Release Notes for Cisco 3300 Series Mobility Services Engine for Software Release 6.0.75

Last Revised: June 11, 2009

These release notes describe features, enhancements, and caveats for software release 6.0.75 for Cisco 3300 Series Mobility Services Engines and its two services: Context-Aware Software (CAS) and Adaptive Wireless Intrusion Prevention System (wIPS).

Note Before installing this software, refer to the "System Requirements" section on page 3 for details on compatibility with Cisco Wireless LAN Controllers and Cisco Wireless Control Systems (WCS).

Note You must purchase licenses from Cisco to retrieve information on tags and clients from access points. Refer to the "Ordering CAS Client and Tag Licenses for the Mobility Services Engine" section on page 6 for details. You must also purchase licenses You must purchase licenses from Cisco to support wIPS monitor mode access points from access points. Refer to the "Ordering Adaptive wIPS Licenses for the Mobility Services Engine" section on page 7.

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 6.0:

- **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.

  Note You must purchase licenses from Cisco to retrieve contextual information on tags and clients from access points. Refer to the "Ordering CAS Client and Tag Licenses for the Mobility Services Engine" section on page 6.

- **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 using Cisco monitor mode access points. Proactive threat prevention is also supported to create a hardened wireless network core that is impenetrable by most wireless attacks.

  Note You must purchase licenses from Cisco to support wIPS monitor mode access points from access points. Refer to the "Ordering Adaptive wIPS Licenses for the Mobility Services Engine" section on page 7.

Note Evaluation licenses for 100 clients,100 tags, and 20 access points (wIPS) come standard on each mobility services engine installed with release 6.0. Evaluation licenses are good for 60-days.

Note CAS and wIPS can operate simultaneously on the Cisco 3350 and Cisco 3310.

Note Refer to the online version of the *Cisco Context-Aware Software Configuration Guide, Release 6.0* for details on configuring and monitoring CAS on the mobility services engine at: http://www.cisco.com/en/US/docs/wireless/mse/3350/6.0/CAS/configuration/guide/mse_cg60.html

Note Refer to the online version of the *Cisco Wireless Intrusion Prevention System Configuration Guide, Release 6.0* for details on configuring and monitoring wIPS on the mobility services engine at:
http://www.cisco.com/en/US/docs/wireless/mse/3350/6.0/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	6.0.75.0
	Controller	6.0.182.0
		5.2.157.0 and 5.2.178.0
		5.1.151.0 and 5.1.163.0
		4.2.130 (or later)
		Note Release 5.0.x is not supported with release 6.0.
	Cisco WCS	6.0.132.0 (or later).
	Cisco WCS Navigator	1.5.132.0 or later.

1. Release 5.2 is the minimum software requirement for the controller, WCS, and mobility services engine to support 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

Upgrading from Release 5.x to 6.0

⚠ **Caution** The number of supported clients, tags, and access points (wIPS) is reset to 100 clients, 100 tags, and 20 access points when you upgrade to release 6.0. All tracking beyond these limits is lost. These limits correspond to the 60-day evaluation licenses that are standard on mobility services engines.

⚠ **Caution** You must backup the mobility services engine database before upgrading from release 5.x to 6.0 to preserve client, tag, and access point configurations. You can restore the database after the software upgrade.

To upgrade to release 6.0, follow these steps:

Step 1 Register the Product Authorization Key (PAK).

   a. Client and wIPS licenses are registered at www.cisco.com/go/license.

   b. Tag licenses are registered at www.aeroscout.com/content/support.

