Release Notes for Cisco Mobility Services Engine, Release 7.5.102.101

First Published: September, 2013
OL-29334-01

These release notes describe the requirements, features, limitations, restrictions (caveats), and related information for release 7.5.102.101 of the Cisco mobility services engine and its services.

- Connected Mobile Experiences
- Wireless Intrusion Protection System (wIPS)
- Mobile Concierge Service
- CMX Analytics Service
- CMX Browser Engage
- CMX HTTP Proxy Service

Note Before installing this software, see the "Upgrading the MSE" section on page 8 for details on compatibility with the Cisco wireless LAN controllers (WLC) and the Cisco Prime Infrastructure.

Note You need licenses to run all the services. For ordering information, see the "Licensing Information for MSE" section on page 14.

Note Cisco 3310 and Cisco 3350 mobility services engines are not supported from Release 7.4 onwards.

Contents

These release notes contain the following sections:

Cisco Systems, Inc.
www.cisco.com

Introduction

This section introduces the Cisco mobility services engine (MSE) and the various services that it supports.

Cisco Mobility Services Engine and Services

The Cisco mobility services engine supports various services within the overall Cisco Unified Wireless Network (CUWN).

The Cisco mobility services engine currently supports the following services in Release 7.5.102.101:

- Connected Mobile Experiences—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.
- Wireless Intrusion Protection Service—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.
- Mobile Concierge—The Mobile Concierge service allows the venue owners and service providers to monitor their WLAN. The Mobile Concierge service delivers a unique, in-store experience to customers who are using smartphones.

  The Mobile Concierge service uses wireless smartphones that have been configured with a set of policies for establishing network connectivity. The Mobile Concierge service facilitates smartphones to discover the available network-based services. Once you are connected to a store's Wi-Fi network, you can join that store's wireless guest network and access a variety of different services including electronic coupons, promotional offers, customer loyalty data, product suggestions, the ability to organize shopping lists, and receive unique digital signatures based on your shopping preferences.
- CMX Analytics Service—The CMX Analytics service analyzes wireless device location information in a particular network. The CMX Analytics service uses the data provided by the Cisco Mobility Services Engine (MSE) to calculate the location of Wi-Fi devices in the Wireless Local Area Network (WLAN). When a wireless device is enabled in a network, it transmits probe request packets to identify the wireless network in its neighborhood. Even after connecting to the access point in the WLAN, the client devices continue to transmit probe request packets to identify other access points for better quality of service. The access points gather these request and the associated RSSI from the various wireless devices and forwards them to the Wireless LAN Controller (WLC). The controller then forwards this information to the MSE.

The basic data that is collected from various APs, when analyzed, produces information and knowledge about the movement and behavior patterns of people who are using Wi-Fi devices in the building. For example, the building can be an airport, shopping mall, city center, and so on. The CMX Analytics service helps the airport authorities or the building owners to understand the movement of passengers or customer within their building. This helps them improve the signage, make changes to the under utilized areas, and so on.

- CMX Browser Engage Service—The CMX Browser Engage is a new way to transform the in-venue experience through browser engagement. This enables organizations to communicate with opt-in mobile users - shoppers, guests, and visitors - through their mobile browser. The CMX Dashboard is the back-end tool designed for administrative users to manage the CMX Browser engage experience. It allows the admin users to configure venue-specific menus, banners, and icons as well as content-aware search.
- HTTP Proxy Service—Currently, CMX Dashboard relies on HTTP traffic flows to provide value added services and messages to the customers at the venue. The router intercepts the HTTP traffic and CMX Dashboard inserts a script at the end of the HTTP traffic. The HTTP Proxy is enabled on the MSE. The HTTP Proxy on the MSE terminates all HTTP traffic intercepted using Policy Based Routing (PBR) and acts as a forward proxy by pulling contents on behalf of wireless clients.

Note From Release 7.5 onwards, Cisco engine is used to track clients and tags. If Aeroscout engine is detected when you are upgrading from Release 7.2 and later Releases to Release 7.5, then a warning message is displayed about removing the AeroScout license and engine. If you accept, then it removes all the partner engine sub services and Cisco Engine will be used to track tags. If you do not accept the removal of partner engine, then the installation will exit.

