



Release Notes for Cisco 2700 and 2710 Location Appliances for Software Release 2.0.48.0

June 2, 2006

These release notes describe features, enhancements, and caveats for software release 2.0.48.0 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 3.2, 3.1, and 3.0.

Contents

These release notes contain the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Important Notes, page 3](#)
- [Caveats, page 4](#)
- [Troubleshooting, page 5](#)
- [Related Documentation, page 7](#)
- [Obtaining Documentation, page 7](#)
- [Documentation Feedback, page 8](#)
- [Cisco Product Security Overview, page 9](#)
- [Obtaining Technical Assistance, page 10](#)
- [Obtaining Additional Publications and Information, page 11](#)



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

© 2006 Cisco Systems, Inc. All rights reserved.

Introduction

Location appliance software release 2.0.48.0 supports Cisco 2700 and 2710 location appliances that operate with Cisco Wireless LAN Solution version 3.2, 3.1, and 3.0. Location appliances enhance the built-in Cisco WCS location capabilities by computing, collecting, and storing historical location data, which can be displayed in Cisco WCS. In this role, the location appliance acts as a server to one or more Cisco Wireless Control System (WCS) servers, collecting, storing, and passing on the location from its assigned Cisco wireless LAN controllers.

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
WCS 3.0	Supported	Supported ¹	Not supported
WCS 3.1	Supported ²	Supported	Supported from WCS 3.1.35.0 onward ³
WCS 3.2	Supported ^{2, 3, 4, 5}	Supported ^{3, 4, 5}	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.

Upgrading to this Software Release

For instructions on using Cisco WCS to install this software on location appliances, refer to the *Cisco Wireless Control System Configuration Guide*.

Click this link to browse to that document:

http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html

Backup of Release 2.0.x and Later Cannot Be Restored on Previous Releases

A backup from this release of location appliance software cannot be restored on a location appliance running an earlier release. Before you upgrade a location appliance to this release, Cisco recommends that you create a backup for the earlier release and archive it. This will allow 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, 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
```

Important Notes

This section describes important operational notes for the location appliance. There are no new features for this release.

Operational Notes

Please review the following operational notes for this release:

Recovering Lost Root Password

If you lose or forget the root password for the location appliance, you can recover the password by doing the following:

-
- Step 1** When the GRUB screen comes up, press **Esc** to enter the boot menu.
Press **e** to edit.
 - Step 2** 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 3** Press **b** to begin boot sequence.
At the end of the boot sequence, a shell prompt appears.
 - Step 4** You can change the root password by entering the **passwd** command.
 - Step 5** Enter and confirm the new password.
 - Step 6** Restart the machine.
-

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.

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.

Caveats

This section lists open caveats in location appliance release 2.0.48.0.

Open Caveats

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

- CSCsc09186—When you perform the location calibration, the process of taking data points can take up to one minute per point if a single controller is unreachable.
Workaround: Verify that controllers are reachable during calibration or remove the controllers that are not accessible.
- CSCsc64772—When aggressive polling or historical parameters are configured in the location server, such as polling for all element categories every 10 seconds and saving history points every minute, the database operations can take longer to complete, and the server can momentarily take longer to respond to requests.
Workaround: No known workaround.
- CSCsd05107—Conducting a client search using the 802.11b/g protocol filter will return the 802.11b users but not the 802.11g users.
Workaround: Do not filter by the 802.11b/g protocol option. Select the all option.
- CSCsd29958—If you modify the SNMP access for a controller in WCS and push the changes to the location server, the changes do not take effect until you either restart the location server or unassign or reassign the controller to the location server on the synchronization page.
Workaround: Restart the location server or reassign to or unassign the controller from the location server on the synchronization page.
- CSCsd36689—Access points in monitor mode do not detect probing clients as efficiently as when configured for local mode. These access points do not track the clients' RSSI values and do not contribute location information to the location appliance.
Workaround: Configure the access points for local mode.

- CSCsd95125—Client list will display client on the correct floor; however, the mini-map will display the client on a different, incorrect floor. Links to a client's resident floor are also incorrect.
Workaround: Upgrade to release 2.1.x and resynchronize WCS and the location appliance to correct the mistaken placement.
- CSCsd95144—Location History may report an incorrect 802.11 state for clients in the Location History table and in the Client Details page when you change from associated to disassociated.
Workaround: No current workaround.

Resolved Caveats

The following caveats are resolved in this release:

- CSCsd18053—Prior to this release, when WCS was configured to use a location appliance to get client statistics via polling and the time difference between WCS and the location was greater than the polling interval, the client statistics would not get new data from the location.
- CSCsd30763—Prior to this release, a period (.) in the name of a summary building or campus name would cause a synchronization error.
- CSCsd59889—When a customer network was configured with 6,500 elements on a single location server and history was being tracked every 30 minutes, network performance issues occurred.
Two issues addressed this issue (1) reminder that version 2.0.x of the location appliance is only designed to support 1,500 elements, and; (2) a recommendation to upgrade to version 2.1.x which provides support for 2,500 elements.
- CSCsd67122—Prior to this release, changes associated with removal of an element (e.g. switch) from a location server were not recognized by the location server until the location server was restarted.

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

Addition to the Quick Install Guide

The *Quick Start Guide: Cisco 2700 Series Location Appliance* should include the following information for location appliances.

When you have a non-default port or HTTPS turned on, you must pass the correct information along with the command. For example, *getserverinfo* must include `-port <<port>> -protocol <<HTTP/HTTPS>>`. Similarly, for stopping the server, *stoplocserver* - `port <<port>> -protocol <HTTP/HTTPS>`.

Additional Sections for the Location Appliance Installation Guide

Configuring NTP Server

You can configure NTP servers to set up the time and date of the 2700 location appliance.

The `/etc/ntp.conf` file is the main configuration file in which you place the IP addresses or DNS names of the NTP servers you want to use (see the following example).

```
server ntp.mydomain.com # my corporate NTP
server 192.168.2.5 # my second NTP
```

To get NTP configured to start at bootup, enter the following:

```
[root@loc-server1]# chkconfig ntpd on
```

To start, stop, and restart NTP after booting, follow these examples:

```
[root@loc-server1]# service ntpd start
[root@loc-server1]# service ntpd stop
[root@loc-server1]# service ntpd restart
```

After configuring and starting NTP, make sure it is working properly. To test whether the NTP process is running, use the following command:

```
[root@loc-server1]# pgrep ntpd
```

You should get a response of plain old process ID numbers.

Enter the `ntpdate -u<serverIP>` command to force your server to become instantly synchronized with its NTP servers before starting the NTP daemon for the first time (see the following example).

```
[root@loc-server1]# service ntpd stop
[root@loc-server1] ntpdate -u 192.168.1.100
Looking for host 192.168.1.100 and service ntp
host found: ntpl.my-site.com
12 Aug 08:03:38 ntpdate[2472]: step time server 192.168.1.100 offset 28993.084943 sec
[root@smallfry tmp]# service ntpd start
```

For more information on the NTP configuration, consult the Linux configuration guides.

Connecting to the Console

The DB9 pinout to connect to the console is as follows:

Table 2 *Pin Assignments for DB9 Pinout*

Pin	Assignments	Description
1	DCD	Data Carrier Detect
2	RD	Receive Data
3	TD	Transmit Data
4	DTR	Data Terminal Ready
5	SG	Signal Ground
6	DSR	Data Set Ready
7	RTS	Request to Send
8	CTS	Clear to Send
9	Ring	Ring Indicator

Related Documentation

This section lists documents related to location appliances:

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

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 © 2006 Cisco Systems, Inc. All rights reserved.