Release Notes for Cisco 3300 Series Mobility Services Engine, Release 7.0.220.0

First Published: October 25, 2011
OL-24938-02

These release notes describe open and resolved caveats for Release 7.0.220.0 of the Cisco 3300, 3350, 3600, and 3355 mobility services engines and its two services:

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

Note Before installing this software, see the "System Requirements" section on page 4 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 10 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 11.

Contents

These release notes contain the following sections:

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

Introduction

This section introduces the Cisco 3300 series mobility services engine (MSE) and the 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 7.0.220.0:

- 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 10.

- 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 11.

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

Software and Aeroscout CLE Compatibility Matrix

Table 1 lists the compatibility matrix for the various releases of WCS, Controllers, 2710 Location Based Services, MSE 3300 series, and Aeroscout CLE.

Table 1 Software and Aeroscout CLE Compatibility Matrix

Release Date	WLC	WCS	2710 LBS	MSE 3300	Aeroscout CLE	NCS
22nd June 2007	4.1.171.0	4.1.83.0	3.0.37.0	—	—	—
13th August 2007	4.1.185.0	4.1.91.0	3.0.42.0	—	—	—
26th October 2007	4.2.61	4.2.62.0	3.1.35.0	—	—	—
28th January 2008	—	4.2.62.11	—	—	—	—
14th March 2008	4.2.112.0	4.2.81.0	3.1.36.0	—	—	—
27th May 2008	4.2.130	4.2.97.0	3.1.38.0	—	—	—
29th September 2008	4.2.176.0	4.2.110.0	3.1.42.0	—	—	—
14th February 2008	5.0.148.0	5.0.56.0	4.0.32.0	—	—	—
15th April 2008	—	—	4.0.33.0	—	—	—
1st August 2008	5.0.148.2	5.0.72.0	4.0.38.0	—	—	—
21st July 2008	4.2.130	5.1.64.0	5.1.30.0	5.1.30.0	2.1 (4.0.10.5)	—
9th January 2009	5.1.163.0	5.1.65.4	5.1.35.0	5.1.35.0	2.1 (4.0.10.5)	—
24th November 2008	5.2.157.0	5.2.110.0	5.2.91.0	5.2.91.0	2.2.1 (4.0.13-18)	—
10th February 2009	5.2.178.0	5.2.130.0	5.2.91.0	5.2.91.0	2.2.1 (4.0.13-18)	—
25th June 2009	5.2.193.0	5.2.148.0	5.2.100	5.2.100	2.2.1 (4.0.13-18)	—
11th June 2009	6.0.182.0	6.0.132.0	6.0.85.0	6.0.85.0	3.2.1 (4.0.15.12) or 3.2 (4.0.14.14)	—

Table 1 Software and Aeroscout CLE Compatibility Matrix (continued)

Release Date	WLC	WCS	2710 LBS	MSE 3300	Aeroscout CLE	NCS
9th November 2009	6.0.188.0	6.0.170.0	6.0.97.0	6.0.97.0	3.2.1 (4.0.15.12) or 3.2 (4.0.14.14)	—
17th February 2010	6.0.196.0	6.0.181.0	6.0.101.0	6.0.103.0	3.2.1 (4.0.15.12)	—
30th August 2010	6.0.199.4	6.0.196.0	6.0.102.0	6.0.105.0	4.2.4.4	—
4th April 2011	6.0.202.0	6.0.202.0	6.0.202.0	6.0.202.0	4.2.4.4	—
6th June 2010	7.0.98.0	7.0.164.0	—	7.0.105.0	4.2.3.5	—
14th April 2011	7.0.116.0	7.0.172.0	—	7.0.201.0	4.2.3.5	—
25 October 2011	7.0.220.0	7.0.220.0	—	7.0.220.0	4.3.1.19	1.0.2.29

System Requirements

The following minimum releases are required to configure and monitor CAS on the Cisco 3300 mobility services engine, WCS, and Wireless LAN Controller (See Table 2).

