Release Notes for Cisco 3300 Series Mobility Services Engine, Release 7.2.103.0

First Published: February 06, 2012
OL-24938-03

These release notes describe open and resolved caveats for Release 7.2.103.0 of the Cisco 3300, 3350, and 3355 mobility services engines and its two services:

- Context Aware Service (CAS).
- Adaptive Wireless Intrusion Protection System (wIPS).
- Cisco Mobility Services Advertisement Protocol (MSAP).

Note Before installing this software, see the "System Requirements" section on page 5 for details on compatibility with Cisco wireless LAN controllers and Cisco Prime Network Control System (NCS).

Note You will require Context-Aware and Adaptive wIPS license to run Context-Aware Service and wIPS Service. For ordering information, see the "Ordering Licenses for the Mobility Services Engine" section on page 12.

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 7.2.103.0:

- Context Aware Service (CAS)—Allows a mobility services engine to simultaneously track thousands of mobile assets and clients by retrieving contextual information such as presence, location, telemetry data, and historical information.

  CAS relies on two engines for processing the contextual information it receives. The Context Aware Engine for clients and tags (“KC” licenses) processes data for Wi-Fi clients and tags using the RSSI information. The Context-Aware Engine for tags (“KT” licenses) processes data for Wi-Fi tags using RSSI and TDoA information). Both these engines can be deployed together or separately depending on the business needs.

  Note For ordering information, see the “Ordering Licenses for the Mobility Services Engine” section on page 12.

- 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 and Enhanced Local Mode (ELM) Access Points. Proactive threat prevention is also supported to create a hardened wireless network core that is impenetrable by most wireless attacks.

  Note For ordering information, see the “Ordering Licenses for the Mobility Services Engine” section on page 12.

- Cisco Mobility Services Advertisement Protocol (MSAP)—The Cisco Mobility Services Advertisement Protocol (MSAP) provides functionality to deliver advertisements over Wi-Fi infrastructure. MSAP facilitates MSAP capable mobile devices to receive service advertisements. Once the mobile device receives the service advertisements, it can display their icons and data on its user interface, facilitating the process of users discovering what is available in their surroundings.

In addition, MSAP can be used by the mobile devices that have been configured with a set of policies for establishing network connectivity. The MSAP provides requirements for clients and servers and describes the message exchanges between them.

Note Evaluation licenses for 100 clients, 100 tags, and 10 wIPS monitor mode access points come standard with MSE installed with Release 6.0 and later for 60 days.

Note CAS and wIPS can operate simultaneously on the Cisco MSE-3310, 3350, 3355, and Virtual Appliance.

Note See the online version of the *Cisco Context-Aware Software Configuration Guide, Release 7.2,* 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/3350/7.2/CAS/configuration/guide/CAS_72.html

Note See the online version of the *Cisco Wireless Intrusion Prevention System Configuration Guide, Release 7.2* 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/3350/7.2/wIPS/configuration/guide/wips_72.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 Compatibility Matrix

Table 1 lists the compatibility matrix for the various releases of Cisco Mobility Services Engine, Cisco Wireless Control System, Cisco Prime Network Control System, and Cisco MSE.

Table 1 Cisco MSE Compatibility Matrix

Release Date	WLC	WCS	NCS	2710 Location Appliance	MSE 3350	MSE 3310	MSE 3355	MSE Virtual Appliance	Aeroscout CLE
06 February 2012	7.2.103.0	–	1.1.0.58	–	7.2.103.0	7.2.103.0	7.2.103.0	7.2.103.0	4.4.1.4
25th October 2011	7.0.220.0	7.0.220.0	1.0.2.29	–	7.0.220.0	7.0.220.0	7.0.220.0	–	4.3.1.19
14th April 2011	7.0.116.0	7.0.172.0	–	–	7.0.201.0	7.0.201.0	7.0.201.0	–	4.2.3.5
6th June 2010	7.0.98.0	7.0.164.0	–	–	7.0.105.0	7.0.105.0	7.0.105.0	–	4.2.3.5

Table 1 Cisco MSE Compatibility Matrix (continued)

