Release Notes for Cisco Wireless Control System 6.0.170.0 for Windows or Linux

Last Revised: November, 2009

These release notes describe open caveats for the Cisco Wireless Control System 6.0.170.0 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 Mobility Services Engine
- Cisco WCS Navigator
- Cisco 2700 Series Location Appliance
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 5500 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, 1500, and 1524 Series Lightweight Access Points
- Cisco Aironet 1310 and 1410 Bridges
- Cisco Aironet Access Points running Lightweight Access Point Protocol (LWAPP) or Control and Provisioning of Wireless Access Points protocol (CAPWAP)

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.

- 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.
  - 200 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 450 Cisco wireless LAN controllers.
  - 3.2-GHz Intel processor.
  - 2.13-GHz Intel Quad Core X3210 processor.
  - 2.16-GHz Intel Core2 processor.

  - 4-GB RAM.
  - 80 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.
  - 1.86-GHz Intel Dual core processor.
  - 2-GB RAM.
  - 50 GB minimum free disk space is needed on your hard drive.

Note For all server levels, AMD processors equivalent to the listed Intel processors are also supported.

Note The free disk space listed is a minimum requirement, but several variables (such as backups) impact the disk space.

Operating Systems Requirements

The following operating systems are supported:

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

  Windows 2003/SP2 64-bit installations are not supported. A 32-bit operating system running on a 64-bit capable hardware is 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. A 32-bit operating system running on a 64-bit capable hardware is supported.
- Windows 2003 and Redhat Linux version support on VmWare ESX 3.0.1 version and above.

  Individual operating systems running WCS in VmWare must follow the specifications for the size of WCS you intend to use.

Client Requirements

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

Note Cisco recommends Mozilla Firefox 3.0 for best performance.

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.

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.

Wireless LAN Controller Requirements

Cisco WCS 6.0.170.0 supports management of the following wireless LAN controllers:

- 4.2.61.0
- 4.2.99.0
- 4.2.112.0
- 4.2.130.0
- 4.2.176.0
- 4.2.205.0
- 4.2.207.0
- 5.1.151.0
- 5.1.163.0
- 5.2.157.0
- 5.2.178.0
- 5.2.193.0
- 6.0.182.0
- 6.0.188.0

Location Server, Mesh, and MSE

Cisco WCS 6.0.170.0 supports management for the following location server, mesh, and mobility service engine (MSE) software:

- MSE release and Context Aware Software 6.0.97.0

  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 6.0* for more information.

- Location server 6.0.97.0

  Note See the *Release Notes for Location Appliance Software Release 6.0.97.0* for more information.

- WLC running mesh release 4.1.192.35M and later.

WCS on WLSE Appliance

Cisco WCS on a WLSE appliance supports up to 1,500 Cisco Aironet lightweight access points and 161 Cisco wireless LAN controllers. The required processor is a 3.16 GHz Intel Xeon processor (or AMD equivalent) with 3 GB of RAM and 38 GB of free hard drive space.

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

Finding the Software Release

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

Upgrading to a New Software Release

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

- 4.2.62.0
- 4.2.62.11
- 4.2.81.0
- 4.2.97.0
- 4.2.110.0
- 4.2.128.0
- 5.1.64.0
- 5.1.65.4
- 5.2.110.0
- 5.2.130.0
- 5.2.148.0
- 6.0.132.0

Note Any release posted after 5.2.148.0 will not be eligible for upgrade to release 6.0.170.0.

Upgrading WCS

This section provides instructions for upgrading WCS on either a Windows or Linux server. It handles the steps you would normally follow to accomplish a manual upgrade (shut down WCS, perform a backup, remove the old WCS version, install new version, restore the backup, and start WCS). If you choose to use the installer, it searches for any previous WCS versions.

Note You must have software release 4.1.91.0 before you can automatically upgrade to 4.2.

If you choose to use the easy upgrade process, it provides error checking at each step and gives an informative message if an error causing an exit occurs. An upgrade-*version*.log is also produced and provides corrective measures.

Note For steps on upgrading WCS in a high availability environment, refer to Chapter 14 of the *Cisco Wireless Control System Configuration Guide*.

