



Release Notes for Cisco 2700 and 2710 Location Appliances for Software Release 3.0.42.0

November 6, 2007

These release notes describe features, enhancements, and caveats for software release 3.0.42.0 for Cisco Location Appliances. This release of location appliance software supports both Cisco 2700 and 2710 location appliances and operates with Cisco Wireless LAN Solution versions 4.1, 4.0, 3.2, and 3.1.



Note

Refer to the online version of the *Cisco 2700 Series Location Appliance Installation and Configuration Guide* for details on the physical installation and initial configuration of the location appliance at http://www.cisco.com/en/US/products/ps6386/prod_installation_guides_list.html

Contents

These release notes contain the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Important Notes, page 5](#)
- [Screen and Path Changes, page 9](#)
- [Caveats, page 9](#)
- [Troubleshooting, page 14](#)
- [Documentation Updates, page 14](#)
- [Related Documentation, page 14](#)
- [Obtaining Documentation, page 15](#)
- [Documentation Feedback, page 16](#)
- [Cisco Product Security Overview, page 16](#)
- [Obtaining Technical Assistance, page 17](#)
- [Obtaining Additional Publications and Information, page 18](#)



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

© 2007 Cisco Systems, Inc. All rights reserved.

Introduction

Location appliance software release 3.0.42.0 supports Cisco 2700 and 2710 location appliances that operate with Cisco Wireless LAN Solution versions 4.1, 4.0, 3.2, and 3.1.

Location appliances compute, collect, and store historical location data using Cisco wireless LAN controllers and access points to track the physical location of wireless devices. The collected location data can be viewed in GUI format in the Cisco Wireless Control System (WCS), the centralized WLAN management platform.

System Requirements

You can install this software release on any 2700 or 2710 location appliance.

Compatibility Matrix

Table 1 describes compatibility between WCS and location server versions.

Table 1 *WCS and Location Server Compatibility Matrix*

WCS \ Location Server	LOC 1.1	LOC 1.2	LOC 2.0	LOC 2.1	LOC 3.0
WCS 3.0	Supported	Supported ¹	Not supported	Not supported	Not supported
WCS 3.1	Supported ²	Supported	Supported from WCS 3.1.35.0 onward ³	Supported from WCS 3.1.35.0 onward ³	Supported from WCS 3.1.35.0 onward ^{3,6,8}
WCS 3.2	Supported ^{2, 3, 4, 5}	Supported ^{3, 4, 5}	Supported	Supported ⁶	Supported ^{6,8}
WCS 4.0	Supported ^{2, 3, 4, 5, 6}	Supported ^{3, 4, 5, 7}	Supported ⁷	Supported	Supported ⁸
WCS 4.1	Supported ^{2, 3, 4, 5, 6, 9}	Supported ^{3, 4, 5, 7, 9}	Supported ^{7, 9}	Supported ⁹	Supported

1. Certain antenna attributes are ignored by WCS.
2. Certain antenna attributes are ignored by the location server.
3. Asynchronous notification features are ignored by the location server.
4. Backup and restore operations for the location server may time out.
5. Searching for elements by a specific MAC address or asset name will not work until the location server SW is upgraded.
6. Battery level and location notification update features are ignored by the location server. Location smoothing parameters and contributing access point debug options are ignored by the location server.
7. Battery level and location notification update features are ignored by Cisco WCS. Location smoothing parameters and contributing access point debug options are ignored by Cisco WCS.
8. Cisco Compatible Extension (CX) tags, telemetry, chokepoint, and emergency capabilities are ignored by Cisco WCS.
9. Cisco CX tags, telemetry, chokepoint, and emergency capabilities are ignored by the location server.

Upgrading to this Software Release

For instructions on using either Cisco WCS or a console port to download this software on location appliances, refer to the “Updating Location Appliance Software” section in the “Installation and Configuration” chapter of the *Cisco 2700 Series Installation and Configuration Guide (78-17180-02 and later)*.

Click this link to browse to that document:

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

Database File Must Be Copied to a Separate Directory Prior to Software Upgrade in Releases 2.xxx and 3.0.37.0

To prevent an overwrite of the location appliance database during a software upgrade, you must backup (less than 8 GB) or copy (8 GB or greater) the database file *server-eng.db* to a secure location prior to installation of release 2.1.x and 3.0.37.x.