Release Date	WLC	WCS	NCS	2710 Location Appliance	MSE 3350	MSE 3310	MSE 3355	MSE Virtual Appliance	Aeroscout CLE
4th April 2011	6.0.202.0	6.0.202.0	–	6.0.202.0	6.0.202.0	6.0.202.0	6.0.202.0	–	4.2.4.4
30th August 2010	6.0.199.4	6.0.196.0	–	6.0.102.0	6.0.105.0	6.0.105.0	–	–	4.2.4.4
17th February 2010	6.0.196.0	6.0.181.0	–	6.0.101.0	6.0.103.0	6.0.103.0	–	–	3.2.1 (4.0.15.12)
9th November 2009	6.0.188.0	6.0.170.0	–	6.0.97.0	6.0.97.0	6.0.97.0	–	–	3.2.1 (4.0.15.12) or 3.2 (4.0.14.14)
11th June 2009	6.0.182.0	6.0.132.0	–	6.0.85.0	6.0.85.0	6.0.85.0	–	–	3.2.1 (4.0.15.12) or 3.2 (4.0.14.14)
25th June 2009	5.2.193.0	5.2.148.0	–	5.2.100	5.2.100	5.2.100	–	–	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	5.2.91.0	–	–	2.2.1 (4.0.13-18)
24th November 2008	5.2.157.0	5.2.110.0	–	5.2.91.0	5.2.91.0	5.2.91.0	–	–	2.2.1 (4.0.13-18)
9th January 2009	5.1.163.0	5.1.65.4	–	5.1.35.0	5.1.35.0	5.1.35.0	–	–	2.1 (4.0.10.5)
1st August 2008	4.2.130.0	5.1.64.0	–	5.1.30.0	5.1.30.0	5.1.30.0	–	–	2.1 (4.0.10.5)
21st July 2008	5.0.148.2	5.0.72.0	–	4.0.38.0	–	–	–	–	–
15th April 2008	–	–	–	4.0.33.0	–	–	–	–	–
22nd June 2007	5.0.148.0	5.0.56.0	–	4.0.32.0	–	–	–	–	–
13th August 2007	4.2.176.0	4.2.110.0	–	3.1.42.0	–	–	–	–	–
26th October 2007	4.2.130.0	4.2.97.0	–	3.1.38.0	–	–	–	–	–
28th January 2008	4.2.112.0	4.2.81.0	–	3.1.36.0	–	–	–	–	–
14th March 2008	–	4.2.62.11	–	–	–	–	–	–	–
27th May 2008	4.2.61	4.2.62.0	–	3.1.35.0	–	–	–	–	–
29th September 2008	4.1.185.0	4.1.91.0	–	3.0.42.0	–	–	–	–	–
14th February 2008	4.1.171.0	4.1.83.0	–	3.0.37.0	–	–	–	–	–

System Requirements

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

Table 2 Minimum Software Requirements

Service	System	Minimum Software Release
Context-Aware Software, Wireless Intrusion Prevention System[1], and Cisco Mobility Services Advertisement Protocol[2]	Mobility services engine	7.2.103.0 7.0.202.10 7.0.201.204 7.0.105.0 6.0.103.0 (or later)
	Controller	7.2.103.0 7.1.91.0 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 NCS	1.1.0.58 1.2.x.x
	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, NCS, and mobility services engine to support the Cisco Adaptive Wireless Intrusion Prevention System.
2. Release 7.2 is the minimum software requirement for the controller to support the Cisco Mobility Services Advertisement Protocol.

Upgrading the MSE

For instructions on automatically downloading the software using NCS 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, 7.0.112.0 to 7.2.103.0 using the NCS. There is a defined procedure to do so. Oracle has been introduced as the database vendor for MSE. The solid database is discontinued starting with Release 7.0.201.204.

There are four scenarios to upgrade MSE to 7.2.103.0 from 6.0, 7.0.105.0 and 7.0.112.0:

Upgrading the MSE to 7.2.103.0 from Older Releases Without Data Migration

To upgrade from older releases to 7.2.103.0 without data migration, follow these steps:

Step 1 Back up the existing database using NCS. 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 7.2.103.0 to the MSE appliance.

