



# Release Notes for Cisco Wireless Control System 6.0.132.0 for Windows or Linux

---

**June 2009**

These release notes describe open caveats for the Cisco Wireless Control System 6.0.132.0 for Windows or Linux, which comprises part of the Cisco Unified Wireless Network Solution (Cisco UWN).

The Cisco Wireless Control System is hereafter referred to as *Cisco WCS*.

## Contents

These release notes contain the following sections.

- [Cisco Unified Wireless Network Solution Components, page 2](#)
- [Requirements for Cisco WCS, page 2](#)
- [Important Notes, page 9](#)
- [New Features, page 11](#)
- [Caveats, page 15](#)
- [Troubleshooting, page 29](#)
- [Related Documentation, page 29](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 29](#)



# 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 6.0.132.0 supports management of the following wireless LAN controllers:

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

## Location Server, Mesh, and MSE

Cisco WCS 6.0.132.0 supports management for the following location server, mesh, and mobility service engine (MSE) software:

- MSE release and Context Aware Software 6.0.85.0

**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 6.0.85.0

**Note**

See the *Release Notes for Location Appliance Software Release 6.0.85.0* 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



**Note** Any release posted after 5.2.130.0 will not be eligible for upgrade to release 6.0.132.0.

## 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.

### 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 email address when configuring high availability. WCS tests the email server configuration and if the test fails (because the mail server cannot connect), WCS does not allow the high availability configuration.

**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 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.

## 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

The following new features are available with WCS release 6.0.132.0.



### Note

Refer to the *Cisco Wireless Control System Configuration Guide, Release 6.0* for more details and configuration instructions.

## New Controller Platform

- **Cisco 5508 Wireless LAN Controller**—This controller supports up to 250 lightweight access points and 7000 clients through eight Gigabit Ethernet distribution system ports. Cisco 5508 controllers have no restrictions on the number of access points per port. However, Cisco recommends using link aggregation (LAG) or configuring dynamic AP-manager interfaces on each Gigabit Ethernet port to automatically balance the load.



### Note

The 5500 series controllers can run only controller software release 6.0.182.0 or later. Refer to the *Cisco 5500 Series Wireless Controller Installation Guide* for more information on this controller.

- **Licensing**—Two types of licenses are required in order to use the 5500 series controllers: an image-based license (base or wplus), which determines the feature set that the controller uses, and an ap-count license (base-ap-count or wplus-ap-count), which determines the number of access points that the controller supports (12, 25, 50, 100, or 250). The base license supports the standard

base software set, and the wplus license supports the premium wireless plus (WPLUS) software set.

The WPLUS software set provides the standard base feature set as well as this functionality:

- Datagram Transport Layer Security (DTLS) data encryption for added security across remote WAN and LAN links
- Support for OfficeExtend access points, which are used for secure mobile teleworking
- Support for the 1130AG and 1240AG series indoor mesh access points, which dynamically establish wireless connections in locations where it might be difficult to connect to the wired network.
- **Data Encryption**—Cisco 5500 series controllers enable you to encrypt CAPWAP control packets (and optionally CAPWAP data packets) that are sent between the access point and the controller using Datagram Transport Layer Security (DTLS). If an access point does not support DTLS data encryption, DTLS is enabled only for the control plane, and a DTLS session for the data plane is not established.

## Access Point Additions and Changes

- **OfficeExtend Access Points**—Cisco Aironet 1130 series and 1140 series access points that are joined to a Cisco 5500 series controller with a wplus license can be configured to operate as OfficeExtend access points. This feature provides secure communications from a controller to an access point at a remote location, seamlessly extending the corporate WLAN over the Internet to an employee's residence. The teleworker's experience at the home office is exactly the same as it would be at the corporate office. Datagram Transport Layer Security (DTLS) encryption between the access point and the controller ensures that all communications have the highest level of security
- **Power over Ethernet (PoE)**—When a dual-radio 1250 series access point is powered using 15.4-W PoE, it cannot operate at full functionality, which requires 20 W. The access point can operate with dual radios on 15.4-W PoE, but performance is reduced in terms of throughput and range. If full functionality is required on 15.4 W, you can remove one of the radios from the 1250 series access point chassis or disable it in controller software release 6.0 so that the other radio can operate in full 802.11n mode. After the access point radio is administratively disabled, the access point must be rebooted for the change to take effect. The access point must also be rebooted after you re-enable the radio to put it into reduced throughput mode.

## Mesh Access Point Additions and Changes

- Controller software release 6.0.182.0 supports the following Cisco Aironet mesh access points:
  - **Cisco Aironet 1522 and 1524 outdoor mesh access points**  
The 1522 access point has two simultaneously operating radios: a 2.4-GHz radio used for client access and a 5-GHz radio used for data backhaul.
  - **Cisco Aironet 1130AG and 1240AG indoor mesh access points**  
The 1130AG and 1240AG access points have two simultaneously operating radios: a 2.4-GHz radio used for client access and a 5-GHz radio used for data backhaul.
- **Dynamic Rate Adaptation**—You can now set the bridge data rate to **auto**. When you do so, the mesh backhaul chooses the highest rate such that the next higher rate cannot be used due to unsuitable conditions for that specific rate (and not because of conditions that affect all rates).

- **Intrusion Detection System (IDS)**—You can disable IDS reports on outdoor mesh access points. When you disable this feature, no IDS reports are generated, which preserves bandwidth on the backhaul. When you enable this feature, IDS reports are generated for all traffic on the backhaul.