Note Transfer of the database file using FTP or SFTP to a different machine or an */opt/backups* directory is recommended to provide a secure location.

After the new software is installed, you must transfer the database file *server-eng.db* back into the */opt/locserver* directory.

- If the database file is 8GB or greater, copy the database file to a secure directory by entering the following commands:

```
/opt/locserver/db/linux/server-eng.db
/opt/locserver/db/linux/solid.ini
/opt/locserver/db/dbopts.db (if it exists)
/opt/locserver/attach/*
```

To keep the database under 8 GB in size, note the following recommendations:

- Reduce the frequency of history polling of elements (clients and tags)
- Increase the frequency of history pruning to reduce overall database size (Location > Location Servers > *Administration* > *History Parameters*).
- If the database file is less than 8GB, a backup is recommended prior to the install.



Note The database file can be copied to any secure directory other than */opt/locserver*. For more details, refer to the WCS database backup and restore processes in Chapter 11 of the Cisco Wireless Control System Configuration Guide found at the following URL:
http://www.cisco.com/en/US/products/ps6305/products_configuration_guide_book09186a008082d824.html

Backup of Release 2.0.x or Later Cannot be Restored on Earlier Releases

A backup of location appliance software releases 2.0.x and later cannot be restored on any location appliance running an earlier software release. Before you upgrade a location appliance to 2.0.x release or later, Cisco recommends that you create a backup of the earlier release and archive it. This will enable you to convert an upgraded system to an earlier release, if necessary.

Location Appliance Image is Compressed

If you download the server image *.gz file using WCS, the location appliance automatically decompresses (unzips) it, and you can proceed with the installation as before. If you manually download the compressed *.gz file using FTP, you must first decompress the files before running the installer. These files have been compressed under the LINUX operating system and must be decompressed using the *gunzip* utility program. The unzip method you use is defined by the filename you are trying to unzip.

To make the bin file executable, use the following command:

```
chmod +x filename.bin
```

Secure Shell V1.0 is No Longer Supported

Support for secure shell (SSH) version 1 (v1) is not supported in releases 2.1.x and later due to known security issues; however, SSH version 2 (v2) is supported.



Note

After installing release 3.0.42.0, you must reboot the location appliance to remove support of SSH v1.0.



Note

To remove ssh support for releases 2.0.x and earlier, you must manually edit the `sshd_config` file to remove support for ssh v1.0 by adding **Protocol 2** to the end of the script as noted below.

```
#override default of no subsystems
Subsystem sftp /usr/libexec/openssh/sftp-server
```

Protocol 2

- With this addition, the script will match that of releases 2.1.x and later.
 - A restart is required to reread the config file after the edit is made.
-

Updated Location Appliance Software Version Shown in WCS After Polling

After a software update, the new location appliance software version does not immediately appear in location server queries on WCS. Up to five minutes is required for the new version to appear. WCS, by default, queries the location appliance every five minutes for status.

Important Notes

This section describes important information about new features and operational notes for software release 3.0.42.0 for location appliances.

Operational Notes

The following operational notes are relevant to this release.

Mandatory Default Root Password Change

You must change the default root password during initial configuration of the location appliance to ensure optimum network security.

- For releases 2.1.34 and later, you are prompted to change the password during the setup script.
- You can also change the password using the Linux command, “passwd.”

Hostname and IP Address of Location Appliance Must be Defined in the /etc/hosts File for SNMP

SNMP initialization fails and subsequent initialization of the location module fails if the /etc/hosts file does not have an entry for the location appliance's host name and IP address. The location appliance will continue to run but SNMP polling and location calculation will not occur and will not be reported in the log file. (see CSCsj54172 in the Open Caveats section for workaround details).

Mandatory Upgrade of Location Software Required to Reflect New 2007 Daylight Saving Time Dates

The United States has changed the start and end dates of Daylight Saving Time (DST) for 2007. In 2007, DST within the US will begin on the second Sunday in March and end on the first Sunday in November. A mandatory upgrade to release 2.1.42.0 or greater which incorporates support for this new DST period is required to prevent incorrect time reporting during certain periods of DST. Specifically, not upgrading your location appliance to version 2.1.42.0 will result in incorrect time reporting from March 11, 2007 through April 2, 2007 and from October 29, 2007 through November 4, 2007.