Note For ordering information, see the "Licensing Information for MSE" section on page 14.

Note Starting from Release 7.4, the evaluation licenses for 100 clients, 100 tags, and 10 wIPS monitor mode access points come standard on each mobility services engine installed for 120 days, which earlier from Release 6.0 till Release 7.3 was installed for 60 days.

Note From Release 7.4 onwards, licensing is going to be AP based and supports 100 AP evaluation license for Connected Mobile Experiences which is limited to 100 elements (clients, tags, interferers, etc combined).

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.

Note Upgrade from MSE Release 7.5.102.0 to Release 7.5.102.101 is supported.

Table 1 Cisco MSE Compatibility Matrix

MSE 3355	MSE 3350	MSE Virtual Appliance	AeroScout CLE	WCS	WLC	Prime Infrastructure / NCS
7.5.102.101	—	7.5.102.101	—	—	7.5.102.0	1.4.0.45
					7.4.110.0	
					7.4.100.60	
					7.4.100.0	
					7.3.112.0	
					7.3.101.0	
					7.2.111.3	
					7.2.110.0	
					7.2.103.0	
					7.0.240.0	
					7.0.235.3	
					7.0.235.0	
					7.0.230.0	
					7.1.91.0	
					7.0.220.0	
					7.0.116.0	
					7.0.98.218	
					7.0.98.0	

Table 1 Cisco MSE Compatibility Matrix (continued)

MSE 3355	MSE 3350	MSE Virtual Appliance	AeroScout CLE	WCS	WLC	Prime Infrastructure / NCS
7.4.110.0	—	7.4.110.0	4.5.2.16 4.4.2.11	—	7.4.110.0 7.4.100.60 7.4.100.0 7.3.112.0 7.3.101.0 7.2.111.3 7.2.110.0 7.2.103.0 7.0.240.0 7.0.235.3 7.0.235.0 7.0.230.0 7.1.91.0 7.0.220.0 7.0.116.0 7.0.98.218 7.0.98.0	2.0 1.4.0.45 1.3.0.20
7.4.100.0	—	7.4.100.0	4.5.2.16 4.4.2.11 4.4.2.7	—	7.4.100.60 7.4.100.0 7.3.112.0 7.3.101.0 7.2.111.3 7.2.110.0 7.2.103.0 7.0.240.0 7.0.235.3 7.0.235.0 7.0.230.0 7.1.91.0 7.0.220.0 7.0.116.0 7.0.98.218 7.0.98.0	1.4.0.45 1.3.0.20

Table 1 Cisco MSE Compatibility Matrix (continued)

MSE 3355	MSE 3350	MSE Virtual Appliance	AeroScout CLE	WCS	WLC	Prime Infrastructure / NCS
7.3.101.0	7.3.101.0	7.3.101.0	4.4.2.4	—	7.3.112.0 7.3.101.0 7.2.111.3 7.2.110.0 7.2.103.0 7.0.240.0 7.0.235.3 7.0.235.0 7.0.230.0 7.1.91.0 7.0.220.0 7.0.116.0 7.0.98.218 7.0.98.0	1.3.0.20 1.2.1.12 1.2.0.103
7.2.110.0	7.2.110.0	7.2.110.0	4.4.2.4	—	7.2.111.3 7.2.110.0 7.2.103.0 7.0.240.0 7.0.235.3 7.0.235.0 7.0.230.0 7.1.91.0 7.0.220.0 7.0.116.0 7.0.98.218 7.0.98.0	1.3.0.20 1.2.1.12 1.2.0.103 1.1.1.24 1.1.0.58
7.2.103.0	7.2.103.0	7.2.103.0	4.4.1.4	—	7.2.103.0 7.0.240.0 7.0.235.3 7.0.235.0 7.0.230.0 7.1.91.0 7.0.220.0 7.0.116.0 7.0.98.218 7.0.98.0	1.3.0.20 1.2.1.12 1.2.0.103 1.1.124 1.1.0.58