---

**Note** IDS reporting is enabled for all indoor mesh access points and cannot be disabled.

---

- **Licensing**—In order to use indoor mesh access points with a 5500 series controller, a wplus license must be used on the controller.




---

**Note** Outdoor mesh access points do not require a wplus license.

---

- **Serial Backhaul**—The 1524SB access point has two 5.8-GHz backhaul radios: one uplink and one downlink. Each radio is configured with a different backhaul channel, so there is no need to use the same shared wireless medium between the north-bound and south-bound traffic in a mesh tree-based network.
- **Telnet**—In previous mesh software releases, Telnet is enabled by default. However, in controller software release 6.0, controllers block Telnet sessions by default, so you need to enable Telnet if you want to use it.

## New MSE Features

- **Mobility Service Coexistence**—The Cisco 3300 Series Mobility Services Engine (MSE) now supports coexistence of multiple mobility services. It supports adaptive wireless intrusion prevention system (wIPS) and context-aware services on the same appliance.
- **License Support**—The Cisco 3300 Series Mobility Services Engine now supports a 60 day mobility services evaluation license.

## New WCS Features

- **Ease of Use Enhancements**—The following GUI changes have been made: 1) streamlined workflows and unified tab designs that reduce the number of clicks required to complete operational tasks, 2) consistent cross-links that support quick access to actionable and relevant information, 3) customized displays based on user-defined parameters that support easy filtering, adding, sorting, editing, and removal of displayed information, and 4) breadcrumb trail that retraces the user's navigation path forward and backward through a variety of WCS screens.
- **Monitoring Enhancements**—The following areas have been enhanced to simplify WLAN monitoring: 1) users can easily edit tab categories and contents to meet their specific requirements, 2) new floormap tool icons and interface support customization of displayed components and visualization of network status and alarms, 3) network status and alarms summary is now in the left-hand corner of Cisco WCS, 4) Cisco WCS search tool is now at the top of the interface to support simple and advanced searches, and 5) all WLAN campuses, buildings, and floor are hierarchically listed in a new collapsible and expandable mapping tree, facilitating quick visualization of network locations.
- **Streamlined Configuration Templates**—This feature includes the following for the streamlining and simplifying of templates: 1) mouse-over feature that provides a quick description of each template, enabling users to quickly find the template that meets their requirements, 2) quick creation and scheduling of templates through an enhanced user interface, 3) over 60 configuration templates

from the Controller Launch Pad (including system, WLAN, security, 802.11a/n, 802.11b/g/n, mesh, management, CLI, and location), 4) one place to see a list of the templates applied to a controller, and 5) access point configuration templates that are quickly customizable for 802.11a/b/g/n lightweight, autonomous (standalone), or mesh access points.

- **Enhanced Client Management**—Client monitoring has been enhanced to support quicker access to critical client information and tools across the wired and wireless network. CDP information was added to allow visibility to access point details even when the access point is disassociated from the controller. When access points are not associated to any controller, the CDP neighbor information helps to find to which switch the access point is connected. New features include: 1) client details screen with new information and an aggregation of existing information into an easy-to-read format, 2) streamlined access to the client troubleshooting tool and its step-by-step processes from anywhere in WCS, 3) access to client mobility information including how and why a client roamed across the wired and wireless network, and 4) quicker access to common tools from the client monitoring screen.
- **Expanded Flexible Reporting**—The new Report Launch Pad delivers fully customizable reporting that includes: 1) flexible user-defined report parameters for configuration, scheduling, sending, and saving, 2) mouse-over feature that provides a quick description of each report enabling users to quickly find the report that will meet their requirements prior to running the report, and 3) over 40 customizable reports on topics including access points, clients, controllers, inventory, compliance, guests, mesh, performance, security, and the RF environment.
- **Enhanced WCS Licensing**—The management of WCS licensing was enhanced.
- **Dynamic Interface Template**—This feature provides the ability to tie WLANs to unique VLANs.
- **Switch Port Tracing Enhancements**—This feature provides additional functionality to the switch port tracing that was introduced in release 5.2. It provides additional flexibility when adding switch credential information and enhances rogue access point reports.
- **Guest Access Enhancements**—The following enhancements were made for guest access: 1) the ability to configure default lifetime greater than one day, 2) the ability to import customized logos on the printed page, 3) the ability to print guest account credentials on a page, 4) enhanced navigation and look and feel, 5) customized print page header, 6) deletion of expired guests, and 7) the option for lobby ambassadors to see all accounts.
- **Advanced AP Timers**—Some advanced timer configuration for H-REAP and local mode is now available for the controller on WCS.
- **WLAN Status Scheduling**—This feature provides the ability to enable and disable multiple WLANs at a specified time for one or more wireless LAN controllers.
- **Customer Feedback Link**—Under the Help Menu is a Submit Feedback selection that allows you to provide input on the product.
- **Learning Modules**—Several short video clips have been added under the Help Menu to show the process for executing common tasks.
- **Maps Ease of Use Enhancements**—Some of the ease of use enhancements for maps include the following: 1) customizable views, 2) cloning selected campus, buildings, and floors, 3) search filters to filter campuses, buildings, and floors with specific severities, 4) automatic expansion of Tree View to first level, and 5) short cut icons to perform menu operations.
- **OfficeExtend AP**—This feature provides the ability to configure and manage wireless teleworker networks by extending the corporate network using a remote wireless access point.
- **Client Link**—Cisco Aironet 1140 and 1250 series access points support *client link*, a spatial-filtering mechanism used at a transmitter to improve the received signal power or signal-to-noise (SNR) ratio at an intended receiver (client). Client link uses multiple transmit

antennas to focus transmissions in the direction of an 802.11a or 802.11g client, which increases the downlink SNR and the data rate to the client, reduces coverage holes, and enhances overall system performance. Client link works with all existing 802.11a and 802.11g clients.