Step 2 Backup the mobility services engine database and the Aeroscout database:

   a. To backup the mobility services database (network designs controller configurations, clients, and access points), follow these steps:

      1. Choose **Services > Mobility Services**.

      2. Click the name of the mobility services engine for which you want to backup the database.

      3. Choose **Maintenance > Backup** from under the System menu (left).

      4. Enter a name for the backup file. Click Submit (see Figure 1).

   b. To backup the AeroScout database (tag licenses, chokepoints, and TDOA receivers) refer to the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User's Guide* at

      http://support.aeroscout.com

Figure 1 **System > Maintenance Window**
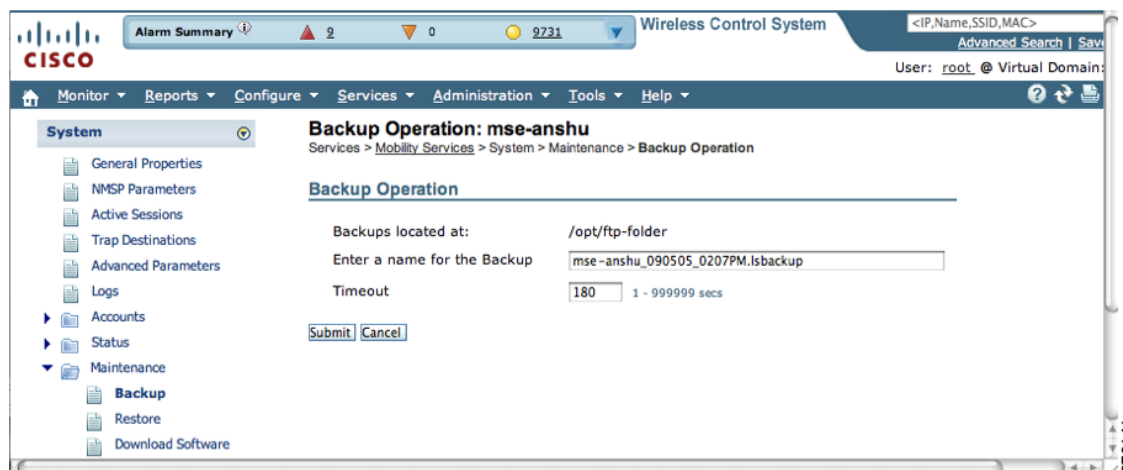
Step 3   Download release 6.0:

   a.   Choose **Services > Mobility Services**.

   b.   Click the name of the mobility services engine on which you want to upgrade the software.

   c.   Choose **Maintenance > Download Software** from under the System menu.

   d.   Select either an uploaded image or browse and upload an image. Click **Download**.

Step 4   Install release 6.0 using the mobility services engine CLI using one of the following options:

   a.   To overwrite existing software, enter:

```
/etc/init.d/msed stop
cd /opt/installers
./<mse software file name>
```

   b.   To do a fresh install, enter:

```
/etc/init.d/msed stop
cd/opt/mse/uninstall
```

Enter the following once in the uninstall directory.

```
./uninstall
```

Enter **no** when prompted to keep the old database.

```
/c opt/installers
./<mse software file name>
```

Step 5   Restore the mobility services engine and AeroScout database:

   a.   To restore the mobility services database, follow these steps:

   1.   Choose **Services > Mobility Services.**

   2.   Click the name of the mobility services engine on which you upgraded the software.

   3.   Choose **Maintenance > Restore** from under the System menu.

   4.   Select the file to restore from the drop-down menu. file. Click **Submit**.

   b.   To restore the AeroScout database refer to the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User's Guide* at

   http://support.aeroscout.com

Step 6   Install licenses:

Refer to Chapter 2 of the *Context-Aware Services Configuration Guide, Release 6.0* at
http://www.cisco.com/en/US/products/ps9806/products_installation_and_configuration_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.

CAS and wIPS License Requirements

For complete details on ordering and downloading licenses refer to the *Cisco 3300 Series Mobility Services Engine Licensing and Ordering Guide for Context-Aware Mobility Software, and Adaptive wIPS, Release 6.0* at:
http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html

- Client and wIPS licenses are installed from Cisco WCS (Administration > License Center).
    - Refer to Chapter 2 of the *Cisco Context-Aware Service Configuration Guide, Release 6.0* and *Cisco Adaptive Wireless Intrusion Prevention System, Release 6.0*, respectively.
- Tag licenses are installed using the *AeroScout System Manager*. Refer to the "Installing Tag Licenses" section in Chapter 2 of *Cisco Context-Aware Service Configuration Guide, Release 6.0*.

