



Release Notes for Cisco Wireless Control System 4.1.83.0 for Windows or Linux

April 30, 2007

These release notes describe open caveats for the Cisco Wireless Control System 4.1.83.0 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 7](#)
- [Caveats, page 10](#)
- [Troubleshooting, page 21](#)
- [Related Documentation, page 21](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 21](#)



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

©2007 Cisco Systems, Inc. All rights reserved.

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 4.1.83.0.
- Cisco Wireless Control System Navigator software release 4.1.83.0
- Location appliance software release 3.0.37.0
- 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.

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 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 or later with all critical and security Windows updates installed.



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. 64-bit installations are not supported.



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 or later, 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 the same or a more recent release than the one on the controller. For example, you cannot have a 4.1 controller being managed by a 4.0 WCS. 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

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.

802.11n

802.11n radios are not supported for use with Cisco WCS 4.1.83.0. 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 4.1.83.0 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://ftp-sj.cisco.com/cisco/crypto/3DES/wireless/aironet/WLA/2700/LOC2700-L-K9-3-0-37-0-ReleaseNotes.pdf>.



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 Change to the WCS bin folder.

Step 3 Perform one of the following:

Enter **passwd root-user <newpassword>** to change the WCS root password. 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.

New and Changed Information

New Features

The following new features are available in WCS 4.1.83.0.



Note

Refer to the *Cisco Wireless Control System Configuration Guide*, Release 4.1.83.0 for details and configuration instructions for each of these features.

- LDAP database support—You can configure a Lightweight Directory Access Protocol (LDAP) server as a backend database for use with local EAP. The LDAP server is queried for the credentials (username and password) of a particular user and uses them to authenticate the user.
- Management frame protection (MFP) enhancement—MFP support is now available for CCXv5 client devices. In the previous 4.0 software release, only infrastructure MFP was available. MFP provides security for the otherwise unprotected and unencrypted 802.11 management messages passed between access points and clients. This release allows a client to detect a spoofed management frame at the first instance of an attack and generate an intrusion detection system (IDS) alert to the device interface.
- Access control list (ACL) enhancements—You can now apply an ACL to the controller central processing unit (CPU), or you can create reusable grouped IP addresses and protocols. An ACL is a set of rules used to limit access to a particular interface (for example, if you want to restrict a wireless client from pinging the management interface of the controller). With these reusable entities, mappings can be created and rules can be auto generated subject to the condition.
- Load-based call admission control (CAC) for VoWLAN—This feature allows lightweight access points and controllers to consider three additional variables when deciding how many voice calls to allow on the network: the bandwidth used by all traffic types, co-channel access point loads, and co-located channel interference. The access point accounts for these three new variables when determining if there is sufficient bandwidth to support a new VoWLAN call. Previously, only bandwidth-based CAC was supported.
- Symmetric mobility tunneling—Using this feature, a foreign controller now sends a Layer 3 roaming client's packet back to its anchor controller through EtherIP tunneling rather than through a dynamic interface. The source IP address of the packet designated for the client and the traffic source from the client take the same path in reverse direction.
- Guest N+1 redundancy and mobility failover—Mobility group members can now send ping requests to one another to check for data and control paths among them to find failed members and reroute clients. This functionality provides guest N+1 redundancy for guest tunneling and mobility failover for regular mobility. Guest N+1 redundancy allows detection of failed anchors. After a failed anchor controller is detected, all the clients anchored to this controller are deauthenticated so that they can quickly become anchored to another controller. This same functionality is also extended to regular mobility clients through mobility failover. This feature enables mobility group members to detect failed members and reroute clients.
- Expedited bandwidth requests—This feature enables CCXv5 clients to attach a priority to specific types of call requests, such as emergency 911 calls, or to specific devices that are tagged as high priority, such as a senior executive's call from an IP soft phone while on the road.

