Release Notes for Cisco Wireless Control System 4.0.100.0 for Windows or Linux

November 14, 2007

These release notes describe open caveats for the Cisco Wireless Control System 4.0.100.0 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

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 4.0.100.0.
- Location appliance software release 2.1.34.0, 2.1.39.0, or 2.1.42.0
- Cisco 2700 Series Location Appliance
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 4100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco Wireless Services Modules (WiSMs) for Cisco Catalyst 6500 Series Switches
- Cisco WLAN Controller Network Modules for Cisco Integrated Services Routers
- Cisco Aironet 1000, 1130, 1200, 1240, 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 3,000 Cisco Aironet lightweight access points, 1,250 standalone access points, and 750 Cisco wireless LAN controllers.
  - 3.16-GHz Intel Xeon Quad processor with 8 GB RAM and 200-GB hard drive.
  - 80 GB minimum free disk space is needed on your hard drive.
- Standard Server—Supports up to 2,000 Cisco Aironet lightweight access points, 1,000 standalone access points, and 150 Cisco wireless LAN controllers.
  - 3.2-GHz Intel Dual Core processor with 4-GB RAM and 80-GB hard drive.
  - 40 GB minimum free disk space

- Low End Server—Supports up to 500 Cisco Aironet lightweight access points, 200 standalone access points, and 125 Cisco wireless LAN controllers.

    – 3.06-GHz Intel processor with 2 GB RAM and 30-GB hard drive.

    – 30 GB minimum free disk space is needed on your hard drive.

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

Note Cisco WCS can simultaneously manage multiple Cisco wireless LAN controllers running different software versions. Cisco WCS running Cisco UWN Software Release 4.0 can simultaneously manage controllers running release 4.0 to support Cisco Aironet lightweight access points and controllers running release 3.2 to support Cisco Aironet mesh access points. A single Cisco WCS can manage these controllers up to the maximum number of controllers and access points supported by Cisco WCS.

Supported Operating Systems

The following operating systems are supported:

    – Windows 2003/SP1 or later with all critical and security Windows updates installed. No 64-bit operating system installations are supported.

    – Red Hat Linux Enterprise Server 4.0 or Advanced Server 4.0. Only 32-bit operating system installations are supported. No 64-bit operating system installations are 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 1,500 Cisco Aironet lightweight access points and 100/375 Cisco wireless LAN controllers. The required processor is a 3-GHz Intel Pentium with 3 GB of RAM and 38 GB of available hard drive space.

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 than the controller software release. If an upgrade is planned, upgrade the Cisco WCS first to prevent any unexpected problems. Cisco WCS supports database upgrades only from the following official Cisco WCS releases:

- 3.1.20.0
- 3.1.33.0
- 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

Important Notes

This section describes important information about Cisco WCS.

Applying a Combination of Valid L2 Policies with Conditional Redirect

A failure occurs if you apply a combination of valid L2 policies along with conditional web redirect as a L3 policy. The L2 and L3 policies should be set independently. First, set the L2 policy while keeping WLAN disabled, apply the setting to the controller, set the L3 policy to conditional web redirect, and then enable the WLAN.

Changing the Default Password

The Cisco WCS default root password is *public*. Cisco advises changing the default password after the initial installation. Follow these steps to change the Cisco WCS default password.

Step 1 Log in as **root**.

Step 2	Select **Administration > Accounts**.
Step 3	From the User Name column, click **root**.
Step 4	Enter a new password in the New Password text box and retype the new password in the Confirm New Password text box.

Limits to WebAuth Support on Hybrid-REAP Access Points

Access points in Hybrid-REAP mode support WebAuth only with Open Authentication if the wireless LAN (WLAN) has local switching enabled.

Compatibility

This release of Cisco WCS for Windows or Linux is compatible with wireless LAN controller and Cisco Aironet lightweight access point operating system 3.1 or later. Previous releases of Cisco WCS should not be used with the 4.0.100.0 controller software release.