Ordering CAS Client and Tag Licenses for the Mobility Services Engine

CAS software licenses are based on the number of Wi-Fi client and Wi-Fi tag devices tracked. The Cisco 3350 Mobility Services Engine allows for the tracking of up to 18,000 devices (combined count of Wi-Fi clients and Wi-Fi tags) and the Cisco 3310 Mobility Services Engine allows for the tracking of up to 2,000 devices (combined count of Wi-Fi clients and Wi-Fi tags).

Licenses for Cisco Compatible Extensions (CX) tags (version 1 or later) and clients are offered independently. The client's license also includes tracking of rogue clients and rogue access points.

Licenses for tags and clients are offered in quantities ranging from 1,000 to 12,000 units and can be combined to meet the location tracking requirements of a CAS deployment. For example, combining the AIR-CAS-3KC-K9, AIR-CAS-12KC-K9, and AIR-CAS-1KT-K9 licenses provide tracking of 15,000 Wi-Fi clients and 1,000 Wi-Fi tags on a Cisco 3350 (see Table 2).

CAS License Ordering Summary

Order numbers for client and tag licenses are summarized in Table 2.

Table 2   *Order Numbers for Client and Tag Licenses*

Order Number	Licenses
Client Licenses[1]	
AIR-CAS-1KC-K9	License for tracking 1,000 client devices.
AIR-CAS-3KC-K9	License for tracking 3,000 client devices.
AIR-CAS-6KC-K9	License for tracking 6,000 client devices.
AIR-CAS-12KC-K9	License for tracking 12,000 client devices.

Table 2   Order Numbers for Client and Tag Licenses (continued)

Order Number	Licenses
Tag Licenses	
AIR-CAS-1KT-K9	License for tracking 1,000 tag devices.
AIR-CAS-3KT-K9	License for tracking 3,000 tag devices.
AIR-CAS-6KT-K9	License for tracking 6,000 tag devices.
AIR-CAS-12KT-K9	License for tracking 12,000 tag devices.

1. All client licenses include tracking of rogue clients and rogue access points.

Ordering Adaptive wIPS Licenses for the Mobility Services Engine

Adaptive wIPS software licenses are based on the number of full-time monitoring access points (often referred to as *monitor mode acess points*) that are deployed in the network. The licenses may be combined to arrive at the number of monitor mode access points required to run the Adaptive wIPS deployment. For example, combining AIR-WIPS-AP-5, AIR-WIPS-AP-25, and AIR-WIPS-AP-500 licenses provides support for 530 monitor mode access points.

Adaptive wIPs License Ordering Summary

Order numbers for Adaptive wIPS licenses are summarized in Table 3.

Table 3   Order Numbers for Adaptive wIPS Licenses

Order Number	Licenses
AIR-WIPS-AP-5	License for 5 monitor mode Cisco access points.
AIR-WIPS-AP-25	License for 25 monitor mode Cisco access points.
AIR-WIPS-AP-100	License for 100 monitor mode Cisco access points.
AIR-WIPS-AP-500	License for 500 monitor mode Cisco access points.
AIR-WIPS-AP-UNL1	License for 2000 monitor mode Cisco access points. **Note** Cannot be combined with other wIPS licenses.

Important Notes

This section describes important information about new features and operational notes for CAS, wIPS, and the mobility services engine for release 6.0.75.

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

Operational Notes

Mobility Services Engine

Automatic Installation Script for Initial Setup

An automatic setup wizard is available to help you initially set up 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

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**.

Networks with Large Access Point Deployments Might Experience Slower Location Updates

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 (CSCsk18810).

Large Burst of Notifications Might Cause Drop of Notifications

A mobility services engine might fail to send notifications if it receives a large burst of notifications. The dropped notification count appears on the Services > Context Aware Notifications window.

Refer to CSCsu43201 in the Open Caveats section for workaround.

Configuration Changes for Greater Location Accuracy

In some RF environments, where location accuracy is around 60 to 70% or where incorrect client or tag 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   Please contact TAC for assistance in modifying these parameters.

