Release Notes for Cisco Wireless Control System 5.2.148.0 for Windows or Linux

June 2009

These release notes describe open caveats for the Cisco Wireless Control System 5.2.148.0 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, 1140, 1200, 1230, 1240, 1250, 1310, and 1500 Series Lightweight Access Points
- 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.
  - 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.
  - 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.
  - 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 several variables (such as backups) impact the disk space.

Operating System Requirements

The following operating systems are supported:

- Windows 2003/SP2 and Windows 2003 R2/SP2 32-bit installations with all critical and security Windows updates installed.

  Windows 2003/SP2 64-bit installations are not supported.

  Windows 2003 32-bit installations provide support for up to 64 GB of RAM provided Physical Address Extension (PAE) is enabled. Refer to Windows documentation for instructions on enabling this mode.
- Red Hat Linux Enterprise Server 5.X 32-bit operating system installations.

  Red Hat Linux Enterprise Server 5.X 64-bit operating system installations are not supported.
- Windows 2003 and Redhat Linux version support on VmWare ESX 3.0.1 version.

  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 7.0 with the Flash plugin or Mozilla Firefox 3.0.X.

Note Cisco recommends Mozilla Firefox 3.0 for best results.

Note Internet Explorer 6.0 is currently supported, but support will be removed in a future release.

Using a web browser running on Windows 2003 to access the WCS web GUI is not recommended because recommended Windows 2003 security settings may 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.

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

Client Requirements

The Cisco WCS user interface requires Internet Explorer 7.0 with the Flash plugin or Mozilla Firefox 3 or later.

Note Cisco recommends Mozilla Firefox 3.0 or later for best results.

Note Internet Explorer 6.0 is currently supported, but support will be removed in a future release.

Using a web browser running on Windows 2003 to access the WCS web GUI is not recommended because recommended 2003 security settings may cause browsing problems.

The client running the browser must have a minimum of 1 GB of RAM and a 2-GHz processor. The client device should not be running any CPU or memory-intensive applications.

Note The minimum screen resolution that is recommended for both WCS and Navigator use is 1024 x 768 pixels.

Finding the Software Release

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

Upgrading to a New Software Release

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

- 4.2.62.0
- 4.2.62.11
- 4.2.81.0
- 4.2.97.0
- 4.2.110.0
- 4.2.128.0

- 5.0.56.0
- 5.0.56.2
- 5.0.72.0
- 5.1.64.0
- 5.1.65.4
- 5.2.110.0
- 5.2.130.0

Note This release is not eligible for upgrade to release 6.0.132.0.

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

Wireless LAN Controller Requirements

Cisco WCS 5.2.148.0 supports management of the following wireless LAN controllers:

- 4.2.61.0
- 4.2.99.0
- 4.2.112.0
- 4.2.130.0
- 4.1.173.0
- 4.2.176.0
- 4.2.205.0
- 5.0.148.0
- 5.1.151.0
- 5.1.163.0
- 5.2.157.0
- 5.2.178.0
- 5.2.193.0

Location Server and Mesh

Cisco WCS 5.2.148.0 supports management for the following location server and Mesh software:

- MSE release 5.2.100.0 and Context Aware Software

  Note Client and tag licenses are required in order to retrieve contextual (such as location) information within Context Aware Software. See the *Release Notes for Mobility Service Engine for Software Release 5.2.91.0* for more information.

- Location server 5.2.100.0

  Location appliances operating with release 4.0 are compatible with Cisco WCS release 5.0. Location appliances operating with release 5.1 are compatible with Cisco WCS release 5.2.

  Location appliance software is 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, 4.1.192.22M MESH, or 4.1.192.35M MESH

Important Notes

This section describes important information about Cisco WCS.

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.

Notifications in Junk Email Folder

If a domain name is not set in the email settings, notifications may end up in the junk email. When the primary device is down, no email notifications are received, but the log message indicates that an email was successfully sent.

