Release Notes for Cisco 3300 Series Mobility Services Engine, Release 7.0.112.0

February 2011

These release notes describe open and resolved caveats for Release 7.0.112.0 of the Cisco 3300, 3350, and 3355 Mobility Services Engines and its two services:

- Context Aware Service (CAS)
- Adaptive Wireless Intrusion Protection Service (wIPS).

Note Before installing this software, see 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. See the "Ordering CAS Client and Tag Licenses for the Mobility Services Engine" section on page 7 for more information. You must purchase licenses from Cisco to support wIPS monitor mode access points. See the "Ordering Adaptive wIPS Licenses for the Mobility Services Engine" section on page 8.

Contents

These release notes contain the following sections:

- Introduction, page 2
- System Requirements, page 3
- Upgrading to This Release, page 4
- Important Notes, page 8
- New Feature Support, page 15
- Caveats, page 18
- If You Need More Information, page 21

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

- Troubleshooting, page 21
- Related Documentation, page 22
- Obtaining Documentation and Submitting a Service Request, page 22

Introduction

This section introduces the Cisco 3300 series Mobility Services Engine (MSE) andthe various services that it supports.

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 7.0.112.0:

- Context Aware Service (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.

  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. See the "Ordering CAS Client and Tag Licenses for the Mobility Services Engine" section on page 7.

- Wireless Intrusion Protection Service (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. See the "Ordering Adaptive wIPS Licenses for the Mobility Services Engine" section on page 8.

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 and later. Evaluation licenses are good for 60 days.

Note CAS and wIPS can operate simultaneously on the Cisco 3350, 3355, and 3310 mobility services engines.

Note See the online version of the *Cisco Context-Aware Software Configuration Guide, Release 7.0,* for details on configuring and monitoring CAS on the mobility services engine at the following URL: http://www.cisco.com/en/US/docs/wireless/mse/3350/7.0/CAS/configuration/guide/CAS_70.html

Note See the online version of the *Cisco Wireless Intrusion Prevention System Configuration Guide, Release 7.0* for details on configuring and monitoring wIPS on the mobility services engine at the following URL: http://www.cisco.com/en/US/docs/wireless/mse/3350/7.0/wIPS/configuration/guide/wips_70.html

Note See 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 the following URL: 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 Series Mobility Services Engine, WCS, and Wireless LAN Controller. (See Table 1).

Table 1 Minimum Software Requirements

Service	System	Minimum Software Release
Context-Aware Software and Wireless Intrusion Prevention System[1]	Mobility Services Engine	7.0.112.0 7.0.105.0 6.0.103.0 (or later)
	Controller	7.0.98.0 6.0.188.0 (or later) 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	7.0.164.0 6.0.132.0 (or later)
	Cisco WCS Navigator	1.6.164.0 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 the Cisco Adaptive Wireless Intrusion Prevention System.

Upgrading to This Release

For instructions for automatically downloading the software using WCS or for manually downloading the software using a local or remote connection, see 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 the following URL:

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

This section consists of the following topics:

- Upgrading from Release 5.x to 6.0.x or 7.0.x, page 4
- Compressed Software Image, page 6
- Updated Software Version Shown in WCS After Polling, page 6
- CAS and wIPS License Requirements, page 7
- Ordering CAS Client and Tag Licenses for the Mobility Services Engine, page 7
- Ordering Adaptive wIPS Licenses for the Mobility Services Engine, page 8

Upgrading from Release 5.x to 6.0.x or 7.0.x

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 When upgrading mobility services engine from 6.0 to 7.0.x, if any limits have been set on wireless clients or rogues, they will get reset because of the wired client limit change in 7.0.x.

Caution You must back up 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.x, follow these steps:

Step 1 Register the Product Authorization Key (PAK).

Note You receive a PAK when you order a license. If you have lost your PAK, you can use your sales order or the UDI number of the mobility services engine to register.