Automatic Installation Script for Initial Setup

Beginning with release 2.1.34, an automatic setup wizard is available to step you through the initial setup of the location appliance. You also have the option of setting up the location appliance manually.

An example of the complete automatic setup script (and manual setup process) is provided in the *Cisco 2700 Series Installation and Configuration Guide*. You can find this document online at http://www.cisco.com/en/US/products/ps6386/prod_installation_guides_list.html.

Location History Timestamps Match Browser's Locale

The WCS timestamp is based on the browser's location and not on the location appliance settings. Changing the time zone of the WCS or on the location appliance does not change the timestamp for the location history.

Recommended Settings for Absolute and Relative Discard RSSI Times (Location Parameters)

No value less than the default value of 3 minutes should be set for Relative Discard RSSI Time.

No value less than the default value of 60 minutes should be set for Absolute Discard RSSI Time.

Path: **Location > Location Server > Location Server > Advanced > Location Parameters**

Recommended Wireless Adapter Clients for Calibration

We recommend using Cisco Aironet 802.11 a/b/g Wireless Cardbus Adapter Clients (AIR-CB21AG) with the latest drivers for calibrating location models. The client should be Cisco CX compatible and version 2 or greater. Adapter client versions less than 2.0 are not ideal for calibration.

Recovering Lost Root Password

If you lose or forget the root password for the location appliance, do the following:

-
- Step 1** When the GRUB screen comes up, press **Esc** to enter the boot menu.
 - Step 2** Press **e** to edit.
 - Step 3** Navigate to the line beginning with "kernel," and press **e**.
At the end of the line enter a space and the number one (1). Press **Enter** to save this change.
 - Step 4** Press **b** to begin boot sequence.
At the end of the boot sequence, a shell prompt appears.
 - Step 5** You can change the root password by entering the **passwd** command.
 - Step 6** Enter and confirm the new password.
 - Step 7** Restart the machine.
-

Synchronization Notes

Assign a Controller/Network Design/Event Group to a Location Appliance Before Using Auto-Synch

With auto-synchronization, controllers, network designs, and event groups that are detected as unsynchronized are synchronized automatically. Before this automatic synchronization can be enabled, you must assign a controller, event group, or network design to a location appliance.

Controller Name Must be Unique Before Synchronization

The assigned controller names must be unique. If the controller names are duplicated, the synchronization process occurs only on one controller.

Verify WCS and Location Server Software Compatibility Before Synchronization

The software versions for WCS and the location server must be compatible for synchronization to perform properly. Please see the compatibility matrix noted in [Table 1](#) of this release note for WCS and location server compatibility.

New Feature Support

Please note the new feature support added in release 3.0:

Chokepoint and Emergency Notifications for Cisco CXv1 Asset Tags (NEW Notification Parameter)

You can add chokepoint and emergency event definitions on a per-group basis and define what conditions trigger an event notification. Chokepoint and emergency notifications are only reported for Cisco CX v.1 compliant tags.

Refer to the “Adding an Event Definition” section in Chapter 6 of the *Cisco Location Appliance Configuration Guide, Software Release 3.0*.

Path: **Location** > **Notifications** > **Settings** > *Group Name* > *Add Event Definition*

Chokepoint Mapping to Enhance Tag Location Reporting (NEW Configure Parameter)

Installation of chokepoints within a network provides enhanced location information for active RFID tags. When an active Cisco CX version 1 compliant RFID tag enters the range of a chokepoint, it is stimulated by the chokepoint. The MAC address of this chokepoint is then included in the next beacon sent by the stimulated tag. All access points that detect this tag beacon then forward the information to the controller and location appliance.

Using chokepoints in conjunction with active Cisco CX compliant tags provides immediate location information on a tag and its asset. When a Cisco CX tag moves out of the range of a chokepoint, its subsequent beacon frames do not contain any identifying chokepoint information. Location determination of the tag defaults to the standard calculation methods based on RSSIs reported by access point associated with the tag.



Note

Chokepoints are initially configured for IP address and Range by the chokepoint vendor’s application. Chokepoints must be added and positioned in Cisco WCS.

