Release Notes for Cisco 3300 Series Mobility Services Engine for Software Release 5.2.100.0

Last Revised: June 25, 2009

These release notes describe features, enhancements, and caveats for software release 5.2.100.0 for Cisco 3300 Series Mobility Services Engines and its two services Context-Aware Software (CAS) and Cisco Adaptive Wireless Intrusion Prevention System (wIPS).

Note Before installing this software, refer to the "System Requirements" section on page 2 for details on compatibility with Cisco Wireless LAN Controllers and Cisco Wireless Control Systems (WCS).

Contents

These release notes contain the following sections:

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

Introduction

Cisco 3300 Series Mobility Services Engine and Services

The Cisco 3300 Series Mobility Services Engine supports various services within the overall Cisco Unified Wireless Network (CUWN).

The Cisco 3300 Series Mobility Services Engine currently supports the following services in release 5.2:

- **Context-Aware Software (CAS)**–Allows a mobility services engine to simultaneously track thousands of mobile assets and clients by retrieving contextual information such as location, temperature, and availability from Cisco access points.

  CAS relies on two engines for processing the contextual information it receives. The *Context Aware Engine for Clients* processes data received from Wi-Fi clients and the *Context Aware Engine for Tags* processes data received from Wi-Fi tags. Both of these engines can be deployed together or separately depending on the business need. This service was introduced in release 5.1.

- **Wireless Intrusion Prevention System (wIPS)**–Provides wireless-specific network threat detection and mitigation against malicious attacks, security vulnerabilities, and sources of performance disruption within the CUWN infrastructure. wIPS visualizes, analyzes, and identifies wireless threats, and centrally manages mitigation and resolution of security and performance issues. Proactive threat prevention is also supported to create a hardened wireless network core that is impenetrable by most wireless attacks. This service is new in release 5.2.

> **Note** Refer to the online version of the *Cisco Context-Aware Software Configuration Guide, Release 5.2* for details on configuring and monitoring CAS on the mobility services engine at: http://www.cisco.com/en/US/docs/wireless/mse/3350/5.2/CAS/configuration/guide/mse_cg52.html

> **Note** Refer to the online version of the *Cisco Wireless Intrusion Prevention System Configuration Guide, Release 5.2* for details on configuring and monitoring wIPS on the mobility services engine at: http://www.cisco.com/en/US/docs/wireless/mse/3350/5.2/wIPS/configuration/guide/msecg_wIPS.html

> **Note** Refer to the online versions of the *Cisco 3350 and 3310 Mobility Services Engine Getting Started Guides* for details on the physical installation and initial configuration of the mobility services engines at: http://www.cisco.com/en/US/products/ps9742/prod_installation_guides_list.html

System Requirements

The following minimum releases are required to configure and monitor CAS on the Cisco 3300 Mobility Services Engine, Cisco WCS and Cisco Wireless LAN Controller (Table 1).

Table 1   *Minimum Software Requirements*

Service	System	Minimum Software Release
Context-Aware Software and Wireless Intrusion Prevention System[1]	Mobility services engine	5.2.100.0
	Controller	5.2.157.0 (or later 5.2.x release)
		5.1.151.0
		4.2.130
		Note Release 5.0.x supports Context-Aware Software
	Cisco WCS	5.2.148 (or later)
	Cisco WCS Navigator	1.4.148.0 (or later)

1. Release 5.2 is the minimum software requirement for the controller, WCS, and mobility services engine to support for Cisco Adaptive Wireless Intrusion Prevention System.

Upgrading to this Software Release

For instructions for automatically downloading the software using Cisco WCS or for manually downloading the software using a local or remote connection, refer to the "Updating Mobility Services Engine Software" section in Chapter 2 of the *Cisco 3350 Mobility Services Engine Getting Started Guide* and *Cisco 3310 Mobility Services Engine Getting Started Guide.*

You can find these documents at:

http://www.cisco.com/en/US/products/ps9742/prod_installation_guides_list.html

Software Image is Compressed

If you download the mobility services engine image *.gz file using Cisco WCS, the mobility services engine 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 decompress the files before running the installer. These files are 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

Updated Software Version Shown in Cisco WCS after Polling

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

Important Notes

This section describes important information about new features and operational notes for CAS, wIPS, and the mobility services engine for release 5.2.100.0.