- Client and wIPS licenses are registered at the following URL: https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet
- Tag licenses are registered at the following URL: http://www.aeroscout.com/support

Step 2 Back up the mobility services engine database and the AeroScout database:

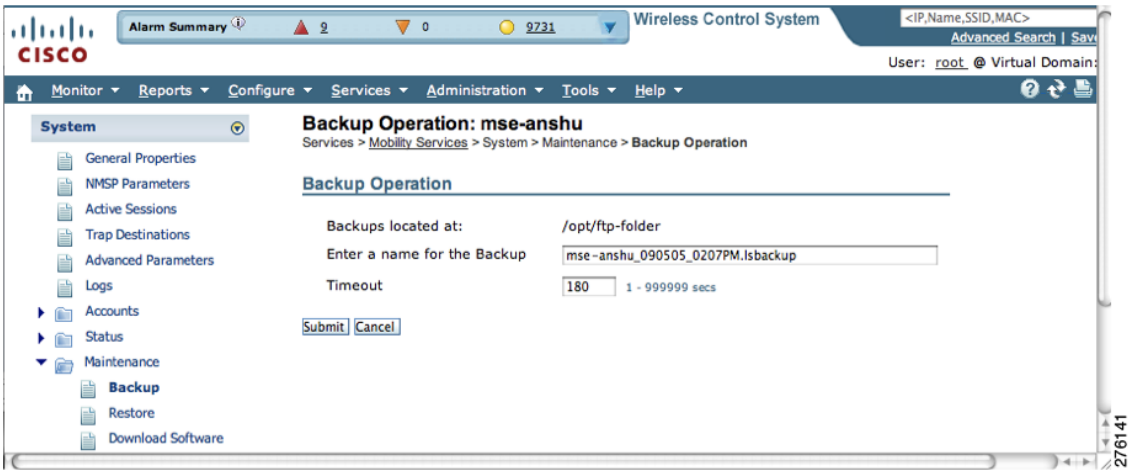
a. To back up the mobility services database (network designs controller configurations, clients, and access points), follow these steps:

1. Choose **Services > Mobility Services**.
2. Click the name of the mobility services engine for which you want to back up the database.
3. Choose **Maintenance > Backup** from System left sidebar menu.
4. Enter a name for the backup file.
5. Click **Submit** (see Figure 1).

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

http://www.aeroscout.com/support

Figure 1 System > Maintenance Window



Step 3 Download release 7.0.112.0:

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. Choose either an uploaded image or browse and upload an image.

e. Click **Download**.

Step 4 Install release 7.0.112.0 using the MSE CLI:

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
./uninstall
```

Note enter this once in the directory. Enter **no** when prompted to keep the old database.

```
cd /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 the System sidebar menu.
4. Choose the file to restore from the drop-down list.
5. Click **Submit**.

b. To restore the AeroScout database see the *AeroScout Context-Aware Engine for Tags for Cisco Mobility Services Engine User's Guide* at the following URL

http://www.aeroscout.com/support

Step 6 Install licenses:

See Chapter 2 of the *Context-Aware Services Configuration Guide, Release 7.0* at the following URL: http://www.cisco.com/en/US/products/ps9806/products_installation_and_configuration_guides_list.html

Compressed Software Image

If you download the mobility services engine image *.gz file using 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 WCS After Polling

After a software update, the new mobility services engine software version does not immediately appear in mobility services engine queries on WCS. Up to 5 minutes is required for the new version to appear. WCS, by default, queries the mobility services engine for status every 5 minutes.

CAS and wIPS License Requirements

Client and wIPS licenses are installed from WCS (Administration > License Center). See, Chapter 2: "Adding and Deleting Mobility Services Engines and Licenses" in the *Cisco Context-Aware Service Configuration Guide, Release 7.0,* and *Cisco Adaptive Wireless Intrusion Prevention System, Release 7.0*, respectively.

Tag licenses are installed using the *AeroScout System Manager*. See the "Installing Tag Licenses" section in Chapter 2: "Adding and Deleting Mobility Services Engines and Licenses in the *Cisco Context-Aware Service Configuration Guide, Release 7.0*.

For complete details on ordering and downloading licenses, see the *Cisco 3300 Series Mobility Services Engine Licensing and Ordering Guide for Context-Aware Mobility Software, and Adaptive wIPS, Release 7.0,* at the following URL:

http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html

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 3310 Mobility Services Engine allows for the tracking of up to 2000 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 license also includes tracking of rogue clients and rogue access points.