## Caveats

This section lists open and resolved caveats in Cisco WCS 6.0.132.0 for Windows and Linux.

### Open Caveats

#### Caveats Associated with Release 6.0.132.0

These caveats are open in Cisco WCS 6.0.132.0 and are tied exclusively to that release:

- CSCsj23423—The AP template is partially visible when switching between tasks and dates.  
Workaround: Refresh the page or revisit the link.
- CSCsv34264—An attempt to generate an ID certificate throws an SNMP Error.  
Workaround: None.
- CSCsv34781—The user is unable to synchronize WLC to the MSE after the WLC sysname changes.  
Workaround: Before deleting the WLC from WCS, unsynchronize it from the MSE, then delete; or change the sysname back to the original and then synchronize.
- CSCsw80427—A discovered H-REAP template displays the wrong PAC timeout value.  
Workaround: Configure the H-REAP template from WCS instead.
- CSCsx38955—After a database restore and upon synchronization, a controller can be assigned to multiple MSEs that are running wIPS. No error message displays.  
Workaround: Unassign controller wlc1 from one of the MSE and synchronize
- CSCsx72413—When you enable the Diagnostic Channel for a WLAN and apply it to a device, audit differences appear in the WLAN.  
Workaround: After you apply the diagnostic channel changes to the device in WCS, run Refresh Config from Controller.
- CSCsx77870—Some configurations are missing from the Audit on Selected Parameters page.  
Workaround: None.
- CSCsy07751—When adding a new config group in WCS, the “Copy Templates from Controller” feature does not function properly.  
Workaround: Do not use the Copy Templates from Controller feature. Discover the templates separately and manually add them to the config group.
- CSCsy31176—When you successfully add a controller in WCS, the controller list page should appear, but instead the add controller page reappears.  
Workaround: Click Configure > Controllers to go to controller list page.
- CSCsy31225—The Access Point Details page left navigation pane disappears when you click an access point link from Configure > Controllers > <controller\_ip> > Access Points > Cisco APs list page.

Workaround: To navigate to the Controller page from Configure > Access Points > Access Point Details, click the controller link available for the Registered Controller field.

- CSCsy31617—The Category column under Monitor > Alarms displays an incorrect sorting order.

Workaround: None.

- CSCsy31679—WCS displays an incorrect sorting order for Audit Status located on the Monitor > Controllers page.

Workaround: None.

- CSCsy57155—Web passthrough with pre-auth ACL fails to apply to release 5.2, 4.2, and 5.1 WLC.

Workaround: Configure WLAN with pre-auth ACL on the individual controller webUI or CLI.

- CSCsy72020—WCS returns an exception when saving a WCS CLI template. This occurs when more than 400 WLAN config lines are added and the template is saved.

Workaround: Create the CLI template with less than 400 WLAN config lines.

- CSCsy74747—Ethernet switches are not partitioned. All users in all partitions can view all ethernet switches.

Workaround: None.

- CSCsy78058—When you use Advanced Search to search for Telemetry tags and attempt to save the search, WCS fails to save the search and fails to conduct the search.

Workaround: None.

- CSCsy78668—GUI buttons and the table format on the client troubleshooting page need to be updated.

Workaround: None.

- CSCsy79232—WCS fails to save the apply device status to a report if WCS contains more than 25 controllers.

Workaround: None.

- CSCsy84499—GUI buttons and the table format on the logged-in guest user page need to be updated.

Workaround: None

- CSCsy86778—WCS allows you to assign the same profile name to a WLAN and to a guest LAN. When you search currently logged-in guest users, WCS shows inaccurate results.

Workaround: Create unique profile names for WLANs and Guest LANs.

- CSCsy89181—Sorting doesn't work correctly on some Monitor > Clients page columns.

Workaround: None.

- CSCsy89369—The same page is shown even if you click on different profile statuses.

Workaround: None.

- CSCsy94947—WCS displays an AP Authorization failed trap with the MAC address of the MSE when the NMSP session between WLC and MSE fails. When an MSE attempts to establish an NMSP session with the WLC and the authorization fails, the WLC sends a trap to WCS. This trap does not display enough information for WCS to distinguish this as an MSE-related trap. WCS defaults to an AP authorization failure trap with an MSE MAC address.

Workaround: None.

- CSCsy97570—When you click a client device on the Monitor > Client page, the client detail page takes over one minute to appear.



Workaround: None.

- CSCsy98346—After you configure a WLAN template with customized webauth pages, WLCs are not listed.

Workaround: Configure the webauth pages from the WLC UI or CLI.

- CSCsz00316—When 802.11a Status is enabled, WCS sometimes displays this message when you try to edit a data rate setting:

Row already updated or deleted by another transaction.

Workaround: Disable 802.11a Status.

- CSCsz02466—Microsoft Internet Explorer version 6 sometimes fails to display accurate results for the Client Count Customization feature.

Workaround: Use Firefox or Microsoft Internet Explorer 7 when using the Client Count Customization feature.

- CSCsz04879—When you use the Detecting APs option, you sometimes see duplicate reports or incorrect RSSI values.

Workaround: Use the WLC web GUI to look at detecting APs related data.

- CSCsz05363—The WCS location configuration template might display an incorrect location path loss configuration for the normal client burst interval if you do not check the normal client box.

Workaround: Check the normal client box before you attempt an audit.

- CSCsz05548—Client List page can sometimes take 30-500 seconds to load.