Features and operational notes are summarized separately for the mobility services engine, CAS and wIPS.

Operational Notes

Operational notes for the mobility services engine, CAS and wIPS are summarized under separate headings.

Mobility Services Engine

Automatic Installation Script for Initial Setup

An automatic setup wizard is available to help you initially setup the mobility services engine.

An example of the complete automatic setup script is provided in the *Cisco 3350 Mobility Services Engine Getting Started Guide* and *Cisco 3310 Mobility Services Engine Getting Started Guide*.

You can find these documents online at:

http://www.cisco.com/en/US/products/ps9742/prod_installation_guides_list.html

Controller and Associated Mobility Services Engine Must be Mapped to the Same NTP and WCS Server

Communications between the mobility services engine, Cisco WCS and the controller are in universal time code (UTC). Configuring NTP on each system provides devices with the UTC time. An NTP server is required to automatically synchronize time between the controller, Cisco WCS and the mobility services engine.

The mobility services engine and its associated controllers must be mapped to the same NTP server and the same Cisco WCS server.

Local time zones can be configured on a mobility services engine to assist network operations center personnel in locating events within logs.

Note You can configure NTP server settings during the automatic installation script. Refer to the *Cisco 3350 Mobility Services Engine Getting Started Guide* or *Cisco 3310 Mobility Services Engine Getting Started Guide* for details on the automatic installation script. You can find these documents online at: http://www.cisco.com/en/US/products/ps9742/prod_installation_guides_list.html

Mobility Services Engine Cannot be Managed by Multiple Cisco WCS Stations

Management of the mobility services engine by multiple Cisco WCS stations is not supported. However, currently the software does not reject this configuration or provide a warning message when this configuration is made in error.

Mandatory Default Root Password Change

You must change the default root password of the mobility services engine during the automatic installation script to ensure optimum network security.

You can also change the password using the Linux command, **passwd**.

Deleting Admin User Causes Loss of Connectivity to Cisco WCS

If the admin user is removed from the mobility services engine, the connection to Cisco WCS is lost. Additionally, you cannot recreate the user at the System > Accounts > User window as it is no longer available (CSCsv03394).

Refer to the workaround for CSCsv03394 in the Open Caveats section for details on how to recover from this occurrence.

Configuration Changes for Greater Location Accuracy

In some RF environments, where there is poor location accuracy or where incorrect client floor location map placements occur, you might need to modify the moment RSSI thresholds in the *aes-config.xml* file in the *opt/locserver/conf/* directory of the mobility services engine (CSCsw17583).

The RSSI parameters that might need modification are:

- locp-individual-rssi-change-threshold
- locp-aggregated-rssi-change-threshold
- locp-many-new-rssi-threshold-in-percent
- locp-many-missing-rssi-threshold-in-percent

⚠
Caution   Refer to the *Cisco Mobility Services Engine – Context Aware Mobility Solution Deployment Guide* for guidelines on modifying the parameters:
http://www.cisco.com/en/US/products/ps9742/prod_tech_notes_list.html

⚠
Caution   Please contact TAC for assistance in modifying these parameters.

NMSP Aggregation Window Default Value

Starting from release 5.1 of Controllers, a command was introduced to adjust the NMSP aggregation window using CLI with a default value of 2 seconds. In the previous releases of Controllers, prior to 5.2, before this command was introduced, the default value of the aggregation window was 8 seconds on the Controllers.

But, for example, when you synchronize an MSE with Controllers of version 5.1, 5.2 and 4.2, the aggregation window is set to the largest which is 8 seconds. For more information, see config nmsp notify-interval measurement command description in the *Cisco Wireless LAN Controller Command Reference* for 5.2 (CSCsx52016).

CAS

Synchronization Required When Upgrading to Release 5.2 or Importing CAD Floor Images

When upgrading to release 5.2 from release 5.x (and earlier) synchronization is required after the software upgrade.

Synchronization is also required after upgrading to release 5.2, if the floor images used in Cisco WCS are CAD images.

Release 4.1 of AeroScout MobileView Required for Northbound Notifications

If a release of AeroScout MobileView *earlier than 4.1* is in use, incorrect responses are sent to those northbound notifications received from the mobility services engine. Northbound notifications are then resent by the mobility services engine, overloading the notification queue and resulting in reports of dropped notifications (CSCsx56618).