Licenses for tags and clients are offered in quantities ranging from 1000 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 1000 Wi-Fi tags on a Cisco 3350 mobility services engine (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 1000 client devices.
AIR-CAS-3KC-K9	License for tracking 3000 client devices.
AIR-CAS-6KC-K9	License for tracking 6000 client devices.
AIR-CAS-12KC-K9	License for tracking 12,000 client devices.
Tag Licenses	
AIR-CAS-1KT-K9	License for tracking 1000 tag devices.
AIR-CAS-3KT-K9	License for tracking 3000 tag devices.
AIR-CAS-6KT-K9	License for tracking 6000 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 access 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 or AIR-WIPS-AP-2000	License for 2000 monitor mode Cisco access points. **Note** Cannot be combined with other wIPS licenses.
AIR-WIPS-AP-UNL2	License for 3000 monitor mode Cisco access points **Note** The Cisco 3350 mobility services engine supports a maximum of 3000 Monitor Mode access point licenses.

Note From the 7.0.105.0 Release onwards, the evaluation license for wIPS monitor mode access points is 10.

Important Notes

This section describes important information about the operational notes and navigation changes for CAS, wIPS, and the mobility services engine for release 6.0.103.0 and later releases.

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

This section consists of the following topics:

- Operational Notes for a Mobility Services Engine, page 9
- Operational Notes for CAS, page 12
- Operational Notes for wIPS, page 15
- WCS Screen and Navigation Changes, page 15

Operational Notes for a Mobility Services Engine

This section lists the operational notes for an mobility services engine and consists of the following topics:

- Automatic Installation Script for Initial Setup, page 9
- Parameter Changes During Upgrade from 5.0.x to 6.0.x or 7.0.x, page 9
- Controller and Associated Mobility Services Engine Must be Mapped to the Same NTP and WCS Server, page 9
- Mandatory Default Root Password Change, page 10
- Root Password Configuration, page 10
- Configuring WCS Communication Username and password using MSE setup.sh, page 10
- Revoking MSE License Using MSE CLI, page 11
- Networks with Large Access Point Deployments Might Experience Slower Location Updates, page 11
- Configuration Changes for Greater Location Accuracy, page 11

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 the following URL:

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

Parameter Changes During Upgrade from 5.0.x to 6.0.x or 7.0.x

You will notice a change in the tracking limits when you:

1. Configure tracking limits in 5.0.x.
2. Upgrade to 6.0.x or 7.0.x.

   If limits are greater than licensed counts, limits are removed and licensed counts are enforced instead.

(CSCtd57386).

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

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

Note During first time login, even if you choose Skip (S), you will be prompted to enter the password. This is because it is mandatory to change root password during first time login.

Root Password Configuration

During the first time MSE setup script run, the **Skip** option provided for configuring root password is not honored even if it is specified. This is because the first time login and setup script invocation enforces the default credential change. So this prompts you to change the password (CSCsz44105).

Configuring WCS Communication Username and password using MSE setup.sh

You can configure the WCS Communication username and password using the MSE setup.sh script file.

Scenarios which you might encounter while configuring the WCS Username and password:

- If you configure a new WCS username and password, the password provided is applicable for the new WCS username created.
- If you only configure WCS username without configuring WCS password, then the default password admin is applied to the configured username.
- If you only configure WCS password without configuring the WCS username, then the password for the admin user is changed.
- If you configure an existing user name for the WCS username and also configure the password, then the password for that existing user is changed.

Note These users are API users, and they do not have corresponding OS users on MSE appliance.

(CSCtj39741).

Revoking MSE License Using MSE CLI

You can also revoke an MSE license from MSE CLI manually without using WCS.

To revoke an MSE license:

Step 1 Login to an MSE using CLI.

Step 2 Navigate to /opt/mse/licensing/

Step 3 Delete the license file by running this command:

`rm /opt/mse/licensing/`*license file name*`.lic`**

where *license file name* is the name of the license file.