Refer to the “Refer to the “Adding Chokepoints to the WCS Database and Map” section in Chapter 7 of the *Cisco Location Appliance Configuration Guide, Software Release 3.0*.”

Path: **Configure** > **Chokepoints** > *Add Chokepoint*

Email Notifications for Location Server Alarms (NEW Alarm Parameter)

Cisco WCS lets you send alarm notifications to a specific email address. Sending notifications through email enables you to take prompt action when needed. You can select the alarm severity types (critical, major, minor and warning) that are emailed to you.

Refer to the “Emailing Alarm Notifications” section in Chapter 8 of the *Cisco Location Appliance Configuration Guide, Software Release 3.0*.

Path: **Monitor** > **Alarms** > *Email Notifications*

Excluding Ad Hoc Client Tracking and Reporting (NEW Polling Parameter)

You can turn off tracking of ad hoc rogue clients so that they are not displayed on Cisco WCS maps or their events and alarms reported.

Refer to the “Editing Polling Parameters” section in Chapter 4 of the *Cisco Location Appliance Configuration Guide, Software Release 3.0*.

Path: **Location** > **Location Servers** > *Location Server* > *Polling Parameters*

Location Protocol (LOCP) (NEW Advanced Menu Parameter)

LOCP is the location protocol that manages communication between the location server and the controller. Transport of telemetry, emergency and chokepoint information between the location server and the controller is managed by this protocol.

You can configure its parameters to adjust for slow response in latency in the network.

Refer to the “Editing LOCP Parameters” section in Chapter 4 of the *Cisco Location Appliance Configuration Guide, Software Release 3.0*.

Path: **Location** > **Location Servers** > *Location Server* > **Advanced** > *LOCP Parameters*

Location Server Utilization Report (NEW Report)

In Cisco WCS, you can generate a utilization report for a location server. By default, reports are stored on the Cisco WCS server.

The location utilization report summarizes and charts the following information in two separate charts for a prescribed period of time:

- Chart 1 summarizes and graphs CPU and memory utilization
- Chart 2 summarizes and graphs client count, tag count, rogue client count, rogue access point count and ad hoc rogue count

You can generate a utilization report for the location server on both an immediate and scheduled basis. Once defined, the report can be saved for future diagnostic use on an ad hoc basis or scheduled to run and report on a regular basis.

Refer to the “Generating Reports” section in Chapter 8 of the *Cisco Location Appliance Configuration Guide, Release 3.0*.

Path: **Report** > **Performance Reports** > *Location Server Utilization*

Overlapping Tags (NEW Monitor Parameter)

When multiple tags are within close proximity of one another a summary tag is used to represent their location on a WCS map. The summary tag is labeled with the number of tags at that location. When you move the mouse over the overlapping tag on the map, a panel appears with summary information for the overlapping tags. A distinct panel exists for each overlapping tag.

Refer to the “Overlapping of Tags” section in Chapter 8 of the *Cisco Location Appliance Configuration Guide, Release 3.0*.

Path: **Monitor** > **Maps**

Query and Display of Telemetry Data for Cisco CX v1 Compliant Tags (NEW Monitor Parameter)

You can query for telemetry capable data tags in WCS and display in the Tag Properties page those Cisco CX v1 compliant attributes transmitted by the tags. Attributes which might display for the tags are GPS location, battery extended information, pressure, temperature, humidity, motion, status and emergency code.

Refer to the “Querying of Tags” section in Chapter 8 of the *Cisco Location Appliance Configuration Guide, Release 3.0*.

Path: **Monitor > Tags > New Search**

Screen and Path Changes

The following location appliance features are found on different Cisco WCS screens than in release 4.0 and release 2.1 for the location appliance.

- Analyzing Element Location Accuracy Using Testpoints

You can use this feature to validate location accuracy of rogue and non-rogue clients and asset tags information generated either automatically by access points or manually by calibration.

Refer to the “Analyzing Element Location Accuracy Using Testpoints” section in Chapter 7 of the *Cisco Location Appliance Configuration Guide, Software Release 3.0* for more details

Path: **Location > Location Servers > Advanced > Advanced Parameters and Monitor > Maps**

- Polling frequency for location server, clients and tags

Configuring polling frequency for all elements is centrally managed on the Polling Parameters page.

