Release Notes for Cisco 3300 Series Mobility Services Engine, Release 7.2.110.0

First Published: May, 2012
OL-24938-04

These release notes describe the requirements, features, limitations, restrictions (caveats), and related information for release 7.2.110.0 of the Cisco 3300, 3350, and 3355 mobility services engines and its 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 6 for details on compatibility with the Cisco wireless LAN controllers (WLC) and the Cisco Prime Network Control System (NCS).

Note You will require Context-Aware and Adaptive wIPS licenses to run the 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 7.2.110.0:

- 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.
- 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 displays their icons and data on its user interface, facilitating the process of 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 on each mobility services engine 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 *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 *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 *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 the Cisco mobility services engine, Cisco Wireless Control System, Cisco Prime Network Control System, and Cisco Wireless LAN controller.

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
May 2012	7.2.110.0	—	1.1.1.24	—	7.2.110.0	7.2.110.0	7.2.110.0	7.2.110.0	4.4.2.4
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
	7.1.91.0	7.0.220.0	—	—	7.0.220.0	7.0.220.0	7.0.220.0	—	
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	—	—	7.0.201.204	7.0.201.204	7.0.201.204	—	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) o 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) o 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	—	—	—	—	—

Table 1 Cisco MSE Compatibility Matrix (continued)

Release Date	WLC	WCS	NCS	2710 Location Appliance	MSE 3350	MSE 3310	MSE 3355	MSE Virtual Applianc e	Aeroscout CLE
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 Service Software, Wireless Intrusion Prevention System[1], and Cisco Mobility Services Advertisement Protocol[2]	Mobility services engine	7.2.110.0 7.2.103.0 7.0.230.0 7.0.220.0 7.0.201.204 7.0.112.0 7.0.105.0 6.0.103.0 6.0.105.0 (LBS)
	Controllers	7.2.110.0 7.2.103.0 7.1.91.0 7.0.235.0 7.0.230.0 7.0.220.0 7.0.116.0 7.0.120.0 7.0.98.0 6.0.202.0 6.0.199.4 6.0.1960. 6.0.188.0 6.0.182.0 6.0.108.0 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	1.1.1.24 1.1.0.58

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 the 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 the following topics:

Upgrade Scenarios

Starting from Release 7.0.201.204, you will not be able to restore databases from Releases 5.0, 6.0, 7.0.105.0, and 7.0.112.0 to 7.2.110.0 using the NCS. Oracle has been introduced as the database vendor for MSE. The solid database will be discontinued starting with Release 7.0.201.204.

There are four scenarios available to upgrade MSE to 7.2.110.0 from 6.0, 7.0.105.0, and 7.0.112.0:

Upgrading the MSE to 7.2.110.0 from Older Releases Without Data Migration

To upgrade from older releases to 7.2.110.0 without data migration, follow these steps:

Step 1 Back up the existing database using the NCS. (We recommended this).

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

Step 2 Transfer the *.tar file for 7.2.110.0 to the MSE appliance:

```
CISCO-MSE-L-K9-7-2-110-0-64bit.db.tar
```

Step 3 Place the file in the /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-K9-7-2-110-0-64.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-K9-7-2-101-0-64bit.bin.gz

Step 5 To decompress (unzip) the file, execute: gunzip CISCO-MSE-L-K9-7-2-110-0-0-64bit.bin.gz.

Step 6 Enter the following command: **`chmod +x CISCO-MSE-L-K9-7-2-110-0-64bit.bin`**

Step 7 Stop the MSE service using the following command: **`service msed stop`**

Step 8 Uninstall the existing MSE software. Choose **deletion of database** when prompted.

Step 9 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, stop, or add an MSE to the NCS.

Upgrading the MSE to 7.2.110.0 from Older Releases with Data Migration

To upgrade the MSE from to 7.2.110.0 with data migration, follow these steps:

Step 1 Back up the existing database using the NCS. (We recommended this).

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

Step 2 Transfer the *.tar file for 7.0.201.204 to the MSE appliance:

`CISCO-MSE-L-K9-7-2-110-0-64bit.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 those 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 that you want to preserve across the upgrade to 7.2.110.0, do not uninstall it.

Step 4 Untar the file: tar -xvf CISCO-MSE-K9-7-2-110-0-64.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-K9-7-2-101-0-64bit.bin.gz

Step 5 To decompress (unzip) the file, execute: gunzip CISCO-MSE-L-K9-7-2-110-0-64bit.bin.gz

Step 6 Enter the following command: **`chmod +x CISCO-MSE-L-K9-7-2-110-0-64bit.bin`**

Step 7 Stop the MSE service using the following command: **`service msed stop`**

Step 8 Invoke the installer ./CISCO-MSE-L-K9-7-2-110-0-64bit.bin and answer the questions when prompted.