Using the Installer to Upgrade WCS for Windows

Follow these steps to upgrade WCS (on a Windows platform) using the automated upgrade:

Step 1 Insert the Windows Cisco WCS CD into the CD-ROM drive and double click the WCS-STANDARD-K9-6.0.X.Y.exe file where 6.0.X.Y is the software build. If you downloaded the installer from Cisco.com, double click the WCS-STANDARD-WB-K9-6-0-X-Y.exe file that you downloaded to your local drive.

Step 2 The Install Anywhere window appears and prepares the system for installation. After a few seconds, the Introduction window appears, followed by the license agreement window. You must click the "I accept the terms of the License Agreement" option to continue.

Step 3 At this point, the install wizard detects whether a previous version of WCS is installed and specifies whether the current version is eligible for an automated upgrade. If your most recent WCS version cannot participate in the automated upgrade, you receive such a notice. You must then choose **Install** and must switch to the manual upgrade. (Refer to the *WCS Software Configuration Guide* for manual upgrade instructions.) If your WCS version is eligible for an automated upgrade and the previous qualifying version of WCS is detected, choose **Upgrade** and continue to Step 4. This method is preferred.

Step 4 Several of the values from the previous installation are retained as part of the upgrade. These include the following:

- the ports
- the root password
- the root FTP password
- the TFTP server file location
- the FTP server file location
- the multi-homed server interfaces

Step 5 Choose a folder in which to install the Cisco WCS at the Choose Install Folder window. It must be a different location than the previous installation. Click **Next** to continue.

Step 6 Choose a folder location in which to store the shortcuts. It must be a different location than the previous installation.

Step 7 Continue to follow the prompts that appear. You are notified when the system checks for required space, uninstalls previous versions, backs up files, restores, and so on. A prompt appears asking if you are ready to start WCS as a service. Click **Yes**.

Note The upgrade log is located in the standard log directory (\webnms\logs) if the automated upgrade completes. If the automated upgrade did not complete, the upgrade log is located in the user home directory.

Note If WCS is configured to use TACACS+ or RADIUS for external authentication, the custom vendor attribute list should be updated in the TACACS+ or RADIUS server with any new permissions. The attribute list for the appropriate UserGroup can be found at Administration > AAA > UserGroups. Click the **Export** link for the appropriate user group. Refer to Chapter 14 of the *Cisco Wireless Control System Configuration Guide* for additional information regarding upgrading.

Using the Installer to Upgrade WCS for Linux

Follow these steps to upgrade WCS (on a Linux platform) using the automated upgrade:

Step 1 Using the command line, perform one of the following:

a. If you are installing from a CD, switch to the /media/cdrom directory.

b. If you are installing from Cisco.com, switch to the directory in which the install file was downloaded. For example, if the install file was placed in /root/Desktop, enter **cd /root/Desktop**.

Step 2 Enter **./WCS-STANDARD-K9-6.0.X.Y.bin** (for CD users) or **./WCS-STANDARD-LB-K9-6-0-X-Y.bin** (for Cisco.com users) to start the install script.

Step 3 The Install Anywhere message appears and prepares the system for installation. After a few seconds, the Introduction appears, followed by the license agreement statement. You must accept the license agreement to continue.

Step 4 At this point, the install wizard detects whether a previous version of WCS is installed and specifies whether the current version is eligible for an automated upgrade. You receive a notification whether or not your most recent WCS version is eligible for the automated upgrade.

Step 5 If you cannot continue to the automated upgrade because your current WCS version is not eligible, choose **Install** and continue to the manual upgrade (refer to the *WCS Configuration Guide* for manual upgrade instructions). You can also choose to do a manual upgrade rather than the recommended automated upgrade by choosing **Install** and continuing to the manual upgrade, but this is not recommended. If your current WCS version is eligible for the recommended automated upgrade, choose **Upgrade** and continue to Step 6.

Step 6 Several of the values from the previous installation are retained and carried over as part of the upgrade. These include the following:

- the ports
- the root password
- the root FTP password
- the TFTP server file location
- the FTP server file location
- the multi-homed server interfaces

Step 7 Choose a folder in which to install the Cisco WCS. It must be a different location than the previous installation. Click **Next** to continue.