Refer to the “Editing Polling Parameters” section in Chapter 4 of the *Cisco Location Appliance Configuration Guide, Software Release 4.1* for more details.

Path: **Location > Location Servers > Location Server > Polling Parameters**

Caveats

This section lists open and resolved caveats in location appliance release 3.0.42.0.

Open Caveats

The following caveats are open (unresolved) in this release:

- CSCsd36689—Access points in monitor mode do not detect probing clients as accurately as they do when in local mode. These access points do not track the clients’ RSSI values.

Workaround: Operate in local mode for the most accurate operation, if possible.

- CSCse34650—After performing a calibration using a Cisco CX compatible client on a floor with multiple controllers, it has been observed that some access points do not contribute enough calibration data points. This inaccuracy may be reflected on the Location Inspector quality accuracy page.

Workaround: There is no known workaround.

- CSCsh47150—Moving a building from one location to another within a campus might cause synchronization issues. After moving a building within a campus, the synchronization page indicates that the building already exists and attempts to pull it, if you initiate a synchronization at that time it will result in an inaccurate mapping of access points.

Workaround: Unassign the campus or building elements from the location server, then synchronize. Reassign the campus or building elements and then synchronize again.

- CSCsh79227—When connectivity between the location appliance and the controller is lost, alerts are not reported in WCS. Alerts are only reported when WCS loses connectivity to a controller.

Workaround: Check for connectivity between the location appliance and the controller. Also, check the location events table for SNMP unreachable messages.

- CSCsi12681—In cases where secure shell (SSH) versions earlier than 4.2, which do not support the GSSAPIDelegateCredentials option, are installed on the location appliance, third party security scanners might indicate security issues.

Workaround: Manually close all open ports on the location appliance and upgrade the location appliance SSH to version 4.2.

- CSCsi17755—When updating the time manually in the location appliance to adjust for daylight savings time, WCS does not display the manually entered time. The time remains one hour off.

Workaround: Do not manually adjust the time on the location appliance for daylight savings time. The system adjusts automatically to daylight savings time.

- CSCsi21064—Chokepoint heatmap circle on the map does not automatically resize after using the zoom in and out feature. Chokepoint mapping is only accurate when displaying in the default map size.

Workaround: None.

- CSCsi34248—The test fire function does not work for location change and battery level notifications. Test-fire verifies that an event notification is sent by the location appliance when a defined event definitions is triggered.

Workaround: None.

- CSCsi45791—When the battery remaining percentage (%) value is unknown (binary 1111), WCS displays the battery remaining percentage (%) in the Battery Life field for Cisco CX v1 asset tags as "-1%" rather than the correct value of "unknown."

Workaround: None.

- CSCsi46367— For some asset tags, the location history function (Monitor > Tags > *Location History*) does not automatically display any tag entries beyond the first listed when the play button is clicked.

Workaround: Click on the history item individually to retrieve information for the desired asset tag. You can access this information by selecting the Location History option from the Select a command drop-down menu on the Tag Properties page ((Path: Monitor > Tags > *Tag*)).

- CSCsi51747—WCS does not display a tamper count for tampering notifications received from the Cisco CX v1 tags.

Workaround: None.

- CSCsj54172—SNMP initialization fails and subsequently initialization of the location module fails when the `/etc/hosts` file does not have an entry for the location appliance's host name and IP address. The location appliance will continue to run but SNMP polling and location calculation is not occurring and is not reported in the log file.

Workaround: Stop the location appliance and run the `setup.sh` command for the location appliance and assign the location appliance a hostname. Verify that the `/etc/hosts` file includes the hostname and IP address for the location appliance. Restart the location appliance.

- CSCsj71650—The serial console port on the location appliance might “hang” when connected to certain models of USB serial converters.

Workaround:

1) If SSH access to the location appliance is available, add the character “-L” to the `agetty` text (process which handles the serial console) in the `/etc/inittab` file and then reboot the location appliance.

An example of the edit to the text is noted below:

```
co:2345:respawn:/sbin/agetty -L ttySO 9600 vt100-nav
```

2) Use a USB serial converter from another manufacturer.

