Release Notes for Cisco Wireless Control System 4.2.81.0 for Windows or Linux

March 2008

These release notes describe open caveats for the Cisco Wireless Control System 4.2.81.0 for Windows or Linux, which comprises part of the Cisco Unified Wireless Network Solution (Cisco UWN).

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

Contents

These release notes contain the following sections.

- Cisco Unified Wireless Network Solution Components, page 2
- Requirements for Cisco WCS, page 2
- Important Notes, page 5
- New and Changed Information, page 6
- Caveats, page 8
- Troubleshooting, page 17
- Related Documentation, page 17
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page 18

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) software release 4.2.81.0
- Location appliance software release 3.1.36.0
- Cisco WCS Navigator release 1.1.81.0
- Cisco 2000, 2100, 4100, and 4400 Series Wireless LAN Controllers running software release 4.2.112.0
- Catalyst 3750G Wireless LAN Controller Switches
- Cisco Wireless Services Modules (WiSMs) for Cisco Catalyst 6500 Series Switches
- Cisco WLAN Controller Network Modules for Cisco Integrated Services Routers
- Cisco Aironet 1000, 1100, 1130, 1200, 1230, 1240, 1250, 1310, and 1500 Series Lightweight Access Points
- Cisco Aironet 1310 and 1410 Bridges
- Cisco Aironet Access Points running LWAPP

Requirements for Cisco WCS

The following server hardware and software is required to support Cisco WCS for Windows or Linux.

Hardware Requirements for Server

Cisco WCS can be run on a workstation or server, and access points can be distributed unevenly across controllers.

Note AMD processors that are equivalent to the Intel processors listed below are also supported.

- High-end server—Supports up to 3,000 Cisco Aironet lightweight access points, 1,250 standalone access points, and 750 Cisco wireless LAN controllers.
  - 3.16-GHz Intel Xeon Quad processor with 8-GB RAM.
  - 80-GB minimum free disk space is needed on your hard drive.
- Standard server—Supports up to 2,000 Cisco Aironet lightweight access points, 1,000 standalone access points, and 150 Cisco wireless LAN controllers.
  - 3.2-GHz Intel Dual Core processor with 4-GB RAM.
  - 40 GB minimum free disk space is needed on your hard drive.

- Low-end server—Supports up to 500 Cisco Aironet lightweight access points, 200 standalone access points, and 125 Cisco wireless LAN controllers.
  - 3.06-GHz Intel processor with 2-GB RAM.
  - 30 GB minimum free disk space is needed on your hard drive.

Note The free disk space listed is a minimum requirement but may be different for your system, depending on the number of backups.

Note Cisco WCS can simultaneously manage multiple Cisco wireless LAN controllers running different software versions. Cisco WCS running Cisco UWN Software Release 4.2 can simultaneously manage controllers running release 4.2.112.0 to support Cisco Aironet Lightweight access points and controllers running release 4.1.191.24M to support Cisco Aironet mesh access points. A single Cisco WCS can manage these controllers up to a maximum number of controllers and access points supported by Cisco WCS.

Operating System Requirements

The following operating systems are supported:

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

  Windows 2003/SP2 64-bit installations are not supported.
- Red Hat Linux Enterprise Server 5.0 32-bit operating system installations.

  Red Hat Linux Enterprise Server 5.0 64-bit operating system installations are not supported.
- Windows 2003 and Redhat Linux version support on VmWare ESX 3.0.1 version and above.

  VmWare must be installed on a system with these minimum requirements:
  Quad CPU running at 3.16 GHz, with 8 GBs RAM, and a 200 GB hard drive or eqivalent.

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

Note Cisco WCS can be installed on Red Hat Linux Enterprise Server 4.0, but version 4.0 will not be supported in future releases. Plan on migrating to Red Hat Linux Enterprise Server 5.0.

Supported Browsers

The Cisco WCS user interface requires Internet Explorer 6.0/SP1 with the Flash plugin. The Cisco WCS user interface has been tested and verified using a Windows workstation.

Browsing on Windows 2003 Cisco WCS servers is not recommended because recommended Windows 2003 security settings cause browsing problems.