Workaround: None.

- CSCsz06840—WCS shows a difference for CDP parameters on access points after saving the Switching.

Workaround: Perform the Refresh Config from Controller. The difference does not display.

- CSCsz11535—On the WLAN configuration scheduled task page, the Selected WLANs table list is not inline with the heading and footer of the table.

Workaround: None.

- CSCsz12395—For omni-directional antennas, WCS shows the access point information with the antenna angle at 90 degrees, which makes a customer think it is a directional antenna.

Workaround: None.

- CSCsz19497—Buildings created under the Root Area appear in all virtual domains including domains to which they are not assigned. The problem happens when there are multiple virtual domains partitioned by campus and buildings, as well as buildings directly created under the Root Area.

Workaround: Move the Root Area buildings to a campus.

- CSCsz24278—Downloaded log files do not include all log files.

Workaround: Wait for a period of time and try to download the logs again. The download eventually succeeds.



**Note** If "wcs-X-X.logs" is included in the download, then all logs are included.

- CSCsz24549—WCS causes an audit mismatch by displaying the wrong attributes for port physical mode or by editing the port speed parameters.

Workaround: None.

- CSCsz28308—The config group template and audit results sometimes show a mismatch, even when you update the config templates from the controller.

Workaround: None.

- CSCsz29526—When you use more than one MSE or location appliance to run an accuracy test on a floor and one of the devices is running a 5.x release and one is running a later release, the accuracy test fails.

Workaround: Make sure the devices are running the same release version, or use only one device during the accuracy test.

- CSCsz33239—Under background tasks, the Controller Configuration Backup task sometimes fails with this message:

```
com.cisco.server.common.errors.IllegalOperationException:
MEDIATION-5,TransferConfig!171.71.128.75,uploadMode,No access
```

Workaround: Add the controller with proper credentials.

- CSCsz34211—A rogue client discrepancy occurs on the rogue AP page.

Workaround: None.

- CSCsz39570—The AP Inventory report yields results despite the fact that no access points exist on WCS.

Workaround: None.

- CSCsz40279—Prior to version 6.0, the MSE services tracked the maximum allowable elements; starting from 6.0, licensing is enforced. When 6.0 is installed, the services come up in evaluation mode which tracks only 100 elements for CAS and 20 for WIPS. You must install a permanent license for CAS and WIPs.

Workaround: None.

- CSCsz44750—When the WCS search for tags with Telemetry option is enabled, Context Aware notifications are not updated.

Workaround: Stop and restart the MSE server; avoid a search with the Telemetry option checked.

- CSCsz45064—GUI buttons and the table format on the Monitor Mesh AP page need to be updated.

Workaround: None.

- CSCsz45172—When an ACS server sends a TACACS+ authorization reply with a long list of tasks, WCS sometimes closes the TCP connection and declares the ACS dead.

Workaround: Use Radius or shorter task lists.

- CSCsz48241—WCS displays Success for WLANs with media session snooping for unsupported controller versions.

Workaround: Even though WCS displays successfully applied WLANs with media session snooping, it fails to apply to unsupported versions of WLC.

- CSCsz48609—The MAC address format used in a wired client search field is case sensitive. Also, if a space is added in front of the MAC address, the search fails.

Workaround: Use lower case for the MAC address. Ensure there is no extra space in front of MAC address.

- CSCsz51669—On WCS, under the RRM group panel for a controller that is not a group leader, the last update time displays incorrectly.

Workaround: None.

- CSCsz51707—The WCS IE window occasionally displays *Service Temporarily Unavailable* when checking the access points and clients in the WCS map from both local machine and remotely.  
Workaround: None.
- CSCsz53023—Upgrading a controller to 5.2.183.0 and above version does not upgrade the WLAN WEP Key size from unsupported 128-bit to 'UnKnown' or any other supported Key size. Because the MIB is not updated when a controller is upgraded, WCS does not update the Key size.  
Workaround: In WCS, once a controller is upgraded, select the supported WEP Key size for the WLAN and apply it to device. This causes sync up with all WebUI, CLI, and SNMP values.
- CSCsz54353—The Monitor > Clients > Clients Detected by MSE option does not populate the Controller Name column when the client is associated to the local WLC.  
Workaround: The client details page shows the correct information.
- CSCsz58150—When you apply a config group to a controller, an SNMP exception is returned.  
Workaround: You must choose the correct WLC template combinations.
- CSCsz58626—An audit reveals discrepancies between SNMP communities and AP authorization after a conversion from read-write to read-only.  
Workaround: None.
- CSCsz66652—A search of controller licenses using the Type filter criteria yields no results.  
Workaround: None.
- CSCsz68873—When you enable or disable the Power over Ethernet (POE) option and run an audit, WCS displays a mismatch for that setting on the controller.  
Workaround: Refresh the configuration for the controller before running the audit.
- CSCsz69090—WCS displays an SSID string for wired guest LANs on the WLAN list page (Configure > WLC > WLAN), and it should display dashes.  
Workaround: None.
- CSCsz69651—A download to WLC using TFTP from WCS fails with an invalid credentials error.  
Workaround: Manually set the download mode as TFTP from the controller CLI and then initiate the download.
- CSCsz72241—When you restore WCS to the controller's configuration, the username is successfully forwarded to the controller but not the password.  
Workaround: Manually change the access point password from the controller web UI.
- CSCsz72799—When you open WCS using Microsoft Internet Explorer and run a scheduled report that contains more than 60 selections, the browser sometimes hangs.  
Workaround: Use Firefox to open WCS and run the report.
- CSCsz73267—Rogue configuration parameters including RLDP (Monitor Mode APs-Only) and auto containment options are missing from WCS.  
Workaround: Configure these options on the WLC GUI.
- CSCsz75691—The coverage hole alarm values for failed clients, total client, and threshold are all 0 on the Home page.  
Workaround: Enable traps for the coverage hole.
- CSCsz75749—If an SSID contains one or more braces, the report fails to display the TSM information.  
Workaround: Use the client filter if the client MAC address is known.

