CHAPTER 4

Installation and Configuration

Installing and Configuring the Location Appliance

Detailed procedures for installing and configuring the Cisco Location Appliance can be found in the following documents:

- *Release Notes for Cisco Wireless Location Appliance Release 3.0*— http://www.cisco.com/en/US/products/ps6386/prod_release_notes_list.html
- *Cisco Wireless Location Appliance: Installation Guide*— http://www.cisco.com/en/US/products/ps6386/products_installation_and_configuration_guide_book09186a00804fa761.html
- *Cisco Wireless Location Appliance: Configuration Guide*— http://www.cisco.com/en/US/products/ps6386/products_installation_and_configuration_guides_list.html

Configuring Cisco WCS for Location Tracking

It is assumed that the reader has installed either a Windows or Linux-based version of WCS that is appropriately licensed for location use with the Cisco Wireless Location Appliance. Detailed procedures for configuring the Wireless Control System for location use with the Cisco Wireless Location Appliance can be found in the following documents:

- Cisco Wireless Control System Release Notes, Release 4.1— http://www.cisco.com/en/US/products/ps6305/prod_release_notes_list.html
- Cisco Wireless Control System Configuration Guide, Release 4.1— http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html
- Cisco Wireless Location Appliance: Deployment Guide— http://www.cisco.com/en/US/products/ps6386/prod_technical_reference09186a008059ce31.html

Configuring Location Appliance History Parameters

The configuration of Location Server > Administration > History Parameters is discussed in the document entitled *Cisco Wireless Location Appliance Configuration Guide: Editing History Parameters* at the following URL:
http://www.cisco.com/en/US/products/ps6386/products_configuration_guide_chapter09186a008082d72f.html#wp1046373.

Further clarification regarding some of these parameters is provided in the subsections that follow.

A common misconception about the history capabilities of the location appliance is that it somehow stores a historical record of all locations the client has ever encountered. As is discussed in the following two sections, the location application stores history information based on the values of the archive period and archive interval parameters. If a history record for a device is recorded at time T_0 and the archive period is 30, the next history record for that device is written at T_{0+30}. The device may have undergone several changes in location between T_0 and T_{0+30}; however, only the location states at time T_0 and T_{0+30} are recorded in the history database.

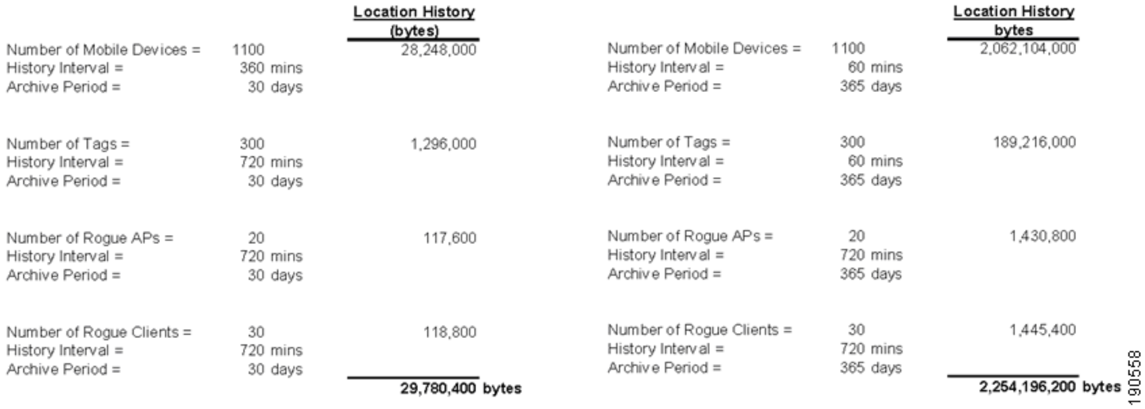
History Archive Period

The history archive period (shown as “Archive For”) specifies the number of days that the location appliance retains location history records for each enabled history collection category. The default archive period is 30 days. Changes to the default history archive period should be done with careful consideration after consultation with your Cisco field technical representative or the Cisco Technical Assistance Center, because longer history periods typically increase the amount of space consumed by the location history database. Because newer history data within the archive period does not overwrite older data, the combination of a large number of devices, an injudicious selection of history categories, and an excessive history archive period can increase the risk of exhausting available free space.

To illustrate this point, we can compare the amount of disk storage that is consumed when selecting one combination of history category, archival period, and archival interval versus another. To do this, let us assume an environment consisting of 1100 WLAN clients, 300 asset tags, 20 rogue access points, and 30 rogue clients. Figure 4-1 illustrates the effect on consumed disk storage of the following:

- Increasing the default archive period to 365 days for all device categories
- Reducing the default history archive interval for clients (“mobile devices”) and asset tags to 60 minutes.