Table 1 Cisco MSE Compatibility Matrix (continued)

MSE 3355	MSE 3350	MSE Virtual Appliance	AeroScout CLE	WCS	WLC	Prime Infrastructure / NCS
7.0.240.0	7.0.240.0	—	4.3.1.10	7.0.240.0	7.0.240.0 7.0.235.3 7.0.235.0 7.0.230.0 7.1.91.0 7.0.220.0 7.0.116.0 7.0.98.218 7.0.98.07	1.3.0.20 1.2.1.12 1.2.0.103 1.1.1.24 1.1.0.58 1.0.2.29
7.0.230.0	7.0.230.0	—	4.3.1.19	7.0.230.0	7.0.235.0 7.0.230.0 7.1.91.0 7.0.220.0 7.0.116.0 7.0.98.218 7.0.98.07	1.3.0.20 1.2.1.12 1.2.0.103 1.1.1.24 1.1.0.58 1.0.2.29
7.0.220.0	7.0.220.0	—	4.3.1.19	7.0.220.0	7.1.91.0 7.0.220.0 7.0.116.0 7.0.98.218 7.0.98.0	1.3.0.20 1.2.1.12 1.2.0.103 1.1.1.24 1.1.0.58 1.0.2.29 1.0.1.4
7.0.201.204	7.0.201.204	—	4.2.4.4	7.0.172.0	7.0.116.0 7.0.98.218 7.0.98.0	1.3.0.20 1.2.1.12 1.2.0.103 1.1.1.24 1.1.0.58 1.0.2.29 1.0.1.4 1.0.0.96

Table 1 Cisco MSE Compatibility Matrix (continued)

MSE 3355	MSE 3350	MSE Virtual Appliance	AeroScout CLE	WCS	WLC	Prime Infrastructure / NCS
7.0.112.0	7.0.112.0	—	4.2.4.4	7.0.164.3	7.0.98.218	1.3.0.20
				7.0.164.0	7.0.98.0	1.2.1.12
						1.2.0.103
						1.1.1.24
						1.1.0.58
						1.0.2.29
						1.0.1.4
						1.0.0.96
7.0.105.0	7.0.105.0	—	4.2.4.4	7.0.164.3	7.0.98.218	1.3.0.20
						1.2.1.12
						1.2.0.103
						1.1.1.24
						1.1.0.58
						1.0.2.29
						1.0.1.4
						1.0.0.96

Upgrading the MSE

For instructions on automatically downloading the software using the Prime Infrastructure 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 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

There are four scenarios available to upgrade MSE to 7.5.102.101 from 6.0, 7.0.105.0, and 7.0.112.0:

Upgrading the MSE to 7.5.102.101 from Older Releases Without Data Migration

To upgrade from older releases to 7.5.102.101 without data migration, follow these steps:

Step 1 Back up the existing database using the Prime Infrastructure. (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 7.5.102.101 to the MSE appliance:

```
CISCO-MSE-L-K9-7-5-102-101-64bit.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-K9-7-5-102-101-64.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-K9-7-5-102-101-64bit.bin.gz

Step 5 To decompress (unzip) the file, execute: gunzip CISCO-MSE-L-K9-7-5-102-101-0-64bit.bin.gz.

Step 6 Enter the following command:

```
chmod +x CISCO-MSE-L-K9-7-5-102-101-64bit.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 Prime Infrastructure.

Note The MSE appliance needs to be rebooted using the "reboot" command before starting the MSE services. The MSE reboot command is located in the directory /opt/mse/framework/bin/.

Upgrading the MSE to 7.5.102.101 from Older Releases with Data Migration

To upgrade the MSE to 7.5.102.101 from older releases with data migration, follow these steps:

Step 1 Back up the existing database using the Prime Infrastructure. (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 7.5.102.101 to the MSE appliance:

`CISCO-MSE-L-K9-7-5-102-101-64bit.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 Prime Infrastructure 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 7.5.102.101, do not uninstall it.

