Release Notes for Cisco Mobility Services Engine Release 8.0.150.x

First Published: November 12, 2017
Last Modified: July 1, 2019

This document describes what is new and important in Cisco Mobility Services Engine (MSE) Release 8.0.150.x, including the requirements, upgrade instructions, open and resolved caveats, and related information. Unless otherwise noted, Cisco Mobility Services Engine is referred to as Cisco MSE in this document.

Note Before installing the Cisco MSE software, see the "Upgrading Cisco MSE" section on page 3 for details on compatibility with the Cisco Wireless Controllers (WLC) and Cisco Prime Infrastructure. Complete compatibility information is provided in the *Cisco Wireless Solutions Software Compatibility Matrix* at: https://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html.

Note Cisco MSE 3310 and Cisco MSE 3350 are not supported beyond Cisco MSE Release 7.3.

Contents

These release notes contain the following sections:

Cisco Systems, Inc.
www.cisco.com

Introduction

Note Licenses are required to run all services. For information about ordering, see the "Cisco MSE Licensing Information" section on page 12.

Cisco MSE supports these services within the overall Cisco Unified Wireless Network (CUWN):

- Context Aware Service (also known as Location Service)—This is the core service of Cisco MSE that turns on Wi-Fi client tracking and location API functionality. It allows Cisco MSE 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 (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 (APs). Proactive threat prevention is also supported to create a hardened wireless network core that is impenetrable by most wireless attacks.
- Cisco CMX Analytics Service—Collects and analyses the basic data from various APs. The Cisco CMX analytics service 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 Cisco CMX Analytics service helps the airport authorities or the building owners to understand the movement of passengers or customers within their building. This helps them improve the signage, make changes to the underutilized areas, and so on.

  For an improved Analytics experience, we recommend using Cisco CMX Release 10.2.2. No new features will be added to the Analytics engine for Cisco MSE Release 8.0.
- Cisco CMX Connect and Engage Service—The Cisco CMX Connect and Engage service provides Connect, a guest Wi-Fi onboarding solution, as well as zone and message configuration for the Cisco CMX Software Development Kit (SDK).

Note From Cisco MSE Release 7.5 onwards, Cisco location 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, the installer will remove all partner engine sub services. If you do not accept the removal of partner engine, then the installer will exit.

Note Starting from Cisco MSE release 7.4, the evaluation licenses for 100 clients, 100 tags, and 10 wIPS monitor mode access points are a standard on each Cisco MSE. The licenses are valid for a period of 120 days; from Release 6.0 till Release 7.3 the licenses were valid for a period of 60 days.

Note From Cisco MSE release 7.4 onwards, licensing is based on AP count and not on tracked device count.

What's New in This Release

What's New in Cisco MSE Release 8.0.150.0

This release delivers a number of critical bug-fixes. There are no new features added in this release. For bugs addressed in this release, see the "Caveats" section on page 33.

For more information about instructions on how to configure the Cisco MSE features, see the *Cisco Connected Mobile Experiences Configuration Guide*, *Cisco Wireless Intrusion Prevention System Configuration Guide*, *Cisco CMX Analytics Service Configuration Guide*, *Cisco CMX Connect and Engage Configuration Guide*, and *Cisco MSE Virtual Appliance Configuration Guide* at: https://www.cisco.com/en/US/products/ps9742/products_installation_and_configuration_guides_list.html

Software Compatibility Matrix

For information, see the "Cisco MSE Compatibility Matrix for Software Versions 7.5.x through 8.x" section in the *Cisco Wireless Solutions Software Compatibility Matrix*: https://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html.

Upgrading Cisco MSE

For instructions on automatically downloading the Cisco MSE software using Cisco 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*: https://www.cisco.com/en/US/products/ps9742/prod_installation_guides_list.html

Only users with Cisco MSE Release 7.4 or later will be able to upgrade to Cisco MSE Release 8.0.150.x. The following scenarios are available to upgrade from Cisco MSE Release 7.4x to Cisco MSE Release 8.0.150.x.

Note Do not uninstall the releases 7.4, 7.5, 7.6, or 8.x, instead stop the Cisco MSE and run the installer.