Figure 4-1 ***Impact of History Interval and Archive Period on Database Size***



		Location History (bytes)			Location History bytes
Number of Mobile Devices =	1100	28,248,000	Number of Mobile Devices =	1100	2,062,104,000
History Interval =	360 mins		History Interval =	60 mins	
Archive Period =	30 days		Archive Period =	365 days	
Number of Tags =	300	1,296,000	Number of Tags =	300	189,216,000
History Interval =	720 mins		History Interval =	60 mins	
Archive Period =	30 days		Archive Period =	365 days	
Number of Rogue APs =	20	117,600	Number of Rogue APs =	20	1,430,800
History Interval =	720 mins		History Interval =	720 mins	
Archive Period =	30 days		Archive Period =	365 days	
Number of Rogue Clients =	30	118,800	Number of Rogue Clients =	30	1,445,400
History Interval =	720 mins		History Interval =	720 mins	
Archive Period =	30 days		Archive Period =	365 days	
		29,780,400 bytes			**2,254,196,200 bytes**

Although the estimates shown in Figure 4-1 are only an approximation (they do not account for per record display string sizes and database overhead, for example), you can see that database size increases from about 30 MB to over 2.25 GB because of these changes in location history alone. The database backup mechanism on the location appliance requires that there be at least as much free space available as is used in order to support reliable extraction and compression, thereby bringing the total estimated space requirement to over 5 GB.

History Database Pruning

Database pruning is especially important in situations when there is a high risk of a situation occurring where available hard disk space becomes critically low. If low available disk space situations re-occur, more aggressive data pruning intervals may be warranted such that pruning occurs more frequently and well in advance of a low disk space situation. These aggressive data pruning intervals may need to be combined with a shorter history archive interval if the adjusted pruning intervals alone are not sufficient in addressing the low free disk space situation.

Configuring Location Appliance Advanced Parameters

The configuration of Location Server > Administration > Advanced Parameters is discussed in the document entitled *Cisco Wireless Location Appliance Configuration Guide: Editing Advanced Parameters* at the following URL:
http://www.cisco.com/en/US/products/ps6386/products_configuration_guide_chapter09186a008082d72f.html#wp1050981.

Further clarification regarding a subset of the Advanced Parameters is provided in the following subsections.

Absent Data Cleanup Interval

The “Absent Data Cleanup Interval” or ADCI (range 1 to 99,999 minutes) specifies the amount of time that an entry is kept for a tracked entity (WLAN client, tag, rogue access point, or rogue client) in the active location database. The ADCI specifies the amount of time that must expire before the tracked device entry is removed from the active location database if no recent updates have been received for that device.

For example, if the RSSI information for an asset tag was last recorded by the location appliance two days ago and the cleanup interval is set to the default value of 1440 minutes (24 hours or 1 day), the station will be removed from the active location database after the expiration of the 24 hour absent data cleanup interval. Note that once the device is removed from the active location database, it will not be possible to “scroll back” and review the last known location of the device using the “load location server data as old as” dropdown menu control.

The limit of 2500 total tracked devices in the location appliance applies strictly to those devices that are in the active location database. Once the total number of devices (clients, tags and rogues) in the active database reaches 2500, additional devices cannot be tracked by this location appliance until some of the currently tracked devices contained in the active location database expire and are pruned from the database.

In some cases, the default value for the Absent Data Cleanup Interval may be found to excessively delay the clean-up of devices that have been recently removed from the tracked environment. A good case in point might be a location appliance with 1500 tracked asset tags and client stations, where an operator has enabled rogue location tracking in an environment with a high concentration of rogue devices. If the system were to discover 1000 rogue devices, for example, these would be added to the active location database and would bring the total number of tracked devices for this location appliance to its maximum capacity of 2500. If location tracking of tagged assets and WLAN clients are considered to be a higher priority than the tracking of rogue devices, a potential problem could exist. If new tags or clients are added to the environment, there may not be any available capacity to track them until some of the currently tracked devices (existing WLAN clients, asset tags or rogue devices) expire and are pruned from the active location database.

Note Version 4.2 of the location-aware Cisco UWN introduces a enhancement that allows for individual limits to be placed on what portion of the location appliance’s aggregate tracked device capacity is allocated to each tracked device category (i.e. WLAN clients, asset tags, or rogue devices).

It is important to note that in this situation, disabling the tracking of rogue devices in the location appliance entirely will not immediately remove the 1,000 tracked but unwanted rogue devices from the active location database. Rather, the Absent Data Cleanup Interval will by default maintain each currently tracked rogue device in the active location database for a period of 1440 minutes past the time of its last RSSI update. Plainly put, in the case of our example using the default value for the ADCI, disabling rogue location tracking today will not prune those tracked device entries from the active location database until approximately the same time tomorrow.