WCS on WLSE Appliance

Cisco WCS on a WLSE appliance supports up to 1500 Cisco Aironet lightweight access points and 100/375 Cisco wireless LAN controllers. A 3-GHz Intel AMD Pentium processor with 3 GB of RAM and 38 GB of free hard drive space is required.

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

Cisco WCS User Interface

The Cisco WCS user interface requires Internet Explorer 6.0/SP1 or later, with the Flash plug-in. The Cisco WCS user interface has been tested and verified using Internet Explorer 6.0 on a Windows workstation.

Note The screen resolution should be set to 1024 x 768 pixels for both WCS and Navigator.

Client Requirements

In order for clients to access WCS, they must have a minimum of 1 GB RAM and a 2-GHz processor. The client device should not be running any CPU or memory-intensive applications.

Finding the Software Release

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

Upgrading to a New Software Release

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

- 4.0.66.0
- 4.0.81.0
- 4.0.87.0
- 4.0.96.0
- 4.0.97.0
- 4.0.100.0
- 4.1.83.0
- 4.1.91.0
- 4.2.62.0

- 4.2.62.11

Important Notes

This section describes important information about Cisco WCS.

Compatibility

This release of Cisco WCS for Windows or Linux is compatible with wireless LAN controller and Cisco Aironet lightweight access point release 4.0.66.0 or later.

Note This version of WCS cannot add controllers running software release 4.0 or earlier. The open caveat listed as bug number CSCso32118 occurs.

For compatibility issues with the location server, refer to the *Release Notes for Cisco 2700 and 2710 Location Appliances for Software Release 3.1.36.0* at this location:

http://www.cisco.com/en/US/products/ps6386/prod_release_notes_list.html.

You may experience compatibility problems if you add a controller with a newer release than the WCS release. For example, 5.0 controller software releases should not be added to WCS 4.2.

Flash Player Software Version 9.0.115.0

Flash Player software version 9.0.115.0 is required for the full WCS benefit.

Refresh Controller Values

If the audit reveals configuration differences, you can either restore WCS values on the controller or refresh controller values to synchronize WCS with the controller. Choose **Restore WCS Values** or **Refresh Controller Values**.

If you choose to refresh the controller values, a Refresh Config window appears displaying the following message: “Configuration is present on WCS but not on device, do you wish to:” Choose one of the following options:

- **Retain**—The WCS refreshes the configuration from the controller but will not delete any devices or configurations that no longer exist in the controller configuration. For example, if the WCS database shows an AP1, but that access point is no longer present in the controller configuration, WCS will not delete AP1 from its database.
- **Delete**—WCS deletes the configuration of the controller from its database and retrieves a new configuration from the controller. Delete is the recommended option so that WCS matches the most recent configuration you are refreshing from WLCs.

Note On the Refresh Config window, only the configuration objects for this controller in the WCS database are updated. Upon refresh, the WCS templates are not updated.

Windows XP Cannot Load CAD Files

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

One of the following actions can be taken:

- Uninstall Internet Explorer 7 and install Internet Explorer 6.
- Leave Internet Explorer 7 and install the missing DLLs.

Cisco WCS Supported on Windows 2003 English and Japanese Operating Systems Only

Cisco WCS is supported only on English or Japanese versions of the Windows 2003 operating system. Display problems sometimes occur when you install and run Cisco WCS on operating systems translated to other languages or with locale settings other than English or Japanese.

Report Name Change

If you are upgrading to 4.2, the Rogue Detected by AP Report is renamed to Rogue AP Events. All other reports (Audit, Client, Inventory, Mesh, and Performance) are upgraded with the same name.

User Assistant Cannot Configure Controller

User assistants cannot configure or monitor controllers. They can only configure LocalNet Users in the controller, but they must access the Configure > Controller path to configure these local net features. If you create a user assistant user under the group category, login as that user, and go to Monitor > Controller, you receive a permission denied message as expected behavior.

New and Changed Information

New Features

The following new features are available in WCS 4.2.81.0

Note Refer to the *Cisco Wireless Control System Configuration Guide*, *Release 4.0* for details and configuration instructions for each of these features.