- CSCsz75902—The wrong interface is used on high availability re-registration during VmWare setup.  
Workaround: None.
- CSCsz76058—When the dynamic power control report is run, the wrong power assignment mode is returned for the monitor access point.  
Workaround: Choose Configure > Controllers > 802.11a/n > Parameters for the correct dynamic power control mode.
- CSCsz78329—The online help for scheduled and on-demand accuracy is not mapped correctly.  
Workaround: Launch the online help manually and look up the accuracy tool related help page.
- CSCsz78383—The VoIP call graph report takes longer than expected to display the results.  
Workaround: Narrow the search criteria to fewer access point.
- CSCsz80636—If you delete an AP group template, WCS moves the access points to a default group and then resets.  
Workaround: None.
- CSCsz80839—The Rogue AP Event report takes longer than expected to show the results.  
Workaround: Shorten the duration by searching for specific access points or a subset of access points.
- CSCsz80919—WCS does not distinguish between voice clients and V5 clients. No alerts are given to the user.  
Workaround: You can confirm voice or v5 client requests either with the web UI or CLI.
- CSCsz82240—The downstream packet delay data is missing from the TSM QoS computation.  
Workaround: None.
- CSCsz84382—If discrepancies exist on the rogue AP rule detail page, they do not necessarily appear at the controller level audit.  
Workaround: Do an audit at each rogue AP rule page.
- CSCsz85015—If you choose Monitor > Client > Troubleshooting, the dot1x authentication test is not getting triggered on the client side. WCS reports the test status as “not run.”  
Workaround: None.
- CSCsz85603—When you delete access points from the default access point group, WCS reboots the access points and they later rejoin the default group.  
Workaround: Create a new access point group and assign access points to it before deleting them from the default group.
- CSCsz89419—TACACS+ Authorization packet sends PAP as authentication field type, even if set to CHAP.  
Workaround: None. This does not affect any functionality in WCS.
- CSCsz91240—When you search a Client detail report by client username, WCS sometimes takes a long time to display the results. The problem occurs when the client historical database contains over one million records, and when client traps are enabled on the controllers.  
Workarounds:
  1. Create the report by MAC address:
    - Perform a quick search by username.

- Find the client MAC address of the username
- Run the client detail report by the client MAC address.

2. Turn off client traps on the controllers if you don't need to keep client sessions containing less than 15 minutes of granularity.

- CSCsz93996—An incorrect message appears when you try to generate a report for more than 5 access points or radios.

Workaround: Select one radio and run the above reports.

- CSCsz95495—If you make modifications to the H-REAP config (such as disabling the least latency controller join option) using access point templates, the OEAP reboots when the template is applied. This is not expected behavior.

Workaround: You can modify the access point configuration on the Configure > Controller > AP Details page.

- CSCsz96369—An “invalid type by” error is returned in the Client Sessions report if you upgraded from version 4.2 or 5.2 to version 6.0.

Workaround: Create a new report and view from there.

- CSCsz96466—If you create a WLAN with webauth security, create a guest user mapped to the WLAN, and then forward it to WLC, you cannot delete the WLAN on the Configure > Controller > WLAN page. An exception error is returned.

Workaround: Delete the guest user associated to the WLAN. You can then delete the WLAN without any exception.

- CSCsz96510—If you try to delete a WLAN with a mobility anchor configured, an unknown exception is returned.

Workaround: Disassociate the mobility anchor on the WLAN page.

- CSCsz96549—When a guest user with limited lifetime is discovered from a Discover Templates from Controller function, the wrong expire and end time is shown.

Workaround: Create the guest user from the wcs-guest user template rather than using Discover Templates from Controller.

- CSCta00548—From version 4.2 to 6.0, all web auth configuration (including internal, external, and customized) returns an SNMP failure across all supported controllers.

Workaround: Configure all web auth from the web GUI. Or do not leave URLs blank when you configure a webauth template. Enter data in the customized and external webauth URLs by changing to different webauth types.

- CSCta02499—On the Summary > Controller page, WCS incorrectly shows the remaining period of an evaluation license for 5500 series controllers.

Workaround: The Administration > License Center > Controllers > Files window shows the correct information.

- CSCta04203—WCS sometimes fails to display clients in a partition that contains the access point to which the client is associated but which does not contain the controller to which the access point is associated.

Workaround: Add the controller to the partition.

- CSCta05459—WCS creates a guest user template and a local net user for the same config when a guest user that was created on a controller performs a refresh config.

Workaround: Create the guest user from WCS rather than from the controller.

- CSCta05909—WCS fails to perform a View History for a guest count graph.  
Workaround: You can use the guest count graph to see week, month, and year.
- CSCta08270—WCS does not allow email addresses with more than 32 characters.  
Workaround: None.
- CSCta18874—In some Windows installations in locales outside of the U.S., WCS startup fails.  
Workaround: Modify the WCS\_Install\_Directory\bin\startServer.bat file. Change *set MAX\_HEAP\_SIZE=m* to set *MAX\_HEAP\_SIZE=1024m*.

## Bugs Opened Prior to Release 6.0.132.0

These caveats are open in releases prior to Cisco WCS 6.0.132.0 and still remain open.