To work around this and remove the unwanted devices from the active location database more expeditiously, we can temporarily set the Absent Data Cleanup Interval to a much lower value for a brief duration in order to accelerate the pruning of any unwanted tracked devices from the active location database. For example, our hypothetical operator might choose to temporarily set the Absent Data Cleanup Interval to sixty minutes after disabling location appliance polling for rogue devices. Sixty minutes after this setting has been applied, the location appliance will remove all devices from the active location database for which updated information has not been received from WLAN controllers within the last hour, including the undesired rogue devices. Once this has occurred, the "Number of Tracked Elements" field shown on the Location Servers > Advanced Parameters menu page should decrease, reflecting the number of devices removed from the active location database.

The Absent Data Cleanup Interval is a single parameter that applies to all device categories. Thus, a potential drawback of temporarily lowering the ADCI in this way is that the removal of tracked devices from the active location database occurs in a non-selective fashion. That is to say, all devices for which information updates have not been received by the location appliance meeting the ADCI time criteria will be removed. In our example, this means that not only would our unwanted rogues be removed, but so would any clients or asset tags for whom we have not received any updates in the last sixty minutes as well. Such behavior could prove surprising to location client users that have come to depend on a 24 hour window of prior location information in order to locate "lost" assets for which current location information is not available.

In lab testing, it was found that the use of the location history database can partially mitigate this in cases where tracked devices have been removed from the active location database but are later re-detected by the UWN. In such cases, any prior collected location history records will once again be available, unless their history archive period has expired and the history records themselves have been pruned. History records for devices that have been deleted from the active location database, but have not been re-detected by access points, will not be accessible via location clients.

In some cases, it may be desirable to alter the default value for Absent Data Cleanup Interval on a more permanent basis. One example of such a case might be an facility that employs location tracking but has a large number of transient Wi-Fi devices, such as client laptops, PDAs and so on, residing onsite only a few hours before moving on, and then not returning for several days. Another example might be a logistics cross-docking facility that may only contain 2000 tagged asset containers during any four hour period, but through whose doors a volume of 10,000 or more tagged asset containers may pass within a 24 hour period.

In either of these cases, the quantity of track-able Wi-Fi client devices or asset tags actually on site at any one time may be significantly less than the maximum tracked device capacity of the location appliance. However, the number of transient devices that may pass through the facility over a 24 hour period will easily exceed 2500. Should this occur while using the default value for Absent Data Cleanup Interval, there may be a risk of the location appliance's tracking capacity becoming exhausted, as devices that may have left the facility several hours ago will not be removed from the active location database until the 24 hour ADCI has expired. Setting the value for Absent Data Cleanup Interval to a lower value (say, for example, four hours or 240 minutes) would expedite the cleanup of these migrated devices and release tracked device capacity on the location appliance for use by recent device arrivals.

Reducing the value of the Absent Data Cleanup Interval is not without its tradeoffs, however. For further discussion of the Absent Data Cleanup Interval, the potential tradeoffs involved in changing it and how this may factor into your overall design approach, it is recommended that the reader consult the examples given in Multiple Location Appliance Designs, page 5-33.

Memory Information

- DB Disk Memory—A misnomer, this parameter does not refer to "memory" on the location appliance. Rather, it displays the amount of disk space that has been consumed by the location appliance database. This information is useful when determining whether a database de-fragmentation should be performed (see Advanced Commands, page 4-6).
- Run Java GC—This command runs a general memory clean-up immediately. Normally, memory cleanup is initiated by the system automatically and thus does not require manual initiation. Therefore, Java General Cleanup need only be run when directed by the Cisco Technical Assistance Center (TAC) or Cisco Engineering.

Advanced Commands

The Defragment Database advanced command defragments the location database and reclaims allocated but unused disk space. A database defragmentation can be beneficial if free disk space on the location appliance is running low because of large database size, or if the response time of the location appliance appears noticeably slower when data is requested by location clients.

To determine how much free space is currently available on the location appliance, it is necessary to log into the location appliance via either the CLI serial console or an SSH session. When logged in, use the Linux command **df -H** to display disk free space, as follows:

```
[root@AeS_Loc root]# df -H

Filesystem            Size  Used Avail Use% Mounted on
/dev/sda2              77G  3.2G   70G   5% /
/dev/sda1             104M   16M   83M  16% /boot
none                  526M     0  526M   0% /dev/shm

[root@AeS_Loc root]#
```

Note The **df –H** command is used above because it is a commonplace practice for most computer disk manufacturers to assume 1 GB = 1,000,000,000 bytes. The **–H** option displays output as powers of 1000 rather than 1024. Use **df –h** if your preference is for the contrary.

The **df** display output shown here is for a location appliance containing a hard disk drive with an unformatted capacity of 80 GB. Notice that there are two main file systems defined: /dev/sda1, which is the Linux boot file system; and /dev/sda2, which contains the root directory as well as the location application and all databases. You can clearly see from the display above that only 5 percent of all available space on /dev/sda2 is currently being used. That being the case, there is an abundance of free space available and defragmentation is unlikely to be required at this time.