`CISCO-MSE-L-K9-7-2-103-0-64bit.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-K9-7-2-103-0-64.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-K9-7-2-103-0-64bit.bin.gz

Step 5 To decompress (unzip) the file, execute: gunzip CISCO-MSE-L-K9-7-2-103-0-0-64bit.bin.gz.

Step 6 Execute the following command:

chmod +x CISCO-MSE-L-K9-7-2-103-0-64bit.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 NCS.

Upgrading the MSE to 7.2.103.0 from Older Releases with Data Migration

To upgrade the MSE from older releases 7.2.103.0 with data migration, follow these steps:

Step 1 Back up the existing database using NCS.

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 7.0.103.0 to the MSE appliance.

`CISCO-MSE-L-K9-7-2-103-0-64bit.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 NCS 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 5.0, 6.0 or 7.0 installed with data you want to preserve across upgrade to 7.2.103.0, do not uninstall it.

Step 4 Untar the file: tar -xvf CISCO-MSE-K9-7-2-103-0-64.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-K9-7-2-103-0-64bit.bin.gz

Step 5 To decompress (unzip) the file, execute: gunzip CISCO-MSE-L-K9-7-2-103-0-64bit.bin.gz.

Step 6 Execute the following command: chmod +x CISCO-MSE-L-K9-7-2-103-0-64bit.bin.

Step 7 Invoke the installer ./CISCO-MSE-L-K9-7-2-103-0-64bit.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 the MSE to 7.2.103.0 from 7.0.201.204 or Later Releases

To upgrade the MSE to 7.2.103.0 from 7.0.201.204 or later releases, follow these steps:

Note Complete database installation is not required here since we are upgrading from 7.0.201.204 or later releases.

Step 1 Download CISCO-MSE-L-K9-7-2-103-0-62bit.bin.gz to the MSE using the standard NCS download software page.

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

```
cd/opt/installers
./CISCO-MSE-L-K9-7-2-103-0-64.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.

Upgrading MSE to 7.2.103.0 from 7.0.220.0

To upgrade MSE to 7.2.103.0 from 7.0.220.0, follow these steps:

Note Complete database installation is not required here since we are upgrading from 7.0.220.0

Step 1 Download CISCO-MSE-L-K9-7-2-103-0-62bit.bin.gz to the MSE using the standard NCS download software page.

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

```
cd/opt/installers
./CISCO-MSE-L-K9-7-2-103-0-64.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 6.0, 7.0.105.0, or 7.0.112.0 to 7.2.103.0

To restore an old database onto MSE 7.2.103.0, follow these steps:

Note The regular Restore option on NCS cannot be used to restore an older database of older releases such as 6.x, 7.0.105.0, or 7.0.112.0 onto 7.2.103.0.

Step 1 Stop the running MSE 7.2.103.0.

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 NCS.

Step 5 To migrate data to 7.x.x.x, follow the steps in the "Upgrading the MSE to 7.2.103.0 from Older Releases with Data Migration" section on page 7.

Compressed Software Image

If you download the mobility services engine image *.gz file using NCS, 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

The MSE virtual appliance software is distributed as an Open Virtualization Archive (OVA) file. You can install the MSE virtual appliance using any of the methods for deploying an OVF. For more information on deploying the MSE virtual appliance, see Chapter 5: "MSE Delivery Modes" in the *Cisco Context-Aware Service Configuration Guide, Release 7.2,* and *Cisco Adaptive Wireless Intrusion Prevention System, Release 7.2*, respectively.

Updated Software Version Shown in NCS After Polling

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

CAS and wIPS License Requirements

Client and wIPS licenses are installed from NCS (Administration > License Center). See, Chapter 2: "Adding and Deleting Mobility Services Engines and Licenses" in the *Cisco Context-Aware Service Configuration Guide, Release 7.2,* and *Cisco Adaptive Wireless Intrusion Prevention System, Release 7.2*, 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 7.2*.

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 7.2,* at the following URL:

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

Ordering 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).

Cisco Context-Aware licenses are based on the number of Wi-Fi endpoints tracked (endpoints include Wi-Fi clients, interferers, wired devices, and Wi-Fi tags). The Cisco Mobility Services Engine 3355 allows for the tracking of up to 18000 endpoints (combined count) and the Mobility Services Engine 3310 allows for tracking of up to 2000 endpoints (combined count). The MSE virtual appliance can track up to 50000 endpoints depending on server resources. The licenses are additive.