Internet Explorer Error

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

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

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

Follow these steps to re-register the DLLs:

Step 1 Open a command-line window in Windows XP (Start > All Programs > Accessories > Command Prompt).

Step 2 Run these commands one at a time in the following order. After each command successfully runs, you should receive a pop-up message that the DllRegisterServer in_*something*.dll succeeded.

1. regsvr32 msscript.ocx
2. regsvr32 dispex.dll
3. regsvr32 vbscript.dll
4. regsvr32 scrrun.dll
5. regsvr32 urlmon.dll

6. regsvr32 actxprxy.dll
7. regsvr32 shdocvw.dll

Step 3 Restart the computer.

Notes about Google Earth

When you launch Google Earth, this message appears:

```
Google Earth could not write to the current cache or myplaces file location. The values
will be set as follows:
My Places Path:"C:\Document and Settings\userid\Application Data\Google\GoogleEarth"
Cache Path: "C:\Documents and Settings\userid\Local Settings\Application
Data\Google\GoogleEarth"
```

This is expected behavior.

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

Deletion of TFTP Server Is Not Updated in the Configuration Backup

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

Conflicting Ports Interrupt WCS Start

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

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

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

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

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 5.2.148.0 for Windows and Linux.

Open Caveats

These caveats are open in Cisco WCS 5.2.148.0:

- CSCsq17505—Duplicate data columns exist in client count table.

  Workaround: None

- CSCsq19055—View Scheduled task lacks detail for partial success status.

  Only the listed access point name and radio types are shown; no detailed information pertaining to for which radio success or failure.

- CSCsq35059—HA status on disabling is not intuitive.

  On HA configuration page, configuration mode is shown as “HA configured only” and does not imply much to the user.

  On HA status page, the “status” current state is shown as “HA not enabled”. Since it is difficult to distinguish between “HA not enabled” and “HA not configured” states, the state can be changed to “HA disabled”. In the latest image 5.2.43.0, disabling HA shows the state “HA Configured only”, which does not imply anything to the user.

  Workaround: None.

- CSCsq59009—Online help /version information not provided on secondary WCS UI.
- CSCsq79704— CAPWAPP has not replaced LWAPP in WCS.
- CSCsr03122—Monitor—clients graphs do not appear unless mouse over is performed.

  Under Monitor > Clients, the client count graph lists as empty. It does not show up unless the user does a mouse—over. Once the cursor is pointed the graph appears.

- CSCsr73730—WCS shows probing clients details information incorrectly.

  WCS shows probing clients detailed information incorrectly for security setting. WCS should specify N/A as security setting for probing clients.

  Workaround: None.

- CSCsr84754 —Autonomous access point related enhancement is not included in online help.
- CSCsr88839—WCS shows Java error for downloading autonomous image.

  WCS shows Java error when downloading autonomous image if Telnet or SSH not enabled on the autonomous access point. WCS fails to specify valid reason for failure.

  Workaround: Check to see if Telnet or SSH is enabled on the autonomous access point before downloading a new image to the access point using WCS.

- CSCsr98749—HA states on primary/secondary not intuitive when secondary WCS restarts.

  Enabling HA and restarting the secondary WCS server results in the primary WCS server showing configuration mode HA Alone, but on the secondary it is shown as Stand Alone. This configuration mode state makes it easy to confuse it with other states such as Secondary Alone, etc....

- CSCsu00006—WCS fails to include guest sessions used by reports.
- CSCsu07033—Need improved error messages when incorrect info is sent through access point CLI template.

  From WCS UI > Configure > Autonomous AP templates, CLI template. When a template is created using incorrect text as commands and then sent to to IOS access points, the WCS UI displays a Java error. The WCS UI should show a better error message.

- CSCsu08646—WCS differentiation of 2 backhaul interfaces needs improvement.

  WCS shows two tabs with the same label 802.11a. It is better if WCS could differentiate between 802.11a 5.8Ghz and 4.9GHz band.

- CSCsu09158—No mention of IP or Hostname can be entered when enabling HA.