Step 4 Restart the MSE process.

`/etc/init.d/msed restart`

The MSE license is revoked.

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 slowdown 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.

See 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.

Operational Notes for CAS

This section lists the operational notes for a mobility services engine and consists of the following topics:

- Synchronization Required When Upgrading to Release 7.0.112.0 or Importing CAD Floor Images, page 12
- Floor Change or Minimum Distance Required for Location Transitions to Post to the History Log, page 12
- Release 4.1 of AeroScout MobileView Required for Northbound Notifications, page 12
- Issues with the Aeroscout Tag Engine version 4.0.14.14 bundled with MSE release, page 13
- Non-Cisco Compatible Extensions Tags Not Supported, page 13
- Non-Cisco Compatible Extensions Tags Not Supported, page 13
- Cisco Compatible Extensions, Version 1 Tags Required at a Minimum, page 13
- Monitoring Information Varies for Clients and Tags, page 14
- Calibration Models and Data Apply Only to Clients, page 14
- Advanced Location Parameters Apply Only to Clients, page 14
- Location History Time stamps Match Browser's Location, page 14
- PDAs with Limited Probe Requests Might Affect Location, page 14
- Mandatory Setting Required on Intel 802.11n and 802.11 b/g/n Client Cards for Accurate Calibration, page 14

Synchronization Required When Upgrading to Release 7.0.112.0 or Importing CAD Floor Images

When upgrading to release 7.0.112.0 from release 6.x (and earlier) you must synchronize after the software upgrade and also when CAD-generated floor images are imported into WCS.

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

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

Navigation 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.

The workaround for this is to upgrade to Mobile View version 4.1(CSCsx56618).

Issues with the Aeroscout Tag Engine version 4.0.14.14 bundled with MSE release

Tag Location accuracy is greatly reduced if placing APs on floor after MSE synchronization (CSCtd84383).

Post Restore, Aeroscout Engine is not sometimes not able to stay registered (CSCtf91050).

To avoid these issues Aeroscout Tag Engine needs to be upgraded using the following steps:

Step 1 After your product registration has been verified, go to AeroScout Support Portal and download the appropriate CLE (Context-Aware Engine for Tags + System Manager).

Step 2 Install a new CLE version following the steps below:

a. Upload the new CLE installation file, for example: aeroscout-engine-4.2.3.5.x86_64.tar.gz to MSE under /opt/mse/locserver/partner-engine/ through an SFTP session.

b. Open a Secure Shell (SSH) session using the IP address of the MSE appliance.

c. Stop the MSE using the following command:

```
/etc/init.d/msed stop.
```

d. Entering the following command to change directory to /opt/mse/locserver/partner-engine/ by :

```
cd /opt/mse/locserver/partner-engine/.
```

e. Enter the following command to remove the AeroScout directory:

```
rm -Rf aeroscout.
```

f. Enter the following commands to install the new CLE:

```
tar -xf 4.2.3.5.x86_64.tar.gz
```

g. Enter the following command to start the MSE:

```
/etc/init.d/msed start.
```

For more details, see *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine Upgrade Guide*.

Step 3 Install AeroScout System Manager on another machine. See the *AeroScout Context-Aware Engine for Tag User Guide*.

Step 4 Install AeroScout License for Context Aware Engine. See the *AeroScout Context-Aware Engine for Tag Quick Start Guide*.

Non-Cisco Compatible Extensions Tags Not Supported

The mobility services engine does not support non-Cisco CX Wi-Fi tags. Additionally, these noncompliant tags are not used in location calculations or shown on 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 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 (Received Signal Strength Indication) 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.

See Chapter 7, "Context-Aware Planning and Verification" in the *Cisco Context-Aware Software Configuration Guide, Release 7.0* for more details on client calibration.

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

http://www.aeroscout.com/support

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.

See the "Editing Advanced Location Parameters" section in Chapter 7 of the *Cisco Context-Aware Software Configuration Guide, Release 7.0*.

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

Location History Time stamps Match Browser's Location

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

PDAs with Limited Probe Requests Might Affect Location

Many PDAs do not continuously send out probe requests after an initial association to the 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).