The installer automatically detects if there is an old database present and asks the 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 7.2.110.0 from 7.0.201.204 or Later Releases

To upgrade the MSE to 7.2.110.0 from 7.0.201.204 or later releases, follow these steps:

Note Complete database installation is not required for upgrading from 7.0.201.204. or later releases.

Step 1 Download CISCO-MSE-L-K9-7-2-110-0-62bit.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-K9-7-2-110-0-64.bit.bin
```

Step 3 Answer the questions when prompted.

The installer automatically detects if there is an old database present and asks the relevant questions.

Restoring an Old Database to Release 7.2.110.0

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

Note The regular Restore option on the NCS cannot be used to restore an older database of older releases such as 6.0, 7.0.105.0, or 7.0.112.0 onto 7.2.110.0.

Step 1 Stop the running MSE 7.2.110.0.

Step 2 Uninstall the software. 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
5.2.0	5.2, 6.0, 7.0
6.0	6.0, 7.0

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

Step 5 To migrate data to 7.x.x.x, follow the steps in the "Upgrading the MSE to 7.2.110.0 from Older Releases with Data Migration" section on page 8.

Compressed Software Image

If you download the mobility services engine image *.gz file using the 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 **chmod +x filename.bin** command.

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 the NCS After Polling

After a software update, the new mobility services engine software version does not immediately appear in mobility services engine queries on the 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 the 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 18,000 endpoints (combined count) and Cisco 3310 mobility services engine allows for tracking of up to 2000 endpoints (combined count). The MSE virtual appliance can track up to 50,000 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.

The 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 is not available for “KT” SKUs CAS Wi-fi TDOA SKUs.

Monitor Mode SKUs

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 3355 mobility services engine allows for the tracking of up to 3000 monitoring access points, and the Cisco 3310 mobility services engine allows for the tracking of up to 2000 monitoring access points. The licenses are additive. The 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.

Order Number	Licenses
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 3355 mobility services engine allows for the tracking of up to 3000 local mode access points and the Cisco 3310 mobility services engine allows for the tracking of up to 2000 local mode access points. The MSE virtual appliance can track up to 10,000 local mode access points, depending on the server resources. The licenses are additive.

The enhanced local mode SKUs are as follows:

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.
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.

Note that all licenses are additive and the Cisco 3355 mobility services engine supports up to 18,000 end points, 3,000 WIPS monitor mode, or Enhanced local mode AP, and 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 supports up to 10 access points.
- The applied monitor mode license can be used by the wIPS Service for local mode as well as monitor mode APs. However, since the SKU is monitor mode, it shows up as a permanent license in the monitor mode category. You can also get an additional 10 local mode AP evaluation licenses for the initial 60 days. The wIPS uses local mode licenses when available (10 evaluation licenses are available for 60 days) and then switches to counting the same against the monitor mode license.

Important Notes

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

Note MSE needs to be rebooted (either hard reboot or using the command **`shutdown -r now`**) after it has been upgraded to 7.2.110.0 release.

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

This section contains 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 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, the 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 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 the Console. SSH is no longer 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 the MSE.

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

Configuring the 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 username 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).

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:

- 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 7.2.110.0 or Importing CAD Floor Images

When upgrading to Release 7.2.110.0 from Release 6.x (and earlier), you must synchronize after the software upgrade and also when CAD-generated floor images are imported into the 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 disassociation.
- 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.

AeroScout MobileView Release 4.1 Required for Northbound Notifications

If AeroScout MobileView Release 4.1 and earlier 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 AeroScout MobileView 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.

Non-Cisco Compatible Extensions Tags Not Supported

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

Calibration Models and Data

If AeroScout engine is used for calculation, then calibration models that are done through NCS do not apply to tags. If Cisco tag engine is used, everything done on the NCS calibration models and data uses tag calculation.

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

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.

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 Location

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

PDAs and Smartphone with Limited Probe Requests Might Affect Location

Many PDAs like smartphones 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.