  When enabling HA, the user is asked to configure secondary WCS info, however WCS does not provide info on whether an IP or hostname needs to be added. Hostname does not seem to be working. The UI would be more intuitive if options were provided (IP/Hostname, etc.).

- CSCsu29864—WCS fails to add the native VLAN ID to Trunk VLAN ID when native VLAN changes.
- CSCsu33826—MissingResourceExceptions seen in log file
- CSCsu36055—Audit should show names instead of numbers for VLAN tagging.
- CSCsu36213—Some of the mesh components edited are not refreshed immediately on the home page.
- CSCsu39265—WCS UI is not saving RSSI threshold values shown under MIRAdv parameters.
- CSCsu40552—AP info is not shown initially when AP icons are highlighted in Maps

  The AP Info, Mesh, and Backhaul tabs do not show anything initially.

  Workaround: Click the Access tab and then click on other tabs to show the information.

- CSCsu52928—Event messages are not consistent with IP/hostname.

  Some of the events have both the hostname/IP address, while others have only the IP address.

- CSCsu60467— No restriction or checking on group name when adding users

  When adding user to a MSE using WCS GUI, the group name entered is not validated. Even non-existing group name are accepted. User accounts created with invalid group names cannot log in.

  Workaround: The administrator must manually validate the group name used when adding new user accounts.

- CSCsu76333—Client List page Last status change column with N/A values

  In the client search list page, the Last Status Change column contains N/A as a value for some associated clients. The N/A value is listed for Clients in Associated state:

  - When the client is associated in the network but dwell time is less than 15 min. or polling time of the client statistics background task.
  - If the Client Statistics background task is disabled.

  Workaround: None.

- CSCsu85624—Need improved error message on failback to primary when HM is not running.
- CSCsu87071—E-mail notifications provide incorrect information when second primary fails.

  In a 2:1 setup, e-mail notifications from the second primary provide contradicting info in the standard e-mail notification:

  WCS primary JAYBALE-PC2 [20.20.20.26] has failed.

  WCS secondary 20.20.20.22 [20.20.20.22] has to be manually started

  SInce the secondary is already in a failover state for the first primary, there is no way to initiate failover for the second primary.
- CSCsv69725—WCS UI shows edit view option on WCS >Config > AP page.
- CSCsv85358—Migrated Client Detailed Reports on opening displays popup message.

  Detailed Client Report templates which are migrated from previous releases, when opened would display a pop-up error message box stating "Selected Controller value: All SSIDs is no longer valid. Please update and save accordingly". This is a false error message if the user re-selects the report by criteria then template is saved successfully and report can be generated.

  If Client Associated Reports and Detailed Client report templates are created in previous releases then on upgrade these reports are listed in Detailed client reports section. These report templates when opened would display "Selected Controller value: All SSIDs is no longer valid. Please update and save accordingly" error message box even if the Controller and the SSID is listed in the Report by list box.

  Workaround: The pop-up error message is a false warning error message box. Re-selecting the Report by criteria to controller/SSID and select All controllers or All SSIDs to save the report successfully.
- CSCsx18943—Applying WLAN override configuration via AP templates produces MIB error.

  Applying a WLAN override configuration via AP templates produces the following MIB error:

  java.lang.IllegalArgumentException: GetObject: Class LradIf has no supported MIB attributes for switch version 5.2.170.0
- CSCsx46523—Change of behavior with guests in 5.2 not documented.

  The change of behavior created by CSCsw42812, CSCsw42942 is not properly documented yet. WCS admin users cannot see guest users created by other admin users.

  Conditions: Occurs only in WCS 5.2 and should be an option (to see other admin's users or not) in future releases

  Workaround: None.
- CSCsz28308—Config Group Templates show constant mismatch to controllers.

  Constant mismatch is shown even though the config templates were updated from the controller.

  Conditions: WCS using config group templates.

  Workaround: None

- CSCsz39198—Error running generate proposal for planning mode.