Table 2 Minimum Software Requirements

Service	System	Minimum Software Release
Context-Aware Software and Wireless Intrusion Prevention System[1]	Mobility services engine	7.0.202.10 7.0.201.204 7.0.105.0 6.0.103.0 (or later)
	Controller	7.0.120.0 7.0.116.0 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)
	Cisco WCS	7.0.172.16 7.0.172.0 7.0.164.0 6.0.132.0 (or later)
	Cisco WCS Navigator	1.6.172.16 1.6.172.0 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 the MSE

For instructions on 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 contains of the following topics:

Upgrade Scenarios

Starting from Release 7.0.201.204, you will not be able to restore databases from older Releases 5.0, 6.0, 7.0.105.0, and 7.0.112.0 to 7.0.220.0 using the WCS. There is a defined procedure to do so. Oracle has been introduced as the database vendor for MSE. Solid database will be discontinued starting with 7.0.201.204.

There are four scenarios to upgrade MSE to 7.0.220.0 from 5.0, 6.0, 7.0.105.0, and 7.0.112.0:

Upgrading the MSE to 7.0.220.0 from Older Releases Without Data Migration

To upgrade from older releases to 7.0.220.0 without data migration, follow these steps:

Step 1 Back up the existing database using WCS. This is always recommended.

All data existing on the system will be lost and a fresh blank database will be created.

Step 2 Transfer the *.tar file for 7.0.220.0 to the MSE appliance.

`CISCO-MSE-L-K9-7-0-220-x-64bit.db.tar`

Step 3 Place the file under /opt/installers folder. You should manually FTP this file to the appliance.

Note Use binary mode for the transfer. Make sure that the downloaded file sizes are the same as those on Cisco.com

Step 4 Untar the file: tar -xvf CISCO-MSE-K9-7-0-220-0-64.bit-db.tar.
This gives you the following:

- 5 files
- 4 zips
  - database_installer_part1of4.zip
  - database_installer_part20f4.zip
  - database_installer_part3of4.zip
  - database_installer_part4of4.zip
- 1 Cisco-MSE-L-K9-7-0-220-X-64bit.bin.gz

Step 5 To decompress (unzip) the file, execute: gunzip CISCO-MSE-L-K9-7-0-220-0-64bit.bin.gz.

Step 6 Execute the following command:

chmod +x CISCO-MSE-L-K9-7-0-220-0-64bit.bin

Step 7 Uninstall the existing MSE software. Choose deletion of database when prompted.

Step 8 Invoke the MSE installer.

Doing so installs the new database using the four zip files for the database along with the MSE software.

Initial database installation can take a long time (20 minutes at least -or- approximately). Do not cancel the installer midway through the installation process.

Once installed, follow the regular procedure to start, or stop, or add MSE to WCS.

Upgrading MSE to 7.0.220.0 from Older Releases with Data Migration

To upgrade the MSE from older releases to 7.0.220.0 with data migration, follow these steps:

Step 1 Back up the existing database using WCS.

This is always recommended.

All data existing on the system will be lost and a fresh blank database will be created.

Step 2 Transfer the *.tar file for 7.0.220.0 to the MSE appliance.

`CISCO-MSE-L-K9-7-0-220-0-64bit.db.tar`

Step 3 Place all of the files in the /opt/installers folder.

Note Use binary mode when using FTP. Make sure that the downloaded file sizes are same as these on Cisco.com.

Note The *.tar file cannot be downloaded using the WCS download software interface. It should be manually transferred.

Note Do not uninstall the existing MSE software on the appliance. In other words, if you have 5.x, 6.x or 7.0 installed with data you want to preserve across upgrade to 7.0.220.0, do not uninstall it.