CAS

Synchronization Required When Upgrading to Release 6.0 or Importing CAD Floor Images

When upgrading to release 6.0 from release 5.x (and earlier) you must synchronize after the software upgrade and also when CAD generated floor images are imported into Cisco WCS.

Floor Change or Minimum Distance Required for Location Transitions to Post to History Log

When history logging is enabled for any or all elements (client stations, asset tags, and rogue clients and access points), a location transition for an element is only posted if it changes floors or the element's new location is at least 30 feet or 10 meters from its original location.

Cisco Path: Services > Mobility Services > Device Name > Context Aware Service > Administration > History Parameters.

Logs can be viewed at Services > Mobility Services > Device Name > Systems > Log.

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 6.0 (and 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.

Cisco WCS Online Help Outlines Incorrect Software Download Procedure

In Cisco WCS online help (OLH), the steps in the "Downloading Software to a Mobility Services Engine Using Cisco WCS" section mistakenly notes commands for downloading an *aeroscout-engine*. The *aeroscout-engine* is now bundled within the mobility services engine software. Refer to Chapter 9 of the *Cisco Context-Aware Service Configuration Guide, Release 6.0* for the correct download steps.

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 Only to Clients

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 6.0* 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 6.0.*

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

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).

wIPS

Mobility Services Engine With wIPS Service Enabled Mistakenly Allows a Controller to Be Assigned to Multiple MSEs

When wIPS is configured on the mobility services engine, often a controller can be assigned to more than one mobility services engine in error. By design, a controller can only be assigned to one mobility services engine and an error appears in the Cisco WCS window when you synchronize a mobility services engine and a controller (CSCsx38955).

Cisco WCS Screen and Navigation Changes

- *Services* replaces *Mobility* in the navigation bar of Cisco WCS.
- A centralized license center to install and view license status is available (Administration > License Center).
- *A Switches* tab is a new synchronize option to support the new wired Catalyst switch and wired client feature (Services > Synchronize Services).

New Feature Support

New features for the mobility services engine and services CAS and wIPS are summarized under separate headings.

Mobility Services Engine

Coexistence

Both the CAS and wIPS services can operate on the Cisco 3350 and Cisco 3310 simultaneously.

CAS

For details on all the features discussed in this section, refer to Chapter 7 of the *Cisco Context-Aware Configuration Guide, Release 6.0* at the following link:

http://www.cisco.com/en/US/docs/wireless/mse/3350/6.0/CAS/configuration/guide/msecg_ch7_CAS.html

Location Services for Wired Switches and Clients

You can import the location of wired Catalyst stackable switches (3750, 3750-E, 3560, 2960, IE-3000 switches), switch blades (3110, 3120, 3130, 3040, 3030, 3020), and switch ports into the mobility services engine.

The following Catalyst 4000 series are also supported:

WS-C4948, WS-C4948-10GE, ME-4924-10GE, WS-4928-10GE, WS-C4900M, WS-X4515, WS-X4516, WS-X4013+, WS-X4013+TS, WS-X4516-10GE, WS-X4013+10GE, WS-X45-SUP6-E, and WS-X45-SUP6-LE

Once you define a wired switch and synchronize it with a mobility services engine, details on wired clients connected to a wired switch are downloaded to the mobility services engine over the NMSP connection. You can then view wired switches and wired clients using Cisco WCS.

Import and display of civic and emergency location information (ELIN) meets specifications of RFC4776 which is outlined at:

http://tools.ietf.org/html/rfc4776#section-3.4

Note Catalyst stackable switches and switch blades must be operating at Cisco IOS release 12.2(52) SG.

Cisco WCS Path: Configure > Ethernet Switches

Cisco WCS Supports Backup of Tag, Chokepoint, and TDOA Receiver Configuration Data

Release 6.0 provides support for backup of Tag, Chokepoint, and TDOA Receiver configuration data. In release 5.2, this feature was not supported.