- Configuration Auto Refresh on Upgrade—A new auto refresh option for controller upgrade is added. If you enable the Refresh Config from Upgrade option on the Administration > Settings > Switch Upgrade Settings window when the WLC image changes, the configuration from the controller is automatically refreshed.

- New reports for 802.11n Scaling—The 802.11n Scaling report can help you to find out the client mix in your network and respective utilization of the infrastructure. These reports can also help you discover how the current controller deployment scales up to the given client mix and how you can scale to add more controllers and access points. 802.11n Scaling reports include Client Count and Throughput.
- PoE status for access points—You can now monitor the PoE status of the access points. The PoE status indicates the Power-over-Ethernet status of the access point. The possible values are low, lower than 15.4 volts, lower than 16.8 volts, normal, and not applicable.
- Multiple apply/delete option for the templates—Several templates now include an option to apply and delete templates in the right-hand side drop-down menu on the template list page. This feature has been added to the following templates:
  - NTP Server Template
  - SNMP Community Template
  - RADIUS Auth Server Template
  - RADIUS Acct Server Template
  - Local Management User Template
  - TACACS+ Server Template
  - WLAN Template
  - Telnet/SSH Template (multiple delete option only)
  - System/General Template (multiple delete option only)
- Embedded Access Points—WCS software release 4.2.81.0 provides limited monitoring support for the AP801, an access point that is embedded in the Cisco 880 Series Integrated Services Routers (ISRs). This integrated access point uses its own software image separate from the router and operates as an autonomous access that can be configured and managed locally. Currently, the AP801 is preloaded with autonomous Cisco IOS Release 12.4(10b)JA2 and LWAPP recovery image. The AP801 has a single 2.4-GHz 802.11n radio. For more information on the AP801, refer to the documentation for the 800 series router at this URL:

  http://www.cisco.com/en/US/products/hw/routers/ps380/.

  Note There is no support for for LWAPP images in WCS release 4.2.81.0 for AP801.

- FTP Support for Uploads and Downloads—Both File Transfer Protocol (FTP) and Trivial Transfer Protocol (TFTP) are now supported for uploading and downloading files to and from WCS. In previous software releases, only TFTP was supported.
- Red Hat Linux Enterprise Server 5.0—Support for Red Hat Linux Enterprise Server 5.0 is added.

Changed Information

There is no restriction on the number of hybrid-REAP access points deployed per location. However, the minimum bandwidth restriction remains at 128 kb/s with the roundtrip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes.

Customer-Found Enhancements Addressed in this Release

The following customer-found enhancements have been addressed in 4.2.81.0.

- CSCsi18046—Added an option to delete templates from WCS directly.
- CSCsj27450—Made the rogue access point and rogue client icons different on the map.
- CSCsk01022—WCS reports now show current information after a WLC upgrade.
- CSCsk26769—Fixed the heatmap problems that resulted from the conversion of WLSE to WCS.
- CSCsl80797—Added port admin/OperStatus polling to the device status policy.
- CSCsl87254—Added auto refresh config on a WLC upgrade.
- CSCsm01244—Added a new option (negative auth from TACACS+ server) for local fallback.

Caveats

This section lists open and resolved caveats in Cisco WCS 4.2.81.0 for Windows and Linux.

Open Caveats

These caveats are open in Cisco WCS 4.2.81.0:

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

  Workaround: None.

- CSCsg74466—If you choose Noise > Interference > Coverage (RSSI/SNR) to generate a report on the Monitor > Devices > Access Point page, the report displays a chart with the legend overlaying the display area.

  Workaround: None. You can view the graph on the WLC.

- CSCsh43499 —When different users are trying to troubleshoot the same client, Cisco WCS lets them put the same client on the watchlist at the same time, which Cisco WCS should not allow because the client starts to collect logs from more than one browser. Cisco WCS does not display an appropriate error message.

  Workaround: None.

- CSCsh44930—In the Clients Summary page (Monitor > Clients), typing the MAC address for a mobile client in the Client field and clicking the **Troubleshoot** button does not open up the Client Troubleshooting window.

  Workaround: Search for the client by its MAC address using the Quick Search field and click the link for the returned client to go the Client Details page. On the Client Details page, choose **Troubleshoot** from the Select a command drop-down menu and click **GO**.