Step 4 Untar the file: tar -xvf CISCO-MSE-K9-7-5-102-101-64.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-K9-7-5-102-101-64bit.bin.gz

Step 5 To decompress (unzip) the file, execute: gunzip CISCO-MSE-L-K9-7-5-102-101-64bit.bin.gz

Step 6 Enter the following command: **`chmod +x CISCO-MSE-L-K9-7-5-102-101-64bit.bin`**

Step 7 Stop the MSE service using the following command:

`service msed stop`

Step 8 Invoke the installer ./CISCO-MSE-L-K9-7-5-102-101-64bit.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 7.5.102.101 from Older Releases

To upgrade the MSE to 7.5.102.101 from older releases, follow these steps:

Note Complete database installation is not required for upgrading from 7.2.110.0.

Step 1 Download CISCO-MSE-L-K9-7-5-102-101-64bit.bin.gz to the MSE using the standard Prime Infrastructure download software page.

Step 2 Transfer the software to the /opt/installers directory on the MSE server via FTP or another transport method.

Step 3 Unzip the file: gunzip CISCO-MSE-L-K9-7-5-102-101-64bit.bin.gz

Step 4 Enter the following command:

`chmod +x CISCO-MSE-L-K9-7-5-102-101-64bit.bin`

Step 5 Execute the file with ./CISCO-MSE-L-K9-7-5-102-101-64bit.bin

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

Restoring from an Old Database to 7.5.102.101

To restore from an old database, follow these steps:

Note The regular Restore option on the Prime Infrastructure cannot be used to restore an older database of older releases such as 6.0, 7.0.105.0, or 7.0.110.0 onto 7.5.102.101.

Step 1 Stop the running MSE 7.5.102.101.

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 2 to install a relevant version of MSE.

Table 2 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 Prime Infrastructure.

Step 5 To migrate data to 7.5.102.101, follow the steps in the "Upgrading the MSE to 7.5.102.101 from Older Releases with Data Migration" section on page 10.

Compressed Software Image

If you download the mobility services engine image *.gz file using the Prime Infrastructure, 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 Connected Mobile Experience Configuration Guide, Release 7.5,* and *Cisco Wireless Intrusion Prevention System, Release 7.5*, respectively.

Updated Software Version Shown in the Prime Infrastructure After Polling

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

Connected Mobile Experiences, wIPS, and CMX License Requirements

Client and wIPS licenses are installed from the Prime Infrastructure UI (Administration > License Center). See, Chapter 2: "Adding and Deleting Mobility Services Engines and Licenses" in the *Cisco Connected Mobile Experiences Configuration Guide, Release 7.5, Cisco Wireless Intrusion Prevention System, Release 7.5*, and *Cisco Location Analytics Configuration Guide, Release 7.5* respectively.

For complete details on ordering and downloading licenses, see the *Cisco Mobility Services Engine Licensing and Ordering Guide* at the following URL:
http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html

Licensing Information for MSE

The Cisco MSE is a platform that enables the wireless network to deliver mobility services in a centralized and scalable way. The MSE delivers the following mobility services:

Note From Release 7.4 onwards, licensing is going to be AP based and not end point based. To accommodate this, new L-LS-licenses are introduced in this release.

- Base Location license: Provides advanced spectrum capability and the ability to detect presence and track rogue device, interferers, Wi-Fi clients and RFID tags. Cisco Base Location also enables third-party solutions that use the MSE API.
- Connected Mobile Experiences (CMX) license: Provides CMX Analytics, CMX Engage, and CMX Connect, as well as all the capabilities of the Base Location license. You can upgrade from the Base Location License to the CMX License using the upgrade SKU.
- Wireless intrusion prevention system (WIPS): Protects the network from wireless threats, rogue wireless devices, and denial-of-service (DoS) attacks to improve security and meet compliance objectives and has two options:
  - Monitor Mode licenses are based on the number of full-time monitoring access points deployed in the network.
  - Enhanced Local Mode licenses are based on the number of local mode (data serving) access points deployed in the network.

Licensing is based on the number of access points in the environment. The licenses are additive.

Note Connected Mobile Experiences licenses will be End of Life with standard 6 months of End of Sales and until then both Connected Mobile Experiences and LS licenses will co-exist.