You can use the information in the **df** output along with the knowledge of the size of the location database (from DB Disk Memory described in Memory Information, page 4-6) to approximate the maximum recommended size to which the location appliance database should be allowed to grow. At first glance, this may appear intuitive; that is, max recommended database size = total available disk space – (OS size + location application size). However, you should also account for the creation of a flat file that is used during the database backup process. Using the formula below, you can calculate the maximum recommended size of the location database including this additional free space plus a small additional amount to account for system overhead (such as the downloading of an location appliance upgrade image):

$$MaxDatabaseSize = \frac{TotalSpace - OSApplSpace}{2.3}$$

Where:

- *MaxDatabaseSize* is the maximum recommended size of the database in bytes

Note *MaxDatabaseSize* assumes the user has performed a cleanup of any residual location appliance upgrade images. Multiple residual upgrade images may consume additional free space exceeding these allotments.

- *TotalSpace* is the total amount of available space on /dev/sda2 in GB.
- *OSApplSpace* is the amount of space occupied by the Linux OS and the location appliance application on /dev/sda2. This can be calculated for the example shown above as:

  (the amount of used disk space in Gigabytes) – (the current size of the location appliance database in Gigabytes).

The current size of the location appliance database can be found at WCS > Location Server > Advanced Parameters > DB Disk Memory. In the case of the system used for this example, DB Disk Memory = 24,608,768 bytes or .0246 GB. Thus, OSApplSpace = (3.2 - .0246 GB) or 3.175 GB.

Substituting the values for TotalSpace and OSApplSpace into the equation, you can calculate the maximum recommended size to which the location appliance database should be allowed to grow as (77 GB - 3.175 GB) / 2.3 = 73.825 / 2.3 = 32.0 GB. Therefore, to ensure proper operation of the database backup mechanism in a location appliance with an 80 GB unformatted capacity hard disk drive, the maximum recommended size of the location database (as indicated by DB Disk Memory) should not be allowed to exceed 32 GB.

Configuring Location Appliance Location Parameters

The configuration of Location Server > Administration > Location Parameters is discussed in *Cisco Wireless Location Appliance Configuration Guide: Editing Location Parameters* at the following URL:

http://www.cisco.com/en/US/products/ps6386/products_configuration_guide_chapter09186a008082d72f.html#wp1050973.

Further clarification regarding select parameters is provided in subsequent sections.

Enable Calculation Time

The *enable calculation time* location parameter refers to an advanced debugging option that enables logging of the amount of time that internal localization calculations consume. It is disabled by default and should be enabled *only* on the recommendation of the Cisco Technical Assistance Center (TAC) or Cisco Engineering, because it adds overhead to the location calculations.

Enable OW (Outer Wall) Location

Although the WCS Map Editor allows interior walls to be placed within floor maps, the location appliance only takes into consideration up to 50 “heavy” walls when evaluating path loss models and conducting positioning calculations. Heavy walls are those defined in the Map Editor with attenuation values of 13 dB. When the “Wall Usage Calibration” parameter in WCS (Monitor > Maps > Properties >Wall Usage Calibration) is set to “Auto”, the location appliance will dynamically determine whether to use the attenuation introduced by heavy walls during the calculations performed as part of the calibration process.   The system administrator can, however, opt to include heavy wall attenuation in all cases by setting this parameter to “Use Walls”, or disable the use of heavy walls entirely by setting it to “Do Not Use Walls”.

Enable OW Location is a parameter that was used with software releases prior to release 4.0 of the Cisco UWN (i.e., prior to Release 2.1 of the Cisco Wireless Location Appliance). *Enable OW Location* is still displayed on the Location Server > Administration > Location Parameters menu in Release 4.1 of WCS for backward compatibility with these earlier releases. However, with software Release 4.1, there is no benefit to be gained by changing this parameter from its default setting.

RSSI Discard Times

- Relative RSSI Discard Time—This parameter denotes the relative boundary of RSSI sample times used in location calculations. It specifies the time between the most recent RSSI sample and the oldest usable RSSI sample. The default relative RSSI discard time is 3 minutes. During normal operation of the location appliance, this parameter should be left at the default value and should *not* be changed except on the advice and recommendation of the Cisco Technical Assistance Center (TAC) or Cisco Engineering.
- Absolute RSSI Discard Time—This parameter denotes the absolute boundary of RSSI sample times used in location calculations. The default is 60 minutes, which means that RSSI samples older than 60 minutes are not used in location calculations, regardless of relative RSSI discard time. During normal operation of the location appliance, this parameter should be left at the default value and should *not* be changed except on advice of the Cisco Technical Assistance Center (TAC) or Cisco Engineering.

RSSI Cutoff

In addition to enforcing the aforementioned relative and absolute time constraints against received RSSI reports, the location appliance also applies a parameter known as the *RSSI cutoff*. Subject to the time constraints described in *RSSI Discard Times*, the location appliance retains the four highest signal strength reports plus any signal strength reports that meet or exceed the value specified for RSSI cutoff. The default value for RSSI cutoff is -75 dBm.