Step 8 Choose a folder location to store the shortcuts. It must be a different location than the previous installation.

Step 9 Continue to follow the prompts that appear. You are notified when the system checks for required space, uninstalls previous versions, backs up files, restores, and so on. A prompt appears asking if you are ready to start WCS as a service. Click **Yes**.

Note The upgrade log is located in the standard log directory (\webnms\logs) if the automated upgrade completes. For an incomplete automated upgrade, the upgrade log is located in the user home directory.

Note If WCS is configured to use TACACS+ or RADIUS for external authentication, the custom vendor attribute list should be updated in the TACACS+ or RADIUS server with any new permissions. The attribute list for the appropriate UserGroup can be found at Administration > AAA > UserGroups. Click the **Export** link for the appropriate user group. Refer to Chapter 14 of the *Cisco Wireless Control System Configuration Guide* for additional information regarding upgrading.

Restoring the WCS Database in a High Availability Environment

During installation, you are prompted to determine if a secondary WCS server would be used for high availability support to the primary WCS server. If you opted for this high availability environment and enabled it in the Administration > High Availability window, the status appears as *HA enabled*. Before performing a database restore, you must convert the status to *HA not configured*.

Note If the restore is performed while the status is set to *HA enabled*, unexpected results may occur.

Follow one of these procedures to change the status from *HA enabled* to *HA not configured*:

- Click the **Remove** button on the HA Configuration window (Administration > High Availability).
- Restart the primary server. Go to the secondary HealthMonitor GUI (https://<SecondaryWCS>:8082) and click **Failback**.
  - This procedure is used when one of the following instances has occurred:

    The primary server is down and failover has not been executed, so the secondary server is in SecondaryLostPrimary state.

    or

    The primary server is down and failover is already executed, so the secondary server is in the SecondaryActive state.

The primary server will now be in HA Not Configured mode, and you can safely perform a database restore.

Important Notes

This section describes important information about Cisco WCS.

If you change the report repository path under Administration > Settings > Report, then the existing saved download report will no longer work. To fix this, manually move the files to the new directory by cutting and pasting the files.

Duplicate AP Name

If you see access points with the same name while applying controller templates or adding them to the map, perform a refresh config. The duplicates in the database will be eliminated.

High Availability

You must enter an e-mail address when configuring high availability. WCS tests the e-mail server configuration and if the test fails (because the mail server cannot connect), WCS does not allow the high availability configuration.

Note The e-mail address is optional from this release onwards.

Note High availability is supported on Linux, on Windows 2003, and on VMware environments. Specific operating system support is listed in the "Operating Systems Requirements" section on page 3.

Client Session Report

The new client session report replaces the existing Client Association and Client Detail Report. If you perform an upgrade, Client Association no longer appears in the Reports menu. The data pertaining to these reports migrates successfully, and saved report entries for Client Association and Client Detail reports are migrated. However, the new ClientSessionInfo table is not populated with data from the previous reporting period; the table is populated with client-related data that occurred after upgrade. The new client detail report contains the details of association time, disassociation time, and session timeout along with details of VLAN, session length, client location, Megabit information used, SNR, RSSI, and throughput.

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 E-mail Folder

If a domain name is not set in the e-mail settings, notifications may end up in the junk e-mail. When the primary device is down, no e-mail notifications are received, but the log message indicates that an e-mail 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 deregistered the DLLs below. Re-registering them corrects the problem.

Follow these steps to reregister 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.

Windows XP Cannot Load CAD Files

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

Take one of the following actions:

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

Deletion of TFTP Server Is Not Updated in the Configuration Backup

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

Conflicting Ports Interrupt WCS Start

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

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

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

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

New Features

There are no new features in this software release. However, there are a few enhancements in this release that are listed in the next section.

Enhancements in This Release

The following section list the enhancements in this release. For your convenience in locating the enhancement bugs in Cisco's Bug Toolkit, the bug titles listed in this section are taken directly from the Bug Toolkit database. These enhancement bug titles are not intended to be read as complete sentences because the title field length is limited. In the bug titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.

Note If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

http://tools.cisco.com/Support/BugToolKit/.

To become a registered cisco.com user, go to the following website:

http://tools.cisco.com/RPF/register/register.do

Table 1 lists the enhancements in this release.