- **Workgroup bridge support**—Cisco Aironet autonomous access points operating in WGB mode can now associate to Cisco Aironet lightweight access points to provide an 802.11 wireless connection to wired devices. The autonomous WGB access point learns the MAC address of the wired client and then informs the lightweight access point and controller that the device is operating on the wireless network. This scenario provides transparent bridging for wired clients and secure roaming.
- **High-density support**—To optimize RF channel capacity and improve overall network performance in large multi-cell high-density wireless networks, this release introduces high-density (or pico cell) mode parameters. Using these parameters, you can manually specify global values for receiver sensitivity threshold, clear channel assessment (CCA) sensitivity threshold, and transmit power values across all registered access points.
- **Multiple country code support**—This release allows you to configure up to 20 country codes per controller. This multiple-country support enables you to manage access points in various countries from a single controller.
- **Local EAP**—Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users. Local EAP supports LEAP, EAP-FAST, and EAP-TLS authentication between the controller and wireless clients.
- **TACACS+ support**—Support for TACACS+ is included with this release. TACACS+ is a Cisco protocol that supports authentication, authorization, and accounting (AAA) of administrators. It authenticates administrators and specifies the commands that each administrator is authorized to run, such as show commands or configuration change enablement.
- **Cisco WCS Navigator**—This release introduces the Cisco Wireless Control System (WCS) Navigator, which delivers an aggregated platform for enhanced scalability, manageability, and visibility of large-scale implementations of the Cisco Unified Wireless Network. This powerful software-based solution gives network administrators cost-effective, easy access to information from multiple, geographically diverse Cisco WCS management platforms. It supports partitioning of the unified wireless network at the management level.

Cisco WCS Navigator runs on a server platform with an embedded database. It can support up to 20 Cisco WCS management platforms with manageability of up to 20,000 Cisco Aironet lightweight access points from a single management console.



Note A Navigator license is required to use WCS Navigator. If there is not a license, WCS Navigator does not run and provides an error message indicating that a license cannot be found.

- **Cisco WCS Enterprise License**—With this release, customers can now purchase an enterprise license for Cisco WCS. An enterprise license supports deployment of Cisco WCS on multiple servers up to the maximum number of access points supported by each enterprise license.
- **Reporting**—Cisco WCS now includes new reporting enhancements and new features that improve data management, simplify operations, and increase the flexibility of generating reports. These improvements include manual exporting in CSV or PDF format, automatic exporting according to an established schedule, email generation, grouping, customized network polling, and database archiving either hourly, daily, or weekly. The new reporting categories include inventory, performance, security, clients, access points, and mesh.

- **Ease-of-use enhancements**—A variety of enhancements that improve Cisco WCS ease of use are included with this release. These include improved search capabilities, configurable record sizes, specialized tabs in access point and controller templates to simplify configuration, sorting of list page columns, and configuration of severity level alarms.
- **Client troubleshooting tool**—This release supports a new client troubleshooting tool that allows network administrators to quickly and easily troubleshoot problems with a client. This tool is available from the client monitoring page by entering the client MAC address. Detailed client information is displayed on a troubleshooting dashboard to aid network managers with the troubleshooting of client problems. This tool includes a summary page with a list of the defined problems and suggested troubleshooting actions, as well as a log analysis to capture log messages from the controller and a detailed event history.
- **Guest access enhancements**—Multiple guest access enhancements are included in this release:
 - **Automated guest user access scheduling:** Guest user provisioning personnel can now schedule and customize automated guest access by time of day and date.
 - **Guest user credential emailing:** Pre-provisioned guest users can receive their login credentials by email prior to their arrival at an organization.
 - **Flexible guest access provisioning by wireless LAN controller group:** Guest users can be provisioned to receive network access across an individual wireless LAN controller, a subset of wireless LAN controllers, or all wireless LAN controllers connected to the network.
 - **Mapping of guest users to Cisco WCS maps:** Guest user provisioning personnel can now select the Cisco WCS campus, building, or floor area maps to limit the guest user network access. If no specific area is selected during the setup of the guest user profile, the guest will have full area access within the parameters of the guest wireless LAN controller.
 - **Logging guest user provisioning personnel activities:** The following guest user provisioning personnel activities will now be logged: creation, deletion, or updating of guest user profiles and login of guest user provisioning personnel.
- **Cisco Discovery Protocol (CDP) enhancement**—CDP is a device discovery protocol that runs on all Cisco-manufactured equipment. A device enabled with CDP sends out periodic interface updates to a multicast address in order to make itself known to neighboring devices.
- **New Wireless LAN controller configuration templates**—Several new wireless LAN controller configuration templates have been added in this release including:
 - Simple Network Management Protocol (SNMP) community strings
 - User login policies
 - Rogue access point and client device policies
 - Trusted access point policies
 - Client exclusion policies
- **Data migration from CiscoWorks Wireless LAN Solution Engine**—Selected data can be migrated, in bulk, from CiscoWorks WLSE into Cisco WCS. CiscoWorks WLSE must be running software release 2.15 or later in order to use this function. The exported CiscoWorks WLSE .tar file includes the background floor map image, the access point placement on each floor, and the antenna angle and down-tilt information.
- **Increased scalability**—With this release, as well as Cisco Unified Wireless Network Software Release 4.0.197, Cisco WCS supports an increased number of wireless LAN controllers on high end servers. The limits are now 3000 lightweight access points and 750 wireless LAN controllers.
- **Planning mode support for irregularly shaped buildings**—Cisco WCS planning mode now supports drawing irregularly shaped buildings using polygons.