Compressed Software Image

If you download the Cisco MSE image *.gz file using the Cisco Prime Infrastructure, the Cisco MSE automatically decompresses (unzips) it, and you can proceed with the installation as described in the "Upgrading from Cisco MSE Release 7.4.x to Cisco MSE 8.0.120 through 8.0.140.9" section on page 7.

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 by using the **tar zxvf** command. For more information, see the Manually Downloading Software section in the *Cisco Connected Mobile Experiences Configuration Guide, Release 8.0*.

To make the .bin file executable, use the **chmod +x <filename.bin>** command.

The Cisco MSE virtual appliance is distributed as Open Virtualization Format (OVF) for VMware

For more information on deploying the Cisco MSE virtual appliance, see the *Cisco MSE Virtual Appliance Configuration Guide, Release 8.0*.

Upgrading from Cisco MSE Release 8.x to Cisco CMX Release 10.x

To install Cisco CMX Release 10.x on a server running Cisco MSE Release 8.x, either:

- Use the ISO file if you are upgrading a physical appliance, as described in the "Uploading the Cisco CMX/MSE ISO Image to the Cisco MSE 3365 Using Newer CIMC Versions" section of the "Uploading the Cisco CMX/MSE ISO Image to the Cisco MSE 3365" chapter in the *Cisco Connected Mobile Experiences Configuration Guide, Release 8.0*: https://www.cisco.com/c/en/us/td/docs/wireless/mse/8-0/MSE_CMX/8_0_MSE_CAS/8_0_MSE_CAS_chapter_010010.html
- Install Cisco CMX Release 10.x s on a new VM, as described in the "MSE Virtual Appliance on the VMware Virtual Machine" chapter in the *Cisco MSE Virtual Appliance Installation and Configuration Guide, Release 8.0:* https://www.cisco.com/c/en/us/td/docs/wireless/mse/8-0/MSE_Virtual_Appliance/guide/Cisco_MSE_VA_Config_Guide/Installing_MSE_Virtual_Appliance.html

Downgrading from Cisco CMX Release 10.x to Cisco MSE Release 8.x

- You can downgrade a device installed with Cisco CMX Release 10.x to Cisco MSE Release 8.x, as described in the "Uploading the Cisco CMX/MSE ISO Image to the Cisco MSE 3365 Using Older CIMC Versions" section of the "Uploading the Cisco CMX/MSE ISO Image to the Cisco MSE 3365" chapter in the *Cisco Connected Mobile Experiences Configuration Guide, Release 8.0*: https://www.cisco.com/c/en/us/td/docs/wireless/mse/8-0/MSE_CMX/8_0_MSE_CAS/8_0_MSE_CAS_chapter_010010.html

Upgrading from Cisco MSE Release 8.0.120.0 through 8.0.140.9 to Cisco MSE to 8.0.150.x

Caution Ensure that you have copies of your Cisco MSE license files before performing the upgrade. If you do not have copies of the Cisco MSE license files, copy the *.lic files under the /opt/mse/licensing folder of the Cisco MSE to your local machine.

Note We recommend that you back up the Cisco MSE by using Cisco Prime Infrastructure.

Note You also need to install the Encryption Upgrade patch during this upgrade process. Make sure to download this patch file when you download the Cisco MSE to 8.0.150.0 software image.

Step 1 You can either manually download the software image or download the software image by using Cisco Prime Infrastructure.

To manually download the software image:

a. Download the applicable 8.0.150.x software image from Cisco.com. For example, the image name for Cisco MSE Release 8.0.150.0 is CISCO-MSE-L-K9-8-0-150-0-64bit.bin.tar.gz.

Note If you are downloading the Cisco MSE image file on a Windows system, remember that some browsers modify the downloaded filename. If the downloaded filename is not correct, you must update it to the correct filename before using Cisco Prime Infrastructure to transfer the file, or directly copying the file to Cisco MSE.

b. Untar the Cisco MSE software image in the /opt/installers directory.

c. From the Cisco Prime Infrastructure UI, select **Services > Mobility Services Engine** to download the software to a Cisco MSE.