Step 4 Untar the file: tar -xvf CISCO-MSE-K9-7-0-220-0-64.bit-db.tar.
This gives you the following:

- 5 files
- 4 zips
  - database_installer_part1of4.zip
  - database_installer_part20f4.zip
  - database_installer_part3of4.zip
  - database_installer_part4of4.zip
- 1 Cisco-MSE-L-K9-7-0-220-X-64bit.bin.gz

Step 5 To decompress(unzip) the file, execute: gunzip CISCO-MSE-L-K9-7-0-220-0-64bit.bin.gz.

Step 6 Execute the following command: chmod +x CISCO-MSE-L-K9-7-0-220-0-64bit.bin.

Step 7 Invoke the installer ./CISCO-MSE-L-K9-7-0-220-0-64bit.bin and answer the questions when prompted.

The installer will automatically detect if there is an old database present and ask relevant questions.

Sample Upgrade Questions

```
Installation Check
----------------------
The system appears to have a Cisco Mobility Services Engine already installed. If you
choose Continue", all the currently installed components will be removed permanently
(Only database and license files will be preserved
   ->1 - Exit
     2 - Continue


ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT: 2


-------------------------------------------------
-------------------------------------------------
Data Migration Check
-------------------------------------------------
The currently installed version of the MSE database is not directly compatible with the
new version. The system will now migrate the database from existing database to the new
system. Choose an appropriate option below -


   ->1 - Proceed to migrate data from previous release
     2 - Abort Installation


ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT: 1
-------------------------------------------------
-------------------------------------------------
Do you wish to migrate history data too? It can take a long time if history data is large
in size (Y/N): y
```

```
Exporting data from currently installed database.
This may take a while .....
Data migration successfully completed. Will now proceed with installation of new image.

Installing...
----------------------

-------------------------------------------------
-------------------------------------------------

-------------------------------------------------
-------------------------------------------------
Database Installation
-----------------------
The installer will now install the database. This may take a long time (- 15 minutes).
Do not cancel the installer.

PRESS <ENTER> TO CONTINUE:

-------------------------------------------------
-------------------------------------------------

!!!!!! IMPORTANT NOTE !!!! :
---------------------------------
The system is minimally configured right now. It is strongly recommended that you run the
setup script under /opt/mse/setup/setup.sh to configure all appliance related parameters
immediately after installation is complete. The hostname must be set correctly on the
system. The Cisco MSE platform will NOT start if it is configured incorrectly or not
configured at all. Additionally, it is strongly recommended that the Cisco MSE is
configured to use the same NTP servers as the controllers with which it will be
synchronized. This is essential to the correct operation of the Cisco Mobility Services
Engine. Both these parameters may be configured as part of the setup script.

PRESS <ENTER> TO CONTINUE:
-------------------------------------------------
-------------------------------------------------
Importing Data
-------------------------------------------------
Loading data into newly installed database. This may take a while ......
PRESS <ENTER> TO CONTINUE:
```

Upgrading MSE to 7.0.220.0 from 7.0.201.204 or Older Releases

To upgrade MSE to 7.0.220.0 from 7.0.201.204, 7.0.201.0, 7.0.112.0, follow these steps:

Note Complete database installation is not required here since for upgrading from 7.0.201.204.

Step 1 Download CISCO-MSE-L-K9-7-0-220-0-62bit.bin.gz to the MSE using the standard WCS download software page.

Step 2 Log in to the MSE console as root and execute the following commands:

```
cd/opt/installers
./CISCO-MSE-L-K9-7-0-220-0-64.bit.bin
```

Step 3 Answer the questions when prompted.

The installer will automatically detect if there is an old database present and ask relevant questions.

Restoring an Old Database from 5.0, 6.0, 7.0.105.0, or 7.0.112.0 to 7.0.220.0

To restore an old database onto MSE 7.0.220.0, follow these steps:

Note The regular Restore option on WCS cannot be used to restore an older database of older releases such as 5.0, 6.0, 7.0.105.0, or 7.0.112.0 onto 7.0.220.0.

Step 1 Stop the running MSE 7.0.220.0.