The application of the RSSI cutoff threshold is illustrated in the following examples:

- Four RSSI reports of -68dBm, -70dBm, -72dBm, and -80dBm—All four reports are retained because they are the four highest reports.
- Five RSSI reports of -66dBm, -68dBm, -70dBm, -72dBm, and -74dBm—All five reports are retained because they all meet or exceed the default RSSI cutoff threshold.
- Five RSSI reports of -66dBm, -68dBm, -70dBm, -72dBm, and -80dBm—The first four reports are retained, the fifth report of -80dBm is discarded because it does not meet the default RSSI cutoff threshold of -75 dBm and there already exists four other signal reports that meet or exceed the threshold.

Configuring Location Appliance Notification Parameters

The configuration of Location Server > Administration > Notification Parameters is discussed in *Cisco Wireless Location Appliance Configuration Guide: Configuring Notification Parameters* at the following URL:
http://www.cisco.com/en/US/products/ps6386/products_configuration_guide_chapter09186a008082d744.html#wp1053921.

Further clarification regarding select parameters is provided in the following sections.

Queue Limit

The Queue Limit parameter specifies the size of the output notification queue of the location appliance. This value normally defaults to 500. The location appliance drops any outbound notifications above this limit if the output notification queue size is exceeded. Therefore, if you notice that some outbound notifications are being dropped (via the Notifications Dropped field), you may want to increase the queue limit size.

Retry Count

For each matching condition, the Retry Count specifies the number of northbound notification “firings” that will be allowed for the same device (over and above the initial firing) before the wait period specified by the Refresh Time parameter begins. Thus, the total number of “firings” of northbound notifications allowed between Refresh Time periods will be equal to one plus the value specified for Retry Count. The default value for Retry Count is one.

Keep in mind that:

- More than one physical northbound notification message can be sent per “firing” (for example SMTP, Syslog, SNMP, or SOAP).
- Retry Count and Refresh Time apply independently to each matching device MAC address.
- Retry Count and Refresh Time apply independently to event definitions. However, event definitions that apply the same trigger conditions to the same device MAC addresses will share a Retry Count/Refresh Time parameter set.

As an example, assume that the location appliance has been configured to transmit SNMP, email and syslog northbound notifications when a high-priority condition arises for a specific asset tag. For the purpose of this example, let us assume the high priority event is the depression of a call button on an asset tag, such as the AeroScout T2 or T3. Also assume that the notification Refresh Time is set to sixty minutes and the notification Retry Count is set to one (the default values). Under these conditions, the location appliance will generate SNMP, email and syslog northbound notifications for each high-priority event occurring for this tag, up to a maximum of two northbound notifications. After the value of one plus the Retry Count has been reached, the location appliance will skip firing any further northbound notifications for this condition and device for the time period specified by the Refresh Time. Once the Refresh Time has expired, this cycle will repeat unless the event has been cleared.

Refresh Time

Refresh Time specifies the length of the wait period between transmission of northbound notification sets for a specific event condition and device, as described above in Retry Count, page 4-9. After the expiration of the Refresh Time, the event condition is eligible for re-evaluation and, if still present, may once again result in the generation of northbound notifications.

Refresh Time and Retry Count are used cooperatively to help limit the number of northbound notifications that are repeatedly generated for uncleared events. Retry Count limits the number of northbound notifications that are sent by the location appliance, while Refresh Time imposes a “waiting period” during which time no further northbound notifications will be sent for this event condition and device.

Refresh Time is specified in minutes, with the default being 60 minutes.

Notifications Dropped

This is a read-only counter field indicating the total number of notifications that have been dropped from the notification queue since the location appliance was started. Note that stopping and restarting the location appliance software application (locserverd) will reset this counter. The Notifications Dropped counter should be used in conjunction with the Queue Limit parameter to reduce the number of total dropped notifications.

Configuring Location Appliance LOCP Parameters

The configuration of Location Server > Administration > LOCP Parameters is discussed in *Cisco Wireless Location Appliance Configuration Guide: Configuring LOCP Parameters* at the following URL: http://www.cisco.com/en/US/products/ps6386/products_configuration_guide_chapter09186a008082d72f.html#wp1050918.

Location Appliance Dual Ethernet Operation

The Cisco Wireless Location Appliance is equipped with two 10/100/1000BASE-T Gigabit Ethernet ports that can be used to “dual-home” the location appliance to two different IP networks. This makes it a simple affair, for example, to configure a location appliance for service on network “A” while affording it the capability to be managed out-of-band on network “B” if the need arises. Complete step-by-step guidelines to accomplish this are available in *Cisco Wireless Location Appliance Installation Guide: Configuring the Location Appliance* at the following URL: http://www.cisco.com/en/US/products/ps6386/products_installation_and_configuration_guide_chapter09186a00804fab8e.html#wp1040488.