Context-Aware SKUs

Following licenses are for tracking Wi-Fi clients, interferers, wired devices, and Wi-Fi tags using Received Signal Strength Indication (RSSI).

Order Number	Licenses
Physical Delivery SKUs	
AIR-CAS-1KC-K9	License for tracking 1000 endpoints.
AIR-CAS-3KC-K9	License for tracking 3000 endpoints.
AIR-CAS-6KC-K9	License for tracking 6000 endpoints.
AIR-CAS-12KC-K9	License for tracking 12,000 endpoints.
Electronic Delivery SKUs	
L-CAS-1KC	License for tracking 1000 endpoints.
L-CAS-3KC	License for tracking 3000 endpoints.
L-CAS-6KC	License for tracking 6000 endpoints.
L-CAS-12KC	License for tracking 12,000 endpoints.

Following licenses are for tracking Wi-Fi tags with choke points, using RSSI and time difference of arrival (TDoA).

Order Number	Licenses
Physical Delivery SKUs	
AIR-CAS-KT-K9	License for tracking 1000 Wi-Fi tags.
AIR-CAS-3KT-K9	License for tracking 3000 Wi-Fi tags.
AIR-CAS-6KT-K9	License for tracking 6000 Wi-Fi tags.
AIR-CAS-12KT-K9	License for tracking 12,000 Wi-Fi tags.

Note Electronic Delivery not available for “KT” SKUs Adaptive Wireless IPS Software.

Monitor Mode SKUs

Monitor Mode Cisco Adaptive Wireless Intrusion Prevention system (Adaptive wIPS) monitor mode software licenses are based on the number of full-time monitoring access points deployed in the network. The Cisco Mobility Services Engine 3355 allows for the tracking of up to 3000 monitoring access points, and the MSE 3310 allows for the tracking of up to 2000 monitoring access points. The licenses are additive. MSE virtual appliance can support up to 10000 monitoring access points, depending on server resources.

Order Number	Licenses
Physical Delivery SKUs	
AIR-WIPS-AP-5	Supports 5 monitor mode Cisco access points.
AIR-WIPS-AP-25	Supports 25 monitor mode Cisco access points
AIR-WIPS-AP-100	Supports 100 monitor mode Cisco access points
AIR-WIPS-AP-500	Supports 500 monitor mode Cisco access points
AIR-WIPS-AP-2000	Supports 2000 monitor mode Cisco access points
Electronic Delivery SKUs	
L-MM-WIPS-5	Supports 5 monitor mode Cisco access points.
L-MM-WIPS-25	Supports 25 monitor mode Cisco access points.
L-MM-WIPS-100	Supports 100 monitor mode Cisco access points.
L-MM-WIPS-500	Supports 500 monitor mode Cisco access points.
L-MM-WIPS-2000	Supports 2000 monitor mode Cisco access points.

Enhanced Local mode

Cisco wIPS enhanced local mode software licenses are based on the number of local mode (data serving) access points that are deployed in the network. The Cisco Mobility Services 3355 allows for the tracking of up to 3000 local mode access points and the mobility services engine 3310 allows for the tracking of up to 2000 local mode access points. MSE virtual appliance can track up to 10000 local mode access points, depending on the server resources. The licenses are additive.

Enhanced Local Mode SKUs:

Order Number	Licenses
Physical Delivery SKUs	
AIR-LM-WIPS-5	Supports 5 enhanced local mode access points.
AIR-LM-WIPS-25	Supports 25 enhanced local mode access points.
AIR-LM-WIPS-100	Supports 100 enhanced local mode access points.
AIR-LM-WIPS-500	Supports 500 enhanced local mode access points.
AIR-LM-WIPS-2000	Supports 2000 enhanced local mode access points.
Electronic Delivery SKUs	
L-LM-WIPS-5	Supports five enhanced local mode access points
L-LM-WIPS-25	Supports 25 enhanced local mode access points

Order Number	Licenses
L-LM-WIPS-100	Supports 100 enhanced local mode access points
L-LM-WIPS-500	Supports 500 enhanced local mode access points
L-LM-WIPS-2000	Supports 2000 enhanced local mode access points

Please note that all licenses are additive and MSE-3355 supports up to 18,000 end points or 3,000 WIPS monitor mode or Enhanced local mode AP & the virtual appliance can support 50,000 endpoints or 10,000 monitor mode or enhanced local mode APs.

