



Release Notes for Cisco 2700 and 2710 Location Appliances for Software Release 2.1.42.0

November 6, 2007

These release notes describe features, enhancements, and caveats for software release 2.1.42.0 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 4.0, 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 4](#)
- [Caveats, page 9](#)
- [Troubleshooting, page 12](#)
- [Documentation Updates, page 12](#)
- [Related Documentation, page 13](#)
- [Obtaining Documentation, page 13](#)
- [Documentation Feedback, page 14](#)
- [Cisco Product Security Overview, page 15](#)
- [Obtaining Technical Assistance, page 16](#)
- [Obtaining Additional Publications and Information, page 17](#)



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 2.1.42.0 supports Cisco 2700 and 2710 location appliances that operate with Cisco Wireless LAN Solution versions 4.0, 3.2, 3.1, and 3.0. 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
WCS 3.0	Supported	Supported ¹	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
WCS 3.2	Supported ^{2, 3, 4, 5}	Supported ^{3, 4, 5}	Supported	Supported ⁶
WCS 4.0 ⁷	Supported ^{2, 3, 4, 5, 7}	Supported ^{3, 4, 5, 7}	Supported ⁷	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 update notification update features are ignored by WCS. Location smoothing parameters and contributing access point debug options are ignored by WCS.
7. Battery level and location update notification update features are ignored by the location server. Location smoothing parameters and contributing access point debug options are ignored by the location server.

Upgrading to this Software Release

For instructions on using either Cisco WCS or a console port to install 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

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, 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 v2 is supported.



Note

After installing release 2.1.x, you must reboot the location appliance to remove support of SSH v1.



Note

To remove SSH v1 support for releases 2.0.x and earlier, you must manually edit the `sshd_config` file to remove support for SSH v1 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 or operational notes for software release 2.1.42.0 for location appliances.

Operational Notes

The following operational enhancements and updates are associated with this release.

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 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 Install

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

An example of the complete automatic installation script (and manual installation 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.

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 1-1 of this release note for WCS and location server compatibility.

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 CCX compatible and version 2 or greater. Adapter client versions less than 2.0 are not ideal for calibration.

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 > Administration > Location Parameters**

Software Restart Button Removed

The Software Restart Button is no longer available on the Advanced Parameters page.

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

Enhanced Maintenance Backup Operation

Progress of an active backup and its completion percentage now appear on the Backup Operation page for location servers. You can also open another window while the backup continues in the background.

Path: **Location > Location Server > Maintenance > Backup**

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.”

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.
-

New Feature Support

Please note the new feature support added since 2.0.48.0.

Smooth Location Positions (NEW Location Parameter)

You can adjust smoothing for a particular element. Options range from Off (no smoothing) to Maximum smoothing. The Off (no smoothing) option is appropriate for an item that is in constant movement such as an asset tag on medical equipment or store inventory. Maximum smoothing is appropriate for an item that is generally immobile.

Path: **Location > Location Server > Administration > Location Parameters**

Location Changes (NEW Event Notification)

Location Change events are generated by the location server when client stations, asset tags, rogue clients and rogue access points move from one location to another. Events are also logged when cleared.

Path: **Location > Notifications**

Battery Level (NEW Event Notification)

Battery Level events are generated by the location server for all tracked asset tags. Events are also logged when cleared.

Path: **Location > Notifications**

Number of Tracked Elements and Tracked Elements Limit (NEW Advanced Parameters)

Up to 2,500 elements can be tracked by a location server. This total value plus the current number of elements being tracked appears on the Advanced Parameters page. A major alert appears when the 2,500 limit is met.

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

Cisco UDI (NEW Advanced Parameter)

You can view the product identifier, version identifier, and serial number for a location server on the Advanced Parameters page. These values are unique to each location appliance.

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

Import and Export of Asset Information (NEW Administration Parameters)

You can import asset information stored in a flat text file into a location server. Information imported in the file must be in the following format: #Class, MAC Address, Asset Category, Asset Group, Asset Name.

Exported information is stored in the same format. You can name the file or keep the default file name of assets.out.

Path: **Location > Location Server > Administration > Import Asset Information OR Export Asset Information**

Display Contributing Access Points for Client and Tag Locations (NEW Monitor Parameters)

Client and Tag location can be monitored with respect to the access point that generated the signal. Strength of the access point signal and age of the last reading is also reported. This expanded information for clients and tags is available on the map page. To view, pass the mouse over the relevant client or tag. To enable, check the **Location Debug** option box found on the Tag Properties and Client Properties pages.

Path: **Monitor > Devices > Tag OR Client**



Note

Additional information is available in the “Monitoring Clients” and “Monitoring Tagged Assets” sections of Chapter 7 in the *Cisco Location Appliance Configuration Guide*.

Display Last Detected Information for Clients and Tags with Filtering Option (NEW Monitor Parameters)

You can set how often the location server updates its client and tag location information from their respective summary pages. Information updates can be as often as every 5 minutes.

To initiate this option for tags, you would select the desired polling frequency from the **Last Detected Within** menu.



Note

You can also define which tags are polled by defining additional search criteria such as location server, asset name or floor area via the **Search for Tags by** menu.