- CSCsh82165 —During the installation and uninstallation of WCS or Navigator, the following error message occasionally appears on Linux devices:  
`Command.run(): process completed before monitors could start.`  
Workaround: Because the error message has no effect, a workaround is not required.
- CSCsj36002—When you troubleshoot a client, the generated logs are not truncated into files of 2-MB size.  
Workaround: None. Issue has no adverse effects on functionality.
- CSCsj61673—The event log generated for the Cisco Compatible Extension v5 client is duplicated after time.  
Workaround: Stop the event log capture by clicking **Stop** when the log has been retrieved.
- CSCsj77046—The controller addition message mentions only WiSMs.  
Workaround: Go to the Configure > Controllers page to see the complete list of successfully added controllers.
- CSCsk01665—If you try to add any template with a negative test case and apply it to a device, the object is not created, but the Apply To field is incremented as expected.  
Workaround: Confirm the correct information by logging onto the device, or use the audit from the configuration side to confirm.
- CSCsk78181—Frame Logs file(cap) does not contain frames data in the file.  
Workaround: None.
- CSCsk81958—WCS shows wireless clients connected to autonomous access points as rogue clients.  
Workaround: None.
- CSCsm75896—When you audit WLC from WCS, the following error message appears after you attempt a restore: “*Restore Config Report Restore failed for following configuration(s) Name Error "StdSignaturePattern <IP address/ID> - MIB access failed."* This error occurs if extra or missing standard signatures exist on WLC compared to what WCS has in its database for that WLC.  
Workaround: None; restoring WCS signatures is not possible on WCS.
- CSCsm80253—DHCP failure in client troubleshooting provides unclear messages.  
Workaround: None.
- CSCsm99598—A blank page appears when the ID certificate is downloaded from Configure > Controller > Security > ID Certificate. The certificate download is unsuccessful.

Workaround: Download the ID certificate from the controller GUI.

- CSCso59323—The PSK ASCII key always displays HEX under controller WLAN and templates.

Workaround: In the controller GUI, you can change the PSK format from the drop-down menu.

- CSCso83838—The message that indicates when the current load on the radio is exceeded fails to specify which access point name or radio MAC has exceeded the load.

Workaround: None.

- CSCsq17846—An error is received if you download software on a WLC using WCS regardless of whether you use FTP, TFTP, or the GUI. This error occurs only if the access point is already downloading software from the WLC.

Workaround: Use the WLC GUI to get a better error message.

- CSCsq34438—WCS shows wrong values for channel and client profiles with OFDM.

Workaround: You can reference the WLC because it shows the values correctly.

- CSCsq35574—The EAP-FAST parameters Authority ID and Server Key do not accept entries of 17 or more characters.

Workaround: None.

- CSCsq38486—The profile VLAN mapping is not updated correctly on the access point, even though the native VLAN is applied correctly.

Workaround: Configure the hybrid REAP configuration with native VLAN and forward it to the access point. The native VLAN is correctly applied. Change the profile name on the same native VLAN and forward the mapping to the access point. The profile name VLAN mapping is correctly applied. It can also be applied from the WLC UI.

- CSCsr68574—If WCS shows a mismatch of values between WLC and WCS and the Restore WCS Values to Controller option is chosen, the stored configuration does not successfully pass to the controller.

Workaround: None.

- CSCsu39828—Even if activity for an infrastructure client is no longer occurring, the client still remains on the WCS map.

Workaround: None.

- CSCsz28308—Config group template and audit consistently display a mismatch even when the config template is updated from the controller.

Workaround: None.

- CSCsz39198—An unknown exception appears when running Generate Proposal. If the image size is more than 16 Mega Pixels (on a Windows platform) an exception may get thrown due to a JVM bug (the JVM runs out of memory).

- Workaround: Open the image in an image editor and reduce the size of the image. The best supported size is approximately 12 Mega Pixels.

- CSCsz91711—The copy and replace function does not copy information (such as host name and IP address) to the WLC.

Workaround: None.

- CSCsz95770—When you choose Monitor > Alarms and view the interference alarm detail, it is missing information for the top 5 access points, some exceptions are returned, and some values are not correct.

Workaround: Look in Monitor > Event to view alarm details.

- CSCsz95961—The Voice Parameter template fails when it is applied to controllers.  
Workaround: None.
- CSCsz96528—The Mesh AP Detail page (Configure > Access Point and open Mesh access point) displays with an error message.  
Workaround: Try accessing the page with Firefox. Only Internet Explorer 6 and 7 have the issue.

## Resolved Caveats

These caveats are resolved in Cisco WCS 6.0.132.0:

- CSCsi26963—The Client Association report now includes records older than 7 days.
- CSCsi73823—The summary page correctly displays the number of access point radios and the number of active clients for that building in the radio count column.
- CSCsi80575—The DSCP value is set as *any* after applying an ACL template.
- CSCsj11792—The busiest access point features work even for those access points not placed on a map.
- CSCsk45060—Deleted profiles in the WLAN override list are now removed from AP templates as expected.
- CSCsl53950—The Alarm Status on the access point icon for single radios now displays correctly in maps. For example, if you select protocol 802.11a/n, the access point icon for b/g radios now displays as gray.
- CSCsl80359—The guest user scheduler and task scheduler are now in synch.
- CSCsm14307—The config group audit feature is now working.
- CSCsm58636—On the WCS Configure > Access Point page, the correct maximum power values appear.
- CSCso38204—The Windows version of WCS now completes a backup without failure.
- CSCso43754—The AP801 is now shown in the access point list during the conversion process.
- CSCso49557—The time to load the Tools > Voice Audit page has been reduced.
- CSCso63900—When you search clients from WCS, the list no longer contains multiple entries for the same client.
- CSCso73532—The Client Detail page now has the same information as the client page when you do a search for clients and pick from the list.
- CSCsq12690—The device type is now shown for the detecting phone on the interferer list.
- CSCsq15741—The Mesh controllers in the WCS logs contain no longer contain exceptions.
- CSCsq22287—The WCS graph shows the access point uptime only when the access point is actually running.
- CSCsq38650—WCS no longer applies unsupported Fortress and Cranite securities to a WLC 4.2.112.0 and later.
- CSCsr04276—The error reporting when adding a controller to WCS has been improved.
- CSCsr40503—On the discovered SNMP template, the netmask now has the correct IP address order.
- CSCsr54896—The alarms and events messages are now generated separately per user.
- CSCsr65578—The Monitor lite account login is now accepted.