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 6.0.x to 7.0.x

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

1. Configure tracking limits in 6.0.x.
2. Upgrade to 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 NCS Server

Communication between the mobility services engine, NCS, 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, NCS, and the mobility services engine.

The mobility services engine and its associated controllers must be mapped to the same NTP server and the same NCS 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 NCS Communication Username and Password using MSE setup.sh

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

Scenarios which you might encounter while configuring the NCS username and password are as follows:

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

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.

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 Context Aware Service > Advanced > Location Parameters page on NCS.

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.

Operational Notes for CAS

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

Synchronization Required When Upgrading to Release 7.2.103.0 or Importing CAD Floor Images

When upgrading to Release 7.2.103.0 from Release 6.x (and earlier) you must synchronize after the software upgrade and also when CAD-generated floor images are imported into NCS.

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.

Note The other conditions for history logging are as follows:

- Clients: Association, authentication, re-association, re-authentication, or dissociation.
- Tags: Tag Emergency button.
- Interferers: Interferer severity change, cluster center change, or merge.

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.

NCS Online Help Outlines Incorrect Software Download Procedure

In NCS online help (OLH), the steps in the "Downloading Software to a mobility services engine Using NCS" 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 NCS 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 NCS.

Monitoring Information Varies for Clients and Tags

Note This information is missing if the AeroScout Tag Engine is used.

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

Calibration models and data do not apply only to tags if AeroScout engine is used for tag calculation. It always applies to Wireless clients, Interferers, Rogue APs, and Rogue Clients.

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

Advanced location parameters does not apply to tags if AeroScout engine is used and otherwise it works always. 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 NCS time stamp is based on the browser's location and not on the mobility services engine settings. Changing the time zone on NCS 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 like phones and other Wi-Fi devices with power save mode 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 NCS page when you synchronize a mobility services engine and a controller (CSCsx38955).

NCS Screen and Navigation Changes

- *Services* replaces *Mobility* in the navigation bar of NCS.
- 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 MSE 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.

High Availability

The mobility services engine is a platform for hosting multiple mobility applications. Every active MSE is backed up by another inactive instance. The purpose of the secondary MSE is to monitor the availability and state of the primary MSE. The high availability is supported on all services. You can use either manual or automatic failover. Failover should be considered temporary. The failed MSE should be restored to normal as soon as possible, and failback will be re-initiated. The longer it takes to restore the failed MSE, the longer the other MSEs sharing the secondary MSE must run without failover support. Failover times of <1 minute enhances the redundancy and availability of the mobile services with no incremental license cost.

See the *Cisco Context-Aware Software Configuration Guide, Release 7.2,* for details on setting up the high availability the following URL:
http://www.cisco.com/en/US/docs/wireless/mse/3350/7.2/CAS/configuration/guide/CAS_72.html

Virtual Appliance

MSE is also offered as a virtual appliance. When the MSE is located on the virtual appliance, the license installation is done using a VUDI (Virtual Unique Device Identifier) instead of UDI. The MSE virtual appliance software is distributed as an Open Virtualization Archive (OVA) file. When the MSE is located on the virtual appliance, the license is validated against VUDI instead of UDI. Unlike the MSE physical appliance, the customer must have an activation license for the virtual appliance. Without an activation license, the MSE starts in evaluation mode. Even if the licenses are present on the host, it rejects the permanent license if the activation license is not installed. You can install the MSE virtual appliance using any of the methods for deploying an OVF supported by the VMware environment. The recommended deployments for a virtual appliance are UCS and ESX/ESXi. Additional virtual foot print provides flexible deployment options with the same CAS/wIPS pricing.

The high availability is available for both physical and virtual appliance bit it cannot be cross paired/mixed. A virtual appliance must be backed up by another virtual appliance. A virtual appliance MSE HA configuration is a 1:1 pairing only.