- Cisco Wireless Mesh Enhancements—Additional Cisco WCS enhancements are implemented to provide better monitoring of the wireless mesh network. These wireless mesh traps include poor SNR link, parent change, child moves, access point changes parent frequently, console port event, MAC authorization failure, queue overflow, and child excluded parent. Also, background scanning allows the Cisco Aironet 1510 Lightweight Outdoor Mesh access points to actively and continuously monitor neighboring channels for more optimal paths and parents. Because the access point is searching on neighboring channels as well as the current channel, the list of possible alternate optimal paths and parents is greater.
- Chokepoint support—This release supports high-accuracy deterministic local-based notifications enabled through chokepoints. Chokepoint-based notifications are triggered by Cisco Compatible Extensions Wi-Fi tags as they come within range of a chokepoint. All chokepoints must be configured and brought online with the vendor's chokepoint management software in order to ensure proper network connectivity and set device ranges. Chokepoints should be added to Cisco WCS only after they have been configured by the vendor's chokepoint management software.
- Japanese Microsoft Windows Support—This release adds support for the use of Cisco WCS on a server running the Japanese version of Microsoft Windows. Cisco WCS will run in English.

Changed Information

- There is no deployment restriction on the number of hybrid-REAP access points per location. However, the minimum bandwidth restrictions remains 128 kbps with the roundtrip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes.
- The wildcard character in the search window is an asterisk (*). In 4.0.96.0, it was a percent mark (%).

Caveats

This section lists open and resolved caveats in Cisco WCS 4.1.83.0 for Windows and Linux.

Open Caveats

These caveats are open in Cisco WCS 4.1.83.0:

- 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.

- CSCse93014—Cisco WCS works in conjunction with Cisco Aironet Lightweight Access Points, Cisco Wireless LAN Controllers, and the Cisco Wireless Location Appliance by providing tools for wireless LAN planning and design, system configuration, location tracking, security monitoring, and wireless LAN management. Cisco WCS contains multiple vulnerabilities that can result in information disclosure, privilege escalation, and unauthorized access through fixed authentication credentials.

Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070412-wcs>

Workaround: None at this time.

- CSCse94732—There is a WCS and controller template mismatch while configuring CCKM and 802.1x.

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.

- CSCsg46060—The RADIUS template creation screen has only one check box to accept a shared secret key.

Workaround: None at this time.

- CSCsg75059—WCS has an extra DEFAULT entry in the drop-down list to set the type of shared key when enabling WPA with PSK as AKM.

Workaround: Select Hex or Ascii and set the shared key.

- 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.

- CSCsg83836—While using the Map Editor, the floor plan graphic is distorted. The issue happens when the system compresses a very high resolution image to fit into Macromedia Flash and make it editable in the Map Editor. Because the image is already compressed to fit into Macromedia Flash, compressing the image further distorts it.

Workaround: Do not use a high-resolution image. Scale down the image to a resolution that can be loaded into a browser and clearly displayed without having to zoom the image. A free image resolution reduction tool is available at: <http://www.jhllabs.com/ie/>.

- CSCsh04469—The 802.11 state for probing clients displays as dissociated for unique client reports.

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.

- CSCsh37337—The Reports graph does not display the Y axis at times.