- Cisco MSE 3355 supports up to 2,500 access points for Base Location/CMX or 5000 access points for wIPS.

- Cisco MSE virtual appliance supports up to 5,000 access points, depending on the server resources for Base Location/CMX or 10,000 access points for wIPS. All licenses are additive. The new scaling numbers for Base Location and CMX licenses are as follows:
  - For Low End VA—200APS
  - For 3355 MSE and Standard VA—2500APS
  - For High End VA—5000APS
- There is no change to endpoint support and MSE 3355 supports 25,000 endpoints and high end virtual appliance supports 50000.

SKUs for Cisco MSE Location Services

Table 3 lists the Cisco MSE Location Services software licenses.

Note You must select L-MSE-PAK to order these licenses.

Table 3 Cisco MSE License SKUs

Base Location Services License SKU	CMX License SKU	Upgrade from Base Location license to CMX license	wIPS Monitor Mode SKUs	wIPS Enhanced Local Mode SKUs	Description
L-LS-1AP	L-AD-LS-1AP	L-UPG-LS-1AP	L-WIPS-MM-1AP	L-WIPS-ELM-1AP	Supports 1 access point
L-LS-100AP	L-AD-LS-100AP	N/A	L-WIPS-MM-100AP	L-WIPS-ELM-100AP	Supports 100 access points
L-LS-1000AP	L-AD-LS-1000AP	N/A	L-WIPS-MM-1000AP	L-WIPS-ELM-1000AP	Supports 1000 access points

Cisco Mobility Services Licenses for High Availability

No separate license is required for high availability. To enable high availability, you need to deploy a primary Cisco MSE appliance with Cisco Connected Mobile Experiences and wIPS licenses, and a secondary Cisco MSE appliance without any Cisco Connected Mobile Experiences or wIPS license.

Table 4 lists the ordering support for physical and virtual appliance.

Table 4 Ordering Support for Physical and Virtual Appliaace

MSE Model	SKU	Service SKU	Description
MSE 3355 (Physical Appliance)	AIR-MSE-3355-K9	CON-SNT-MSE3355	Hardware and licenses support
MSE Virtual Appliance	L-MSE-7.0-K9	CON-SAU-LMSE7K	Software and licenses support

Important Notes

This section describes the operational notes and navigation changes for Connected Mobile Experiences, 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, Connected Mobile Experiences, 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:

How and When to Use the db.tar installer

Note You can use the db.tar installer file when you want to install the MSE newly along with the fresh DB installation. The recommended method is to follow the usual Upgrade process unless you want a fresh installation.

- Stop the MSE software (`/etc/init.d/msed stop`).
- You must delete the following directories if you want to reinstall again:
  - `/opt/mse`
  - `/opt/data`
  - `/opt/oracle`
  - `/opt/ORCLfmap`
  - `/opt/installers/*`
- Scp the db.tar file to `/opt/installers` directory and untar it at that location.

- Run the MSE installer.

Reboot MSE After Fresh Installation or Upgrade

After a new installation or upgrade of the MSE software, you must reboot the MSE using the "reboot" command.

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 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.

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

Communication between the mobility services engine, the Prime Infrastructure, 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, Prime Infrastructure, and the mobility services engine.

The mobility services engine and its associated controllers must be mapped to the same NTP server and the same Prime Infrastructure 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 Mobility Services Engine Getting Started Guide 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.

Configuring the Prime Infrastructure Communication Username and Password Using MSE setup.sh

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

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

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

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 the Prime Infrastructure.

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.

AeroScout Engine Module Changes

Starting Release 7.5, the AeroScout engine module is removed from both the Connected Mobile Experiences setup and location code. During installation, if you are upgrading from Release 7.2 and later to Release 7.5, then you will be prompted to remove the AeroScout engine. If you agree to remove, the it removes the AeroScout engine and by default, the Cisco Tag Engine is started as part of Connected Mobile Experiences. If you do not agree to remove the AeroScout engine, then installation will exit.