- CSCsh47150—Moving a building between campuses or moving a building outside of a campus requires a clean resynchronization with the Location Appliance.

  Workaround: After moving a building, go to the Location synchronization page, unassign the Network Designs, submit the synchronization, reassign Network Designs, and resynchronize.

- CSCsh81856—While installing, the password field is only partially encrypted.

  Workaround: Only one or two of the letters show up during installation. After the password is created and you click **Enter**, the screen proceeds to the next session.

- CSCsh82165—Upon install or uninstall, the following error message sometimes displays: “Command.run( ): process completed before monitors could start.”

  Workaround: This message is irrelevant. No workaround is necessary.

- CSCsi26963—The Client Association report does not include any records older than 7 days.

  Workaround: None.

- CSCsi15088—The local net user mapping to a profile ID is not updated if the profile ID changes on the controller.

  Workaround: Change the profile ID of the local net user using the controller GUI or CLI and refresh the configuration in Cisco WCS to keep the controller and Cisco WCS in sync.

- CSCsi18312—The link test option in the Client AP Association History does not work.

  Workaround: Use the link test option on the Client Details page.

- CSCsi18453—The wireless LAN apply fails when the controller does not have the interface associated with the wireless LAN template.

  Workaround: When applying the wireless LAN template on the list of controllers, you must verify that the associated interface exists on all the controllers.

- CSCsi24635—A Cisco WCS alarm appears on the alarm dashboard when WCS on navigator becomes unreachable. If you click the alarm, you get the Alarm Details page. When you further click to get the event history, the events page is empty.

  Workaround: None.

- CSCsi26963—The Client Association report does not include any records older than 7 days.

  Workaround: None.

- CSCsi46344—There are certificate download errors on the Cisco WCS.

  Workaround: Certificates can be downloaded directly to the controller rather than via the Cisco WCS.

- CSCsj36002—The logs generated while troubleshooting a client are not truncated into 2-MB files.

  Workaround: None.

- CSCsj61673—The event log generated for the client gets duplicated after a time interval.

  Workaround: Stop the capture of the event log by clicking **Stop** when the log has been retrieved.

- CSCsj72272—You cannot enable the Accept Signed Certificate option on the Configure > Controller Template > AP Authorization page.

  Workaround: You can also perform this operation on the Configure > Controller > Security > AP Authorization page with the Edit AP Policies option from the Select a command drop-down menu.

- CSCsj77046—If you add controllers (with comma separation) which are combinations of WiSMs (2000s and 4400s), the status messages makes it appear as if only the WiSMs were added.

  Workaround: On the Configure > Controllers page, you can see a complete list of controllers that were added successfully.

- CSCsj79103—WCS release 4.0.81.0 allows installation on a 64-bit operating system. WCS is tested only on a 32-bit operating system, and installation on a 64-bit operating system should be prevented.

  Workaround: Uninstall WCS from the 64-bit operating system device and install it on a 32-bit device.

- CSCsj99244—When using Cisco WCS on a Japanese Windows operating system, the location server backup fails.

  Workaround: You can modify the AM and PM values of the backup filename to English before performing the backup.

- CSCsk01665—If you add any template with a negative test case and try to apply the template to the device, the object is not created in the device even though the Apply To field is incremented.

  Workaround: Confirm that the object is added by logging onto the device and using an audit to check the configuration.

- CSCsk16619—The 11n radio is shown as an 11g radio on the autonomous 1250 access point.

  Workaround: None.

- CSCsk17031—The history page loads slowly when trying to view the location history of a tag or client.

  Workaround: Make sure the history interval for client, tags, rogue clients, and access points is not significantly high on the Location Server > Administration > History Parameters page. You can also frequently purge the data.

- CSCsk17038—If more than 1000 elements (clients and tags) are tracked by the location server on a single floor, the performance for maps on that floor is affected.

  Workaround: Turn off the client and tags layer on the map so you can see the access points and other information on the map. Viewing over a thousand items on a single map is not practical. You should use the search option on the Monitor > Clients or Monitor > Tags page to look at the clients.

- CSCsk18826—The Location > Synchronization page takes awhile to load if several hundred controllers are being loaded.