Operational Notes for wIPS

This section lists the operational notes for a mobility services engine.

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, 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 WCS page when you synchronize a mobility services engine and a controller (CSCsx38955).

WCS Screen and Navigation Changes

- *Services* replaces *Mobility* in the navigation bar of 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

The new features for the mobility services engine, CAS, and wIPS are summarized under separate headings.

This section consists of the following topics:

- Cisco 3355 Mobility Services Engine Support, page 15
- Common CAS and wIPS Features, page 15
- Context-Aware Software Features, page 16
- Context-Aware Software with Cisco CleanAir Features, page 17
- Adaptive Wireless Intrusion Prevention Software Features, page 18

Cisco 3355 Mobility Services Engine Support

The 7.0.112.0 release supports the new Cisco 3355 Mobility Services Engine.

Common CAS and wIPS Features

Both the CAS and wIPS services can operate on the Cisco 3350 and 3310 mobility services engines simultaneously. CAS and wIPS can now be deployed with the Cisco 3350, or the 3310 platforms.

Both platforms support services separately or concurrently as needed.

For information about the coexistence and scalability of services, see the *Cisco 3300 Series Mobility Services Engine Licensing and Ordering Guide.*

The MSE 3300 Series platform offers the advantage of centralizing support of mobility services within the Cisco WLAN infrastructure and enables third-party application integration through a common API.

Context-Aware Software Features

This section summarizes the features for Context-Aware Software and consists of the following topics:

- Troubleshooting and Notification Enhancements, page 16
- Granular Synchronization, page 16
- Performance and Accuracy Enhancements, page 16

Troubleshooting and Notification Enhancements

The following new troubleshooting and configuration enhancements have been implemented in Release 7.0.112.0:

- Mobility Services Engine support of up to 300 notifications per second per destination
- Enhanced network mobility services protocol (NMSP) troubleshooting GUI
- Improved error logging
- Better visibility into northbound notifications
- Enhanced synchronization history

The enhanced notification capabilities allow you to receive a great number of real-time notifications in a timely manner.

The improved error logging and enhanced troubleshooting provides information when data is not being updated properly, It helps you to troubleshoot the problems and provide a way to trace the path of data and drill down to the exact problem.

Granular Synchronization

This feature enables location tracking of all Wi-Fi and interference devices across the WLAN with synchronization on a per-floor and per-building level. It also increases the efficiency of tracking Wi-Fi devices or interference devices on a per-floor or per-building basis across large campus or distributed deployments.

Performance and Accuracy Enhancements

The following Performance and Accuracy features have been implemented in this release:

- Post calculation enhancements
- History bounding
- Notification statistics
- Detailed view of the number of destinations configured with status
- Type of each destination

With these performance improvements, the accuracy is now improved to the average of 5m and CFD of 7m 90% of the time.

Context-Aware Software with Cisco CleanAir Features

This section summarizes the features for the Context-Aware Software with CleanAir and consists of the following sections:

- Reporting Capability for Interferers, page 17
- Correlation of Interference Devices Across Multiple Wireless LAN Controllers, page 17
- Interference History Tracking and Playback, page 17
- Location of Interferers Including Zone of Impact, page 18

Reporting Capability for Interferers

This reporting option provides reporting capabilities for the top 10 worst interference devices. By default it displays all interferers which have severity greater than or equal to 5 and further filtering can be done by band, severity and options. These report tables provide instant visibility into the 10 worst interference incidents currently being reported to the system. Interferers are classified by band (802.11b/g/n or 802.11a/n).

You can use workflow links to efficiently view interference reports in the context of location or drill down to the radio level to perform troubleshooting and analysis.

This feature allows you to perform very granular analysis and to get a better understanding of the impact that devices causing interference have on the network.

Correlation of Interference Devices Across Multiple Wireless LAN Controllers

This feature enables multiple access points to hear the same interference event. The MSE correlates and aggregates interference events that span more than one WLC. It will identify and clarify that a source of interference is coming from a single interference device.

