Release Notes for Cisco Wireless Control System 4.1.92.0 for Windows or Linux

March 3, 2008

These release notes describe open caveats for the Cisco Wireless Control System 4.1.92.0 for Windows or Linux, which comprises part of the Cisco Unified Wireless Network Solution (Cisco UWN).

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

Contents

These release notes contain the following sections.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco Unified Wireless Network Solution Components

The following components are part of the Cisco UWN Solution and are compatible in this release:

- Operating system (Wireless LAN Controller and Cisco Aironet Lightweight Access Point)
- Cisco Wireless Control System (Cisco WCS) software release 4.1.92.0.
- Cisco Wireless Control System Navigator software release 1.0.90.
- Location appliance software release 3.0.42.0
- Cisco 2700 Series Location Appliance
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 4100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Catalyst 3750G Wireless LAN Controller Switches
- Cisco Wireless Services Modules (WiSMs) for Cisco Catalyst 6500 Series Switches
- Cisco WLAN Controller Network Modules for Cisco Integrated Services Routers
- Cisco Aironet 1000, 1100, 1130, 1200, 1230, 1240, 1310, and 1500 Series Lightweight Access Point
- 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.

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 3000 Cisco Aironet lightweight access points and 750 Cisco wireless LAN controllers.
  - 3.15 GHz Intel Xeon Quad processor with 8-GB RAM and 200-GB hard drive.
  - 80-GB minimum free disk space on your hard drive.

  The following operating system is supported:

  - Windows 2003/SP1 and SR2 with all critical and security Windows updates installed. 64-bit installations are not supported.

    Note SP2 is not supported at this time.

Note Cisco WCS is supported only on English or Japanese versions of the Windows 2003 operating system. Even though Japanese locale browsers are supported, non-ASCII characters are not. 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.

- Red Hat Enterprise Linux Enterprise Server 4.0 or Advanced Server 4.0. Only 32-bit OS installations are supported. 64-bit installations are not supported.
- Windows 2003 version support on VmWare ESX 3.0.1 version and above.

Note When running WCS on a dedicated VmWare server, these minimum hardware requirements are necessary based on WCS high-end server hardware specifications:

— Quad CPU running at 3.15 GHz
— 8 GBs RAM
— 200 GB 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.

- Standard Server
  - Supports up to 2000 Cisco Aironet lightweight access points and 500 Cisco wireless LAN controllers.
  - 3.2 GHz Intel Dual Core processor with 4-GB RAM and 80-GB hard drive.
  - 40-GB minimum of free disk space on your hard drive.

  The following operating system is supported:
  - Windows 2003/SP1 or later with all critical and security Windows updates installed. 64-bit installations are not supported.

Note Cisco WCS is supported only on English or Japanese versions of the Windows 2003 operating system. Even though Japanese locale browsers are supported, non-ASCII characters are not. 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.

  - Red Hat Enterprise Linux Enterprise Server 4.0 or Advanced Server 4.0. Only 32-bit OS installations are supported. 64-bit installations are not supported.
- Low End Server
  - Supports up to 500 Cisco Aironet lightweight access points and 125 Cisco wireless LAN controllers.
  - 3.06-GHz Intel processor with 2-GB RAM and 30-GB hard drive.
  - 30 GB minimum free disk space on your hard drive.

  The following operating system is supported:

– Windows 2003/SP1 or later with all critical and security Windows updates installed. 64-bit installations are not supported.

Note Cisco WCS is supported only on English or Japanese versions of the Windows 2003 operating system. Even though Japanese locale browsers are supported, non-ASCII characters are not. 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.

– Red Hat Enterprise Linux Enterprise Server 4.0 or Advanced Server 4.0. Only 32-bit OS installations are supported. 64-bit installations are not supported.

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 Internet Explorer 6.0 on 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 Cisco wireless LAN controllers.

Note 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 version by choosing Help > About the Software.

Upgrading to a New Software Release

In order to be compatible, the Cisco WCS release must be at least the same release or a later release than the software release running on the controller. For example, Cisco WCS running release 4.0 cannot manage a controller running release 4.1. If an upgrade is planned, upgrade the Cisco WCS first to eliminate any unexpected issues. Cisco WCS supports database upgrades only from the following official Cisco WCS releases:

- 3.2.23.0
- 3.2.25.0
- 3.2.40.0
- 3.2.51.0

- 3.2.64.0
- 4.0.43.0
- 4.0.66.0
- 4.0.81.0
- 4.0.87.0
- 4.0.96.0
- 4.1.64.0
- 4.1.83.0
- 4.1.91.0

Important Notes

This section describes important information about Cisco WCS.