Operational Notes for Connected Mobile Experiences

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

Synchronization Required When Upgrading to Release 7.5.102.101 or Importing CAD Floor Images

When upgrading to Release 7.5.102.101 from Release 6.x (and earlier), you must synchronize after the software upgrade and also when CAD-generated floor images are imported into the Prime Infrastructure.

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.

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 the Prime Infrastructure 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 Prime Infrastructure.

Monitoring Information Varies for Clients and Tags

In the Monitor > Clients page (when Location Debug is enabled), you can view information on the last heard access point and its corresponding Received Signal Strength Indicator (RSSI) reading.

Calibration Models and Data

Calibration models always applies to Wireless clients, Interferers, Rogue APs, and Rogue Clients.

See Chapter 7, "Context-Aware Planning and Verification" in the *Cisco Connected Mobile Experiences Configuration Guide, Release 7.5* for more details on client calibration.

Advanced Location Parameters

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 Connected Mobile Experiences Configuration Guide, Release 7.5*.

See Services > Mobility Services > Device Name > Context Aware Service > Advanced > Location Parameters.

Location History Time stamps Match Browser Location

The Prime Infrastructure time stamp is based on the browser location and not on the mobility services engine settings. Changing the time zone on the Prime Infrastructure 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.

Prime Infrastructure Screen and Navigation Changes

- *Services* replaces *Mobility* in the Prime Infrastructure 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).

Operational Notes for CMX Analytics Service

This section lists the operational notes for CMX Analytics service and contains the following topics:

WebGL Compatibility

The CMX Analytics in Release 7.5 provides ability to view the analytic results in both 2D (Open Street Maps) and 3D (WebGL) environments. This provides improved understanding of results on multiple floor paths or when dwell times are calculated throughout a multi-storey building. The 3D environment presents the same information as the 2D environment.

WebGL is an advanced feature that provides graphic capabilities. All borowsers do not support WebGL on a particular hardware. Verify your browser compatibility in the Get WebGL website. If your browser supports WebGL, then you must see a spinning cube.

If your browser does not support WebGL, you must do the following:

- Update your latest drivers for video card.
- For Google Chrome, follow the instructions given for WebGL and 3D Graphics in the Google Chrome support website.
- For Firefox, follow these steps to enable WebGL:
  - Download the latest build of Firefox browser and launch Firefox on your computer.
  - In the browser address line, enter **about:config**
  - In the Search text box, enter webgl to filter the settings
  - Double click **webgl.enabled_for_all_sites**
  - Set the **webgl.enabled_for_all_sites=true**
- For Safari, follow these steps to enable WebGL:
  - Choose **Safari** > **Preferences**.
  - Click the **Advanced** tab.
  - Select the **Show Develop menu in menu bar** check box.
  - Choose **Enable WebGL** from the Develop menu.

Note If your system does not support 3D, then the analytic results are displayed only in 2D Open Street Maps view.

- Internet Explorer 10 does not have the built-in support for WebGL and Microsoft has not announced any plans for implementing it in the future. WebGL support can be manually added to Internet Explorer using third-party plugins. For more information, see the WebGL for Internet Explorer website.

Jboss Issue

Sometimes CMX Analytics service does not start up because of a stray Jboss process that runs as a root user. If Analytics engine does not start and if you notice a stray Jboss process with root permissions running, then you must to do the following:

- Stop CMX Analytics service from the Prime Infrastructure.
- Kill the Jboss process. command
- Run the `chown -R nobody:nobody /opt/mse/analytics` command.
- Start CMX Analytics service from the Prime Infrastructure.

New Feature Support

This section provides a brief description of what is new in this release. For more information about these features, see the Cisco MSE Connected Mobile Experiences Configuration guide, MSE wIPS configuration guide, Cisco CMX Analytics Service Configuration Guide, and Cisco CMX Browser Engage Service Configuration Guide.

AeroScout Engine Module Changes

Starting Release 7.5, the AeroScout engine module is removed from both the Connected Mobile Experiences setup and location code. During installation, if you are upgrading from Release 7.2 and later to Release 7.5, then you will be prompted to remove the AeroScout engine. If you agree to remove, then it removes the AeroScout engine and by default, the Cisco Tag Engine is started as part of Connected Mobile Experiences. If you do not agree to remove the AeroScout engine, then installation will exit.