This feature not only provides visibility into the source of interference but identifies that it is the same interference that might be causing problems across larger network coverage areas. This feature indicates when to resolve a single source of interference, so that time is not wasted looking for multiple sources.

Interference History Tracking and Playback

The MSE collects and stores location tracking information on reported interference devices and provides details for forensics and analysis. The visual playback capability shows the exact movement and impact as the interferer moves within the network for the selected time of playback.

Historical interference tracking information and detailed playback allows you to correlate problems and quickly troubleshoot network issues.

This information also allows regular long- term tracking of organizational trends and provides visibility for monitoring non-Wi-Fi device usage and for policy enforcement.

The report launch pad interface allows highly customizable views of all reported interference devices so that you can get the required information and the visibility.

Location of Interferers Including Zone of Impact

This feature provides detailed location and information about the visibility of an interference device, including the zone impacted, from a Wireless Control System floor map. By default, interferers on b/g band are displayed on the map.

You can also see the zone of impact based on the interferer status, severity, and interferer type from the Interferer Filter page.

This feature saves valuable time in finding an interference source so that it can be permanently mitigated or policy can be changed.

The level of detailed visibility also provides valuable information on the impact not only to networks but to specific clients within the zone of impact, saving time in troubleshooting and reducing the cost for IT support.

For details on all the features discussed in this section, see the *Cisco Context-Aware Configuration Guide, Release 7.0,* at the following link:

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

Adaptive Wireless Intrusion Prevention Software Features

This section summarizes the features for the wIPS (Adaptive Wireless Intrusion Prevention Software) and consists of the following topics:

- Supported on Cisco 3350 and 3310 Series Mobility Service Engine, page 18
- SNMP Traps, page 18

Supported on Cisco 3350 and 3310 Series Mobility Service Engine

wIPS is supported on 3350 and 3310 series mobility services engines in release 6.0 and 7.0.x. Previously, wIPS was supported only on the 3310 mobility services engine in release 5.2.

SNMP Traps

For details on all the features discussed in this section, see the *Cisco Adaptive Wireless Intrusion Prevention System Configuration Guide, Release 7.0* at the following link:

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

Caveats

The following sections list Open Caveats and Resolved Caveats in Release 7.0.112.0 for Windows and Linux. For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are taken directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.

- Spelling errors and typos may be corrected.

Note If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website: http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs

To become a registered cisco.com user, go to the following website: http://tools.cisco.com/RPF/register/register.do

This section consists of the following topics:

- Open Caveats, page 19
- Resolved Caveats, page 19

Open Caveats

Table 4 lists the open caveats in Version 7.0.112.0.

Table 4 Open Caveats

ID Number	Caveat Title
CSCtg42616	The View Only Notification privilege also allows modification to the track definitions.
CSCtg79058	The WiFi TDoA receivers and Chokepoint list page returns empty results.
CSCsw66937	Tags cannot be located from non-root Virtual Domain in WCS.
CSCtg34826	Delete a controller from WCS, synchronize and check the NMSP connection status. The deleted controller does appear in the NMSP connection status.
CSCtg50685	The location accuracy claim of 10 meters, 90% is changed to 7meters, 90% from 7.0.x release onwards. However, the note in the Inspect Location Readiness page still shows 10 meters, 90%.

Resolved Caveats

Table 5 lists the Release 6.0.x caveats resolved in Release 7.0.112.0.

Table 5 Resolved Caveats

ID Number	Caveat Title
CSCtd99643	TaglocationListBytelem API does not return all status records.
CSCtf90266	From MSE Release 6.0.103.0 onwards, if we set a trigger on the MSE by using Java API, an empty AesTrackDefn definition list appears for the GetTrackGroupInfoList API. Also the consequent trigger does not work.
CSCtc15111	Storing data during Calibration leads to Matlab memory allocation error (WCS)
CSCtc58035	The Rogue AP Location History is not generated.
CSCta34216	The MSE failed to restart after setting the history parameter **Archive days** to 0.