Cisco WCS Upgrade

The following notes have been added to the "Upgrading WCS" section on page 11-14 of the *Cisco Wireless Control System Software Configuration Guide*.

Note Scheduled task settings are not preserved when you upgrade from WCS 4.0 or earlier releases. Make sure to record your settings manually if you wish to retain them or go to Administration > Background Tasks after starting WCS to check or change the settings as necessary.

Note If you upgrade to a WCS software release later than 4.0.87.0 from a release prior to 4.0.87.0, the users, user groups, tasks, and user passwords do not migrate. Upgrading to 4.0.87.0 before upgrading to a later release migrates the users, user groups, tasks, and user passwords.

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.

802.11n

802.11n radios are not supported for use with Cisco WCS 1.0.90.0. These radios will be supported in a future Cisco WCS release. Please disregard any 802.11n-related parameters that appear on the GUI pages for this release.

IPSec Not Supported

Software release 1.0.90.0 does not allow you to choose IPSec as a Layer 3 Security option. None and VPN Passthrough are the only available options. If you upgrade to this release from a previous release that supported IPSec as a Layer 3 Security option, any WLANs that are configured for this feature become disabled. If you want to configure IPSec, you must use a version of controller software prior to 3.2 or wait for a future release.

Compatibility

This release of Cisco WCS for Windows or Linux is compatible with wireless LAN controller and Cisco Aironet lightweight access point release 3.2.78.0 or later. Previous releases of Cisco WCS should not be used with the 4.1.171.0 controller software release.

For compatibility issues with the location server, refer to the *Release Notes for Cisco 2700 and 2710 Location Appliances for Software Release 3.0.37.0* at this location:

http://www.cisco.com/en/US/docs/wireless/location/2700/release/notes/larn3037.html.

Note You may experience compatibility issues if you add a controller with a newer release than the WCS release. For example, 4.1.171.0 controller software release should not be added to WCS 4.0.

Recovering the WCS Password

You can change the WCS application root user or FTP user password. This option provides a safeguard if you lose the root password. An executable was added to the installer /bin directory (passwd.exe for Windows and passwd.sh for Linux). Follow these steps to recover the passwords and regain access to WCS.

Note If you are a Linux user, you must be the root user to run the command.

Step 1 Stop WCS.

Step 2 On a Windows operating system, change to the WCS bin folder. (Linux does not have a WCS bin folder.)

Step 3 Perform one of the following:

Enter **passwd root-user <newpassword>** to change the password on the root account for WCS (not the root account for access to the operating system on which WCS is running). The *newpassword* is the root login password you choose.

or

Enter **passwd location-ftp-user <newuser> <newpassword>** to change the FTP user and password. The *newuser* and *newpassword* are the FTP user and password you choose.

Step 4 The following options are available with these commands:

- -q — to quiet the output
- -pause — to pause before exiting

- -gui — to switch to the graphical user interface
- -force — to skip prompting for configuration

Step 5 Start WCS.

Restoring Data

To restore data that is larger than 8-GB unzipped from a WCS version prior to 4.1, the restore requires the following steps.

Step 1 From the command prompt, change to the WCS4.x\bin directory.

Step 2 Enter **dbadmin.bat -gui -largedb restore**. The usual restore database screen appears.

Proceed as you would normally for a restore. Refer to the Performing Maintenance Operations chapter of the *WCS Software Configuration Guide* for those instructions.

Caveats

This section lists Open Caveats and Resolved Caveats in Cisco WCS 4.1.92.0 for Windows and Linux.

Open Caveats

These caveats are open in Cisco WCS 4.1.92.0:

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

  Workaround: None at this time.

- CSCsd07119—Applying a template to a controller results in the error message "SNMP operation to device failed" with no additional explanation. This happens if the template contains parameters that are incompatible with other configuration settings on the controller.

  Workaround: To determine which template parameters are causing the problem, use controller GUI to make the same configuration change. The controller GUI will return a specific error message indicating the problem. Then, either correct the template being applied, or modify the controller settings so that the template can be applied without errors.