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

http://support.aeroscout.com

Note Configuration data must be backed up prior to any backup or software update of the mobility services engine. Refer to the "Upgrading to this Software Release" section on page 3.

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

wIPS

For details on all the features discussed in this section, refer to the *Cisco Adaptive Wireless Intrusion Prevention System Configuration Guide, Release 6.0* at the following link:

http://www.cisco.com/en/US/products/ps9817/products_installation_and_configuration_guides_list.html

Supported on Cisco 3350 and Cisco 3310

Cisco wIPS is supported on Cisco 3350 and 3310 mobility services engines in release 6.0. Previously, wIPS was supported only on the Cisco 3310 in release 5.2.

Caveats

This section lists open and resolved caveats in release 6.0.75.

Open Caveats

The following caveats are open (unresolved) in release 6.0.

- 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.

- CSCsr41614—WCS requires that MAC addresses be entered in one of the following formats (see related caveat CSCsy85829):

  ```
  a1:b2:c3:d4:e5:f6 (lowercase)
  A1:B2:C3:D4:E5:F6 (uppercase)
  ```

  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.

- CSCsu43201—A mobility services engine fails to send notifications if it receives a large burst of notifications. The dropped notification count appears on the Services > Context Aware Notifications window. When notifications drop, the following message might be seen in the MSE log:

  ```
  2/05/09 16:38:18 TRACE[async] [59] DROP MSG: com.aes.datamodel.track.AesDestDefn@4
  <NorthboundNotificationEvent>...</NorthboundNotificationEvent> , Current queue size =
  500
  ```

  A burst of events might occur at startup when the mobility services engine retrieves elements (clients, tags, access points) from the controller all at once and generates events for each of these retrievals (if applicable). It might also occur when the mobility services engine is tracking tags which are beaconing in the order of seconds. Tags beacon at a constant rate when stationary but might beacon more often when moving. If the tag traffic is very high, this too causes a burst in notifications. The condition is more likely to occur when Northbound Notifications are enabled for tags (Services > Mobility Services > Device Name > Context Aware Service > Advanced > Notification Parameters).

  Workaround: Do one or more of the following steps to ensure all notifications are sent:

  1) Disable notifications at startup and enable after startup is complete.

  2) Ensure that the event listener is never down.

  3) If using *AeroScout MobileView*, verify that version 4.1 or later is installed.

  4) Increase the size of the queue limit at the Services > Mobility Services Engine > Device Name > Context Aware Service > Advanced > Notification Parameters window. You can increase this to 18,000 for the mobility services engine.

5) Ensure tags are beaconing in the order of minutes, not seconds. Even in cases of movement, a tag should beacon no more frequently than 30 seconds.

- CSCsv34781—A controller that is synchronized to a mobility services engine with one system name cannot later be synchronized to the same mobility services engine with a different system name.

    Workaround: Unassign and the reassign the controller.

- CSCsx38955—When wIPS is configured on the mobility services engine, often a controller can be assigned to more than one mobility services engine in error. By design, a controller can only be assigned to one mobility services engine and an error noting should appear in the Cisco WCS window when you synchronize a mobility services engine and a controller. This error does not occur when wIPs is configured.

    Workaround: Unassign the controller from all but one mobility services engine and synchronize.

- CSCsx44787—When a controller is operating with release 4.1 or earlier and is communicating with controllers installed with release 4.2 or later and a location server or mobility services engine (supported in release 5.1 and later) is in the network, clients might bounce between association and disassociation states. Additionally, location calculations might stop.

    Workaround: Upgrade controllers to release 4.2 or later.

- CSCsx49328—When a location configuration is removed from a Catalyst 3K switch port, the change is not reflected in Cisco WCS. The removed location still shows up as the device location in WCS. This issue is not seen on Catalyst 4K switches.

    Workaround: Assign a new empty location identifier to the switch port.

- 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*.

- CSCsx53833—In some cases, the mobility services engine might hang or exit during startup.

    Workaround: Internal code was added in release 6.0 to watch for this state and then restart the mobility services engine.