See the *Cisco Context-Aware Software Configuration Guide, Release 7.2,* for more details on virtual appliance at the following URL:
http://www.cisco.com/en/US/docs/wireless/mse/3350/7.2/CAS/configuration/guide/CAS_72.html

MSAP Service

The Cisco Mobility Services Advertisement Protocol (MSAP) provides functionality to deliver advertisements over Wi-Fi infrastructure. MSAP facilitates MSAP capable mobile devices to receive service advertisements. Once the mobile device receives the service advertisements, it can display their icons and data on its user interface, facilitating the process of users discovering what is available in their surroundings. In addition, MSAP can be used by the mobile devices that have been configured with a set of policies for establishing network connectivity. The MSAP provides requirements for clients and servers and describes the message exchanges between them.

GPS Coordinate Support

This feature transforms the geometric location co-ordinates of a device tracked by MSE to geo-location coordinates (latitude and longitude) and provides it to the external entities through northbound and southbound interfaces.

Context-Aware Service Software Feature

This section summarizes the feature for Context-Aware Service software and contains the following topic:

Context-Aware support for Flex Connect

This feature provides rich location information via Cisco 3300 Mobility Services Engine and Context Aware Service software. Enhanced security is used to track thousands of mobile devices with alerts, notifications for rogue devices, and deployment optimization for Wi-Fi clients and tagged assets.

Configuration Wizard

This feature makes adding / configuring MSE a simple one step process. This feature simplifies the MSE configuration.

Support for Multiple IPV6 and IPV4 Address of Wireless Clients

Only wireless clients have IPV6 addresses in this release.You can search for an MSE-located client using the NCS Advanced Search feature. Each client can have up to 16 IPV6 addresses and 4 IPV4 addresses.

Client Northbound Notification

You can use the NCS to define and enable user-configured conditional notifications and northbound notifications. Northbound notifications define which tag notifications the mobility services engine sends to the third-party applications. Client notifications are forwarded. By enabling northbound notifications in the NCS, the following five event notifications are sent: chokepoints, telemetry, emergency, battery, and vendor data.

Adaptive Wireless Intrusion Prevention Software Feature

This section summarizes the feature for Adaptive Wireless Intrusion Prevention software and contains the following topic:

wIPS Alarm Enhancements

There are 9 new security penetration and DoS alarms in this release. This provides additional threat protection thus enhancing the security to the wireless infrastructure. The following are the new alarms available in this release:

- Identical Send and Receive Address - Alarm ID 178
- Bad EAP-TLS frame - Alarm ID 181
- HT-Intolerant degradation of service - Alarm ID 182
- DoS: Probe response - Alarm ID 188
- DoS: Re-association Request Flood - Alarm ID 189
- DoS: Beacon flood - Alarm ID 195
- DoS: MDK3-Destruction attack - Alarm ID 196
- Karma tool detected - Alarm ID 197
- WiFiTap tool detected - Alarm ID 198

Caveats

This section lists Open Caveats and Resolved Caveats in Release 7.2.103.0 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 4 lists the open caveats in Release 7.2.103.0.

Table 4 Open Caveats

ID Number	Caveat Title
CSCtu07020	Headline: Monitor > Google Earth Maps > Import CSV page shows an error. Symptom: Monitor > Google Earth Maps > Import CSV page shows an error. Condition: This happens while re-importing the csv file. The following error message is displayed: Error: Saving Folder details to the database. COMMON-1. Workaround: Remove all the APs and reimport them.
CSCtt01955	Headline: No alarm is seen if the primary MSE is down and the secondary MSE cannot failover. Symptom: Alarm is not generated when primary MSE goes down and the secondary MSE is not able to failover. Conditions: This happens when the automatic failover is configured but the secondary MSE is not able to failover after the primary MSE goes down. Workaround: Look into the health monitor log in the MSE to verify the situation.
CSCtw74040	Headline: MSE HA: The Primary device type is changed to secondary MSE after failover. Symptom: The MSE device type is changed to secondary MSEs device type after failover. Conditions: This occurs when primary and secondary MSE are not using the same type/model. Workaround: None.
CSCtw84684	Headline: Peak client and peak tags are shown at the bottom of the chart. Symptom: The client/tag graph on CAS general page shows peak client and peak tag count as 0. Conditions: This occurs in NCS version 1.1 and MSE version 7.2.103.0. Workaround: None.
CSCtw90736	Headline: After applying the MSE license, the screen changes to dark and the browser becomes grayed out. Symptom: If a certain chain of events occur, there is a Java script error on the License File page and on closing the dialog box, the browser remains grayed out. Conditions: This occurs during the following conditions: • Select Add License and click Ok without adding the license. • Select Add License and click Cancel. • Select Add License and choose the license file and install it. Close the pop-up message which is returned. Workaround: Refresh the browser.