- CSCse42296 —If a WLAN template already exists in WCS, it is not updated when you modify the WLAN settings on the controller.

  Workaround: Use WCS to make changes to the WLAN settings and then apply these changes to all controllers.

- CSCse94732—There is a WCS and controller template mismatch while configuring CCKM and 802.lx.

  Workaround: When the template is entered, the user will be able to see the CCKM and 8021.x.

- CSCsg23691—Some columns in the printed report table are missing when using a portrait page orientation.

  Workaround: The page orientation must be set to "Landscape" to print the reports correctly.

- CSCsg75318—There are anomalies with the search feature.

  Workaround: Every search can be created new. If a search is saved, selecting it again and applying the search should help.

- CSCsg92667—When you change the country code on the controller, a trap is generated and sent, and the trap log is updated in the controller. WCS however does not update the alarm entry.

  Workaround: None at this time.

- CSCsh34273—When configuring a controller template in WCS, there is an option for enabling external policy server failure. Enabling this option does not have an impact on the controller because it is not supported in the latest version of the controller software. This option is available only for backward compatibility.

  Workaround: None at this time.

- CSCsh40682 —In the Maps page (Monitor > Maps), old names still show because the name hierarchy does not get updated.

  Workaround: None at this time.

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

  Workaround: None at this time.

- 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. In the Client Details page, select **Troubleshoot** from the Command drop-down list 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.

- CSCsh51052—Extra dots appear in the bridge group name. There is a '...' extension to the bridgegroup Name appearing in one of the screens in WCS. This does not affect any change on configuration applied to the controller.

  Workaround: None at this time.

- CSCsh67523—When you choose Configure > AP Templates > 802.11a Parameters or 802.11b Parameters, the list of channel numbers should only contain those that are valid for the specified country code rather than the complete list.

  Workaround: None at this time.

- CSCsh71088—When changing the L2 security setting for a WLAN from None to CKIP and applying the changes to the controller, WLAN becomes disabled. This happens only the first time you change the L2 security setting from None to CKIP. There are no problems in subsequent edits.

  Workaround: Change the L2 security setting for the WLAN back to None and then to CKIP again.

- CSCsh71519—AN SNMP error message appears during image transfer from WCS to a controller stating that the transfer failed, even though the transfer was successful. This happens if the boot break is enabled on the controller. When the boot break is enabled, the controller reboots at the end of the installation process and waits during the boot process for user input. WCS cannot

communicate with the controller at this point, and it times out after several attempts to communicate with the controller. WCS cannot verify a successful software installation and it cannot contact the controller, so it reports an upgrade failure. The failure message is partially accurate because the installation has not been completed. However, provided nothing else went wrong during the installation, all that needs to be done to rectify the problem is to log into the controller and prompt it to continue to boot.

Workaround: Log into the controller and prompt it to continue to boot.

- CSCsh73488—When applying a controller template for web authentication with the web authentication type set to External, an SNMP error occurs on WCS ("SNMP operation to Device failed").

  Workaround: Apply the settings directly on the controller instead of using WCS.

- CSCsh75401 —Create a local EAP profile in WCS, but do not apply it to the controller. Then create a WLAN template, apply this EAP profile, and apply the template to the controller. The operation fails, but WCS creates the WLAN in its database.

  Workaround: None at this time.

- CSCsh80122—WCS access point templates push the same information to all access points (MAPs or RAPs) in the mesh environment.

  Workaround: After the template is configured, all access points may change to the same applied role. If so, the values should be changed via individual controller pages.

- CSCsh80451 —If by mistake you download a 2006 image to a 2106 controller, WCS does not validate properly and displays a message indicating that there was a failure while storing in Flash, which is misleading because it appears as a space issue when it is not. The CLI displays the correct message stating that the image version has a mismatch, but both the controller GUI and WCS mention Flash.

  Workaround: Before downloading an image, make sure that the image and the controller are of same type (same series).

- CSCsh80858 —While modifying an active CPU ACL using WCS, inserting a rule may break the connectivity between WCS and the controller.

  Workaround: To recover connectivity, run the following command from the controller CLI:

  config acl cpu none

  Then reapply the ACL template to the controller using WCS.