Table 1 Enhancements in This Release

Enhancement Bug ID	Description
CSCsy05283	Filter options should give controller name instead of controller IP
CSCsz34155	WCS HA: Send an e-mail to admin when connectivity is restored
CSCsz19732	AP profile status does not have location field for floor area
CSCsy14052	Sorting should be provided for home page components like AP uptime
CSCsz85998	H-MR: need tooltip on alarm message column
CSCsy69465	H: Configuring WCS HA without e-mail notification
CSCsu71231	WCS should show the snmp community mode ro/rw currently in use
CSCsx09031	WCS should include High availability: Pri/Sec WLC name and IP address
CSCsz57818	TCP MSS knob missing on WCS
CSCsz00743	AP link latency values inconsistent in WCS and Controller Web UI
CSCsy98952	Add controller name in Controller config group
CSCsu04274	Pushing TACACS server template fails if index gap exists
CSCsz57776	WCS should support advanced EAP parameters
CSCsz57800	CPU utilization for Talwar controllers
CSCsy33352	Capability to save settings of Filter
CSCsy70252	While viewing an AP heatmap, if we could right click on an AP and config
CSCsz40865	WCS: No way to correlate the RSSI easily on the map
CSCsz51300	WCS: Diagnostics enhancement - LogViewer tool
CSCsk87735	Add ability to view AP specific alerts from Map View
CSCsy94129	Adding "Block Ack" alarm
CSCsz04851	WCS: Enhancement: Add option to e-mail WCS log files
CSCsz07762	Cannot sort by client count in Monitor>Maps
CSCsy91908	In building view give breakup of a/n & b/n client count
CSCsz78271	Allow Floor index to be customizable
CSCsz78923	WCS Planning Mode needs support for 40Mhz channel width
CSCsz57680	Shared credentials for guest accounts
CSCta31668	Enhance Auto-Upgrade Logging

AP Image Predownload

This feature allows you to download the upgrade image to the controller, and then download the image to the access points while the network is still up. A new CLI and controller GUI allow you to specify the boot image for both devices and to reset the access points when the controller resets.

Ability to Limit AP Transmit Power

You use this feature to configure a maximum transmit power that access points cannot exceed. When you configure a maximum transmit power, RRM does not allow any access point attached to this controller to exceed this transmit power level (whether the power is set by RRM TPC or by Coverage Hole Detection). For example, if you configure a maximum transmit power of 11 dBm, then no access point would transmit above 11 dBm unless the access point is configured manually.

RRM Fixes for Medical Devices

This feature improves the way that QoS interacts with the RRM scan defer feature. In deployments with certain power-save clients, you sometimes need to defer RRM's normal off-channel scanning to avoid missing critical information from low-volume clients (for example, medical devices that use power-save mode and periodically send telemetry information).

You can use a client's WMM UP marking to tell the access point to defer off-channel scanning for a configurable period of time if it receives a packet marked UP.

Use this controller CLI command to configure this feature for a specific WLAN:

config wlan channel-scan defer-priority *priority* [**enable | disable**] *WLAN-id*

where *priority* = 0 through 7 for user priority (this value should be set for 6 on the client and on the WLAN).

Use this command to configure the amount of time that scanning will be deferred following an UP packet in the queue:

config wlan channel-scan defer-time *msec WLAN-id*

Enter the time value in milliseconds (ms); the valid range is 100 (default) to 60000 (60 seconds). This setting should match the requirements of the equipment on your wireless LAN.

You can also configure this feature on the controller GUI by selecting WLANs, and either editing an existing WLAN or creating a new one. On the WLANs > Edit page, click the **Advanced** tab. Under Off Channel Scanning Defer, select the scan defer priorities and enter the defer time in milliseconds.

Note Off Channel Scanning is essential to the operation of RRM, which gathers information about alternate channel choices such as noise and interference. Additionally, Off Channel Scanning is responsible for rogue detection. Devices that need to defer off-channel scanning should use the same WLAN as often as possible. If there are many of these devices (and the possibility exists that off-channel scanning could be completely disabled by the use of this feature), you should implement an alternative to local AP off-channel scanning, such as monitor access points, or other access points in the same location that do not have this WLAN assigned.

