Release Notes for Cisco Wireless Control System 4.2.128.0 for Windows or Linux

May 2009

These release notes describe open caveats for the Cisco Wireless Control System 4.2.128.0 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
- 4.2.110.0

Note You cannot auto upgrade from Cisco WCS release 4.2.81.0 to 4.2.128.0 using Red Hat Linux Enterprise Server 5.0 (refer to bug CSCsq27887). You must initiate the manual upgrade process to do the upgrade. Refer to the Upgrading WCS section in the *Wireless Control System Configuration Guide*.

Note When you upgrade to a higher release that requires intermediate version steps (for example, from 4.1.x to 5.2.x), the releases in the upgrade path must be in both chronological order and version order. For example, if you need to upgrade from WCS release 4.1.92 to release 5.2.130, you must install a 4.2.x release as an interim step. However, you should not install release 4.2.128 (released in May, 2009) because it was released after 5.2.130 (released in February, 2009), and release 5.2.130 does not support upgrades from release 4.2.128. The release date for each WCS software release appears on the WCS release notes page at this URL:
http://www.cisco.com/en/US/products/ps6305/prod_release_notes_list.html

Important Notes

This section describes important information about Cisco WCS.

Wireless LAN Controller Requirements

Cisco WCS 4.2.128.0 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
- 4.2.205.0

Location Server and Mesh

Cisco WCS 4.2.128.0 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 4.2.128.0 for Windows and Linux.

Open Caveats

These caveats are open in Cisco WCS 4.2.128.0:

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

  Workaround: None.

- 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.

- 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.

- 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.

- 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.

- 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—When trying to view the location history of a tag or a client, the history page loads slow.

  Workaround: Under Location Server-->Administration--> History Parameters, make sure that the history interval for client, tags , rogue clients and access points is not very aggressive. Also, make sure data pruning happens more frequently.

- 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.

- 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.

- 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.

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

  When navigating to the controller configuration page in the WCS and choosing a controller, the options “LAG Mode on next reboot” and “Broadcast Forwarding” are missing.

  Workaround: Configure these particular options directly from the controller.

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

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

- 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.

- CSCsm80253—If client troubleshooting encounters a DHCP failure, the returned 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.

- 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.

- 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.

- CSCsq31648—An SNMP error message is returned when the EAP-FAST parameters template is applied to the controller.

  Workaround: None.

- 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.

- 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.

- CSCsq45098—When you add a WISM with no peers, you should not have a Select Controllers option.

  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.

- 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.

- CSCsr41614—WCS must accept MAC address in multiple formats.

  WCS requires and accepts only the a1:b2:c3:d4:e5:f6 format for entering or importing MAC addresses.

  Workaround: For bulk imports of MAC addresses, use the built-in functions in Microsoft Excel to convert the MAC addresses to the format that is accepted by WCS.

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

  Workaround: None.

- CSCsx20463—Impossible to differentiate lower L and upper I on guest credentials

  When printing guest user credentials in WCS, it is impossible to differentiate between a lower case L and upper case I; the font makes the two identical. However, when printing the credentials, WCS displays them correctly.

  Workaround: Use WebMaster to edit the stylesheet for the credentials printing page to use another font. The file is located in /webnms/webacs/styles/report05.css.

- CSCsz01574—Client details for guest anchored client shows foreign wlc info.

  Detailed client information on WCS does not show the IP address, username, or correct state. When monitoring the client information through WCS, the information from the foreign WLC appears instead of the anchor.

  Workaround: Create a detailed report. The correct information is available in the detailed report.

Resolved Caveats

These caveats are resolved in Cisco WCS 4.2.128.0:

- CSCsi18312—The link test option in the Client AP Association History now operates normally.
- CSCsi26963—The Client Association report now includes records older than 7 days.
- CSCsk45060—When a WLAN profile is deleted on WLC, the WLAN override profile, which is no longer in use, is also removed from the access point template.