Resolved Caveats

The following caveats are resolved in this release:

- CSCsc09186—Previous to this release, when you performed a location calibration, the process of taking data points could take up to one minute per point if a single controller was unreachable.
- CSCsc39959—Previous to this release, an element search by MAC address or asset information might not have reflected all elements seen in maps and summary lists, when you were operating with WCS release 3.2 and location appliance release 1.x. An upgrade to location appliance release 2.0 was recommended.
- CSCse13406—Previous to this release, on rare occasions, when multiple users were collecting data points for calibration, a user attempting to add a data point might have seen a map image vanish when WCS was resident on a Windows OS machine. The following error message might have appeared, “Unexpected inability to imwrite calmodel progress image.” This was a cosmetic issue only. This caveat did not affect functionality. The workaround involved navigating back to the calibration model and clicking save again; and, then continuing to add datapoints.
- CSCse60657—Previous to this release, in campus environments of 60 buildings or more with multiple-floors, some synchronization errors occurred on the location appliance given the number of images (floor) transferred. Location appliances, by design, are limited to 30 MB for each message transfer.
- CSCse76666—Previous to this release, when a location server was synchronizing with WCS and both polling and location calculation activities were active, a location appliance might have gone into a state in which no location calculations could occur. This intermittent condition could also happen when a heat map was generated. The condition did not occur if polling was turned “off.”
- CSCse76683—Previous to this release, once the 2,500 limit of supported elements for the location appliance was met, no new location calculations were reported for any element beyond the 2,500 limit. Location calculations were reported once an element within the recognized 2,500 elements aged out. This condition occurred even when polling was turned “off.”

- CSCse76793—Previous to this release, in some situations, the antenna name would not appear when you passed a mouse over a given access point on a map even though it did appear on the Position AP page.
- CSCsg15779—Previous to this release, the asset import function for location servers using WCS did not recognize empty lines in a file or spaces between elements; and, did not display an error when a value other than tag or station was seen in the class field.
- CSCsg33783—Previous to this release, you had to change the default root password during initial configuration of the location appliance to ensure optimum network security.
 - For releases 2.1.34 and later, you are prompted to change the password during the setup script.
 - You can also change the password using the Linux command, “passwd.”
- CSCsg46529—Previous to this release, the “last located” information accessed and displayed for clients and tags from the map by mousing over their icons was older than their configured polling periods.
- CSCsh95680—Previous to this release, in some instances when WCS and the location appliance were in the same network, the location debug feature for the client which provided details on the signal strength and access point associated with that client, could not hold an enabled state. A return to the Client Properties screen after enabling the feature, showed that the feature was not checked (disabled) and no RSSI information was seen on the map on the Client Properties page. This behavior was observed when operating with Internet Explorer version 6.0 (6.0.2900.2180). As a workaround, another Internet Explorer version was recommended.
- CSCsi14370—Previous to this release, the Reboot Hardware button found on the Location > Location Server > Advanced > Advanced page in Cisco WCS did not immediately reboot the location appliance. As a workaround, SSH was used to reboot the location appliance from within the shell using the following command: **reboot - h**.
- CSCsi19341—Previous to this release, when SNMP version 1 was used with Cisco WCS, the location appliance failed to track clients. As a workaround, SNMP versions 2c or version 3 were recommended for use with Cisco WCS and the controller.
- CSCsi24866—Previous to this release, the telemetry status value was not correctly displayed by WCS when the value was at its possible maximum of FFFFFFFF. Errors were seen on the Tag Properties page (Path: Monitor > Tags > Tag Properties). All other values were correctly parsed and displayed.
- CSCsi82520—Previous to this release, in some cases the location of elements in outdoor deployments were incorrectly displayed on Cisco WCS maps. Often the elements were grouped in the upper left-hand corner of the map.

The following caveats were resolved in release 2.1.42 and are incorporated into this release:

- CSCsg44373—Previous to this release, calibration was failing because WCS was receiving an erroneous RSSI value of positive (+)127 from the controller. WCS now filters out all RSSI values greater than or equal to zero (0).
- CSCsg67865—Previous to this release, the start and stop dates of daylight savings time (DST) for 2007 were reflected inaccurately in the Java Runtime Environment (JRE) in the location appliance due to a recent United States mandate. In 2007, DST within the US will begin on the second Sunday in March and end on the first Sunday in November. A mandatory upgrade to release 2.1.42.0 which incorporates support for this new DST period is required to prevent incorrect time reporting during certain periods of DST. Specifically, not upgrading to your location appliance to version 2.1.42.0 or later will result in incorrect time reporting from March 11, 2007 through April 2, 2007 and from October 29, 2007 through November 4, 2007.