MSE Licensing

The following are the licensing changes done in Release 7.5:

- MSE 3355 scale increased to 2500 APs for Base and Connected Mobile Experiences (CMX) license.
- High End Virtual Appliance scales to 5000 APs for Base and Connected Mobile Experiences (CMX) license.
- Connected Mobile Experiences and wIPS cannot coexist on the same MSE.

CMX Browser Engage

The CMX Browser Engage is a new way to transform the in-venue experience through browser engagement. This enables organizations to communicate with opt-in mobile users - shoppers, guests, and visitors - through their mobile browser. The CMX Dashboard is the back-end tool designed for administrative users to manage the CMX Browser engage experience. It allows the admin users to configure venue-specific menus, banners, and icons as well as content-aware search.

CMX Visitor Connect (Demo Feature)

Note The CMX Visitor Connect is a demonstration (demo) feature that is not supported by the Cisco TAC. The demo feature is intended for specific customer trials; however, if you are interested in trying this demo feature, we recommend that you use this in the lab environment and not in the production network. This is switched on by default and requires some configuration to work.

The CMX Visitor Connect is an intuitive captive portal that provides visitor management. It is designed to provide the best experience for both mobile and laptop users. The CMX Visitor Connect supports WebPassthru, and Social Media Authentication. This portal is location aware and it allows you to customize the captive portal based on location.

CMX Analytics Enhancements

The following are the new analysis types introduced in Release 7.5:

- Alternate path analysis—The alternative path analysis allows you to determine the device flow between different points in the building. This allows you to place starting and destination points. It shows a break down of the percentage of devices going to each destinations for each starting point and vice versa. If a device visits multiple destinations after visiting a starting point, then only the first one is considered for analysis.
- Heat maps—The heat maps is a graphical representation of data and allows you to view all selected data on the map. The areas where there is a greater presence of data is represented in darker colors. these patterns helps to indicate the real coverage of the access points across a region.

The new CMX Analytics report that has been introduced in Release 7.5 is:

- Device count by time of day

Note The application has a limit on the size of images it can handle. This though is dependent on the hardware, browser and device drivers present. The symptoms are typically black floor plans being shown in the 3D browser. Image file of over 1Mb have caused problems on hardware/software combinations. Google Chrome on PC and Firefox on MAC seem most resilient. However, for performance purposes keeping the image files as small as necessary is encouraged. The images are used to locate the results for the user rather than for any detailed architectural reasons.

HTTP Proxy Service

HTTP Proxy Service—Currently, CMX Dashboard relies on HTTP traffic flows to provide value added services and messages to the customers at the venue. The router intercepts the HTTP traffic and CMX Dashboard inserts a script at the end of the HTTP traffic. The HTTP Proxy is enabled on the MSE. The HTTP Proxy on the MSE terminates all HTTP traffic intercepted using Policy Based Routing (PBR) and acts as a forward proxy by pulling contents on behalf of wireless clients.

Rogue AP Zone Impact

Rogue zone impact feature shows the zone of impact for rogues similar to interferer impact. This helps in easy identification of high impact Rogue APs on the Map. The radius of the impact and the number of valid clients attached is shown on the map through zone of impact.

vWLC Support

You can use the virtual controller with MSE without running the CLI commands.

Auto MAC Address Learning

The auto MAC learning feature is introduced in Release 7.5. This feature protects valid clients on your network from connecting to rogue APs. The MSE is used to validate the clients without any pre-configuration on the MSE. Whenever a client is connecting to Rogue AP, the controller validates whether the client is valid or not with the MSE. If the client is valid, then controller auto contains the client from connecting to the rogue AP. Controller uses the MSE auto MAC learning database to check each re-association request MAC address.

Global Forensic Feature

The wIPS global forensic feature provides wireless packet capture on demand from the Prime Infrastructure. This is a troubleshooting feature and you can use the capture to examine the packets received by the access point. This feature allows the captured data to be stored on a secure FTP server.