- CSCsr91548—You can now change an SNMP community for WLC without a failure.
- CSCsu29541—The guest user import from file no longer fails.
- CSCsu30166—The roam reason is now displayed for clients.
- CSCsu48429—When discovering templates from the controller in WCS, the ACL templates are created and the rules are now included.
- CSCsu49105—The Location Accuracy Tool and test points now read the floor size appropriately.
- CSCsu71562—The CLI template now works for the **show run-config** command.
- CSCsu78331—Mesh links now show up on maps.
- CSCsu79969—WCS now runs a check for the MSE/LBS version (after you add, remove, or add back to a campus) and performs a function to fix any discrepancies.
- CSCsu95615—The Client Association report by MAC address has been adjusted to accommodate a large number of clients.
- CSCsu96326—Mesh access points no longer disconnect when saving maps.
- CSCsu95903—The appropriate antenna options are displaying for the AP801 AGN-A-K9.
- CSCsu96786—The override global username and password option no longer interferes with the editing of the AP configuration page.
- CSCsv02000—Users are no longer given the option to install 5.1.64.0 if they already have 5.2.84.0 installed, unless they are first instructed to uninstall 5.2.84.0.
- CSCsv03403—On MSE > System > Trap destinations, MSE IP addresses are no longer added as a trap destination to MSE.
- CSCsv05911—If you select two controllers (one that is reachable and another that is unreachable) and then select Save Config to Flash, the error about an unreachable controller is no longer returned.
- CSCsv06447—One MSE cannot be managed by multiple WCSs. A warning message is now issued when you attempt to add an MSE to WCS.
- CSCsv11228—The time for WCS login has been reduced when wIPs alarms are large (like around 700kb and 7 GB).
- CSCsv11915—If you create a csv file with Lifetime set to greater than 35 weeks, WCS no longer fails to validate the lifetime.
- CSCsv12274—If you choose an invalid file with the Download Image selection, you now get an “invalid file” message.
- CSCsv12374—You can now choose Configure > Controller > 802.11 > General and change the authentication timeout value without error.
- CSCsv13564—When Recompute RF Prediction is launched, WCS now detects those access points with antenna set as *other* and appropriately displays an error.
- CSCsv17973—Because WiSM controllers cannot have LAG mode disabled, an “SNMP operation to device failed: attempt to set conflicting attribute value” message appeared. The appropriate message stating that LAG mode cannot be disabled on WiSM controllers was added for those users attempting to create a system general template with LAG mode disabled.
- CSCsv19289—The AP detail on a map matches the information on the selected radio.
- CSCsv19369—When you go to the Monitor > AP and Alarms page, the TDD phone now displays as expected.
- CSCsv20762—The Association History page now shows valid location details.
- CSCsv21253—The WLAN template and AP template no longer list duplicate values.

- CSCsv28326—When you use a preauthentication ACL in a WLAN template, the template is forwarded to the controller successfully, and the preauthentication ACL value now reflects the desired change.
- CSCsv29428—TFTP servers are no longer showing up in the FTP server selections.
- CSCsv37742—Dynamic interfaces now appear on non-root Virtual Domains.
- CSCsv42718—A refresh heatmap or calculation of RF prediction operation no longer generates a java exception.
- CSCsv55732—WCS no longer stops processing SNMP traps.
- CSCsv65662—An image/x-rosetta file type is now recognized when importing dwg files.
- CSCsv76635—The controller now uses the correct OID for mobility anchor up and down traps.
- CSCsv78303—Users can now search access points by floor name.
- CSCsv83390—After adding new access points, the heatmap now draws as expected.
- CSCsv94984—The Lifetime default for a lobby administrator can now be more than 1 day.
- CSCsw19979—A reboot is no longer needed when configuring 802.11b/g parameters. The asterisk in the GUI indicating the need for a reboot has been removed.
- CSCsw23291—A scheduled audit report now generates a correct report each subsequent time it runs.
- CSCsw25014—The TACACS Audit report shows correct Shared Key Format value.
- CSCsw32540—The upgrade from version 5.1.64.0 to 5.2.110.0 is now successful.
- CSCsw33510—When you apply a WLAN controller template (Configure > Controller Template > WLAN), the TKIP enable status is now updated on the controller.
- CSCsw35154—The backup location configured by the user is now checked for free space.
- CSCsw35323—The Client Location History no longer provides values for RSSI and SNR.
- CSCsw37251—The ID on the Guest WLAN Details page has been changed to 1.
- CSCsw37398—The random warning in the logs about a deprecated entry in solid.ini has been corrected.
- CSCsw37492—The ACL protocol group *any* now has correct defaults.
- CSCsw42942—A superuser can now see guest users created by lobby administrators.
- CSCsw44695—You can now access client details without a “BaseAP not found” error.
- CSCsw45414—Parameters for newly joined access points are now polled correctly.
- CSCsw49525—WCS is now in synch with the controller after doing a refresh and checking the audit status.
- CSCsw49711—The 11n AP windows no longer shows two types of diversity for a single access point.
- CSCsw52161—A java exception no longer occurs when editing a floor with obstacles.
- CSCsw52617—An upgrade to version 5.2.110.0 no longer fails with an OutofMemory exception.
- CSCsw64323—The AP group template for H-REAP access point is now operating as expected.
- CSCsw68048—Guest reports can now be generated without a permission denied message.
- CSCsw69253—Changed the message of the security alarm so that the controller correctly reports a rogue device spoofing an access point.