- CSCsg68493—Previous to this release, the location appliance exposed an incorrect API call that could be exercised by a partner application extracting maps and resulted in a performance impact. In some circumstances, frequent exercise of map extraction in large access point networks (1200+ access points) could halt the location appliance and make it unresponsive.
- CSCsg83691—Previous to this release, after completion of a full calibration, data point icons would display as generic icons instead of the recognized data point icon. This was seen when location quality was queried (Path: Inspect Location Quality > Calibration Model > *Floor*).
- CSCsg93752—Previous to this release, older versions of floor hierarchies that were stored in the memory cache of the location appliance were not cleared appropriately after their deletion or after resynchronization with WCS. This resulted in the display of older floor hierarchies on the element detail page of WCS.

The following caveats were resolved in earlier releases of 2.1.x and are incorporated into this release:

- CSCsc64772—Previous to this release, when aggressive polling or historical parameters were configured for the location server, such as polling for all element categories every 10 seconds and saving history points every minute, database operations would take longer to complete, and the server momentarily took longer to respond to requests.
- CSCsd03171—Previous to this release, enabling the Advanced Debug option caused the communication setting to reset to the default HTTP setting even when configured for HTTPS.
- CSCsd05107—Previous to this release, conducting a client search using the 802.11b/g protocol filter would list 802.11b users but not 802.11g users.
- CSCsd05623—Previous to this release, if the customer lost the root password for the location appliance, there appeared to be no documented password recovery.

This issue was addressed by adding specific documentation in the 2.048.0 and 2.1.34.0 location appliance release notes and onward and in the location appliance configuration guide (June 2006 and onward.)

- CSCsd29958—Previous to this release, if you modified SNMP access for a controller via WCS and pushed the changes to the location server, the changes did not take effect until you either restarted the location server or unassigned and reassigned the controller to the location server on the synchronization page.
- CSCsd91565—Previous to this release, the total count of installed 802.11 b/g clients displayed on the Client Summary page but did not display on the floor summary page (Monitor > Map).
- CSCsd95125—Previous to this release, the Client list would display the client on the correct floor; however, the mini-map would display the client on a different, incorrect floor. Links to the client's resident floor were also incorrect.
- CSCsd95144—Previous to this release, Location History would often report an incorrect 802.11 state for clients in the Location History table and in the Client Details page when you changed from associated to disassociated.
- CSCse12576—Previous to this release, during the calibration procedure, a Cisco CX v.2 or later compatible client was recommended to take advantage of the latest features. Additionally, the Aironet information element (IE) option had to be enabled on the controller and the wireless LAN on which the client would communicate. If the Aironet IE option was disabled, the calibration procedure often did not generate sufficient data.
- CSCse22079—Previous to this release, you could not delete datapoints added during the calibration procedure.

- CSCse43442—Previous to this release, a logical condition prevented release of internal resources and threads would block up to two minutes when they logged errors. Errors logged included: (1) access points detected by controllers that were not yet assigned to maps; and (2) controllers synchronized for areas that had no maps or unsynchronized maps. The increased blocking time associated with error logging, increased the time required for location calculations and resulted in more infrequent location calculations and delayed information in the user interface and API.

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://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

(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 <http://www.cisco.com/tac>. Click **Technology Support**, choose **Wireless** from the menu on the left, and click **Wireless LAN**.

Documentation Updates

Structural Changes

A chapter was added to the *Cisco Location Appliance Configuration Guide, Release 3.0 version* to address location planning and verification. Refer to the Chapter 7 of that manual for details.

Related Documentation

The following documents are related to location appliances:

- *Cisco 2700 Series Location Appliance Installation and Configuration Guide*
- *Cisco Location Appliance Configuration Guide*
- *Cisco Wireless Control System Configuration Guide*
- *Cisco Wireless LAN Controller Command Reference*



Note

You can see the latest online versions of these documents at the following link:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the [Related Documentation](#) section.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, 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, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, 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. (0601R)

Copyright © 2007 Cisco Systems, Inc. All rights reserved.