New wIPS Signature Support

The following are the new wIPS signatures introduced in Release 7.5:

- AirDrop Session Detected
- DHCP Starvation Attack Detected
- WiFi Protected Setup Pin Brute Force

wIPS Alarm Consolidation

The wIPS alarm consolidation feature aggregates different wireless intrusion incidents reported by access points and provides a concise meaningful alarm. This helps you to quickly isolate potential security issues and concerns. The **Consolidated Alarm Detail > Related Alarm List** group box displays all the alarms related to a particular attack. The Related Alarm List group box also displays information on what consolidation rule was applied to consolidate the alarms.

New wIPS UI Changes

A new simple easy to use wIPS wizard is added to the Prime Infrastructure that allows configuration and deployment of Rogue Policy, Rogue Rules, and wIPS Profiles to multiple controllers/MSE within few clicks.

The wIPS Monitoring Dashboard is enhanced to provide Rogue AP trending charts as well as details of Auto containment actions on Rogue APs as well as wIPS signature attacks. For more information, see the wIPS Configuration Guide, Release 7.5 at:
http://www.cisco.com/en/US/products/ps9817/products_installation_and_configuration_guides_list.html

Caveats

This section lists the open caveats in 7.5.102.101 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 the 7.5.102.101 MSE software release.

Table 5 Open Caveats

ID Number	Caveat Title
CSCui97428	**Headline**: Analytics reports take more time to load when there is no active data coming from the MSE. **Symptom**: Analytics reports take 5-7 minutes to launch. **Condition**: Analytics report take 5-7 minutes to launch when the analytics is not collecting any data from the MSE. **Workaround**: Run the following commands from the MSE console every time the MSE is restarted or analytics is disables and enabled: • `source /opt/mse/install/oracleenv` `$ORACLE_HOME/bin/sqlplus analytics/'getdatabaseparams'@mseorcl` • `SQL>call gatherStats_procedure_package.gatherStats();` It takes a few minutes to execute. • `SQL>exit;`

Table 5 Open Caveats (continued)

ID Number	Caveat Title
CSCug19295	**Headline**: No support for Inter Explorer for Browser Engage. **Symptom**: Internet Explorer browser is not supported with Browser engage and many of the features do not work with the Internet Explorer. **Conditions**: The following funtionalities do not work: • Campaigns—Cannot create with rules • Banners—Cannot upload images • POI—Floor maps does not show up • Floor Navigations—Shows blank page • Accounts—Fail to load the accounts • Menu—Fail to load the menu • Reports—Does not work **Workaround**: None.
CSCui92258	**Headline**: HTTP proxy and the connector UI page display is not correct with Google Chrome version 29. **Symptom**: On Chrome version 29 when we open the CMX Management UI page using https:// , the http proxy page and the connector page has the incorrect http information. On the connector page the CMX dashboard connector does not appear. **Conditions**: The issue is on the Chrome version 29 or higher. **Workaround**: Use Chrome browser version 28 or lower, Internet Explorer version 8 or 9, and Mozilla Firefox.

Resolved Caveats

Table 6 lists the caveats resolved in the 7.5.102.101 MSE software release.

Table 6 Resolved Caveats

ID Number	Caveat Title
CSCui58471	MSE - Oracle enhancements.
CSCui63815	After upgrading to Release 7.5 from Release 7.4, report shows no data for target.
CSCui57967	CMX Analytics does not start after upgrading from Release 7.4 to Release 7.5.
CSCui33540	Report detected vs. connected is not completing.

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 Connected Mobile Experiences Configuration Guide, Release 7.5*

  http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html
- *Cisco Wireless Intrusion Prevention System Configuration Guide, Release 7.5*

  http://www.cisco.com/en/US/products/ps9817/products_installation_and_configuration_guides_list.html
- *Cisco CMX Analytics Configuration Guide, Release 7.5*

  http://www.cisco.com/en/US/products/ps9742/products_installation_and_configuration_guides_list.html
- *Cisco Mobility Services Engine Getting Started Guide*

  http://www.cisco.com/en/US/products/ps9742/prod_installation_guides_list.html
- The Prime Infrastructure Online Help available with the Prime Infrastructure 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.