Separate Partner Engine Software Install Not Required for Tag Contextual Information

In release 5.2, the partner software that supports tag contextual information (temperature, availability, and location calculations) is bundled into the mobility services engine software. No separate download of partner engine software is required as it was in release 5.1.

Non-Cisco Compatible Extensions Tags Not Supported

The mobility services engine does not support non-Cisco CX Wi-Fi tags. Additionally, these non-compliant tags are not used in location calculations or shown on Cisco WCS maps.

Cisco Compatible Extensions, Version 1 Tags Required at a Minimum

Only Cisco CX version 1 tags (or later) are used in location calculations and mapped in Cisco WCS.

Monitoring Information Varies for Clients and Tags

On the Monitor > Clients page (when Location Debug is enabled), you can view information on the last heard access point and its corresponding RSSI reading. This information is not available on the Monitor > Tags page.

Calibration Models and Data Apply to Clients Only

Calibration models and data apply only to clients. Calibration for tags is done using the AeroScout System Manager.

Refer to Chapter 7, "Context-Aware Planning and Verification" in the *Cisco Context-Aware Software Configuration Guide, Release 5.2* for more details on client calibration.

Refer to the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User's Guide* at the following link:

http://support.aeroscout.com

Advanced Location Parameters Apply Only to Clients

Settings for advanced location parameters related to RSSI, chokepoint usage, location smoothing, and assignment of outside walls on floors, are not applicable to tags.

Refer to the "Editing Advanced Location Parameters" section in Chapter 7 of the *Cisco Context-Aware Software Configuration Guide, Release 5.2*.

Cisco WCS Path: Mobility > Mobility Services > *Device Name* > *Context Aware Service* > *Advanced* > *Location Parameters*.

System Backup Does Not Back Up Tag and TDOA Receiver Configuration Data

Cisco WCS does not backup *partner engine* configuration data. The *partner engine* configuration must be backed up prior to any backup or software update of the mobility services engine.

Refer to the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User's Guide* at the following link:

http://support.aeroscout.com

Cisco WCS Path: Mobility > Mobility Services > *Device Name* > *Maintenance* > *Backup*.

Location History Timestamps Match Browser's Location

The Cisco WCS timestamp is based on the browser's location and not on the mobility services engine settings. Changing the time zone on Cisco WCS or on the mobility services engine does not change the timestamp for the location history.

PDAs with Limited Probe Requests Might Affect Location

Many PDAs do not continuously send out probe requests after initial association to the Cisco Unified Wireless Network (CUWN). Therefore, calculating the location accuracy of such PDAs using RSSI readings is not always optimal.

Mandatory Setting Required on Intel 802.11n and 802.11 b/g/n Client Cards for Accurate Calibration

The Cisco CX RM option within Intel's Enterprise Security Profile must be enabled to ensure adequate calibration data points are collected for Intel 802.11n and 802.11 b/g/n client cards. You can use the Intel Client Software PROSET package to enable the Cisco CX RM option in the Enterprise Security Profile (CSCsl40623).

WCS Screen Changes

- Location sensors are now identified as Wi-FI TDOA receivers in menus and screens.
- The path, Mobility > Mobility Service Engines is now Mobility > Mobility Services.
- IP addresses are required when adding chokepoints and Wi-Fi TDOA receivers to maps.
- Horizontal and vertical (x,y) coordinates are now an entry option for Wi-Fi TDOA receiver map placement in addition to manual placement.

New Feature Support

New features for the CAS and wIPS are summarized under separate headings. There are no new features for the mobility services hardware platform.

CAS

For details on all the features discussed in this section, refer to Chapter 7 of the *Cisco Context-Aware Configuration Guide, Release 5.2* at the following link:

http://www.cisco.com/en/US/docs/wireless/mse/3350/5.2/CAS/configuration/guide/msecg_ch7_CAS.html

WCS Location Template

You can define a location template for assignment to multiple controllers and then that configuration is synchronized with multiple mobility services engines. You can set the following general and advanced parameters on the location template.

General parameters–Enable RFID tag collection, set the location path loss for calibrating or normal (non-calibrating) clients, measurement notification for clients, tags, and rogue access points, set the RSSI expiry timeout value for clients, tags, and rogue access points.