Step 2 Uninstall the software. Choose to delete the database.

Step 3 Based on backed up data that you want to restore, follow the matrix in Table 3 to install a relevant version of MSE.

Table 3 Release Matrix

Version of Database to be restored	New version that should be installed
5.2.x	5.2, 6.x, 7.x
6.x	6.x, 7.x

Step 4 Once you have installed the software, restore the desired database backup onto this using the regular procedure from WCS.

Step 5 To migrate data to 7.x.x.x, follow the steps in the "Upgrading MSE to 7.0.220.0 from Older Releases with Data Migration" section on page 6.

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 provides tracking of 15,000 Wi-Fi clients and 1000 Wi-Fi tags on a Cisco 3350 mobility services engine (see Table 4).

CAS License Ordering Summary

The KT SKUs mentioned in this table are used for Tag tracking using Aeroscout Tag engine. The KC SKUs are CAS licenses that include Clients, Tags (Cisco Tag Engine), rogues, interferers etc. Order numbers for client and tag licenses are summarized in Table 4.

Table 4 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 5.

Table 5 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.
AIR-LM-WIPS-5	ELM License for 5 local mode Cisco access points.
AIR-LM-WIPS-25	ELM License for 25 local mode Cisco access points.
AIR-LM-WIPS-100	ELM License for 100 local mode Cisco access points.

Table 5 Order Numbers for Adaptive wIPS Licenses (continued)

Order Number	Licenses
AIR-LM-WIPS-500	ELM License for 500 local mode Cisco access points.
AIR-LM-WIPS-2000	ELM License for 2000 local mode Cisco access points.

Note

- From Release 7.0.105.0 and later, the evaluation license for wIPS monitor mode access points is 10.
- From Release 7.0.200.x and later, the wIPS monitor mode license also includes local mode access points. In other words, the monitor mode SKUs can be used by monitor mode as well as Local Mode access points, whereas local mode SKUs can only be used by licensed local mode APs.

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 contains of the following topics:

Operational Notes for a Mobility Services Engine

This section lists the operational notes for the mobility services engine and contains the following topics:

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 do the following:

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

Communication between the mobility services engine, WCS, and the controller are in Coordinated Universal time (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 while running 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 while running the automatic installation script to ensure optimum network security.

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

Note For the initial login, even if you choose Skip (S), you will be prompted to enter the password. This is because it is mandatory to change the root password at the initial login.

Root Password Configuration

During ISO image load on the MSE and while running the setup script, the skip selection option provided for configuring the root password is not selected. This is because the initial time login and setup script invocation enforces the accepted credential change. So then this prompts you to change the password (CSCsz44105).

Password Expiry and SSH Authentication for a Root User

- There is no expiry of password for a root user. This is not a configurable option in the MSE setup.
- Root users are allowed to log in through Console. SSH no longer is used for root user logins. For a root user, you can configure this option using the MSE setup.sh script file. When you configure this option, the SSH daemons are stopped in MSE.

This is applicable for 3350 series MSEs from 7.0.200.x release and later (CSCti83419).

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 are as follows:

- If you configure a new WCS username and password, the password provided is applicable for the new WCS username created.
- If you only configure the WCS username without configuring the WCS password, then the default password admin is applied to the configured username.
- If you only configure the 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 the 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, follow these steps:

Step 1 Log in to an MSE using CLI.

Step 2 Navigate to /opt/mse/licensing/

Step 3 Delete the license file by running the following 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 in the Services > Context Aware Notifications window.

See CSCsu43201 in the Open Caveats section for a 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 following RSSI parameters might require 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 Contact Cisco TAC for assistance in modifying these parameters.

Scheduled Application Restart

An application restart is scheduled 1 year in advance as a requirement for the Oracle database. You should not modify this schedule.

Operational Notes for CAS

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

Synchronization Required When Upgrading to Release 7.0.220.0 or Importing CAD Floor Images

When upgrading to Release 7.0.220.0 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 new location of the element is at least 30 feet (10 meters) from its original location.