  Workaround: Wait for the page to load completely.

- CSCsk25417—All clients are displayed if you click any header to resort WGB clients.

  Workaround: Choose **Monitor >WGB** to reset the list of WGB clients.

- CSCsk26658—An error occurs if you click on link test for a wired client.

  Workaround: No workaround. A link test is not supported for wired clients. It applies only to wireless clients.

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

  Workaround: None.

- CSCsk28942—While omnidirectional antennas' radiation patterns may have some asymmetry, they generally radiate in all directions. This causes confusion setting antenna orientation and positioning access points in Cisco WCS. Choose the Cisco omnidirectional antenna products and disable it since the specifications of the antenna are known. The following Cisco products should have omnidirectional patterns considered: AIR-ANT5959, AIR-ANT4941, AIR-ANT2422DW-R, AIR-ANT1728, AIR-ANT2506, AIR-ANT3213, AIR-ANT24120, integrated AP1120 antenna, integrated RM21A antenna, AIR-ANT5135D-R, AIR-ANT5135DW-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT58G9VOA-N, AIR-ANT5175V-N, AIR-ANT2455V-N, and integrated AP1130AG antennas.

  Workaround: Set the antenna orientation value to 0.

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

  Workaround: None.

- CSCsk31174—When device status polling and wireless polling are disabled, location information from an access point converted from autonomous to unified does not migrate.

  Workaround: Do not disable device status and wireless status polling.

- CSCsk45060—Within access point templates, the WLAN profiles in the WLAN override list are retained even when profiles are no longer used on any controllers.

  Workaround: None.

- CSCsk47555—On the monitor list page, the access point is shown as local when it should be bridging mode.

  Workaround: Synchronize the controller configuration with Cisco WCS. The current known configuration that Cisco WCS has maintained in the database, until it is synchronized, is displayed.

- CSCsk48985—If you change template parameters of an existing template and then apply it to a different number of controllers, the window shows the template as applied to the original number of controllers.

  Workaround: If you need to change parameters in a template, create a new template.

- CSCsk55422—If an invalid port is entered and then corrected during installation, the installer reports that an error occurred during installation.

  Workaround: None.

- CSCsk79095—The client detail page for WGB clients shows some tabs and commands that are not applied to the WGB client.

  Workaround: None.

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

  Workaround: None.

- CSCsk87607—When you try to download logs from the location server, it times out, and an error is displayed.

  Workaround: Log into the location server via SSH and move or remove the accuracy test debug log files that start with rf-<mac-address>xxx from the /opt/locserver/logs directory.

- CSCsk88821—When you create maps, the floor information for a building is not retained, and Cisco WCS displays an error.

  Workaround: None.

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

  Workaround: Use lowercase only for known rogues.

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

  Workaround: None.

- CSCsl11236—A servlet exception error occurs when changing some 802.11b/g parameters.

  Workaround: None.

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

  Workaround: None.

- CSCsl36016—When you apply a guest user template from a Cisco WCS running 4.2.62 to a WLC running 4.2.61 or 4.1.185, the following error message appears, even though the profile is configured correctly on the controller (with web auth enabled):

```
Please verify selected profiles exist on the controller. Please verify selected
profile has web-auth enabled.
```

Workaround: None.

- CSCsl38408—After resizing a map, the Map Editor does not exit.

  Workaround: None.

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

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

- CSCsl39335—Cisco WCS fails to start. When there is a conflicting port in use, Cisco WCS fails to start and displays the error message *Failed to start WCS Server*. Cisco WCS should display the list of conflicting ports as a reason for failure.

  Workaround: Go to WCS/webnms/logs/wcs-0-0.log on your hard disk and look for the conflicting ports.

  In Windows XP and Windows Server 2003, you can type **NETSTAT -O** to get a list of all the owning process IDs associated with each connection.

  Look in the Task Manager for the respective PID and stop the process using the required port.

- CSCsl40179—On the Cisco WCS GUI, *Tenet_password* is misspelled for the CSV file under Add autonomous access points.

  Workaround: None.

- CSCsl57546—When Cisco WCS displays a rogue device, the detecting access point is displayed by IP address or name depending on how the rogue was detected.