Advanced parameters–Set the RFID tag data timeout value and enable the location path loss configuration for calibrating client multi-band.

Import and Export of Wi-FI TDOA Receiver and Chokepoint Map Positioning Information

You can export chokepoint and TDOA receiver map positioning information to a file and then modify the map position of the chokepoints and TDOA receiver within that file. When you reimport the file, the modified positions of the chokepoint and TDOA receivers are automatically placed on the map. This approach allows faster repositioning of multiple chokepoints or TDOA receivers on a map than manual repositioning.

You can also export port and import these files between one WCS and another as well as create a file offline for later import into WCS.

- The following formats is used when importing and exporting files for the TDOA receiver:
    - [BuildingName],[FloorName],[LSMacAddress],[LSName],[IP Address],[X],[Y],[Z].

- The following formats is used when importing and exporting files for the chokepoint:
    - [BuildingName],[FloorName],[CPMacAddress],[CPName],[IPAddress],[Range],[X],[Y],[Z], [IsPerimeter]

    where *X*, *Y*, and *Z* represent map coordinates, and *IsPerimeter* is only required if the chokepoint is a perimeter chokepoint.

    Cisco WCS Path: Monitor > Maps > *Properties*

Filtering on Northbound Notifications

Filtering on northbound notifications is possible in release 5.2.100 and later. Similar to user-configured conditional notifications, you can limit which event notifications are forwarded.

You can use filtering to focus on specific notifications important to tag monitoring within your network and to limit the overall number of notifications sent. The latter might preserve processing and storage capacity on the northbound platform.

Note Cisco recommends defining northbound notification filters in the *aes-config.xml* file on the mobility services engine rather than Cisco WCS.

You can filter on six northbound parameters as summarized below:

```
<entry key="send-event-on-location-calc">true</entry>
<entry key="send-event-on-every-beacon">true</entry>
<entry key="send-event-on-vendor">true</entry>
<entry key="send-event-on-emergency">true</entry>
<entry key="send-event-on-chokepoint">true</entry>
<entry key="send-event-on-telemetry">true</entry>
```

To send all six northbound notifications with each beacon, ensure that the *send-event-on-location-calc* and *send-event-on-every-beacon* notification types are marked as *true*.

To limit the number of notifications, edit (but do not delete) the specific event entry in the *aes-config.xml* file by marking it as *false*.

For example, to send emergency and chokepoint notifications, change the other four notification types (location, beacon, vendor, and telemetry) to *false*.

The modified *aes-config.xml* file would read as:

```
<entry key="send-event-on-location-calc">false</entry>
<entry key="send-event-on-every-beacon">false</entry>
<entry key="send-event-on-vendor">false</entry>
<entry key="send-event-on-emergency">true</entry>
<entry key="send-event-on-chokepoint">true</entry>
<entry key="send-event-on-telemetry">false </entry>
```

wIPS

Cisco Adaptive Wireless IPS (Cisco Adaptive wIPS or wIPS) is a new service supported on the mobility services engine in release 5.2.

Cisco Adaptive wIPS provides wireless threat detection and performance management. Cisco wIPS combines network traffic analysis, network device and topology information, signature-based techniques and anomaly detection for accurate and complete wireless threat prevention.

Cisco Adaptive wIPS collaborates with Cisco wired network security, to provide more effective wireless security protection. Collaboration with the wired network offers protection against malware, consistent client security posture enforcement and unified wired and wireless security monitoring across the network. This provides a layered approach to wireless security.

Cisco Adaptive wIPS continually monitors wireless traffic on both the wired and wireless network, and uses its network intelligence to analyze attacks to pinpoint and proactively prevent attacks.

Caveats

This section lists open and resolved caveats in release 5.2.100.0.

Open Caveats

The following caveats are open (unresolved) in release 5.2.

- CSCsk17031—The history page loads slowly when you query the location history of a tag or client. Location history is an option in the drop-down menu on the tag and client details page. (Monitor Tags *or* Clients > *MAC address* > *Location history*)

  Workaround: You can increase the interval between historical readings of client, tags, and rogue clients and access points. You can also prune the data more frequently (Mobility > Mobility Services > *Device Name* > *Context-Aware Service* > *Administration* > *History Parameters)*.