  Doing this may temporarily open all traffic to the CPU until the ACL is reapplied. In the worst case scenario, you may need to connect to the controller's console port to recover access.

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

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

- CSCsh81859—An "unknown exception" error is occurring when a user tries a 4.1 (or later) WCS feature on an older release WLC. A new message needs to be added for unsupported features.

  Workaround: None at this time.

- CSCsh83030—WCS allows you to delete the local EAP profile even if it is associated to a WLAN.

  Workaround: None at this time.

- CSCsh83341—While adding access points to maps, the user cannot select multiple access points from different pages.

Workaround: The user can select a section of access points from within each page rather than access points from all pages.

- CSCsh83615 —When you enable CDP on access points using access point templates with the condition that global CDP on the controllers is disabled, the following counterintuitive error message is displayed:

  ```
  Partial failure error: provision failure: Mediation-1, attempt to set conflicting
  attribute value,Lrad,cdpEanble,Lrad!...
  ```

  Also, if you enable CDP from the Access Points page (Configure > Access Points) after selecting an access point, the following error message is displayed if global CDP is disabled:

  ```
  snmp operation to device failed, attempt to set conflicting attribute value.
  ```

  Workaround: Enable or disable CDP on all access points from the controller template first.

- CSCsh90008—A link is not drawn between parent and child. A directional arrow is seen from child to parent, but the link is not drawn.

  Workaround: None.

- CSCsh90255—If the list of access points is large, WCS does not display the list properly.

  Workaround: Use a filtering criteria to minimize the number of access points in the list.

- CSCsh95569—During the Web Auth file download, the JSP file is not reflected properly.

  Workaround: None at this time.

- CSCsh97436 —An error page appears while performing concurrent access point list functions:

  1. Go to the All Access Points page (Configure > Access points).
  2. Select unassociated access points.
  3. Select the **Remove APs** command from the drop-down list.
  4. Click **GO**.
  5. From another WCS browser instance, try to refresh the All Access Points page or sort the list.

     WCS displays an error page.

  Workaround: Execute the **Remove APs** command without having a second browser instance open.

- CSCsh97506—WCS takes a long time (30 minutes or more) to detect that a controller is unreachable. This problem can occur in a network containing a large number of controllers, especially if many controllers become unreachable at once. This can happen if WCS loses connectivity to part of the network.

  Data collection tasks rely on the device status background policy to indicate whether or not a controller is reachable. If device status indicates that the controller is not reachable, then data collection tasks bypass the controller. However, if the controller is reachable, data collection attempts to get the MIB information from the controller using SNMP.

  If the controller is marked as reachable when it is not, data collection tasks attempt to get the MIB information and will have to wait for the SNMP timeout before it moves to the next controller. This can slow down data collection significantly.

  Currently, the device status policy which detects whether or not controllers are reachable cannot run simultaneously with data collection tasks. If many data collections are queued up to run, device status runs after all of them. If many controllers are not reachable, these tasks will take a long time to complete, and the device status will not change to unreachable until all collections have had a chance to run.

Workaround: Either wait for the status to be updated to unreachable, or temporarily disable all data collection background tasks, and once the status is updated, re-enable the tasks.

- CSCsi00372 —Time scale is off in the Unique Clients report.

  Workaround: None at this time.

- CSCsi04160 —In the All Access Points page, selecting **Copy and Replace AP** from the command drop-down list and clicking **GO** does not copy the AP Static IP and AP Group Name values to the new access point.

  Workaround: Enter the AP Static IP and AP Group Name values for the new access point manually.

- CSCsi08786—If you do not select a Config Group entry while applying a template, WCS should warn you to select at least one configuration group.

  Workaround: None at this time.

- CSCsi12492—Phantom templates are created under Config Groups in WCS due to a sync-up issue between WCS and controllers. These templates cannot be removed from WCS and prevent you from creating new templates with the same name.

  Workaround: Remove the guest user template entries in the guestusertemplate table.

- CSCsi14940—When attempting to save an ACL template, an invalid error message displays.

  Workaround: If "Other" is needed for Source or Destination, choose that option only and click **Save** after entering the values.

- 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 WCS to keep the controller and WCS in sync.

- CSCsi17397 —The guest user template activation fails on the controller after a database restore. This happens if the controller and WCS databases are not in sync after the restore.