Assignment of a QoS policy (bronze, silver, gold, and platinum) to a WLAN affects how packets are marked on the downlink connection from the access point regardless of how they where received on the uplink from the client. UP=1,2 is the lowest priority, and UP=0,3 is the next higher priority. These are the marking results of each QoS policy:

- Bronze marks all downlink traffic to UP= 1.
- Silver marks all downlink traffic to UP= 0.
- Gold marks all downlink traffic to UP=4.
- Platinum marks all downlink traffic to UP=6.

Inter-Release Controller Mobility (IRCM)

This feature supports seamless mobility and Cisco Unified wireless network (CUWN) services across controllers with different software versions.

CUWN Service	4.2.x.x	5.0.x.x	5.1.x.x	6.0.x.x
Layer 2 and Layer 3 Roaming	X	–	–	X
Guest Access/Termination	X	X	X	X
Rogue Detection	X	–	–	X
Fast Roaming (CCKM) in a mobility group	X	–	–	X
Location Services	X	–	–	X
Radio Resource Management (RRM)	X	–	–	X
Management Frame Protection (MFP)	X	–	–	X
AP Failover	X	–	–	X

Note IRCM is supported on GD releases only; ED releases, such as 5.2.x, are not supported.

RRM is supported between controllers running different versions of code. However, different RF groups will form for the controllers running different code levels. Therefore, separate RF groups do not have the ability to interact with one another, resulting in two groups of radios calculating power and channel separately.

The effect on the network depends on how close the two RF groups are to one another. For example, if you have two controllers, one running software release 4.2.X.X and one running software release 6.0.X.X, and both controllers service access points that are on the same floor, there will be some impact at the boundary between the two groups of access points on channel and TX power decisions.

If you implement on neighboring floors, the result might be greater channel overlap (interference among access points), but TX power would likely not be affected. Non-neighboring floors would be fine. Implementing mixed controllers releases in a random deployment would likely result in significant issues with TX power assignments but would have a minor impact on channel assignments.

Caveats

The following sections list open and resolved caveats in Cisco WCS 6.0.170.0 for Windows and Linux. For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are taken directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.

Note If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

http://tools.cisco.com/Support/BugToolKit/.

To become a registered cisco.com user, go to the following website:

http://tools.cisco.com/RPF/register/register.do

Open Caveats

Major Open Caveats

There are no major open caveats in Version 6.0.170.0.

Moderate Open Caveats

Table 2 lists the moderate open caveats in Version 6.0.170.0.

Table 2 Moderate Open Caveats

ID Number	Caveat Title
CSCsz05354	4.2 controllers and ap do not show up for ap summary
CSCtc29871	Busiest Client Report taking too long in scale test bed
CSCtc37225	Tx power channel Report taking longer on scale test bed when more than
CSCtc41084	WCS map import from file fails and does not provide an error message
CSCtc43049	WCS not exporting AP placed in outdoor location
CSCtc46407	Getting Warning Message: Unresponsive script, in PCI report
CSCtc49690	WCS: Audit mismatch for LAG mode
CSCta86921	Monitor->AP detail page takes longer to launch when controller unreachable
CSCsv34264	H WCS:SNMP Error thrown while trying to generate ID certificate
CSCsy31225	Left nav disappears on AP config screens

Table 2 Moderate Open Caveats (continued)

ID Number	Caveat Title
CSCtc53219	save settings does not save zoom settings for Map
CSCtc80483	Google Earth Import maps fail
CSCtc37225	Tx power channel Report taking longer on scale test bed when more than
CSCtc44722	All WCS Page navigations get redirected to home page
CSCtc36642	AutoCAD maps becomes blurry when used with MAP Editor

Minor Open Caveats

Table 3 lists the minor open caveats in Version 6.0.170.0.

Table 3 Minor Open Caveats

ID Number	Caveat Title
CSCta77783	Backup and upload third party certificates installed on WLC
CSCta93780	Unable to upload customized web bundle from WLC via WCS

Resolved Caveats

Table 4 lists caveats resolved in Cisco WCS 6.0.170.0.