- CSCsk18810–In networks with a large number of access points (approximately 2000 or more), mobility services engines might experience a slow down in location calculation and heatmap updates for clients, tags and access points.

  Workaround: None.

- CSCsl40623–Fewer data points are collected with Intel 802.11n and 802.11 b/g/n client cards during calibration when the Cisco Compatible Client Extension (CX) RM option is not enabled in the Enterprise Security Profile.

  Workaround: Use the Intel Client Software PROSET package to ensure that the Enterprise Security Profile is selected and that the Cisco Compatible CX RM option in this profile is enabled.

- CSCsm03250–When Cisco WCS logs are downloaded, no logs for the mobility services engine are downloaded.

  Workaround: Click on Mobility > Mobility Services > *Device* > *Logs* > *Download logs* to download location specific logs.

- CSCso74174–Online help could not be launched for the location accuracy tool (Tools > Location Accuracy Tool).

  Workaround: Select **Help** from the Cisco WCS navigation bar. In the online help summary page that appears, select Tools > Location Accuracy Tools.

- CSCsr29356–In some circumstances, access points from different, non-overlapping coverage regions each report a location for the same element (such as a client, tag or rogue client). This disparate location reporting results in an incorrect location calculation for the element.

  Workaround: None.

- CSCsu32450–Synchronization to the Aeroscout engine is lost when you perform a database operation such as restore, clear configuration or defragmentation. This results in no location calculations for the tags during that time.

  Workaround: Whenever you perform a database operation such as restore, clear configuration, or defragmentation, resynchronize the Aeroscout engine from the mobility services engine command line by entering the following commands:

  /etc/init.d/aeroscout-engine stop

  /etc/init.d/aeroscout-engine start

- CSCsr41614—WCS requires that MAC addresses be entered in the following case-sensitive format:

  ```
  a1:b2:c3:d4:e5:f6
  ```

  Workaround: For bulk imports of MAC addresses, it is possible to use the built-in functions in Microsoft® Excel™ to convert the MAC addresses to the format that is accepted by WCS.

- CSCsr52241–WCS sometimes generates unnecessary location server log messages similar to this one:

  ```
  7/20/08 18:20:32.122 ERROR[general] [15] Wrong or missing resource type for
  managedobj / transportSMTPForm.mailType.enum.0
  ```

  Workaround: None.

- CSCsu39828–If a client is associated to an infrastructure SSID and then moves to a rogue access point using a rogue SSID, the WCS map displays the same client twice—as an infrastructure client and a rogue client. When the interface is turned off, the WCS correctly removes the rogue, but it remains on the WCS map as an infrastructure client.

  Workaround: None.

- CSCsu68600–In some cases, the refresh rate for client location history (when the play function is operating) might take longer to refresh than the default rate of 2 seconds. This generally occurs when the client location history log is large (approximately 100 or more entries).

  Workaround: None.

- CSCsu72538–If one of the parameters is entered incorrectly during the automatic setup program, the install fails and the other parameters are not applied.

  Workaround: Rerun the setup script.

- CSCsu79969–When a mobility services engine already has a network design and that design is added or added a second time to Cisco WCS that has a network design with the same campus name, synchronization of the network design fails.

  Workaround: At the Mobility > Synchronize Services window in Cisco WCS, unassign the network design and synchronize, then reassign the network design and synchronize.

- CSCsv00557–WCS does not have the ability to verify that a heat map region is drawn correctly. An inaccurately drawn heat map region can cause computation errors in the calculation of the heat map.

  Workaround: Deleting incorrectly drawn rails and regions from the Monitor > Map menu will allow calibration to go ahead. Then redraw the rails and regions correctly.

- CSCsv03394—If the admin user is removed from the mobility services engine (MSE), the connection between the MSE and Cisco WCS is lost. Additionally, you cannot recreate the user at the System > Accounts > User window as it is no longer available.

  Workaround: To recover the admin user, enter the following commands (noted in **bold)** and then restart the mobility services engine (MSE).