See 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 sent again 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).

Separate Partner Engine Software Install Not Required for Tag Contextual Information

In Release 5.2 and later, 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 in Release 5.1.

WCS Online Help Outlines Incorrect Software Download Procedure

In WCS online help (OLH), the steps in the "Downloading Software to a mobility services engine Using WCS" section mistakenly note commands for downloading an aeroscout-engine. The aeroscout-engine is now bundled within the mobility services engine software. See Chapter 9 of the *Cisco Context-Aware Service Configuration Guide, Release 7.0,* 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 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 (or later) tags are used in location calculations and mapped in WCS.

Monitoring Information Varies for Clients and Tags

In 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 Indicator (RSSI) reading. This information is not available in the Monitor > Tags page.

Calibration Models and Data Apply Only to Clients

Calibration models and data apply only to clients when using Partner Tag Engine, Cisco Tag Engine Calibration Models, and Data Apply to both Tags and 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 URL:

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.

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

See 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 and contains the following topics:

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 (see Administration > License Center).
- A Switches tab is a new synchronize option to support the new wired Catalyst switch and wired client feature (see Services > Synchronize Services).

New Feature Support

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

This section contains of the following topics:

Common CAS and wIPS Features

Both the CAS and wIPS services can operate on the Cisco 3350, 3355, and 3310 mobility services engines simultaneously. CAS and wIPS can now be deployed with the Cisco 3350, 3355 or 3310 platforms.

These 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 contains the following topics:

S60 Enhancement

Currently, client probes are used to extract RSSI information that enables location tracking of these clients. CCXv4 specification included a mandatory S60 component that was later made optional in CCXv5. At the time of this writing, the only 802.11a/b/g Wireless Card Bus Adapter which supported the optional S60 features in compliance to CCXv5 is the Cisco AIR-CB21AG-A-K9 (Kitty Hawk). Therefore, all S60 feature related testing will be tested with the AIR-CB21AG-A-K9. The S60 feature creates a Pathloss Measurement (PLM) request by an AP to be sent to the client which then causes the clients to send bursts of Pathloss Measurement frames, at regular intervals, back to the AP. The packets contain information about the channel and the tx power information. These help sort out the following issues:

- Off channel readings pollute the location calculation. It is not possible to determine with certainly off channel probes.
- Once a client associates, the probes are sent less frequently thus there is less information to calculate location more frequently. Additionally, some clients, by design, send few or no probe requests, and probe requests on channels subject to DFS rules are initially prohibited.
- Some specific client information, such as tx power, is missing from probes.

Cisco Tag Engine

MSE Release 7.0.x and later provides the option of using Cisco Tag Engine as an alternative to Aeroscout Tag Engine for all RFID RSSI-based location calculations. You can select any of the engines when adding MSE to the WCS. This selection could be changed at a later point of time using WCS.

You do not require additional licenses for using the Cisco Tag Engine.

For example, if you have purchased a 12000 client license from Cisco, then you can continue to use the same license even for Cisco Tag Engine. The total device count will now include RFID tags too.

Adaptive Wireless Intrusion Prevention Software Features

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

wIPS Support on Cisco 3350, 3355, and 3310 Mobility Service Engines

wIPS is supported on Cisco 3350, 3355, and 3310 mobility services engines in Release 6.0.x and 7.0.x. Previously, wIPS was supported only on the 3310 mobility services engine in Release 5.2.

wIPS ELM

Broadly, wireless intrusion detection software is a collection of alarms designed to detect an array of attacks on customer networks and equipment. To achieve this goal, a subset of the capabilities of the AirMagnet monitor mode WIPs alarms are being ported to the local mode APs. This allows customers to use their deployed APs to provide protection without needing a separate overlay network.

Caveats

This section lists Open Caveats and Resolved Caveats in Release 7.0.220.0 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.