Table 4 Open Caveats (continued)

ID Number	Caveat Title
CSCtx04514	Headline: An exception occurs when upgrading from 7.0.201.0 to 7.2.103.0 and attempting to configure HA. Symptom: Exception occurs when accessing the MSE HA Configuration page on NCS after MSE is upgraded from an older release to 7.2.103.0. Conditions: This happens only if the MSE is added to NCS and then upgrade to release 7.2.103.0 and configure HA. Workaround: Only the first access to HA configuration page cause exception. Re-click on the HA Configuration page again and it works fine without any issue.
CSCtx22371	Headline: Message after MSE image download misplaced on the NCS MSE download page. Symptom: After successfully transferring software images from NCS to MSE using the Services > Mobility Services Engines > MSE > System > Maintenance > Download Software page, a message is displayed saying that the server software image has been transferred successfully. This message appears misplaced and is shown below the left accordion of the page. Conditions: This happens every time a server software image is transferred successfully from NCS to MSE. Workaround: None.
CSCtx01075	Headline: Incorrect target Client/AP IP address data for wIPS alarm 138 is displayed. Symptom: When the wIPS contains IPV6 address, the NCS will not be able to display this properly. Conditions: None. Workaround: None.
CSCtx38086	Headline: Number of configuration files are not bundled on secondary MSE. Symptom: Configuration files which are deleted on primary MSE are not getting deleted on the secondary MSE. Conditions: This is seen for configuration files of partner tag engine. The secondary MSE does not delete obsolete config files but continue to create new files and fill up disk space. Workaround: Manually delete obsolete configuration files to free up the disk space.
CSCtx55854	Headline: MSE HA setup failed after upgrade. Symptom: The HA setup failed after upgrading both the primary and secondary MSE. Condition: • Upgrade both the primary and secondary MSE. • Restart them. • The status page shows that the HA setup is failed. Workaround: Decommission the pair from the NCS and re-pair them.

Table 4 Open Caveats (continued)

ID Number	Caveat Title
CSCtx60100	Headline: Oracle's flash_recovery_area shows full when it still has space. Symptom: Primary MSE failed due to database error and failover to secondary MSE is also not successful. Condition: Failure due to ORA-00257 error. This can be verified in the MSE log files. Workaround: Increase the flash recovery area size and restart the primary MSE.
CSCtx60118	Headline: MSE framework sevicemix/jetty throw an exception and not handling API call. Symptom: MSE is not responding to API calls from the health monitor. Condition: Exception com.ctc.wstx.exc.WstxIOException is thrown from the MSE framework when the API call is made. Workaround: Restart MSE and verify from the mse log if this exception is no longer thrown.
CSCtx60123	Headline: Secondary MSE failback to primary and then remains in SETUP_FAILED state. Symptom: Failback to primary MSE is successful but to secondary MSE remains in SETUP_FAILED state. Condition: Secondary MSE state becomes SETUP_FAILED after a successful failback to primary MSE. The primary MSE will not be protected by the secondary MSE in this state. Workaround: Restart the secondary MSE.

Resolved Caveats

Table 5 lists the caveats resolved in Release 7.2.103.0.

Table 5 Resolved Caveats

ID Number	Caveat Title
CSCtr24225	Changes to harden the password requirements for MSE.
CSCtt06686	There is tracking and log parameters issue while upgrading from 6.0.202.0 to 7.0.220.0 release.

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 7.2*

  http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html
- *Cisco Adaptive Wireless Intrusion Prevention System Configuration Guide, Release 7.2*

  http://www.cisco.com/en/US/products/ps9817/products_installation_and_configuration_guides_list.html
- The NCS Online Help available with the NCS 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.