Operational Notes for wIPS

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

NCS Screen and Navigation Changes

- *Services* replaces *Mobility* in the NCS navigation bar.
- 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 following new features are available in the MSE release 7.2.110.0.

- MSE Scale: 25 MSE per NCS, page 20
- Tag Multicast Address Configuration, page 20

Tag Multicast Address Configuration

This feature allows you to configure a custom multicast address for CCX tags only. Only two addresses are allowed. After configuring a custom address, the tags can use either the default multicast address specified in the CCX format or the custom configured address (using the CLI) for them to get detected properly on the controller.

MSE Scale: 25 MSE per NCS

Support for MSE scaling is added in this release.

Enhancements

Table 4 lists the enhancements done in Release 7.2.110.0.

Table 4 Enhancements

ID Number	Enhancement Description
CSCts83803	MSE is upgraded to use the latest version of SSL libraries in JAVA. Hence the JAVA is upgraded to jdk1.6.0.31 to use those libraries.
CSCty11741	Several packages in the MSE is upgraded to improve the security related issues.

Caveats

This section lists Open Caveats and If You Need More Information in Release 7.2.110.0 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 5 lists the open caveats in Release 7.2.110.0

Table 5 Open Caveats

ID Number	Caveat Title
CSCtx06605	Headline: MSE 3355 - RAID system fails to recognize disks and does not reboot. Symptom: While booting up, an error message appears on the attached monitor or on serial console saying “all the disks from your previous configurations are moved out”. If this is an unexpected message, please power off your system and check your system and cables to ensure that all disks are present. When the Space key is pressed, the system will not boot from the disk. During boot up, the LSI WebBios loads fine and shows two physical disks but no virtual disks. Condition: This happens when the box has gone through an accidental power interruption (that is, the power plug was pulled while the system was operational). The flash configuration was corrupted/erased due to the power interruption. The RAID card does keep a backup of the configuration on the hard drives too. However, when the card loses the configuration information that is in the flash, it does not automatically pickup the backup configuration information from the hard drives. The information on the hard drives is considered a “foreign configuration” that required user intervention. At this time, the system will wait for the user to take action. Remember that all the data on the hard drives are still intact. Workaround: login to the RAID management tool-WebBIOS. There are two versions of RAID management tool. One that uses extensive menus and requires an attached monitor and another is completely based on the command lines (CLI). The CLI version can be accessed from the serial console. You will see a prompt for this on a serial console right after the error message. Reboot the server and everything becomes normal
CSCtz08103	Headline: After upgrading to MSE 7.2.104.4, the MSE cannot connect to NCS. Symptom: MSE does not come up after the upgrade or shows as unreachable in NCS. Condition: It occurs while installing MSE from the previous version. Workaround: MSE needs to be rebooted. You can use the **`shutdown -r now`** command to reboot. Once the MSE comes up, IPtables load properly and you will not see this issue.

Table 5 Open Caveats (continued)

ID Number	Caveat Title
CSCua20404	Headline: NMSP connections are inactive after rebooting controllers or MSE Symptom: Sometimes NMSP connections are inactive after upgrading/installing new MSE version. Condition: Keyhash on the MSE changes after MSE software is installed. Keyhash on the MSE is used to establish NMSP connections with the WLC. NCS pushes the MSE keyhash to the WLCs via AP / MSE Authorization template If one or more WLCs are unreachable, NCS is unable to push new keyhash to any of the WLCs. Workaround 1: Make sure that all WLCs are reachable and added to NCS with SNMP read-write privileges. Run **Administration > Background Tasks > Mobility Service Status**. Workaround 2: Do the following if all WLCs cannot be made reachable: • SSH to MSE, type cmdshell, run **`show server-auth-info`** command and obtain the MSE keyhash information. • Go to **Configure > Controller Template Launch Pad > Security > AP / MSE Authorization > Controller Template 'MSE MAC Address'** • Enter the correct keyhash from step 1. Save and apply to controllers (do not select unreachable controllers).
CSCty66579	Headline: The Java.lang.ArrayIndexOutOfBoundException is displayed while configuring High Availability on the MSE. Symptom: MSE does not start with the ArrayIndexOutOfBoundsException error shown in the health monitor log. Condition: When the restart preference config file is corrupted. Workaround: Delete the `file/var/mse/futurestartdate` and restart the `MSE/etc/init.d/msed restart` or run `setup.sh` from `/opt/mse/setup/setup.sh` and change the future restart day and time preference.

Resolved Caveats

Table 6 lists the Resolved caveats in Release 7.2.110.0.

Table 6 Resolved Caveats

ID Number	Caveat Title
CSCtx77952	Apply Oracle critical update to MSE
CSCty11741	Bug to track the various security related vulnerabilities for MSE
CSCty54758	Check in the new Aeroscout CLE
CSCtt15167	wIPS has less than 10 MB of memory left
CSCtx60100	Oracle has flash_recovery_area full when it still has space
CSCty44616	Evaluation extension issues

Table 6 Resolved Caveats (continued)

ID Number	Caveat Title
CSCtx77893	Upgrade MSE Linux kernel to eliminate threats
CSCtx55854	MSE HA setup failed after upgrade
CSCty81160	MSE HA: Secondary went down with too many open files error
CSCtz44158	MSE HA setup is failing after MSE restore operation
CSCtz68671	Unsupported ClassVersionError while upgrading MSE from 7.0.201.0 to 7.2.110.0

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.