- CSCsx73711: Whenever a Catalyst 3K switch reloads, all interfaces (with location configurations) will have the same location information as the last interface that has location configuration. This issue is not seen on Catalyst 4K switches.

    Workaround: Re-configure location for ports whenever the switch reloads.

- CSCsy91367—When you configure a tracking limit for tags, the limit value for tags is modified in error. The limit value is a display only value, which displays the maximum number of tags that the mobility services engine supports as determined by the number of tag licenses purchased (Services > Mobility Services > Device Name > Context Aware Service > Administration > Tracking Parameters).

    Workaround: For a summary of installed tag licenses for a specific mobility services engine, refer to the license summary window at Administration > License Center > Summary > MSE.

- CSCsy94947—Cisco WCS mistakenly reports a failed NMSP session between a mobility services engine and a controller as an *AP authorization failure* trap with the MAC address of the mobility services engine.

    Workaround: None.

- CSCsz24853—Searching for a location server or mobility services engine (by name, IP address or MAC address) using the Cisco WCS Navigator always lists *location server* as the Item Type in the search results even when results for a mobility services engine are returned. Search results are found by clicking the link under the Items Matched column.

  Workaround: None.

- CSCsz40211—No warning it displayed when an evaluation license for a mobility services engine is due to expire.

  Workaround: To verify the status of evaluation licenses on a mobility services engine, refer to the Administration > License Center > Summary > MSE window in Cisco WCS.

- CSCsz44105—When the automatic install script is running during initial setup for the mobility services engine, an option to skip the root password is listed. This is an error. You are not allowed to skip this step and the skip option should not be seen. Entering an *S* to skip this step is ignored.

  Example display:

  ```
  Configure root password? (Y)es/(S)kip/(U)se default [Yes]: s
  Changing password for user root.
  You can now choose the new password.
  ```

  Workaround: None.

- CSCsz44750—When the telemetry option is enabled for a tag search, context-aware notifications are not updated.

  Workaround: Disable the telemetry option during tag searches and stop and then start the mobility services engine to restart context-aware notifications.

  To manually stop the mobility services engine, login as root and enter:

  /etc/init.d/msed stop

  To start the mobility services engine, enter:

  /etc/init.d/msed start

- CSCsz48609—The MAC address format used in the wired client search field is case sensitive. Additionally, if a space is added in front of the MAC address, the search fails. Wired client searches are done at the Service > Mobility Services > Device Name > Context Aware Service > Wired > Wired Clients window.

  Workaround: Enter the MAC address in lowercase (xx:xx:xx:xx:xx:xx) in the wired clients search field and do not insert any blank spaces.

- CSCsz51996—The default MSE communication password is set to the root default of *password* in the automatic install script rather than *admin*.

  Workaround: None.

- CSCsz54353—When a client is associated to a local controller, its IP address does not appear in the Controller Name column on the Monitor > Clients window when the option *Clients detected by MSEs* is selected from the Show drop-down menu.

  Workaround: Click Client User Name to view the Controller IP address on the Clients Details window.

- CSCsz59951—In rare circumstances, the mobility services engine might become unresponsive and unreachable (user cannot login in) in a high stress environment.

  Workaround: Reboot and power cycle the mobility services engine.

- CSCsz74218—Third-party partner applications cannot conduct simple and full hierarchy queries for clients, rogue access points, and rogue clients (getClientLocationList, getRogueLocationList, and getRogueAPLocationList). However, third-party applications can make simple and full hierarchy queries of tags. Location retrievals using Cisco WCS are not affected by this bug.

  Workaround: Query for clients, rogue clients, and rogue access points by the floor's object ID rather than the simple and full hierarchy queries which include the floor name.

- CSCsz78329—Online help is not reachable from the Help menu on the Tools > Location Accuracy Tool > *On Demand Accuracy Test* window and the Tools> Location Accuracy Tool > *Scheduled Accuracy Test* window.

  Workaround: Click Help > Online Help at the Tools > Location Accuracy Tool window.