  If Cisco WCS discovers the rogue via a poll, it uses the MAC address of the access point for the access point name. If Cisco WCS learns about the rogue from a trap received from a wireless LAN controller, it uses the real access point name instead.

  Workaround: None.

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

  Workaround: Configure these options from the controller directly.

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

  Workaround: Remove the location server and add it back.

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

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

- CSCsl79599—When you add access lists or WLANs in Cisco WCS, unfounded messages are produced.

  Workaround: Contact Cisco support to determine which database queries can fix the entries.

- CSCsl80359—The guest user account template status does not show correctly.

  Workaround: Check WLC and WCS to see if the account status is the same. If not, reapply the template.

- CSCsl82286—TFTP transfers fail when the TFTP server is not located on the same drive as Cisco WCS.

  Workaround: None.

- CSCsl89809—A UDI Common-1 error is displayed when clicking Restore WCS Values after auditing a controller.

  Workaround: None.

- CSCsm03250—Location logs are not updated when you download logs from Cisco WCS.

  Workaround: Download the location logs manually from the location appliance using the Cisco WCS GUI.

- CSCsm04809—The Cisco WCS radio utilization report shows zero values or incorrect information.

  Workaround: None.

- CSCsm04906—If you specify certain search options and save them, the saved options are not retained when the search is revisited.

  Workaround: None.

- CSCsm17395—Cisco WCS access point rogue location information/report is not accurate. When you look at rogue clients through Cisco WCS, the access points that detected the rogue client might not be indicated.

  Workaround: Check the rogue clients listed directly on the controllers by clicking **Monitor > Security > Rogue Clients** and search using Cisco WCS Controllers. To determine which access points detected the rogue, click on the rogue access point in the list. If the rogue client was detected by a location server, the rogue client's location is indicated.

- CSCsm30661—The Config Group Apply report shows an incorrect number of templates in the config group.

  Workaround: Choose each applicable template individually to add to the config group.

- CSCsm33619—In WCS release 4.2.62.0 under Monitor > Clients, when you perform a quick search or new search, the location information for the client does not appear. If you go to the map where the client's access point is located, the client shows as located by the location server.

  Workaround: Go to the map where the client's access point is located, and the client shows as located by the location server.

- CSCsm50334—If a guest user template (or any other template) fails, the error message is too limited. The failure may be lack of space, but you cannot determine this from the error message.

  Workaround: None.

- CSCsm53129—The 1310 access point with a 2506 antenna shows an incorrect heatmap on the large outdoor map.

  Workaround: None.

- CSCsm66780—If you create a WLAN with an ACL but no rules added, an SNMP error occurs.

  Workaround: None.

- CSCsm70525—When you add new access points to a map or change the position of access points on a map, the map is shrunk so much that it no longer matches the access points that are already in place. You then cannot place new access points or reposition them because the map does not reflect the actual arrangement.

  Workaround: None.

- CSCsm75896—When you audit WLC from WCS, you get an error message after attempting a restore configuration, if extra or missing standard signatures exist on the WLC that are not in the WCS database.

  Workaround: None.

- CSCsm79472—WCS does not back up prior to an auto upgrade.

  Workaround: Manually back up the database.

- CSCsm80253—If client troubleshooting encounters a DHCP failure, the error message is not clear.

  Workaround: None.

- CSCsm80303—The Summary page of the Client Troubleshooting window shows all stages in green, even if 802.1x authentication failed. If 802.1x authentication failed, it should appear as red while the other stages remain gray.

  Workaround: None.

- CSCsm87034—WCS release 4.2.62.11 displays a square cutoff heatmap for a mesh deployment consisting of the 1522 access point for an outdoor environment.

  Workaround: If you modify the bin size in the default outdoor calibration model, you may see a slight improvement, but the coverage may still be inadequate.

- CSCsm93352—The validity date range for PAC upload via FTP is not synchronized with the WLC validity dates.

  Workaround: None.

- CSCsm96146—The coverage threshold alerts in WCS are displayed incorrectly.

  Workaround: None.

- CSCsm96761—The Client Association report shows every record twice.

  Workaround: None.

- CSCsm98102—The controller list query used when applying a TACACS+ template is wrong.