To initiate this option for clients, you would select the desired polling frequency from the Load **Location Server data as old** as menu.

**Note**

You can define which clients are polled by defining additional search criteria such as location server, user name, MAC address or floor area via the **Search for Clients by** menu.

Path: **Monitor > Devices > Tag OR Client**

**Note**

Additional information is available in the “Monitoring Clients” and “Monitoring Tagged Assets” sections of Chapter 7 in the *Cisco Location Appliance Configuration Guide*.

Inspecting Location Readiness and Location Quality (NEW Monitor Parameters)

You can configure Cisco WCS to verify the ability of the existing access point deployment to estimate the true location of an element within 10 meters at least 90% of the time. The location readiness calculation is based on the number and placement of access points.

You can also check the location quality and the ability of a given location to meet the location specification (10 m, 90%) based on data points gathered during a physical inspection and calibration.

Inspecting Location Readiness Using Access Point Data:

You would select **Inspect Location Readiness** from the menu found at the top-right of the Monitor>Maps page. A color-coded map appears showing those areas that do (Yes) and do not (No) meet the 10 meter, 90% location specification.

Path: **Monitor > Maps**

Inspecting Location Quality Using Calibration Data:

After completing a calibration model based on data points generated during a physical tour of the area, select the appropriate **RF Calibration Model** from the menu at the top-right of the Monitor>Maps page. Then select the **Inspect Location Quality** link found on the page that appears.

Path: **Monitor > Maps**

Deployment Planning for Data, Voice, and Location (NEW Monitor Parameter)

You can calculate the recommended number and location of access points based on whether data, and/or voice traffic is active, and/or location is considered. Use the **Planning Mode** option on the Maps page to begin the access point calculation.

Path: **Monitor > Maps**

Analyzing Element Location Accuracy Using Testpoints (NEW Location and Monitor Parameter)

You can analyze the location accuracy of rogue and non-rogue clients and asset tags by entering testpoints on an area or floor map. You can use this feature to validate location information generated either automatically by access points or manually by calibration. Refer to Chapter 5 of the *Cisco Wireless Control System Configuration Guide, Software Release 4.0* for more details.

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

Caveats

This section lists open and resolved caveats in location appliance release 2.1.42.0.

Open Caveats

The following caveats are open (unresolved) in this release (2.1.42.0):

- CSCsc09186—When you perform a 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 those controllers that are not accessible.

- CSCsc39959—An element search by MAC address or asset information may not reflect all elements seen in maps and summary lists, when operating with a release 3.2 WCS and release 1.x location appliance.

Workaround: Upgrade the location appliance to release 2.0 or greater.

- 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.

- CSCse13406—On rare occasions, when multiple users are collecting data points for calibration, a user attempting to add a data point may see the map image vanish when WCS is resident on a Windows OS machine. The following error message may appear, "Unexpected inability to imwrite calmodel progress image." This is a cosmetic issue only. This caveat does not affect functionality.

Workaround: Navigate back to the calibration model and click save again. You can then continue to add datapoints.

- CSCse34650—After performing a calibration using a CCX 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.

- CSCse60657—In campus environments of 60 buildings or more with multiple-floors, some synchronization errors may occur on the location appliance given the number of image (floor) transfers. (Location appliances are limited to 30 MB for each message transfer.)

Workaround: Limit the number of buildings assigned to each Campus structure.

- CSCse76666—When a location server is synchronizing with WCS and both polling and location calculation activities are active, a location appliance may go into a state in which no location calculations can occur. This intermittent condition can also happen when a heat map is generated. The condition does not occur if polling is turned “off.”

Workaround: To prevent this condition from occurring, do the following:

- (1) Turn OFF all polling.
- (2) Wait for a few minutes, as close to the actual polling interval as possible. (This allows ongoing polling and calculation threads time to finish processing).
- (3) Proceed with the synchronization operation.
- (4) Turn ON polling. (*Continued on next page*)

If you are unable to prevent the condition from occurring, restart the location appliance.

- CSCse76683—Once the 2,500 limit of supported elements for the location appliance is met, no new location calculations are reported for any element beyond the 2,500 limit. Location calculations are reported once an element within the recognized 2,500 elements ages out. This condition occurs even when polling is turned “off.”

Workaround: Adjust the Prune Data Interval (History Parameters) to prune recognized elements. Once pruning occurs, reset the Prune Data Interval to its previous value.

- CSCse76793—In some situations, the antenna name may not appear when you pass a mouse over a given access point on a map even though it does appear on the Position AP page.

Workaround: Choose a different name to the antenna and then the correct name and then select Save.

- CSCsg33783—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.”

Workaround: None.

Resolved Caveats

The following caveats are resolved in this release (2.1.42.0):

- CSCsg44373—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 2.1.x releases:

- 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 CCX 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

Software Documentation

The following information is missing in the latest *Cisco Location Appliance Configuration Guide*.

Using HTTPS or Non-Default Ports

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>>*.

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
```

**Note**

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

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 http://www.cisco.com/en/US/products/ps6386/tsd_products_support_series_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>

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

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