- CSCta09154—During an upgrade to release 6.0 (unistall of old code and install of new code) on a mobility services engine, the following messages display on the console screen upon login session timeout:

  ```
  sbin/raid-monitor: line 55:
  raid_status.txt: No such file or directory
  wc: raid_status.txt: No such file or directory
  cat: raid_status.txt: No such file or directory
  ```

  This occurs because a log file that would accept these messages is removed as part of the software upgrade process (during uninstall of software) and therefore the messages display to the screen.

  Workaround: Reboot the mobility services engine to end display of messages.

- CSCta13899—In Cisco WCS online help (OLH), the steps in the "Downloading Software to a Mobility Services Engine Using Cisco WCS" section mistakenly notes commands for downloading an *aeroscout-engine*. The *aeroscout-engine* is now bundled within the mobility services engine software.

  Workaround: Refer to Chapter 9 of the *Cisco Context-Aware Service Configuration Guide, Release 6.0* for correct download steps.

Resolved Caveats

The following caveats are resolved in release 6.0.

- CSCsk17031—The history page loaded slowly when you queried 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 was to increase the interval between historical readings of client, tags, and rogue clients and access points. You could also prune the data more frequently (Services > Mobility Services > Device Name > Context-Aware Service > Administration > History Parameters).

- CSCsm03250—When you downloaded logs from a mobility services engine a copy of the its log files was also written to the WCS logs directory. By design, the latest events for a mobility services engine are always resident in each mobility services engine's logs and are meant to be retrieved from each mobility services engine (Services > Mobility Services > Device Name > Logs > Download Logs). However, when users reviewed the WCS logs, they often referred to mobility services engine events that often were outdated. To prevent confusion to the user, mobility services engine logs (lbs) were removed from the wcs/logs directory.

- CSCsr29356—In some circumstances, access points from different, non-overlapping coverage regions each reported a location for the same element (such as a client, tag or rogue client). This disparate location reporting resulted in incorrect location calculations for the element.

- CSCsr52241—WCS sometimes generated 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
  ```

- CSCsr74789—Available memory on a mobility services engine was exhausted when more than 500 elements (clients, tags, rogue access points, or clients) moved per second.

- CSCsu32450—Synchronization to the AeroScout engine was lost when you performed a database operation such as restore, clear configuration, or defragmentation. No tag locations were calculated during these operations.

  Workaround was to synchronize the AeroScout engine from the mobility services engine command line by entering the following commands whenever you performed a database operation such as restore, clear configuration, or defragmentation:

  /etc/init.d/aeroscout-engine stop

  /etc/init.d/aeroscout-engine start

- CSCsu39828—If a client was associated to an infrastructure SSID and then moved to a rogue access point using a rogue SSID, the WCS map displayed the same client twice—as an infrastructure client and a rogue client. When the interface was turned off, WCS correctly removed the rogue, but it remained on the WCS map as an infrastructure client.

- CSCsu60684—In some cases, the *Ethernet0* port failed initialization after initial install.

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

- CSCsu72538—If one of the parameters was entered incorrectly during the automatic setup program, the install failed and the other parameters were not applied.

- CSCsu87317—No error message displayed when an incorrect mobility services engine UDI was entered for a license file and the license installation failed. Cisco WCS now displays a pop-up message when the license file install fails due to an UDI mismatch.

- CSCsv00557—WCS did not have the ability to verify that a heat map region was drawn correctly. An inaccurately drawn heat map region would cause computation errors in the calculation of the heat map.Workaround was to delete incorrectly drawn rails and regions from the Monitor > Map menu to allow the calibration to go ahead. Then redraw the rails and regions correctly.

- CSCsv03394—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 will no longer available.

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

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   Djq4PhDOAZ1swYkph+7caw== 255   admin
```

1 rows fetched.

Restart the mobility services engine.

- CSCsv03405—WCS trap destinations would vanish from the mobility services engine when added to multiple WCS stations. By design, mobility services engines cannot be managed by multiple WCS; however, no warning message appeared in release 5.x. In release 6.0, a warning message has been added to warn users when multiple WCS stations are configured in error.