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.
- CSCsh51006—To manage WPA1 or WPA2 WLANs on 3.2 and 4.0 controllers, you will need to create separate profiles in WCS. While CSCse95746 allows the creation of multiple profiles with the same SSID, you will need to create two templates, one for 3.2 controllers and another for 4.0 controllers, which is inconvenient.
Workaround: Create two profiles. One profile for 3.2 controllers, with WPA or WPA2 L2 security (profile name needs to match the SSID name), and another for 4.0 controllers, with WPA1+WPA2 L2 security. The profile name does not need to match the SSID name for 4.0.206.0 controllers.
- 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.
- 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.
Workaround: Ignore the error message.
- 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 switchweb 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.
- 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.

- CSCsh87109 —The following WCS client troubleshooting error is misleading:

```
QueryCriteria does not exist
```

This error occurs when you start troubleshooting of a client when it is not yet registered in WCS.

Workaround: Interpret this error as follows: WCS cannot locate the client in the controller and the WCS database.

- CSCsh87118 —Sometimes, client troubleshooting using Internet Explorer 7.0 on a Windows XP system causes the CPU to run at 100%.
Workaround: Try using a different web browser like Firefox.
- CSCsh89306—WCS generates an SNMP error when pushing a web authentication template to a 4.0.206.0 controller. This happens when pushing a web authentication template with the following parameters:
 - Web Auth Type: Default Internal
 - Logo Display: nothing is checked
 - Web Auth Page Title: Welcome to the Delta Guest Network
 - Web Auth Page Message: Welcome to the Delta Guest Network
 - Custom Redirect URL: empty

Workaround: Configure web authentication directly on the controller. Do not use WCS.

- a. Open the web authentication customization template page.
- b. For Web Auth Type, select **External**.
- c. Enter a dummy URL in the External Redirect URL field.
- d. Change the web authentication type to **Default Internal**.
- e. Enter a custom URL in the Custom Redirect URL field.
- f. Save and apply the template.

You should not leave the External Redirect URL and Custom Redirect URL fields blank, even if they are not relevant to the current web authentication type.

- 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.
- 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.
- CSCsh92630—The SSID for a rogue access point disappears intermittently after scheduled tasks.
Workaround: Refreshing the configuration from the controller eventually worked to fix this issue.
- 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 that to fail with SNMP timeout before it moves on. 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, reenable 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.

- CSCsi14131—Under certain conditions, WCS fails to pull a controller configuration. When this happens, you will see the following errors in the WCS logs:

```
3/14/07 11:34:03.531 TRACE[com.aes] THROW
javax.crypto.BadPaddingException: Given final block not properly padded
at com.cisco.server.util.EncryptionUtil.decryptValue(Unknown Source)
```

This problem is caused when WCS cannot read an entry in the database because it is corrupted. The likely cause of the corruption is an unclean shutdown of the database (that is, a reboot of the computer without the proper shutdown).

Workaround: Remove and add the controller in question to WCS. If this does not work, contact TAC for a patch. You must place the patched file under `WCS_DIRECTORY\webnms\classes\com\cisco\server\util`. You must create the directory if it does not exist.

- 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.
- CSCsi15731—When you click the **Save** button on the Schedule Guest User page, a time error message appears. This condition happens due to time differences between the system on which WCS is running and the system on which the client browser is running.
Workaround: To avoid this problem, create the user on the system on which WCS is running.
- 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.
- CSCsi17857—When trying to edit a saved search, only the delete option is available.
Workaround: The user can create a new search rather than attempting to edit the saved search. The user can also delete the search.
- CCSsi18038 —If you create the authentication, authorization, and accounting TACACS + templates and apply them to a controller, and then reapply the templates to the controller, the authentication template succeeds, but authorization and accounting templates fail.
Workaround: Avoid applying the TACACS + templates twice to the same controller.
- CSCsi18071 —When you stop the WCS traffic, 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.
- 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.
- CSCsi20899 —When looking at a rogue client in WCS, the access points that have detected this rogue client may be empty.
Workaround: In the Rogue Clients page (Monitor > Security > Rogue Clients), select **WCS Controllers** from the Search In drop-down list and search for rogue clients on the controller directly. Then, click the link for one of the rogue clients to display its details.
- 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.

- CSCsi24063—Heatmaps do not display properly after a restore.

Workaround: The user can optimize the floor size. The heatmaps display properly in a larger view.

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

Workaround: None at this time.

- 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.

- 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.

- CSCsi31186—When creating a WLAN template on WCS that contains a combination of web authentication settings and either WPA PSK or static WEP, the template fails when pushed to a controller, and WCS generates an SNMP error stating that the combination is not supported.