- CSCsk47555—Access point mode no longer shows as local for mesh access points in bridge in access point monitor list.
- CSCsk62363—The error message has been rewritten to better explain that 21xx platforms do not support wired guest LANs.
- CSCsk87607—A timeout no longer occurs when you download logs from the location server.
- CSCsk93246—WCS has disabled TRACE on Apache Web Servers.
- CSCsl08696—Cisco WCS now allows a name change for RF Calibration Model under WCS > Monitor > Maps > RF Calibration Model.
- CSCsl12105—WCS now upgrades the location server from 3.0.42.0 to 3.1.35.0.
- CSCsl39335—Cisco WCS now starts.
- CSCsl76945—Cisco WCS now applies a MAC filter template to a controller when the interface is set to none.
- CSCsl77656—Cisco WCS no longer displays two instances of the same controller after pushing out a template.
- CSCsl79599—WLC no longer fails processing access-lists and VLANs.
- CSCsl79809—The Cisco WCS RRM template no longer turns off the automatic transmit power setting.
- CSCsl80359—The guest user scheduler and task scheduler are now synchronized.
- CSCsl89809—A UDI Common-1 error is no longer displayed when clicking Restore WCS Values after auditing a controller.
- CSCsm03250—Location logs are now updated when downloading logs from Cisco WCS.
- CSCsm04809—The Cisco WCS radio utilization report now shows correct information.
- CSCsm17395—Cisco WCS access point rogue location information/report is now accurate.
- CSCsm28611—The issues with the rogue access point alarm search have been corrected.
- CSCsm30661—Templates are no longer missing in the report after applying a configuration group.
- CSCsm33619—When you perform a quick search or new search, the location information for the client now appears in WCS release 4.2.62.0 under Monitor > Clients.
- CSCsm50334—If a guest user template (or any other template) fails, the error message was too limited. The message has been rewritten to suggest that lack of space may be the reason.
- CSCsm77314—You can now page through the Configure and Monitor pages when there are more than 20 chokepoints or location sensors (WiFi TDOA receivers).
- CSCsm79472—WCS now backs up prior to an auto upgrade.
- CSCso38204—The WCS backup on a Windows operating system is now completing without failure.
- CSCso40295—When hovering over the menu on a map, WCS now correctly shows the Auth value as Yes and the Status value as Disassociated.
- CSCsq10734—WCS now applies correct dBm values for external antenna types.
- CSCsq21753—The network access control template has been removed.
- CSCsq38650—WCS no longer applies unsupported Fortress and Cranite securities to WLC 4.2.112.0 and higher.
- CSCsq40098—The maximum limit of 16 WLANs per WLC is now recognized, and you cannot configure a 17th WLAN.

- CSCsq86922—Apache has been upgraded to 2.2.11, and OpenSSL has been upgraded to 0.9.8i.
- 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 now correct.
- CSCsr45173—Red Hat 5 is now supported.
- CSCsu29541—If you add guest users from an import file and select Controller List, you can update the remaining controllers.
- CSCsu30166—The roam reason is now displayed for a particular client.
- CSCsu47979—The template for the authentication priority list populates correctly.
- CSCsu62558—The Client Detail page now shows the correct values.
- CSCsu62576—The email end date and times on the guest user creation page now matches on the GUI and the email page.
- CSCsw88127—Any uppercase data entered in the authentication list template is converted to lowercase before sending the data to the controller.
- CSCsw90711—The WCS backup on a Linux operating system is now completing without failure.
- CSCsx57662—An upgrade from 4.2.110.0 to 4.2.XX is now successful.
- CSCsx61109—WCS now specifies which RADIUS server is mapped to the WLAN.
- CSCsx61140—You can now apply the RADIUS authentication server template without an SNMP error.
- CSCsx61300—The tree structure no longer collapses when clicking on Guest User Template.
- CSCsx71540—Clients are now getting IP addresses from the right interface.
- CSCsx77743—The default values for the 802.11b/g RRM Threshold Template are correct.
- CSCsy18592—The proof of concept cross-site-scripting (XSS) issue with embedded Flash components has been corrected.
- CSCsy52185—SA violations have been corrected.
- CSCsy79028—The copyright year has been changed to 2009.
- CSCsy71125—The session timeout value range is now validated on WCS.
- CSCsy71550—The message returned when adding an autonomous access point that is already in WCS has been rewritten for clarity.
- CSCsy78971—An error is no longer received during file download using FTP.
- CSCsy90350—WCS now generates rogue adhoc events during polling only when rogue adhocs exist.

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