To download the software image by using Cisco Prime Infrastructure:

a. Click the name of the Cisco MSE to which you want to download the software.

b. Select **System > Maintenance > Download Software** from the left menu. The **Upload Software Image** screen displays.

c. Click **Select File**, and navigate to the local folder that contains the upgrade file.

d. Select the file and click **Open**. When the filename appears in the Upload Software Image field, click **Import** to send the software to the /opt/installers folder on the Cisco MSE.

e. When using Cisco Prime Infrastructure to transfer the image to Cisco MSE, the file will be decompressed, and the .gz will be removed from the filename. Verify that the Cisco MSE image file is in the Cisco MSE /opt/installers directory. For example, the image name for Cisco MSE Release 8.0.150.0 is CISCO-MSE-L-K9-8-0-150-0-64bit.bin.tar.gz.

Note When copying the Cisco MSE image file directly to the Cisco MSE without using Cisco Prime Infrastructure, the filename of Cisco MSE image will remain unchanged.

f. Use the **cd /opt/installers** command to navigate to the /opt/installers directory.

Step 2 Use the **tar xvf** <*.tar.image-name*> command to unpack the installation files. For example, for Cisco MSE Release 8.0.150.0:

```
tar xvf CISCO-MSE-L-K9-8-0-150-0-64bit.bin.tar
```

This unpack action yields the following files. These files must be in the same directory when running the installer. The installation process uses the MSE_PUB.pem and signhash.bin files to validate the integrity of the Cisco MSE image.

- CISCO-MSE-L-K9-8-0-150-0-64bit.bin (for Cisco MSE Release 8.0.150.0)
- MSE_PUB.pem
- signhash.bin
- Database_Installer.11.2.0.4.tar.gz

Note If the Cisco MSE image file was transfered directly to the Cisco MSE and not downloaded by using Cisco Prime Infrastructure, use the **tar xvf** <*.gz-image-name*> command to decompress and unpack the installer files.

Note Do not untar or unzip the database package.

Step 3 Use the **chown nobody:nobody./**<*image-names*> command to change the permissions of the files. For example, for Cisco MSE Release 8.0.150.0:

```
chown nobody:nobody./CISCO-MSE-L-K9-8-0-150-0-64bit.bin signhash.bin
Database_Installer.11.2.0.4.tar.gz
```

Note A space must be provided between the filenames in the chown command above.

Step 4 Make sure that the Cisco MSE bin file (for example, CISCO-MSE-L-K9-8-0-150-0-64bit.bin) has execute permissions for the root user.

If it does not, use the **chown +x** <*.bin-image-name*> command. For example, for Cisco MSE Release 8.0.150.0:

```
chmod +x CISCO-MSE-L-K9-8-0-150-0-64bit.bin
```

Step 5 Manually stop the Cisco MSE service by using the **/etc/init.d/msed stop** command or the **service msed stop** command.

Step 6 Apply the Encryption Upgrade patch:

a. Extract the Encryption Upgrade patch file (enc-upgrade-patch.tar.gz) to the /opt/installers folder:

```
cd /opt/installers
tar zxvf enc-upgrade-patch.tar.gz
cd /opt/installers/enc-upgrade-patch
```

b. Apply the patch by using the **./apply-patch.sh** command.

Step 7 Use the **/opt/installers/**<*.bin-image-name*> command to install the new Cisco MSE image. For example, for Cisco MSE Release 8.0.150.0:

```
/opt/installers/CISCO-MSE-L-K9-8-0-150-0-64bit.bin
```

Note The installation process takes a minimum of 30 minutes. The actual installation time depends on the amount of data present in your system. After the installation, reboot the system before starting Cisco MSE.

Step 8 After exiting the installer, enter the **reboot** command to reboot Cisco MSE.

See "Upgrading Cisco MSE High Availability" section on page 11 for details on upgrading Cisco MSE high availability.

Upgrading from Cisco MSE Release 7.4.x to Cisco MSE 8.0.120 through 8.0.140.9

Caution Ensure that you have copies of your Cisco MSE license files before performing the upgrade. If you do not have copies of the Cisco MSE license files, copy the *.lic files under the /opt/mse/licensing folder of the Cisco MSE to your local machine.