If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website: http://tools.cisco.com/Support/BugToolKit/.
To become a registered cisco.com user, go to the following website: http://tools.cisco.com/RPF/register/register.do

This section contains of the following topics:

Open Caveats

Table 6 lists the open caveats in Release 7.0.201.210.

Table 6 Open Caveats

ID Number	Caveat Title
CSCtr24225	Headline: Changes to harden the password requirements for MSE. Symptom: The minimum length of the password for MSE should be one character. Also, the password should be a strong password having a lowercase, uppercase, numeric, and special characters. Condition: None. Workaround: None
CSCtt06686	Headline: There is tracking and log parameters issue while upgrading from 6.0.202.0 to 7.0.220.0 release. Symptom: If you have enabled limited tracking of certain devices in 6.0.202.0, those configurations are lost while upgrading to 7.0.220.0 release. This prevents the user defined rules for tracking devices (**Enable Limiting and Limit Values only on Services > Mobility Services Engine > Context Aware Service > Tracking Parameters**) from running. This is true for Logging parameters also. Condition: This happens when an MSE that is running 6.0.202.0 is upgraded to 7.0.201.4 and above releases. The logging parameters on **Services > Mobility Services Engine > System > Logs** are not preserved across the upgrade. Also, the flags for **Enable Limiting and the limit values Services > Mobility Services Engine > Context Aware Service > Tracking Parameters** are not preserved across the upgrade. Workaround: None.
CSCtt15167	Headline: wIPS service memory allocation is not controlled. Symptom: wIPS service is taking more memory than the allocated memory. Sometimes it crashes and comes back automatically. Conditions: This happens when there is lots of wIPS traffic that is received by the wIPS service. Workaround: None.
Release	Headline: Movement detection parameters are set to 0 after upgrade from HMR4. Symptom: Movement detection parameters in the location parameters page has o values. Conditions: This occurs while upgrading from MSE 6.0 release to 7.0.201.204 and 7.0.220.0. Workaround: You should manually reset the values from UI for these parameters: • Individual RSSI change threshold: 5 • Aggregated RSSI change threshold: 3 • Many new RSSI change percentage threshold: 20 • Many missing RSSI percentage threshold: 20

Resolved Caveats

Table 7 lists the caveats resolved in Release 7.0.220.0.

Table 7 Resolved Caveats

ID Number	Caveat Title
CSCtn40852	Images are not showing up correctly in the accuracy report.
CSCto53644	Location history report shows incorrect client status.
CSCto78942	Info fields are showing wrong values when playing tag history.
CSCtk66718	Aeroscout engine fails to start on MSE if the WCS map names have special characters such as “&”.
CSCtq44401	WLC gets unassigned even if there are other APs on the synched maps.
CSCtr83456	MSE became unreachable after 2.5 days of normal enterprise operation.
CSCtj07375	An error message is displayed every few seconds on the MSE 3350 console with 7.0.200.88 load.
CSCtr39419	MSE setup script while configuring ntp, adds incorrect line to ntp.conf.
CSCts02828	MSE service hangs when synchronized with large calibration model.
CSCto79110	Backup/restore fails with large database on MSE.
CSCtq94160	MSE upgrade issue while upgrading from 7.0 to 7.0.220.0 release.
CSCtr06726	MSE database operation is failing in the 7.0.220.0 release.
CSCts02828	MSE service stops when it is synchronized with large calibration model.
CSCto79110	Backup/restore fails with large database on MSE.
CSCtt08080	MSE Apache server does not start if the MSE HTTP option is toggled.
CSCts44203	There is a security issue in the MSE Apache server.
CSCto78596	MSE logs are not getting downloaded. The rundiag.out was not accessible on account of permissions.

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/cisco/web/support/index.html

Click **Troubleshooting**, choose your product, and then click 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 7.0.201.204*
  http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html
- *Cisco Adaptive Wireless Intrusion Prevention System Configuration Guide, Release 7.0.201.0*
  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.