  Workaround: Before editing the GuestUser template in WCS and reapplying it on the controller, make sure that the WLAN template associated with the GuestUser template is present on the controller. If the WLAN template is not present on the controller, reapply the template.

- CSCsi17755—Due to the early daylight savings, manually changing the time on the location server adversely changes the time of the actual appliance.

  Workaround: If the time is not changed on the system manually, the correct daylight savings time will be displayed and used by both WCS and the location server.

- CSCsi18071 —When communication is interrupted to the controller, the message that WCS displays does not provide enough details for understanding the problem. This happens when the traffic between the wireless controller peers are lost because a peer controller is down or is having a network problem.

  Workaround: None at this time.

- CSCsi18369—If a known rogue access point does not send authenticated beacon or probe responses, a message log appears stating that the known rogue is instead an impersonator.

  Workaround: None at this time.

- 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, the user must verify that the associated interface exists on all the controllers.

- CSCsi21064—The Chokepoint Heatmap does not resize when zoomed in or out.

  Workaround: None at this time.

- CSCsi21344 —New daylight savings times are not recognized by WCS, making times in reports off by an hour.

  Workaround: On Windows hosts, try http://www.novell.com/coolsolutions/tools/18674.html to fix the problem.

- CSCsi23198—The search for tags is inaccessible.

  Workaround: This only occurs on Firefox. The user can use IE 6.x and above.

- CSCsi24959—WCS displays an "invalid attribute" error message when you apply a WPA-PSK SSID using WPA1+WPA2 with TKIP with a 7-character password.

  Workaround: Use passwords that are more than 7 characters long.

- CSCsi28571—The graph does not display unless there are more than two data points.

  Workaround: None at this time.

- CSCsi29550—After a restore, WCS truncates six days worth of data. Only the data from the final day appears.

  Workaround: None at this time.

- CSCsi30502—The SNMP Community template with a disabled status gets stored in the controller as enabled. This happens when the SNMP Community template with a disabled status gets applied on multiple controllers.

  Workaround: Go to the individual controller page and disable SNMP configuration.

- CSCsi31142—If you try and create an access point template that has the access point mode set as REAP along with H-REAP configuration having VLAN support enabled and VLAN assigned, you will get a failure message from WCS when attempting to apply the template to the access point.

  Workaround: First push a template to the access point with the access point mode set to REAP. Then push another template to the same access point with the appropriate H-REAP configurations.

- CSCsi35766—Setting symmetric mobility on earlier versions of the controller software does not throw an error when applying the controller template, even though symmetric mobility was not supported.

  Workaround: 1) Apply the controller template without having symmetric mobility to all controllers. 2) Go to the configuration page for the controller running the current version of the software and enable symmetric mobility as needed.

- CSCsi44610—The SSIDs for probing clients occasionally appears blank.

  Workaround: None at this time.

- CSCsi46047—The CDP template on the WCS for controllers displays Disabled by default.

  Workaround: The user can modify the template accordingly.

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

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

- CSCsi46367—The location history page does not display any information beyond the first item.

  Workaround: The user can click the history item individually to receive the required information.

- CSCsi47361—Saving the CDP template may lead to a page error.

  Workaround: None at this time.

- CSCsi48157—Clicking the 802.11a link in the WCS displays the 802.11b/g radio properties instead of the 802.11a radio details.

  Workaround: None at this time.

- CSCsi48189—CDP templates should show valid messages for stacked controllers.

  Workaround: None at this time.

- CSCsi50097—Clients cannot connect to a PSK-enabled WLAN created from WCS. However, clients can connect to a similar WLAN created from the controller GUI.

  Workaround: Do not enable PSK, or create the PSK-enabled WLAN from the controller GUI.

- CSCsi54995—Rogue auto contain needs to change to rogue adhoc auto contain in rogue alarm notifications.

  Workaround: None at this time.

- CSCsi59319—When you log into WCS after a restore, a message appears about establishing a strong password. The message does not provide the UI navigation to make the change.

  Workaround: None at this time. Click your username in the upper-right corner of the GUI to change your password to comply with the local password policy.

- CSCsi60306—Voice TSM graphs should show downlink graphs only. Uplink data should come from the voice clients. The uplink packet loss rate is incorrectly showing a value.

  Workaround: None.