Particular attention should be paid to the fact that the dual onboard Ethernet controllers on the location appliance are *not* intended for redundant or simultaneous connection to the same IP network. Configurations aimed at establishing parallel, load balancing, or redundant Ethernet connections to the same IP network are not recommended at this time.

Changing Location Appliance Default Passwords

Changing the “root” User Linux System Password

The location appliance ships with a default root userid and password. It is recommended that the password for the root userid be changed during initial configuration of the location appliance to ensure optimum network security. This can be done during the execution of the initial setup script as described in “Installation and Configuration” section of the *Cisco 2700 Series Location Appliance Installation and Configuration Guide*, located at http://www.cisco.com/en/US/docs/wireless/location/2700/quick/guide/li31main.html#wp1049597.

When logged in, the Linux command **passwd** can be used to change the root system password as follows:

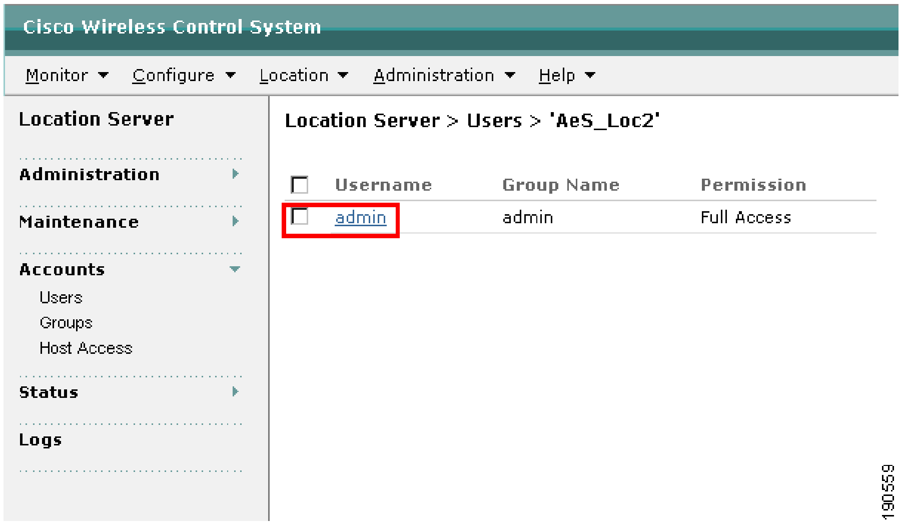
```
AeS_Loc login: root
Password:
Last login: Thu Oct 22 09:53:21 on ttyS0
[root@AeS_Loc root]# passwd
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@AeS_Loc root]#
```

Changing the "admin" Location Server Application Password

The location server application on the location appliance ships with an administrator user account and group predefined. The userid is *admin* and the password is *admin*. After WCS has successfully contacted the location server application using the factory default administrator credentials, the default password on the admin account can be changed to a less well-known value via the WCS menu Location > Accounts > Users menu.

Step 1 Begin by clicking on the **admin** userid, as shown in Figure 4-2.

Figure 4-2 Default Location Appliance User ID

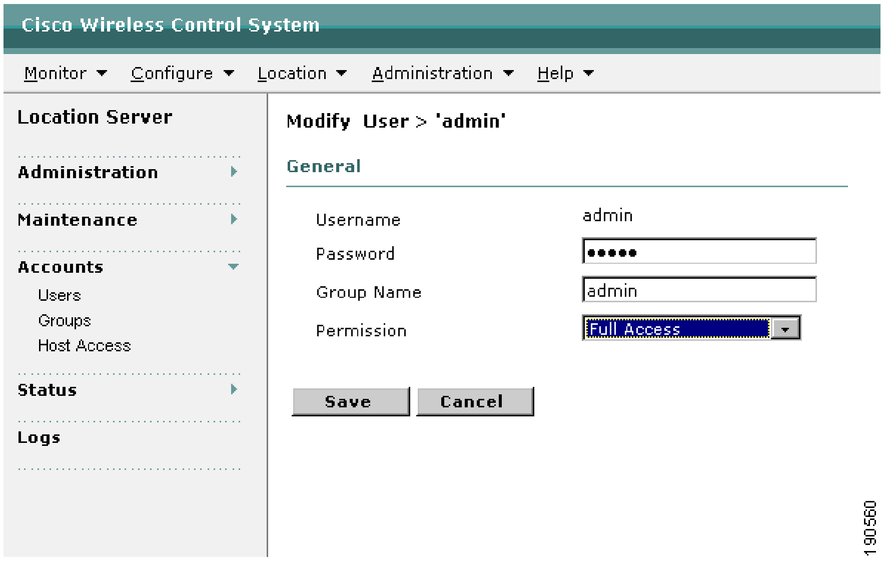


Location Server > Users > 'AeS_Loc2'

□	Username	Group Name	Permission
□	admin	admin	Full Access

Step 2 Clicking on the Admin box brings up the menu shown in Figure 4-3, which allows the password to be changed for the admin userid.