  Enter the following command to generate *dbuserpass:*

  [root@mse ~]# **getdatabaseparams**

  The following displays to the screen:

  ```
  dbuserpass
  ```

  Enter the following command and use the generated *dbuserpass* value:

  [root@mse ~]# **/opt/mse/locserver/bin/tools/solid/solsql "tcp 2315" dba** *dbuserpass*

  The following displays on the screen:

  ```
  Solid SQL Editor (teletype) v.06.00.1049
  Copyright (C) Solid Information Technology Ltd 1993-2008
  Connected to 'tcp 2315'.
  Execute SQL statements terminated by a semicolon.
  Exit by giving command: exit;
  ```

  Enter the following command:

  insert into AESUSER (OBJECTID, PARENTID, CHANGEDON, MASK, USERNAME, PASSWORD, PERMISSIONS, GROUPNAME) VALUES (1,0, 1168465726685,0, 'admin', 'admin', 255, 'admin');

  The following displays on the screen:

  ```
  Command completed successfully, 1 rows affected.
  ```

  Enter the following command:

  commit work;

  The following displays on the screen:

  ```
  Command completed successfully, 0 rows affected.
  ```

  Enter the following command:

  select * from aesuser;

The following displays on the screen:

```
OBJECTID  PARENTID   CHANGEDON     MASK  USERNAME  PASSWORD  PERMISSIONS  GROUPNAME
--------  --------   ------------  ----  --------  --------  -----------  ---------
   1         0       1168465726685  0    admin     admin        255       admin
```

1 rows fetched.

Restart the mobility services engine.

- CSCsv03405–WCS trap destinations vanish from the mobility services engine when added to multiple WCS.

  Workaround: By design, mobility services engines cannot be managed by multiple WCS. Do not add a mobility services engine to multiple WCS. Multiple WCS might cause a reset of trap destinations on the mobility services engine.

- CSCsv06454–The WCS communication password does not apply during the automatic installation script.

  Workaround: Do not delete *admin* user on the mobility services engine from WCS. See CSCsv03394.

- CSCsv13564–When recompute RF prediction is launched, access points with an antenna type of *other* do not display an error message as expected. Instead the RF prediction is calculated and the following error is displayed, "RF Prediction Engine could not retrieve Coverage HeatMaps from the database. Please make sure that the RF Prediction is computed before computing location."

  Workaround: Configure correct antenna. To do so, click Monitor > Map window, select floor on which access point is resident. From the Select a command drop-down menu (on the floor page), select Position APs and then select the appropriate antenna for the access point (left side panel). Recompute RF prediction.

- CSCsv29199–If an FTP download to the mobility services engine fails because the interface is down or the system cannot be reached, an incorrect and unrelated message returns. For example, the following incorrect message might display "Unable to download software image. Reason: Failed to find the file *image filename* in the directory */opt/mse/locserver/../../installers*," rather than a message that the FTP file transfer failed due to the mobility services engine being unreachable.

  Workaround: Check to see if mobility services engine is reachable and if interface is *UP*.

- CSCsv29428–TFTP servers might mistakenly display as FTP servers on the FTP download image page (Configure > Controllers > *Controller > Download software (FTP)*.

  Workaround: None.

- CSCsv31011–After upgrading a controller's software to release 5.2, you might not be able to synchronize the controller and mobility services engine in WCS.

  Workaround: Unassign the controller and synchronize. Reassign the controller to the mobility services engine and then synchronize.

- CSCsv47137–When a WCS database generated by an earlier release than 5.2 is restored, you can only configure background synchronization to run in daily intervals. Release 5.2 supports background synchronization of the mobility services engine in hourly intervals.

  Workaround: Configure background synchronization of the mobility services engine to operate in daily intervals rather than hourly (Administration > Background Tasks).

- CSCsw17583–In some RF environments, where there is poor location accuracy or where incorrect client floor location placements occur, you might need to modify the moment RSSI thresholds in the *aes-config.xml* file in the *opt/locserver/conf/* directory of the mobility services engine.

  The RSSI parameters that can be modified are summarized below

  ```
  <entry key="locp-individual-rssi-change-threshold">5</entry>
  <entry key="locp-aggregated-rssi-change-threshold">3</entry>
  <entry key="locp-many-new-rssi-threshold-in-percent">20</entry>
  <entry key="locp-many-missing-rssi-threshold-in-percent">20</entry>
  ```

  Workaround: Refer to the *Cisco Mobility Services Engine – Context Aware Mobility Solution Deployment Guide* for guidelines on modifying the parameters:
  http://www.cisco.com/en/US/products/ps9742/prod_tech_notes_list.html

  Contact TAC with assistance in modifying the RSSI threshold parameters in the *aes-config.xml* file on the mobility services engine.