Cisco WCS IP Addresses

If you need to change the IP parameters on the Cisco WCS workstation, such as the IP address or the default gateway, shut down Cisco WCS before making the change, and start Cisco WCS after your IP configuration changes are complete.

MCS7800 Servers

The Cisco MCS7800 server hardware is supported, but you must reformat the software so that it can be used as a Cisco WCS server.

Manually Executing Scheduled Tasks

Manually executed scheduled tasks (such as device status, client statistics, rogue access point, and statistics) do not run immediately if any of the other tasks are already running. Instead, Cisco WCS queues and executes them as soon as the running tasks are completed. Wait for the manually executed scheduled tasks to complete.

Slow Imports of FPE Files with More Than 200 Walls

Importing a floor plan editor (FPE) file with more than 200 walls can be slow, and the browser may not report any status or redirect you to any other page.

Workaround: Do not click anywhere on the map page for at least 5 minutes before you try to verify that the file is imported.

Calibrating the Location Model Using Cisco Aironet 802.11a/b/g Wireless Cardbus Adapter Clients

Cisco recommends using a Cisco Aironet 802.11a/b/g Wireless Cardbus Adapter (AIR-CB21AG) with the latest drivers. When using a card for calibrating, make sure it is CCX compatible and Version 2 or later. If the card is earlier than version 2 then it is not ideal for calibration.

Restoring an Upgraded Cisco 2700 Series Location Appliance to an Earlier Release

A backup from the latest release of Cisco 2700 series location appliance software cannot be restored on a location appliance running an earlier release (CSCsb54606).

Workaround: Before you upgrade a location appliance to the latest release, Cisco recommends that you create a backup for the earlier release and archive it in case you need to return an upgraded location appliance to an earlier release.

Managing Cisco Wireless Services Modules Using Cisco WCS

Unlike other wireless LAN controllers, Cisco Wireless Services Modules (WiSMs) use their service ports to communicate with the Cisco Catalyst 6500 series switch supervisor. The Cisco WCS server uses the WiSM data port to connect to and control the WiSM and its associated Cisco lightweight access points (CSCsb49178).

Configuration Mismatch

A configuration mismatch may occur between WCS and the controller if you upgrade from an older version of WCS. To correct the mismatch, follow these steps to refresh the configuration from the controller:

Step 1   Choose **Configure > Controllers**.

Step 2   Click the controller IP address to see details.

Step 3   From the left sidebar menu, choose **System > Commands > Configuration Commands** (Refresh Config From Controller).

Caveats

This section lists open and resolved caveats in Cisco WCS 4.0.100.0 for Windows and Linux.

Open Caveats

These caveats are open in Cisco WCS 4.0.100.0:

- CSCsd83836—The resolution of the WCS Map Editor is distorted and barely readable.

    Workaround: None.

- CSCse42296—If a template for a given WLAN profile exists in WCS and WLAN is modified out of the band of the controller, the template is not updated to reflect the new settings.

    Workaround: Make any desired changes to the WLAN settings in WCS and then apply them to the controllers.

- CSCse90024—Clients cannot connect to access points if 128 WEP encryption is set.

    Workaround: If you are using 1200 or 1130 access points, do not choose 128 WEP encryption.

- CSCsg33092—On a Cisco WCS wired network, a minor rogue access point alarm can be designated as critical severity, but the next time the rogue access point task runs, the following error message appears:

    ```
    RogueAP made as Acknowledged AP.
    ```

    Workaround: None.

- CSCsg45499—If the Rogue AP Alarms on Cisco WCS exceed 20, the No. of Entries field displayed in the last page always exceeds the displayed count by one.

    Workaround: None.

- CSCsg46060—The RADIUS authentication server templates require confirmation fields for shared secret keys.

    Workaround: None.

- 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.

    Workaround: None.

- 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.

    Workaround: None.

- CSCsg51405—You cannot restore a configuration when an ACL with a rule exists. When you try to restore a configuration, the following error message appears:

    ```
    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:

    ```
    SnmpOperationException: [COMMON-1]: COMMON-1
    ```

    Workaround: None.