Figure 4-3 Modifying the Admin Password



Modify User > 'admin'

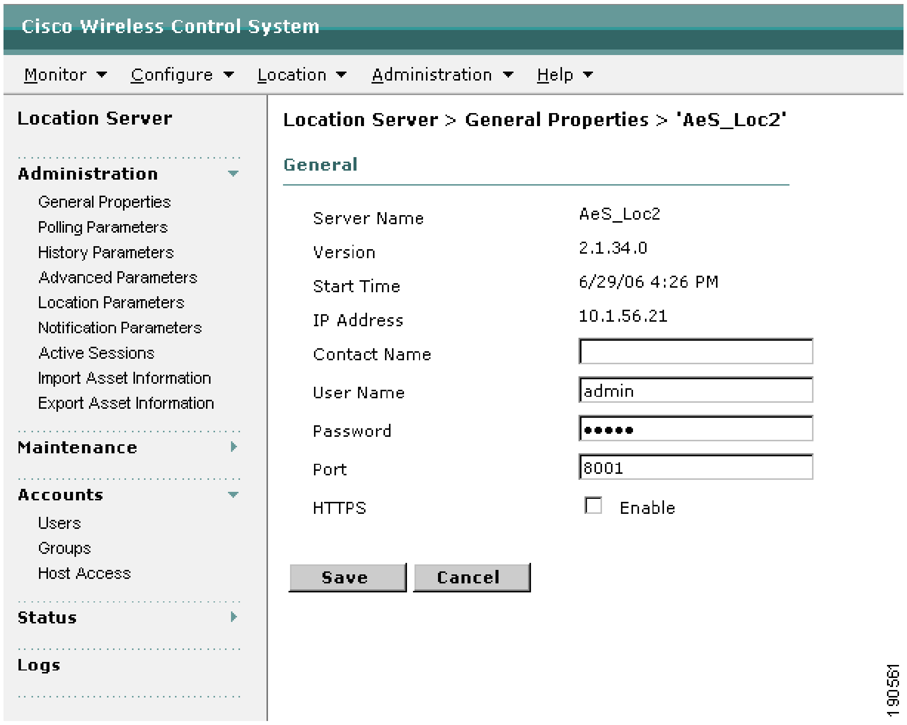
General

Username	admin
Password	●●●●●
Group Name	admin
Permission	Full Access

Step 3 Finally, change the value for the password used by WCS to access the location server application to the new value that was specified in Figure 4-3. This can be performed via Location Server > Administration > General Properties, as shown in Figure 4-4.

Note that any third-party location clients that have been configured to also use the admin userid to access the location server application via the SOAP/XML API needs to be changed accordingly. You may prefer to define a totally separate userid for each third-party location client that accesses the location appliance, instead of allowing them to use the admin account.

Figure 4-4 Specifying Location Server Application Login Credentials



Location Server > General Properties > 'AeS_Loc2'

General

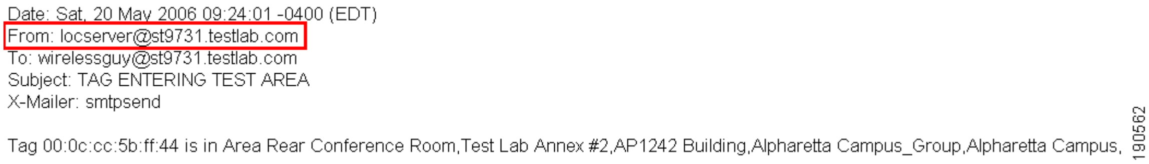
Server Name	AeS_Loc2
Version	2.1.34.0
Start Time	6/29/06 4:26 PM
IP Address	10.1.56.21
Contact Name	
User Name	admin
Password	•••••
Port	8001
HTTPS	□ Enable

Location Appliance Time Synchronization

In order to assure reliable and consistent operation across the network, it is recommended that the WLAN controllers, location appliances and WCS systems within the Cisco UWN maintain synchronized internal clocks. As a general network recommendation, establishing synchronized internal clocks facilitates troubleshooting by making it much easier to correlate log messages between components. Whether viewing independent log files from various components or a combined syslog, having log entries use consistent time stamp references in their message text only serves to make such messages more logical and easier to understand.

This usefulness of consistent timestamps becomes especially clear when multiple location appliances are configured to send asynchronous northbound notifications to a common destination, such as email messages for example. Location appliances configured with the incorrect system time may issue notification messages (as shown in Figure 4-5 bearing incorrect or inconsistent times that may appear confusing to operators at network operations centers (NOCs) or other control points.