Table 5 Resolved Caveats (continued)

ID Number	Caveat Title
CSCtb98803	The controller does not accept the MSE certificate if there is a huge time difference between the controller and the MSE. From 7.0.x release onwards, a message is displayed in the WCS whenever the NMSP communication fails because of the time-sync issues.
CSCtc26905	The MSE keeps using cached username and password even after it has been deleted.
CSCtc71530	The **Location change** notification is changed to **Information** in WCS.
CSCtb97006	In the WCS WiFi TDOA Receivers configuration page, try to sort the columns by 'MAC Address', 'WiFi TDOA Receiver Name' and 'Oper Status'. A Permission Denied message appears.
CSCta54903	The Copy or Replacement action on access point should mark network design unsynchronized in WCS.
CSCtb87143	For filtering parameters, the MAC wild card does not work in disallowed list in WCS.
CSCsz51996	Default MSE communication password to WCS is set to root default instead of being set to admin.
CSCtb48347	The MSE does not recover after the down destination comes back after 90 mins.
CSCtb48311	The MSE results in OutOfMemory due to Notification Scaling issue.
CSCta99248	RFID tags show up on MSE, when unsynchronized with controller.
CSCta60310	The measurement notification timeout range inconsistent with controller.
CSCtc32231	S/P Issue while doing a large database copy during Installation.
CSCsk18810	Performance issues noticed with 2000 access points.
CSCsv34781	Unable to synchronize controller with WCS after controller sysname changes.
CSCsx38955	Same controller can be assigned to different MSEs with wIPS service, and also synchronized after database resolution.
CSCsx53833	On MSE start up, sometimes an error message is seen in the log files and the boot up exits abruptly. This error also appears while using MSE heatmaps.

Table 6 lists the Customer found defects that were fixed in 7.0.112.0

Table 6 Resolved Customer Found Defects

ID Number	Caveat Title
CSCsu43201	MSEs unable to handle burst in notifications.
CSCsy47837	Add ability to filter by MAC address when getting Location logs.
CSCsy84983	Include Location Information as a column in Wired Clients page in WCS.
CSCsy94947	The UCONN in WCS shows AP Auth failed with MAC address of MSE.
CSCsz48902	Description not available for Notifications destination & Transport UI table.
CSCsz68681	In WCS Asset Name and Group cannot be updated after upgrade from G to H.
CSCsz74218	Query criteria with simpleHierarchy/fullhierarchy filelds not working.

Table 6 Resolved Customer Found Defects

ID Number	Caveat Title
CSCta42551	Monitor lite users are able to edit the asset information.
CSCta65696	The MSE hangs due to matlab crash.
CSCta83863	MSE runs on evaluation license in certain conditions.
CSCtc24529	All List APIs with AesQueryCriteria returns StackOverflowError.
CSCtc93717	Issues with GetDeviceListAPI.
CSCtc99604	The GetStationStatsList request without query criteria returns tag stats data.
CSCtd02336	AesEventGen:fireEventTo exceptions seen during Network Design synchronization.
CSCtd07437	The request for GetChanges for AesMobileStation returns AesMobileStationLocation / TagLocation related changes and errors in the logs.
CSCte39401	The MSE logs should report error messages more clearly.
CSCtf17352	The MSE is unreachable because of out-of-memory error.
CSCtf34473	Location History for Rogues is broken.
CSCtf37176	In WCS, under Services > Mobility Services > CAS > Filtering Parameters the message in the balloon for Upload MAC filtering file needs to be corrected.
CSCtf37879	A Warning message is shown when you change the Show filter in the WCS Network Designs synchronization page.
CSCtf63331	WCS homepage shows old probing clients data from the Location Server.
CSCtg00418	Character set encoding issue in GetNetwork Design releated API calls.
CSCtg28465	The java.lang.OutOfMemoryError occurs due to Synchronization.

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, see the Cisco TAC website at the following URL:

http://www.cisco.com/tac

Click **Troubleshooting**, 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 Context-Aware Software Configuration Guide, Release 7.0*
  http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html
- *Cisco Adaptive Wireless Intrusion Prevention System Configuration Guide, Release 7.0*
  http://www.cisco.com/en/US/products/ps9817/products_installation_and_configuration_guides_list.html
- The WCS Online Help available with the WCS product.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.