- CSCsg54554—When you enable Web policy within WCS, you can choose 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.

    Workaround: None.

- 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.

Workaround: None.

- 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
```

Workaround: None.

- CSCsg69862—The RADIUS server ping attribute needs a label.

Workaround: None.

- CSCsg74466—If you generate a report after navigating to Monitor > Devices > Access Points and choosing Noise, Interference, or Coverage (RSSI / SNR) from the Select a report drop-down menu, the legend overlays the chart display area.

Workaround: None.

- CSCsg75059—WCS has an extra *default* value in the shared key list. The extra value must be removed from the authentication key management PSK list, and only ASCII and hex values should remain.

Workaround: None.

- CSCsg84669—When you edit the properties of a client or tag (name, category, etc.), German characters are not displayed correctly.

Workaround: None.

- CSCsg88347—An error message occurs when you try to modify an existing DHCP scope value (by choosing Configure > Controller > System > DHCP scope).

Workaround: None.

- 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)
```

Workaround: None.

- 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.

Workaround: None.

- CSCsg97505—The error message that may appear when editing a DHCP scope needs to be more descriptive.

Workaround: None.

- CSCsg98415—When you delete templates from WCS, the "failure" message that displays for unreachable WLCs could be more descriptive.

Workaround: None.

- CSCsh05313—When you restore data in preparation for updating to a later WCS version, the restore does not complete.

Workaround: None.

- 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.

  Workaround: None.

- CSCsh22237—If tags are associating and disassociating at a very high rate, a "Getting more than x disassociate messages in 30 seconds" alert appears.

  Workaround: None.

- CSCsh25458—The access points on the client location debug are displayed slightly off (down and right) of their actual locations on the map.

  Workaround: None.

- 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.

  Workaround: If you browse to the server a couple of hours later, the server will be running even though you may have received the failure to start message.

- CSCsi18312—The link test option in the Client Access Point Association History does not work. The link displays a blank screen.

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

- CSCsi87606—When you enter script tag in the Template Name field, an error 400 occurs.

  Workaround: None at this time.

- CSCsk28942—When an omnidirectional antenna product is selected and the specifications of the antenna are shown, the Antenna Orientation control should be disabled.

  Workaround: Set the Antenna Orientation value to 0.

- CSCsk55334—A configuration mismatch may occur between WCS and the controller if you upgrade from an older version of WCS.

  Workaround: Refresh the configuration from the controller by following these steps:

  a. Choose Configure > Controllers.

  b. Click on the controller IP address to see details.

  c. From the left sidebar menu, choose **System > Commands > Configuration Commands** (Refresh Config From Controller).

Resolved Caveats

These caveats are resolved in Cisco WCS 4.0.100.0:

- CSCsh40682—If you change building names in a map, the old name still remains.
- CSCsi14131—You are unable to change certain configuration and refresh configurations.
- CSCsi21344—Time issues exist within WCS.
- CSCsi32806—The httpd.conf file needs modification to comply with an Apache bug fix.
- CSCsi47281—The copyright shown during the installation needs updating.
- CSCsi62468—The WCS client user count drops intermittently.
- CSCsi63175—A guest user cannot be created if the profile and SSID are different.

- CSCsi89433—A user without administration rights can still perform scheduled tasks.
- CSCsi94914—The login screen allows only 15 characters but you can enter more than 15 characters.
- CSCsj06763—A 4.0 user may experience a corruption when trying to upgrade.
- CSCsj35017—The WCSAdmin command must be made available for 4.0.
- CSCsj85022—The Linux uninstall should not remove RPMs.
- CSCsk18191—A stack overflow vulnerability in Apache Tomcat may allow for remote code execution attacks.
- CSCsk26636—The Cisco logo needs to be removed and replaced with Univerge for the NEC version 3.2.66.0.

If You Need More Information

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

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

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

Troubleshooting

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

http://www.cisco.com/tac

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

Related Documentation

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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