The following combinations are supported encryption web authentication methods:

- Static WEPS
- WPA using PSK

You should be able to create a template that supports this combination on WCS and push it to a controller. You can create the WLAN template on WCS, but will be unable to push it to a controller.

Workaround: Create the WLAN manually on the controller instead of using WCS.

- CSCsi32806 —WCS users may experience severe latency when navigating through the pages of WCS. This can happen when WCS is running on a Windows platform.

When you experience this problem, pull the logs of WCS (Administration > Logging > Download) and check the error.log file for the following errors:

```
The specified network name is no longer available. : winnt_accept: Asynchronous
AcceptEx failed.
The semaphore timeout period has expired. : winnt_accept: Asynchronous AcceptEx
failed.
```

These errors are the result of a bug in the Apache component of WCS. The Apache bug number is 21425. Complete details are available at http://issues.apache.org/bugzilla/show_bug.cgi?id=21425.

Workaround: Modify the httpd.conf files in the C:\Program Files\WCS4.0\webnms\apache\conf\ and C:\Program Files\WCS4.0\webnms\apache\conf\backup directories as follows:

1. Stop WCS (Start > Programs > Wireless Control System > Stop WCS).

2. Navigate to the C:\Program Files\WCS4.0\webnms\apache\conf\ directory and open the httpd.conf file with a text editor. Then, add the following lines and save the file:
 - Win32DisableAcceptEx**
 - EnableSendfile Off**
 - Enablemmap Off**
 3. Repeat step 2 on the backup copy of httpd.conf located in the C:\Program Files\WCS4.0\webnms\apache\conf\backup directory.
 4. Start WCS (Start > Programs > Wireless Control System > Start WCS).
- 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.
 - CSCsi35928—When trying to delete a Saved Search on Monitor > Maps webpage, WCS displays a Permission Denied webpage.
Workaround: None at this time.
 - CSCsi40454—Client details do not update correctly after the client is reassociated to a different wireless LAN.
Workaround: If the user link is clicked instead, the correct details are displayed.
 - CSCsi44505—The user assistant on WCS can access the controller and client information when completing a quick search.
Workaround: None at this time.
 - 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.
 - CSCsi47327—The Monitor Shunned Clients page displays a Permission Denied page.
Workaround: None at this time.
 - CSCsi47361—Saving the CDP template may lead to a page error.
Workaround: None at this time.
 - CSCsi47842—The Client search option displays the “Location Server” option even when the base license is installed.
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.
- CSCsi48213—When troubleshooting a client, clicking any options from the drop-down menu (i.e., radio measurements) results in an SNMP error message.
Workaround: None at this time.
- 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.
- CSCsi65717—When you install WCS as a service on a Windows operating system, the installation completes without prompting for a reboot. You can start WCS under Programs > Wireless Control System, but if you log off the system, the server stops.
Workaround: You can reboot the system, and WCS starts working as a service.
- Cscsi67939—After you enable location debug for a tag, the map image may not enlarge on the tag properties page.
Workaround: None at this time.
- CSCsi88114—After a WCS upgrade from 4.0 to 4.1 with Red Hat Enterprise Linux ES release 4 (Nahant Update 5), WCS fails to start. The following JAVA error displays:

```
[root@as5 bin]# ./StartWCS
Starting WCS
3914: @?????????????dl failure on line 719Error: failed
/u01/opt/WCS4.1/jre/lib/i386/server/libjvrm.so, because (null)
```

Workaround: Complete these steps.

- a. Edit the <wcs>/bin/startServer.sh file. Insert **/lib:/usr/lib:** before the code that appears at line 84.

With this change, the resulting code should appear as follows:

```
$WEBNMS_HOME/Matlab/sys/os/glnx86:\
/lib:/usr/lib:\
$XVFB_LIB/lib:\
$LD_LIBRARY_PATH
```

- b. Save the file.

WCS starts. If the StartWCS command fails, enter **<wcs>/bin/nmsadmin.sh start**.



Note If you have WCS installed as a service to start on bootup, enter **service WCS start**.

Resolved Caveats

These caveats are resolved in Cisco WCS 4.1.83.0.

- CSCse17963—Because of a corrupted file, the WCS database fails to start.
- CSCse17983—WCS database fails to start because of log file corruption.
- CSCse27704—If you enter a blank value for HTTP when installing WCS, the WebServer process does not start.
- CSCsg01946—If you lose your WCS password and have not backed up your database, there is no mechanism to recover the password.