  Workaround: None.

- CSCsm98667—Two copies of the same search are sometimes created.

  Workaround: None.

- CSCsm99598—When you choose **Download ID Certficate** from the Configure > Controller > Security > ID Certificate window, a blank page is given. The certificate download does not occur.

  Workaround: The ID certificate can be downloaded from the controller.

- CSCsm99634—If you have eight WLANs created on the controller and then try to add the WLAN template to WLC, you should get a warning message that you have added more WLANs than allowed. Also, an asterisk should appear if more WLANs are supported.

  Workaround: None.

- CSCsm99644—The restore cold start trap option is not working. The controller restarts, but the trap is not sent to WCS, and the changes made before the restart are not retained in WCS.

  Workaround: None.

- CSCsm99662—If you choose **Network Access Control** (under Controller Template > Security), you can enter an invalid server IP without getting a warning message.

  Workaround: None.

- CSCsm99726—An 802.11b template created on WCS can successfully load into WLC but returns an error message on WCS. The error message is “SNMP operation to device failed: Attempt to set conflicting attribute value.”

  Workaround: None.

- CSCso16220—If you download WLC software as an administrator or super user from the controller list page, you receive a permission denied error.

  Workaround: If you perform the same function by navigating to Configure > Controller > Commands > Download Software, there is no issue.

- CSCso16846—After you create a guest LAN template, Internet Explorer displays a page error.

  Workaround: Click **OK** to close the error. It does not affect funtionality so it can be ignored.

- CSCso19170—After restoring data, the FTP root folder does not match the settings in ftpd.conf. You will not be able to log in to the FTP server if the folders do not match.

  Workaround: Reset the location-ftp-user by using the %WCS4.2.79.0%bin\ command.

- CSCso32118—When adding controllers running WLC software release 4.0 or earlier to WCS 4.2.81.0, an object not found error is received.

  Workaround: The error does not occur in software release 4.2.62.11.

Resolved Caveats

These caveats are resolved in Cisco WCS 4.2.81.0:

- CSCsh95569—During the Web Auth file download, the JSP file is now reflected properly.
- CSCsi59575—The columns in the exported reports (such as Inventory Reports) are now in the correct format.
- CSCsj56796—The erratic “configuration is different on the device” message now only appears when the situation warrants it.
- CSCsj59749—The color map behind the location of the rogue access point icon now appears correctly on the heatmap.
- CSCsk02071—The “error in getting data from server. Make sure you have connectivity and server is UP” message no longer appears while loading a CAD file in Maps.
- CSCsk08823—On WCS version 4.1.91.0, the profile name (WLAN ID) is now retained when you forward a MAC filtering template with four or more MAC addresses multiple times.
- CSCsk27148—The old backup files are now deleted from WCS.
- CSCsk31447—The administrator error no longer displays when an administrator cancels an access point audit.
- CSCsk31842—WLC version 4.0 now joins WCS with a NAT/PAT employed.
- CSCsk49569—WLAN SSIDs and profiles are no longer mismatched after you apply access point templates for specific WLANs (under access point radio WLAN override).
- CSCsk51302—The “object switch does not exist” error does not appear when you click on Client Troubleshooting in Monitor > Clients.
- CSCsk51549—The Cisco Compatible Extensions version 5 client radio receive sensitivity data rate is now correct when performing a search for associated clients with Monitor > Clients.
- CSCsk52999—The severity of access point displays correctly.