- CSCsw94634—If a controller is already present on the mobility servies engine, and the same controller is added to Cisco WCS and the user tries to synchronize, Cisco WCS will display the following message "delete the controller from MSE and assign the controller to MSE". However, there is no delete check box present. As a result, we cannot assign or unassign the controller.

  Workaround: Remove the controller from Cisco WCS and synchronize with the mobility services engine with delete option checked. Then add the controller back to Cisco WCS and assign it to the mobility services engine and synchronize.

- CSCsx56618–If a release of AeroScout MobileView *earlier than 4.1* is in use, incorrect responses are sent to those northbound notifications received from the mobility services engine. Northbound notifications are then resent by the mobility services engine, overloading the notification queue and resulting in reports of dropped notifications.

  Workaround: Install release 4.1 of *AeroScout MobileView.*

- CSCta04460–When users change access point height and/or access point elevation angle values from the default values of 10 ft and 0 degrees, respectively, these changes are not reflected in the calibration data, resulting in an incorrect calibration model. Any floor on which this calibration model is applied, will generate an incorrect heatmap for all its access points

  Workaround: None.

Resolved Caveats

The following caveats are resolved in release 5.2.100.0:

- CSCsu49105–Location accuracy tool would return inaccurate results or fail when it ran (scheduled or on demand accuracy test) when the meters dimension was used. When a successful scheduled run occurred the floor size was inaccurate. Results varied when using feet and meters as the floor measure.

- CSCsv71119–Changes in software ensure that enabling XML mediation traces now omit passwords in the log files.

- CSCsw34207–Sometimes the latest RSSI readings from access points were not always used in location calculations.

- CSCsx39421–Each user-configured notification was instantly followed by a *clear* notification.

  Absence notifications, though showing 1min in the Cisco WCS window (Mobility > Notifications), could take a lot longer to fire as the timer was dependant upon polling interval. This is no longer the case.

  Sometimes when a destination was removed and another was added to user configured notifications, the older destination would not get deleted. As a result, this old, down destination would still have events fired to it. Since SOAP timeout is slow, it would slow down other event firings and occasionally cause queue overflows.

- CSCsx52837–When rails and regions were in use in releases 5.1.x and 5.2.91 (or earlier), location calculations were often lost or corrupted when rails and regions (inclusion and exclusion) were added, deleted, and added again in succession in Cisco WCS. The following message would display in the logs, "Matrix dimensions must agree."

- CSCsx55843–When several accuracy tests running at the same time completed, WCS would often be unreachable and some services stopped.

- CSCsy34383–A number of java exceptions ocurred when a mobility services engine or location appliance was rebooted. Changes were made to the software to resolve this issue.

- CSCsy77490–When non-Cisco antennas were deployed with Cisco access point in the wireless network, the location for some clients and tags was not being calculated . Generally, theaccess points with the non-Cisco antennas were on the same floor as the clients and tags whose locations were not calculated correctly. Resolution is to change to a Cisco supported antenna that most closely matches the specifications of the non-Cisco antenna.

- CSCsz02125–When a mobility services engine starts up, it checks the database to determine if there are any pending heatmap calculations due to a system shut down. If there are any such calculations remaining, the mobility services engine will proceed with the calculations. This process can be lengthy if a large number of heatmap calculations are pending. If the user adds new map changes and synchronizes Cisco WCS and the mobility services engine when the pending heatmap calculation is in process, another set of heatmap calculations begins in parallel. This parallel processing of heatmap calculations might cause each calculation process to overwrite the other's calculated data.

  This problem might also happen when it is determined the heatmap computed in the last run was not correct and there is concurrent synchronization from Cisco WCS.

  Changes were made in the software to resolve this problem.

The following caveats are resolved in release 5.2.91

- CSCsl08696–User was not able to change the name of WCS calibration models in WCS 4.x releases.

- CSCsl32412–If the user included special characters in a floor name, it would cause conversion errors on the map name for SOAP/XML.