- CSCsi60314—The Mesh Worst SNR Links Report shows root access points with a 0 signal-to-noise ratio (SNR).

  Workaround: None at this time.

- CSCsi61692—If you click on Print View from the Network Summary page and then exit the preview, you receive an error.

  Workaround: Hitting refresh resolves the issue.

- CSCsi63939—The chokepoint definition is not retained after a fresh install and synchronizing with location.

  Workaround: None at this time.

- CSCsi73823—The radio count is computed incorrectly. It calculates the number of active clients for that building rather than the radio count.

  Workaround: None at this time.

- CSCsi79716—A confirmation message does not appear when you change user credentials on the User: Detail page.

  Workaround: None at this time.

- CSCsi79827—A 0% complete status appears when you select a template (but not a controller) and click **Apply** during the creation of a config group. No notification tells you that the task did not go through and no reason is provided as to why it was not successful.

  Workaround: Make sure you select the template and the controller before you click Apply.

- CSCsi80913—If you try to create more than 16 WLAN templates and apply them to the controllers, an error message should appear that tells you that the maximum number of WLAN templates to support is 16.

  Workaround: None at this time.

- CSCsi84233—An invalid message regarding security settings pops up when modifying a WLAN template but not changing the session timeout, even though security settings have not been changed.

  Workaround: Change the session timeout to fall between the 300 and 86400 values and then modify the timeout with the controller GUI.

- CSCsi84683—The Client Association Report in WCS release 4.1 fails to provide client details, and the following message appears: “The specified criteria did not match any data for the report. Please modify the criteria.”

  Workaround: None at this time.

- CSCsi85697—The Message section of the rogue alarm incorrectly reports the number of access points detected. When you request the detecting access points or map levels, a pop-up message reports that the rogue is currently not detected by any radios.

  Workaround: None at this time.

- CSCsi86589—When you apply an Outdoor Calibration model to an outdoor area, Cisco WCS asks you to choose floors and does not show any outdoor areas to be selected.

  Workaround: There is no workaround for outdoor areas that have already been created in WCS. However, you can choose the calibration model when you create a new outdoor area.

- CSCsi87533—After you install WCS, any attempt to restore the database fails.

  Workaround: Reboot the server after the WCS installation is complete and the Windows server has been rebooted. Then stop WCS, restore the database, and restart WCS.

- CSCsi88472—If you enter an invalid DHCP lease time, the error message should state the valid range for the attribute.

  Workaround: None at this time.

- CSCsi88946—The wrong hex key validation is used in WPA.

  Workaround: None at this time.

- CSCsi89307—If you click **Configure** > **Access Points** in WCS release 4.1 and then do a quick search for an access point, the access point details appear when you click the link for that access point. However, you are unable to configure the access point from this page.

  Workaround: Use the advanced search feature to access the correct page.

- CSCsi89978—If you add controllers from one mobility group to another new mobility group, the WCS message says the “object already exists.” A more meaningful message should be created.

  Workaround: None at this time.

- CSCsi92281—The tag box of the Layers window used when opening a floor map is not working as expected.

  Workaround: None at this time.

- CSCsi94155—The Item per Page feature on the Monitoring > Clients page does not work properly in WCS release 4.1. Instead of displaying the configured number of items per page, WCS lists all of the items on the same page.

  Workaround: None at this time.

- CSCsi95122—If you configure WCS for Location Notification alerts, the email notifications (such as a tag panic button emergency) are not dispatched. The alarm console displays the critical alarms, but the email notification is not sent.

  Workaround: Make these modifications to fix the issue:

  1. Change *Alert.categoryName.3=Location Notification* to *Alert.categoryName.3=LBSNotify* in the <wcs>/webnms/classes/com/cisco/server/resources/EventResources.properties file.
  2. Change *faultmanagement.emailConfigList.categoryName.Location_Notification=Location Notifications* to f*aultmanagement.emailConfigList.categoryName.LBSNotify=Location Notifications* in the <wcs>/webnms/webacs/WEB-INF/classes/com/cisco/webui/resources/MonitorResource.properties file.
  3. Login and go to https://<wcs>/webacs/pages/admin/dbupdate.jsp and type the following SQL command: **delete from wcsdb.modb.AlarmEmailFilter where categoryName='Location Notification".**
  4. Restart WCS.