Table 4 Resolved Caveats

ID Number	Caveat Title
CSCsw92658	Rogue AP rules page should provide link to corresponding template page.
CSCta65597	Location Appliance becomes unreachable when syncing large network design
CSCtb89614	Report download allows end user to download any file
CSCsx37305	hreap- ap template shows office extend err msg if native vlan pushed.
CSCsy10299	A check for Pre AUTH acl on 5508 / 2106 for external webauth
CSCsy72020	Not able to save WLC CLI template with more than 400 WLAN config commands
CSCsz72799	WCS UI refreshes continuously by opening a report with >60selections
CSCsz91711	Copy and Replace AP function does not work properly
CSCta24528	Page error on entering invalid file name in Import AP/WiFi TDOA Receiver
CSCta25563	Wcs fails to save hreap-profile vlan mapping no on ap templates.
CSCta27702	Wcs fails to show ethernet interface for 1510 AP running4.1.192.35M
CSCta27939	WCS doesn't send clear rogue ap ignore when autonomous ap is removed
CSCta30422	Controller utilization graph-view history not working.
CSCta32522	WCS does not send e-mail from TEST button if using username/password

Table 4 Resolved Caveats (continued)

ID Number	Caveat Title
CSCta36494	AP migration template does not set correct Controller IP address
CSCta39607	MSE Server Events always displaying 20 entries per page
CSCta41847	WCS 6.0 - AP up/down report is not showing up with non-root user
CSCta42096	Time not visible for memory n cpu graph-Home page
CSCta44430	Wcs show ethernet interface for un associated AP.
CSCta46501	Sorting by SNR not working- associated clients of AP.
CSCta46507	Permission for config audit report denied - user defined group.
CSCta47074	Tools>config audit ui guidelines changes.
CSCta47316	Unable to obtain GoogleEarth map details
CSCta47961	WCS: H: Tabular format is not retained after refresh for client count
CSCta67347	With CAS disabled, Monitor > Clients returns error, generates exception
CSCta92543	Tag should properly escape the HTML.
CSCta92603	WCS map display to be fitted in a limited zone
CSCta94340	Tag reporting showing incorrect controller
CSCta94386	Unable to add multiple controllers to Virtual domain
CSCta94517	Need to include legend in enlarged pie chart view
CSCtb07420	WCS mishandles RADIUS message-authenticator from ACS5
CSCtb08940	WCS stopped running because of OutOfMemoryError
CSCtb47617	WCS: sessionTimeoutBool Error when creating WLAN Templates
CSCtb51301	Scheduled reports fails
CSCtb56664	Remove Over The Air Provisioning (OTAP) in Access Points
CSCtb58708	WCS: Upgrade to 6.0.132.0 takes a long time.
CSCtb61044	RF Configuration Mismatch Details page just white with lines
CSCtb63012	AP Summary Report list incorrect Associated WLANs
CSCtb77551	WCS: Guest Users Count Graph is Empty if not logged in as root
CSCtb79879	Rogue Alarm which got cleared still shows in the Alarm list
CSCtb86471	WCS: Cannot Configure Access Point due to switchKeyNotSet Error
CSCtb89652	Tooltips used in WCS have XSS issues
CSCtc19145	Scheduled reports customized order is not maintained
CSCtc21641	Unable to run Device Inventory report
CSCtc26191	WCS: Idle Client entries need to be removed from the database
CSCtc58290	Redpine tags not displayed on WCS
CSCta60310	Measurement notification timeout range inconsistent with WLC
CSCsz77563	Restore attributes supported in previous release
CSCsq79704	G: Instead of CAPWAPP, LWAP still show up every where in WCS
CSCtb02748	MSE Server Events missing one entry if no paging

Table 4 Resolved Caveats (continued)

ID Number	Caveat Title
CSCtb04161	MissingResourceException seen with key stdSignaturePatternForm.title
CSCtb32176	"Out of Service Radios" label is misleading.
CSCtb59531	AP GROUP VLAN template name only allows 31 char, not 32 as defined
CSCta98910	Rogue rule RSSI min/max settings changed

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/cisco/web/psa/troubleshoot.html

Click **Wireless** and **Wireless LAN Management**. Then choose **Autonomous Wireless LAN** and **Unified Wireless LAN Management**.

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 and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.