- CSCsg36163—When you try to create a Local Management User with the same name as an existing Local Net User, WCS gives an SNMP error. Instead, it should respond with an error that the username is already used and must be unique.
- CSCsg39969—You cannot log in to WCS with a username that exceeds 15 characters.
- CSCsg46529—The times displayed when mousing over the elements on a floor map are not accurate. The WCS query is based on the information table times rather than the location table times.
- CSCsg50192—When you configure an access point template and choose WLAN override on either the 802.11a or 80.211b radios, only 5 SSIDs display. Of those SSIDs that do appear, not all are WCS SSIDs.
- CSCsg51405—You cannot restore a configuration when an ACL with a rule exists. When you try a Restore Config, it displays the following error message:

```
Restore failed for following configuration(s) - Access Control List
10.50.65.42/testing Failed to create object in device
```

Cisco WCS logs display the following error message:

```
SnmOperationException: [COMMON-1]: COMMON-1
```

- CSCsg54554—When you enable Web policy within WCS, you have a choice of authentication or pass through. (You must navigate to Configure > Controllers, choose WLANs > WLANs from the left sidebar menu, and then click Security > Layer 3 to arrive at this parameter.) Enabling wpa1/wpa2 for web policy is not supported on the controller, so a vague error message is generated.
- CSCsg55667—(Duplicate of CSCsb39593) If you install a version of WCS that was installed previously, an error message warns you of the previous install, but the error message reports the wrong version number for the existing version.
- CSCsg58340—The method of adding new rules is not functioning as expected. If you choose Configure > Controller Templates > Access Control > Access Control Lists, you can specify rules. When you go to the Select a command drop-down menu and choose Add New Rule, a sequence number 1 is created. When you go to add another rule, you should be warned that rule 1 already exists before proceeding. Instead, rules with sequence 3, 4, 5, and so on are created regardless of whether another exists.
- CSCsg68269—If a template applied from Cisco WCS attempts to create a WLAN ID greater than 16, the following error message displays:


```
some unexpected internal error has occurred
```
- CSCsg84669—German characters are not displayed correctly when editing the properties of a client or tag (name, category, etc.).
- CSCsg88347—An error message occurs when you try to modify an existing DHCP scope value (by choosing Configure > Controller > System > DHCP scope).
- CSCsg94509—WCS sometimes fails to apply a WLAN template to 4400 and 2000 series controllers when the WLAN is configured for static WEP and 802.1x. WCS displays this message:


```
SNMP operation to Device failed: Unspecified error / Session timeout range invalid -
for 802.1x(300-86400) f or others(0-65535)
```
- CSCsg94525—The setting for the current LWAPP operating mode (found when choosing Configure > Controller IP > System > General) is not retaining its value after an audit is performed.
- CSCsg97505—The error message that may appear when editing a DHCP scope needs to be more descriptive.

- CSCsg98415—When you delete templates from WCS, the "failure" message that displays for unreachable WLCs could be more descriptive.
- CSCsh05313—When you restore data in preparation for updating to a later WCS version, the restore does not complete.
- CSCsh13721—The Edit AP Assignment option in the AP Groups VLANs shows all access points as assigned to the first group, even if the access point has been correctly configured before. The problem is related only to showing the current values. If a change is made, it is correctly saved.
- CSCsh26050—The first time after a migration from a previous release, WCS sometimes fails to start. This occurs only for access points whose antenna name was empty in the earlier release. A "Failed to start WCS server" message appears.
- CSCsh39891—Heatmap generation fails if the floor size is too large.
- CSCsh41937—You may see an incorrect number of clients when hovering over a building map. The building map should show the total number of clients on all the floors in the building.
- CSCsh54607—The user is not prompted with a reboot message for access point reset. Reboot is required for changes to take effect when the WLAN-Override template is configured or pushed to the controller via WCS > Configure > Access Points Template.
- CSCsh57153—A specific search for excluded clients returns a blank results page.
- CSCsh91578—When you upgrade the controller from software release 3.2.193.5 to 3.2.195.10, the self-signed certificate (SSC) feature becomes disabled, which prevents any access point with a self-signed certificate from being able to rejoin the controller.

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>

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0704R)