  Unknown Exception seen when running Generate Proposal. Exception observed in logs:

  4/23/09 19:02:42.41 TRACE[com.aes] [14] [NmsExceptionHandler:execute] THROW java.awt.image.ImagingOpException: Unable to transform src image

  Conditions: Floor plan is a large JPG image about 36 megapixel in size that was put together from multiple pdf files using visio and saved as a JPG.

  Error only occurs with WCS 5.2.110 and 5.2.130. It does not occur with WCS 4.2 and 6.0.

  Workaround: Shrink the size of the image to around 12 megapixel range.

- CSCsz65992—Checkbox to select multiple WLC to assign to MSE is missing

  After adding multiple WLCs to WCS an attempt was made to assigned them to MSE for synch purposes. It was observed that the multiple WLC selection checkbox is missing.

- CSCsz74833—WCS shows SNMP if pico cell-v2 template not supported for ver 4.2 WLC.

  WCS shows SNMP operation failed if user tries to apply pico cell v2 option to 4.2.205.0 version of controller.

  Workaround: None.

- CSCsz81153—Transmit power level can be 1-5 or 1-8.

  WCS documentation is not accurate. It mentions power transmit level settings to to be within a range of 1-5. The actual values for transmit power can also be 1-8 depending on the access points used

  Workaround: None

- CSCsz94791—WCS Doc should specify that restricting a guest to an area is per WLC.

  WCS Documentation should specify that restricting a guest to an area is done for all the APs of the WLCs having also APs registered in the selected area.

  Conditions: In the configuration guides, under the following paragraph:

  http://www.cisco.com/en/US/docs/wireless/wcs/5.2/configuration/guide/5_2manag.html#wp1084506

  A clear note should be added at the end of Step 3, stating the following:

  “When choosing to apply a guest user to a confined area by selecting a campus, building, or floor, the guest user will be available on the controllers having APs registered in the selected area. This will not restrict the guest user only to the APs in the selected areas, but to every APs registered to the controllers which are managing APs in the selected area”.

  Workaround: Use this note until documentation is corrected.

- 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.

- 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.

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

  Workaround: None.

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

  Workaround: None.

- 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.

- 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.

- 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.

- 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.

- CSCta08628—Unable to change DTM period for 802.11a/b/g radios from WCS.

  Configuration at the interface level is valid in release previous to and including 4.2. However, the configuration is available at the WLAN level.

  Workaround: Use the WLAN Advanced tab in the WLC web interface to set the DTM configuration.

- CSCta08270—WCS 5.2 does not allow Lobby Ambassador email credentials with more than 32 characters.

  Workaround: Use email credentials with less than 32 characters.

- CSCsz91711—Copy and Repace AP function does not work properly.

  After performing a Copy and Repace AP function, no information such as Hostname or IP address, was not copied on WLC.

  Workaround: None.

Resolved Caveats

These caveats are resolved in Cisco WCS 5.2.148.0:

- CSCsi26963—The Client Association report does not include any records older than 7 days.
- CSCsk17031—When trying to view the location history of a tag or a client, the history page no longer loads slow.
- CSCsl59647—LAG Mode on next reboot and Broadcast Forwarding options are no longer missing.
- CSCsl80359—Guest user scheduler is now synchronized with task scheduler.
- CSCsq45098—When you add a WISM with no peers, you no longer have a Select Controllers option.
- CSCsr82799—Subcategories now appear in template launch pad.
- CSCsu07853—Config group audit mismatch no longer occurs for local management user.
- CSCsu49105—Accuracy tool now supports Floors configured in Meters Dimension.
- CSCsv37742—Newly created dynamic interfaces are now seen on non-root device.
- CSCsv71119—Password is now omitted from log file.
- CSCsw29310—Lrad Template fields are now encrypted.
- CSCsw40940—ServletException is no longer seen when test firing events.
- CSCsw44695—BaseAP not found error no longer occurs when accessing client details.
- CSCsw71297—Client details for guest anchored client no longer shows foreign WCS details.
- CSCsw88127—WCS no longer sends the access point auth list in case used.
- CSCsw89919—Audit report has been aesthetically modified.
- CSCsw90711—Linux WCS no longer fails to upgrade from 5.0.72.0.
- CSCsw98587—Upgrade time now within specifications.
- CSCsw99057—Remove controller on WCS now shows correct lifetime value.
- CSCsx16210—WCS no longer shows rogue access points as contained.
- CSCsx34113—Windows logout no longer causes Apache process and WCS JVM to exit.
- CSCsx35614—Encryption for unencrypted password during upgrade is now supported.
- CSCsx38422—Virtual domains page now loads without an error.
- CSCsx54987—WCS login page now shows correct copyright dates.
- CSCsx61055—WLAN template no longer fails when diagnostic WLAN is enabled.
- CSCsx61186—access point template no longer shows time out error message.
- CSCsx69190—Blank page no longer appears on Internet Explorer.
- CSCsx70804—Heatmap for 802.11n data rates is now available.
- CSCsx75646—The merge error in guest task no longer appears.
- CSCsx79110—RadiusAuth no longer fails when wrapKeyFormat is set to Hex in.
- CSCsx81224—Access point group template OK button now operates normally.
- CSCsx94017— WLAN template status no longer changes to disable after edit.
- CSCsx96605—Guest users with a lifetime greater than 30days are now rescheduled properly.

- CSCsx96709—WCS no longer allows editing interface on AP group template.
- CSCsx97003—Hover over outdoor map no longer results in an error generated by the access point.
- CSCsy12759—AP stats are no longer deleted every time an AP is deleted.
- CSCsy18565—XSS issue is no longer found in WIPS JSP pages.
- CSCsy18565—XSS issue no longer occurs in WIPS JSP pages.
- CSCsy18592—XSS issue no longer occurs with embedded flash components.
- CSCsy28204—Results are now included in AP report by location and SSID for WLAN IDs greater than eight.
- CSCsy44904—Default option for limiting a guest account has been changed.
- CSCsy51742—Controller records no longer dropped when their key fields fail authentication.
- CSCsy56620—AP summary report now includes pre-g access points.
- CSCsy57509—AP group Vlans are no longer removed.
- CSCsy58555—New mesh link status task is no longer needed to update parent.
- CSCsy58567—WCS map now updates icon properly when access point disassociates.
- CSCsy71550—WCS no longer gives a misleading messages when adding autonomous device.
- CSCsy71911—Misspelling corrected in 4.2.110 upgrade error message.
- CSCsy72791—Access point template task summary no longer displays exception.
- CSCsy79171—guest account status reports now shows guest users.
- CSCsy79249—Disabling Power Injector State no longer fails for LWAPP access point.
- CSCsy88634—Multiple controller config task now shows after upgrade.
- CSCsz04558—WCS no longer shows N/A if regulatory unsupported for a/n if b/g/n is dropped.
- CSCsz04865—WCS now starts with invalid parameter error.
- CSCsz39326—WIPS profile is now applied to multiple WLC.
- CSCsz48002—WCS no longer fails to validate 128-bit WEP n 802.1x key.
- CSCsz49473—WLAN template apply on 5500 controller no longer fails diagnostics.
- CSCsz50692—WCS no longer fails to update several WLCs via templates.
- CSCsz53769—HA failover now operates correctly.
- CSCsz69068—Restore DB no longer fails on upgrade.
- CSCsz70121—Save Guest Accounts on device now correct when guest account not created on WLC.
- CSCsz76870—RRM threshold template coverage issue has been corrected.
- CSCsz81650—WCS no longer shows jsp error for beacon measurement on client.
- CSCsz81655—Link test can now be performed for ccxv5 client.
- CSCsz81669—Copyright year changed to 2009.
- CSCsz96315—Dialog box now appears on MAP view page.
- CSCsz96528—Mesh AP detail page no longer displays an error message.
- CSCta05329—WCS alarm and event page no longer shows page cannot be found.

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