as an administrator or super user from the controller list page, you no longer receive a permission denied error.
- CSCso19170—After restoring data, the FTP root folder matches the settings in ftpd.conf. You can now log into the FTP server because the folders match.
- CCSso20712—The client count report by RAP filter is now selecting RAPs.
- CSCso27008—WCS now returns valid search results.
- CSCso29306—CAD images that are imported for a floor map are now distributed to the location server during synchronization.
- CSCso32118—You can now add controllers running WLC software release 4.0 or earlier to WCS 4.2.81.0 without receiving an object not found error.
- CSCso32170—You can now delete a RADIUS server template from WCS without a generic failure message.
- CSCso33201—For some outdoor access points (including 1510 access points), the heatmap calculation is no longer incomplete with missing values. The cases in a heatmap where low signal strength areas are displayed between high signal strength areas is limited.
- CSCso35676—Radio information on dual-radio autonomous access points is now showing correctly.
- CSCso35894—You can now log into WCS with TACACS management enabled.

- CSCso38149—If you disable DHCP proxy on a Cisco wireless LAN controller running 4.2.99 or 4.2.112, you should not have the option to define a DHCP server on the WLAN or on the interface upon which the WLAN is linked. Now when you apply a WLAN template to a WLAN on a controller with DHCP proxy disabled, you get the expected results rather than a failure error message.
- CSCso38594—When an email is sent for the controller alarm stating that the RADIUS server is deactivated, the email contents no longer include extra MME information.
- CSCso39180—The standalone SE demo license now enables the SE feature.
- CSCso39483—WCS can now authenticate users against TACACS or RADIUS servers.
- CSCso39789—The 802.11 counters report for access points had labels for the x and y axis that caused confusion. The axis contents have been changed.
- CSCso43362—When you check the access point status, the reports from WCS and WLC are now reporting the same. In WCS 4.2.81.0, access point down alarms would appear even though the access point did not actually experience down time.
- CSCso53744—You can now disable the session timeout on an SSID.
- CSCso63312—The search for authenticated clients now yields results.
- CSCso63510—WCS now shows the controller name as the source in alert messages.
- CSCso66270—The reason code that appears on WLANs when you use WPA2+802.1x authentication has been appropriately remapped.
- CSCso68005—The Tx power level on the 802.11n radio shows accurately rather than with only a 0 value.
- CSCso70728—The error message that read “Error in geting data from server. Make sure you have connectivity and the server is UP” has now been corrected with the appropriate spelling of *getting*.
- CSCso76667—Guest user creation no longer fails.
- CSCso99445—When you attempt to refresh a configuration from the controller, you no longer receive an unknown error.
- CSCsq04319—You can now access WCS pages (even from non-IE browsers) without getting the “error in getting data from server. Make sure you have connectivity and the server is UP” message.
- CSCsq09463—If you changed the default disclaimer when creating a lobby user, the changes were not getting retained after a save. The values are now retained after a save.

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, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; 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, 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. (0805R)