- CSCsw71297—The client details for guest anchored clients is now correct.
- CSCsw77819—The WLAN template caveats are shown on all pages.
- CSCsw81527—An internal exception is no longer received while auditing controllers.
- CSCsw85352—In 5.2.110.0, the scroll bar is now visible even if you choose to resize based on available browser space.
- CSCsw88127—The uppercase and lowercase discrepancy between the WCS and WLC for AP Auth and MAC Filtering has been fixed.
- CSCsw89208—When you import a CSV file, a SwitchKeyNotSet error no longer occurs.
- CSCsw90720—The red X displayed on the floorplan when importing more than 10 CAD files has been eliminated.
- CSCsw91189—The wireless status task is operating as expected without a NullPointerException.
- CSCsw91194—When DHCP is used, the audit mismatch for static IP fields has been corrected.
- CSCsw92604—You can now delete an AP rogue rule even if a corresponding template exists.
- CSCsx01811—WLAN override selections are now stored in the AP Template.
- CSCsx02076—WCS now shows the emergency boot image version.
- CSCsx07535—Lightweight access point templates for 1252 diversity settings can now be configured.
- CSCsx09460—Added more search options (such as name and MAC address) for AP templates.
- CSCsx10316—The network design and controllers out-of-sync alarms are now cleared when expected.
- CSCsx11385—The access point information that was last applied is now present on lightweight access point templates.
- CSCsx16210—The status of rogue access points is now correctly displayed.
- CSCsx18358—The AP Name Length is now the same number of characters as WLC.
- CSCsx22488—The recompute function now checks for empty results.
- CSCsx27804—Check boxes have been added to all controller template pages.
- CSCsx30368—When WLAN override is not supported, a logical error message now appears.
- CSCsx38422—The Virtual Domains page loads without error.
- CSCsx38608—The AP Groups template no longer allows a space in the name.
- CSCsx43978—The Location accuracy tool now displays the right end date.
- CSCsx46189—When a WLAN with an ID greater than or equal to 16 is added from WCS, the associated default AP group mappings is picked. Also, when a WLAN is deleted, it is now deleted from any associated ap-groups as well.
- CSCsx46479—Applying an access point template no longer changes the IP address setting on an access point.
- CSCsx50105—The OUI list has been updated.
- CSCsx61140—An SNMP error no longer occurs when applying RADIUS authentication server templates.
- CSCsx65413—WCS now discovers AP10XXs and AP15XXs.
- CSCsx65519—A search for authenticated clients from a floorplan using filters now works as expected.

- CSCsx70804—Heatmap are now being generated for 802.11n data rates in planning mode.
- CSCsx75883—An outdoor calibration model is now applied to an outdoor area.
- CSCsx96605—Guest users with a lifetime greater than 30 days now get properly rescheduled.
- CSCsx97003—An error is no longer generated when you hover over an access point on an outdoor map.
- CSCsx99154—When you edit a floor area by adding or removing access points from a floor area, the Monitor Maps page now reflects the correct access point count until an automatic or manual execution of the Client Statistics background task.
- CSCsx99859—You can now sort the client listings provided at the AP Detail > Current Associated Clients window.
- CSCsy10268—The migration template now reports env\_vars download issues.
- CSCsy27585—Only access points assigned to the SSID/AP group appear in the report by SSID results.
- CSCsy28204—WLAN IDs greater than 8 now produce results for access point report by location and SSID.
- CSCsy30197—The correct information is displayed for 2.4GHz backhaul.
- CSCsy44904—The default option for limiting guest access has been changed.
- CSCsy51742—Controller records are no longer dropped if their key fields fail validation.
- CSCsy58555—A new mesh link status task has been added to update parent links.
- CSCsy66495—Russian characters are now displayed correctly on the Mobility Services > Synchronize WCS and MSE(s) > Network Designs pages.
- CSCsy71550—When you try to add an autonomous access point that is already in the database, an appropriate message is now provided.
- CSCsy88634—The controller configuration tasks are no longer shown multiple times after an upgrade from 5.2 to 6.0.
- CSCsz45064—Mesh monitoring access point pages now follow UI guidelines.
- CSCsz51342—When you are modifying access point parameters for 3200 series WMICs, you no longer receive an SNMP error.
- CSCsz53769—High availability failover is now working as expected.
- CSCsz55693—When an encryption type in a WLAN template is disabled, the first audit now works as expected.
- CSCsz75976—You can now perform an access point search by Location string.
- CSCsz99760—Unlike all other traps in WCS, for wIPS traps, the alarm severity comes encoded in the trap itself.

## 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/web/psa/products/tsd\\_products\\_support\\_troubleshoot\\_and\\_alerts.html](http://www.cisco.com/web/psa/products/tsd_products_support_troubleshoot_and_alerts.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, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)