Figure 4-5 Email Notification Message Bearing Time Stamp of Location Appliance



Date: Sat, 20 May 2006 09:24:01 -0400 (EDT)
From: locserver@st9731.testlab.com
To: wirelessguy@st9731.testlab.com
Subject: TAG ENTERING TEST AREA
X-Mailer: smtpsend

Tag 00:0c:cc:5b:ff:44 is in Area Rear Conference Room,Test Lab Annex #2,AP1242 Building,Alpharetta Campus_Group,Alpharetta Campus, Network Time Protocol (NTP) is the recommended method with which to establish a common clock source and maintain ongoing internal clock synchronization. The Cisco Wireless Location Appliance contains a utility daemon known as *ntpd* that can act as an NTP client to an NTP server located within the enterprise network. A network NTP server provides a common time source reference to all devices, typically using the Coordinated Universal Time (UTC) standard (formerly referred to as Greenwich Mean Time (GMT).

Note In software releases up to and including Release 4.1, proper time synchronization is recommended. However, with Release 4.2 and beyond, proper time synchronization is mandatory for proper authentication between the location appliance and WLAN controllers.

Complete guidance on configuring and activating the ntpd daemon on the location appliance can be found in the following document under the "NTP Configuration and Synchronization for Unified Wireless Network Devices – Set Up NTP on the Location Appliance" section which can be found at the following URL: http://www.cisco.com/en/US/products/ps6366/products_configuration_example09186a0080811274.shtml#setup-la.

NTP setup information can also be found in the *Cisco 2700 Series Location Appliance Installation and Configuration Guide* found at the following URL:

http://www.cisco.com/en/US/docs/wireless/location/2700/quick/guide/li31main.html#wp1057105.

Additional background information and general best practices with regard to NTP in your network may be found in the *Network Time Protocol: Best Practices* document which can be found at the following URL: http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml.

Quiescing the Location Appliance

Although the location appliance is designed to be installed and operated in a continuous fashion, there may be times when it is necessary to power-down the appliance in preparation for extraordinary events such as a physical equipment move or the orderly shutdown of a data center. Simply removing power to the location appliance without undergoing an orderly shutdown may result in any files open at the time becoming corrupted. Although the location appliance's operating system uses an ext3 journaling file system that minimizes the possibility of file system corruption, it is generally regarded as a best practice to follow the procedure outlined below to initiate an orderly shutdown of all appliance software facilities.

To power-down the location appliance, perform the following steps via either the appliance CLI console or a remote SSH device session.

Note For information on how to connect a CLI console to the location appliance, see "Connecting and Using the CLI Console" section in the *Cisco Wireless Location Appliance: Installation Guide* at the following URL: http://www.cisco.com/en/US/products/ps6386/products_installation_and_configuration_guide_book09186a00804fa761.html.

Step 1 Manually stop the location server software by issuing the follow command and observing the indicated:

```
# /etc/init.d/locserverd stop
Shutting down locserverd: Request server shutdown now...
Waiting for server...2 secs
Waiting for server...4 secs
            .
            .
            .
            .
Waiting for server...60 secs
Server shutdown complete.
#
```

Step 2 Before removing power to the location appliance, issue the following command to properly unmount all file systems, stop all services, and initiate an orderly shutdown of the Linux operating system:

```
# shutdown -h now
```

Issuing this command from the CLI console device in the following output:

```
Shutting down console mouse services: [  OK  ]
Stopping sshd:[  OK  ]
Stopping xinetd: [  OK  ]
Stopping crond: [  OK  ]
Saving random seed:  [  OK  ]
Killing mdmonitor: [  OK  ]
Shutting down kernel logger: [  OK  ]
Shutting down system logger: [  OK  ]
Shutting down interface eth0:  [  OK  ]
Shutting down loopback interface:  [  OK  ]
Shutting down audit subsystem[  OK  ]
Starting killall:  [  OK  ]
Sending all processes the TERM signal...
Sending all processes the KILL signal...
Syncing hardware clock to system time
Turning off swap:
Turning off quotas:
Unmounting file systems:
Halting system...
md: stopping all md devices.
flushing ide devices:
Power down.
```

Note that issuing the **shutdown** command from a remote SSH client in your SSH session becoming disconnected. The location appliance still initiates the shutdown procedure, but your SSH session becomes disconnected before the command completes. Therefore, you are not able to view all the command output as you would on a CLI console device. To avoid this lack of visibility, Cisco recommends that a terminal or PC attached to the location appliance console terminal be used to perform this task rather than an SSH session if possible.

Step 3 The final step is to remove power to the location appliance by using the front panel ON/OFF switch to turn the location appliance off. This should be done after the “power down” message is seen on the CLI console (shown in bold above). Note that if using a remote SSH session, you will not see the “power down” message because your session will be disconnected shortly after issuing the shutdown command. In this case, you should wait approximately two minutes for the shutdown command to complete before removing power to the location appliance using the front panel power switch.