- CSCsi95289—The guest users created by the lobby ambassador are not displayed correctly in WCS. The counter of guest users per page is incorrect, and you cannot find the newly created guest user through WCS even though it shows up in the WLC.

  Workaround: None at this time.

- CSCsj01432—If the quick search function is used to find rogue access point alarms, the resulting page provides the wrong search string. Instead of returning rogue access point alarms that match the rogue access point MAC address, all rogue alarms are displayed.

  Workaround: You can filter manually using https://WCSSERVERwebacs/searchAlarmAction.do?severity=10&searchType=rogueAPMac&entity=MACOFAP.

- CSCsj01490—If you try to disable global Cisco Discovery Protocol (CDP) and apply the template to a controller that has no access points connected, the following error message appears: "SNMP operation to Device failed: Attempt to set conflicting attribute value." However, the message should indicate that CDP cannot be disabled on all access points when no access points are connected to the controller.

  Workaround: None at this time.

- CSCsj05489—An unknown exception occurs if you try to create an outdoor area in a campus, provide the image file, and try to save WCS.

  Workaround: None at this time.

- CSCsj06218—WCS gives an unexpected internal error when you create an access point template and assign a name that already exists. The error should be more meaningful.

  Workaround: Avoid creating duplicate access point template names.

- CSCsj06607—An fdisk or similar error occurs when starting WCS.

  Workaround: Add **/sbin/** in the users Linux PATH, and the error disappears.

- CSCsj09208—WCS 4.1 left-hand panel for superusers group displays incorrectly. Also, when upgrading from 4.0.x to 4.1.x, the permissions for superusers group become corrupt. While the root user can still perform tasks, the superusers cannot and receive an "error on page" message.

  Workaround: You can get around this issue by following these steps:

  1. Log in as root.

2. Go to /webacs/pages/admin/dbupdate.jsp.
3. Copy and paste the SQL below and execute it:

```
delete from wcsdb.modb.usergroup_temptask where taskid = (select id from
wcsdb.modb.temptask where taskname = 'Configure Guest Users') AND
usergroupid in (select id from wcsdb.modb.usergroup where
usergroupname!='LobbyAmbassador')
```

- CSCsj16506—If you have a controller running 4.1.171.0 with an existing TACACS+ configuration and you attempt to apply it to other controllers in WCS 4.1.83.0, you get multiple occurrences of the same controller in the template.

  Workaround: None at this time.

- CSCsj17507—When you have TACACS+ enabled on WCS and log in with that account, the caller ID field does not fill in the IP address.

  Workaround: None at this time.

- CSCsj19609—If a user who belongs to the UserAssistant group logs into WCS, the user is unable to navigate to the **Configure > Controller Templates** window. The WCS displays *Permission Denied* so the user is also unable to navigate to **Security > Local Net Users**.

  Workaround: Navigate to **Configure > Controllers > Any Controller**. Navigate to **Security > AAA > Local Net Users** and execute command **Add Local Net User** from the command box. Click **To create a new Template for 'Local Net Users,' click here** to open the new template creation page.

- CSCsj24063—The access point BGN field appears blank after restoring the database from software release 4.1 to 1.0.90.1.

  Workaround: Click **Audit** to synchronize the data.

- CSCsj26844—WCS does not provide an error message in the **Monitor > Access Points** page.

  Workaround: None at this time.

- CSCsj27469—The Quick search alarm count does not match up with the alarm list shown. The Quick search alarm count should only include active alarms (not both active and inactive).

  Workaround: None at this time.

- CSCsj29057—WCS authentication to FreeRadius and SteelBelted Radius fails. The RADIUS servers return the correct attributes, but WCS rejects the authentication.

  Workaround: None at this time.

- CSCsj30700—When creating a new template for a wireless LAN including a new RADIUS server, the template fails to be applied. The error message states: "SNMP operation to Device failed. Attempt to set conflicting attribute value."

  Workaround: Apply the template a second time.

Resolved Caveats

These caveats are resolved in Cisco WCS 4.1.92.0:

- CSCsm70089—Apache Tomcat is the servlet container for JavaServlet and JavaServer Pages Web within the Cisco Wireless Control System (WCS). A vulnerability exists in the mod_jk.so URI handler within Apache Tomcat which, if exploited, may result in a remote code execution attack.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080130-wcs.

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