- CSCsv06454—The WCS communication password did not apply during the automatic installation script. A step was added to the setup script to prompt the user to choose a username for MSE communication with the WCS.

- CSCsv13564—When recompute RF prediction was launched, access points with an antenna type of *other* did not display an error message as expected. Instead the RF prediction was calculated and the following error was 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 was to 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, CSCsv57187—If an FTP download to the mobility services engine failed because the interface is down or the system could not be reached, an incorrect and unrelated message returned. 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 because the mobility services engine was unreachable. Workaround was to check to see if mobility services engine was reachable and if the interface was *UP*.

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

- CSCsv31011, CSCsw50077—After upgrading a controller to a new software release, you often could not synchronize the controller and mobility services engine in WCS.

  Workaround was to unassign the controller and synchronize and then reassign the controller to the mobility services engine and synchronize again.

- CSCsv47137—When a WCS database generated by an earlier release than 5.2 was restored, you could only configure background synchronization to run in daily intervals. Release 5.2 and 6.0 support background synchronization of the mobility services engine in hourly intervals.

- CSCsw17583—In some RF environments, where location accuracy is around 60 to 70% or where incorrect client or tag 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. Issue was resolved by documenting the configuration solution in the release notes. Workaround is to contact TAC for assistance in modifying the RSSI threshold parameters in the *aes-config.xml* file on the location server.

- CSCsw49802—In release 5.0 and earlier, unencrypted user passwords were stored in the mobility services engine and location appliance database. In release 6.0 and later, all user passwords stored in the database are encrypted.

- CSCsx24404—Unused daemons were disabled in the mobility service engine to eliminate any security threat. The installer now disables sendmail, nfslock, portmapper, and cups using chkconfig.

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

- 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. Issue is resolved by documenting the need to install release 4.1 of *AeroScout MobileView* in the release notes.

- CSCsy70790—When simultaneous history queries (getTagHistoryList, getStationHistoryList, getRogueClientHistoryList, and getRogueAPHistoryList) of the mobility services engine were made from a third-party application, no successful response was received. API was modified to resolve the issue.

- CSCsy78058—Advanced searches for telemetry tags did not work.

- CSCsy85829—Some notification queries did not respond when the MAC address was entered in uppercase. Changes were made to accept both MAC addresses in both an uppercase and lowercase format (XX:XX:XX:XX:XX:XX or xx:xx:xx:xx:xx:xx).

- CSCsz01574—No client username displayed and an incorrect authentication state appeared for clients on maps and on the Monitor > Clients window when the option *Clients detected by MSEs* was selected from the show drop-down menu. This occurred when the mobility services engine was in a network in which an anchor and foreign controller configuration was in use. (Related caveat CSCsw71297).

- CSCsz05363—A mismatch in the location path loss calculation between WCS and the controller existed when the Normal Client check box was not checked on the Configure > Controller Template Launch Pad > *Location Configuration > New* window.

- CSCsz10593—Restoring a database to a different mobility services engine showed tag licenses purchased for a different mobility services engine. In addition, some windows in WCS showed the default setting of 100 tags. A license associated with one mobility services engine (with different UDI) should not have been accepted by another mobility services engine.

- CSCsz29526—When multiple mobility services engines and location appliances were running an accuracy test on the same floor and at least one of the systems was running release 5.1, the accuracy test would not complete successfully.

- CSCsz54233—The MAC address field for the wired switch was blank on the Wired Switches detail page. (Services > Mobility Services > Context Aware Service > Wired > Wired Switches.

- CSCsz78471—Adding evaluation extension licenses to the mobility services engine failed when the original evaluation license had expired and the evaluation limit was met. In some cases when the evaluation license was still current, but the limit was met, an evaluation extension was allowed but an incorrect message displayed noting that the device limit exceeded the limit.

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*

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

- *Cisco Context-Aware Software Configuration Guide, Release 6.0*

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

- *Cisco Adaptive Wireless Intrusion Prevention System Configuration Guide, Release 6.0*

    http://www.cisco.com/en/US/products/ps9817/products_installation_and_configuration_guides_list.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