- CSCsm56708–At the Monitor > Security > Rogue Clients window, information for *First Heard* is not accurate, the rogue access points's MAC address was reported as all zeros and no information was supplied for the access point. Additionally, no information was reported for the access point that reported the client. (Note: *Last Reported* is unresolved and is being tracked under CSCsm56708).

- CSCso43692–In some cases synchronization did not properly occur after access points, TDOA receivers or chokepoints were moved to other buildings or campuses. The mobility services engine removed the element from the former site but did not properly add it to the new site.

- CSCso73789–Clients were seen as *Not set* in maps when the import asset information option was used.

- CSCso97850–Location accuracy tool would return inaccurate results or fail when it ran (scheduled or on demand accuracy test). Test accuracy always reported 0.0% accuracy.

- CSCso99286–Database was not updated with the current tag information.

- CSCsq23489–When a large number of obstacles (such as walls, doors, cubicles and glass) were defined on a map (using the map editor) synchronization between Cisco WCS and the mobility services engine would fail. A database error was reported in the log files and a number of the obstacles had erroneous mappings (x, y coordinates).

- CSCsq61215–The serial number of the mobility services engine did not appear on the advanced parameters page of Cisco WCS. (Mobility > Mobility Services > *Device* > *System* > *Advanced Parameters*).

- CSCsq71288–Client statistics listed under location history were blank. Client statistics did appear under Monitor Clients > Statistics.

- CSCsr00359–A superuser could not import civic information. Permission was denied.

- CSCsr20910–Calibration of a large number of elements (greater than 500) would cause a slowdown in WCS.

- CSCsu36268–The log and status options listed under partner engine would disappear after a software download (Mobility > Mobility Services > *Device* > *Partner Engine*). Clicking on the download software option would cause the log and status options to reappear.

- CSCsu46050–In some cases, when a user attempted to save changes made in the map editor, an error message displayed and the changes were not saved.CSCsu49105–Location accuracy tool would return inaccurate results or fail when it ran (scheduled or on demand accuracy test) when the meters dimension was used. When a successful scheduled run occurred the floor size was inaccurate.

- CSCsu60684–In some cases, the ethernet0 port would fail initialization after initial install.

- CSCsu62558, CSCsv13610–In some cases the client details page would often display special characters or garbage in the client data rate field (Monitor > Clients > *Client*).

- CSCsu63552–Periodically, the mobility services engine would stop synchronizing or became unsynchronized after a few days.

- CSCsu74965–Wi-Fi TDOA receivers information was not sent to mobility services engines after synchronization. TDOA receivers in question were installed outside and mapped on outdoor maps in WCS.

- CSCsu81117–Client and tags MAC addresses entered and labeled as *disallowed* on the filtering parameters window in WCS, would display on the floor map and under location history in error.

- CSCsu85459–A switch port trace would mistakenly invoke an error popup message stating that Context-Aware Service was unreachable. The two items, switch port trace and CAS, are not related and the message should not be invoked.

- CSCsu97355–After a network design resynchronization, if a mobility services engine was shutdown, the heat maps did not calculate after system restart. Workaround involved unassigning and reassigning the network design upon restart of the system.

- CSCsv00465–Heatmap calculations would hang and calculations did not occur due to underlying processes.

If You Need More Information

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

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

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

Troubleshooting

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

http://www.cisco.com/tac

Click **Troubleshooting.** Then choose your product and then select the **Troubleshoot and Alerts** heading on the product page to find information on the problem you are experiencing and other service advisories.

Related Documentation

The following documents are related to the mobility services engine:

- *Cisco 3350 Mobility Services Engine Getting Started Guide* and *Cisco 3310 Mobility Services Engine Getting Started Guide*
- *Cisco Context-Aware Software Configuration Guide, Release 5.2*
- *Cisco Adaptive Wireless Intrusion Prevention System Configuration Guide, Release 5.2*
- *Cisco Mobility Services Engine - Context Aware Mobility Solution Deployment Guide* (under Troubleshooting TechNotes)

Note You can see the latest online versions of these documents at the following link:
http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html

Obtaining Documentation, Support, and Security Guidelines

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

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

This document is to be used in conjunction with the documents listed in the Related Documents section.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0812R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only.

Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.Printed in the USA on recycled paper containing 10% postconsumer waste.