- CSCsk55160—If you switch between perimeter and rectangle in the planning mode tool, the coverage area appropriately adjusts, and the message above the radio buttons appropriately updates.
- CSCsk56441—Changes made to the WLC or access points are now updated in the database and reflected in WCS.
- CSCsk70270—Cisco WCS now has AAA (TACACS or RADIUS) debugs.
- CSCsk70905—You can now create a configuration group on Cisco WCS and make changes in the channel and DCA radio channel without getting an error.
- CSCsl00148—The scheduled guest user account status now updates properly.
- CSCsl03053—Client utilization in the station information table now considers both wired as well as 11n clients.
- CSCsl04475—Configuration group templates can be applied to wireless LAN controllers.
- CSCsl17609—The appropriate client traffic statistics are now showing under Monitor > Clients.
- CSCsl24456—The Busiest Client report now displays the appropriate values for throughput, TX, RX, and utilization.
- CSCsl28412—When you mark a critical alarm as known, it now stops sending future e-mail notices.
- CSCsl28793—The portal option is removed from WCS logging.
- CSCsl28879—If you add the DNS host name address (such as sj.cisco.com) on the virtual interface of the controller using WCS, the "Please reset the system for the change to take effect" message now appears.
- CSCsl34472—All digits are retained in the Lifetime field when you add guest users from a CSV file.
- CSCsl34500—You can add Guest users with a CSV file without failure.
- CSCsl38435—When you edit the AAA mode in Cisco WCS, the *Fallback on Local* option correctly portrays the RADIUS and TACACS+ modes.
- CSCsl42358—A quick search for access points on Cisco WCS now displays valid results with partial entries.
- CSCsl56206—When you add AutoCAD .dwg drawing as a map into WCS, the image is no longer blurry.
- CSCsl57317—Cisco WCS template now holds the sort value when advancing screens. When you use Cisco WCS to view a MAC address filter template in a sorted order, advancing to the next screen of MAC addresses maintains the sorting order.
- CSCsl62573—The access point filter from the heatmap with 802.11b/g/n now shows all clients.
- CSCsl67268— The heat map displays all access points, regardless of the radio type, when you use access point filters with 802.11b/g/n.
- CSCsl75176—The access point heat map is properly generated and displayed.
- CSCsl76595—The appropriate alarm displays on the security page after deletion.
- CSCsl76604—In the Cisco WCS Linux version, you can now import a CAD file using the Map Import Floor feature without introducing artifacts not shown in the original CAD drawing.
- CSCsl76945—Cisco WCS now applies a MAC filter template to a controller when the interface is set to none.
- CSCsl77656—Cisco WCS displays only one instance of the controllers after pushing out a template.
- CSCsl79809—The Cisco WCS RRM template does not turn off the automatic transmit power setting.

- CSCsl85320—Cisco WCS e-mail alerts now contain the controller name for the TRAP message.
- CSCsl85479—Client troubleshooting on Cisco WCS now works for clients on wireless LAN controller release 4.1.185.0.
- CSCsl86349—Now only specified values are provisioned when you apply the access point template.
- CSCsl90553—Cisco WCS renaming of CPU ACL templates now works.
- CSCsl91585—Monitor > Alarms eliminates alarms when quick search is performed.
- CSCsl94720—The Retransmit timeout setting is now the same on Cisco WCS and the controllers.
- CSCsm01769—After you restore the database, WCS does not hang.
- CSCsm13333—Commas are now allowed in the Cisco WCS keyadmin.bat file.
- CSCsm15535—You can now add autonomous access points to a Cisco WCS when the access point's configuration includes an snmp-server location string with more than 80 characters.
- CSCsm16356—You can now apply and delete multiple templates.
- CSCsm21026—Floors, buildings, and maps are retained on the Monitor > Maps page. Also, you can now access the whole floor, building, or map.
- CSCsm30661—Templates appear in the report after you apply a configuration group. If you select all templates from a controller and add them to a configuration group, the number of templates in the report and in the configuration group are the same after you apply the configuration group.
- CSCsm87436—When you have 3 TACACS+ servers of the same type configured, you can now edit and apply TACACS+ Templates to WLC without receiving an error.

If You Need More Information

If you need information about a specific caveat that does not appear in these release notes, you can use the Cisco Bug Toolkit to find caveats of any severity. Click this URL to browse to the Bug Toolkit:

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

(If you request a defect that cannot be displayed, the defect number might not exist, the defect might not yet have a customer-visible description, or the defect might be marked Cisco Confidential.)

Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at the following location:

http://www.cisco.com/tac

Click **Technology Support**, select **Wireless** from the menu on the left, and click **Wireless LAN**.

Related Documentation

For information on the Cisco Unified Wireless Network Solution and for instructions on how to configure and use the Cisco UWN, refer to the *Cisco Wireless Control System Configuration Guide* and the *Cisco Wireless LAN Controller Configuration Guide.*

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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