Note We recommend that you back up the Cisco MSE by using Cisco Prime Infrastructure.

Note If you already have Cisco MSE Release 8.0.120.0 installed (either with or without the CSCuv55645.zip patch), you can upgrade up to Cisco MSE Release 8.0.140.9 by using the upgrade procedure described in this section.

Step 1 You can either manually download the software image or download the software image by using Cisco Prime Infrastructure.

To manually download the software image:

a. Download the applicable 8.0.140.x software image from Cisco.com. For example, the image name for Cisco MSE Release 8.0.140.0 is CISCO-MSE-L-K9-8-0-140-0-64bit.bin.tar.gz.

Note If you are downloading the Cisco MSE image file on a Windows system, remember that some browsers modify the downloaded filename. If the downloaded filename is not correct, you must update it to the correct filename before using Cisco Prime Infrastructure to transfer the file, or directly copying the file to Cisco MSE.

b. Untar the Cisco MSE software image in the /opt/installers directory.

c. From the Cisco Prime Infrastructure UI, select **Services** > **Mobility Services Engine** to download the software to a Cisco MSE.

To download the software image by using Cisco Prime Infrastructure:

a. Click the name of the Cisco MSE to which you want to download the software.

b. Select **System** > **Maintenance** > **Download Software** from the left menu.

c. To download the software, perform one of the following tasks:

- To download a software listed in the Cisco Prime Infrastructure directory, click the **Select from uploaded images to transfer into the Server** radio button and choose a binary image from the drop-down list.

  Cisco Prime Infrastructure downloads the binary image to the FTP server directory you specified during the Cisco Prime Infrastructure installation.

- To download a software that is available locally or over the network, select the **Browse a new software image to transfer into the Server** radio button and then click **Choose File**. After locating the file, click **Open**.

d. Click **Download** to send the software to the /opt/installers folder on the Cisco MSE.

e. When using Cisco Prime Infrastructure to transfer the image to Cisco MSE, the file will be decompressed, and the .gz will be removed from the filename. Verify that the Cisco MSE image file is in the Cisco MSE /opt/installers directory. For example, the image name for Cisco MSE Release 8.0.140.0 is CISCO-MSE-L-K9-8-0-140-0-64bit.bin.tar.gz.

Note When copying the Cisco MSE image file directly to the Cisco MSE without using Cisco Prime Infrastructure, the filename of Cisco MSE image will remain unchanged.

f. Use the **cd /opt/installers** command to navigate to the /opt/installers directory.

Step 2 Use the **tar xvf** <*.tar.image-name*> command to unpack the installation files. For example, for Cisco MSE Release 8.0.140.0:

```
tar xvf CISCO-MSE-L-K9-8-0-140-0-64bit.bin.tar
```

This unpack action yields the following files. These files must be in the same directory when running the installer. The installation process uses the MSE_PUB.pem and signhash.bin files to validate the integrity of the Cisco MSE image.

- CISCO-MSE-L-K9-8-0-140-0-64bit.bin (for Cisco MSE Release 8.0.140.0)
- MSE_PUB.pem
- signhash.bin
- Database_Installer.11.2.0.4.tar.gz

Note If the Cisco MSE image file was transfered directly to the Cisco MSE and not downloaded by using Cisco Prime Infrastructure, use the **tar xvf** <*.gz-image-name*> command to decompress and unpack the installer files.

Note Do not untar or unzip the database package.

Step 3 Use the **chown nobody:nobody./**<*image-names*> command to change the permissions of the files. For example, for Cisco MSE Release 8.0.140.0:

```
chown nobody:nobody./CISCO-MSE-L-K9-8-0-140-0-64bit.bin signhash.bin
Database_Installer.11.2.0.4.tar.gz
```

Note A space must be provided between the filenames in the chown command above.

Step 4 Make sure that the Cisco MSE bin file (for example, CISCO-MSE-L-K9-8-0-140-0-64bit.bin) has execute permissions for the root user.

If it does not, use the **chown +x** <*.bin-image-name*> command. For example, for Cisco MSE Release 8.0.140.0:

```
chmod +x CISCO-MSE-L-K9-8-0-140-0-64bit.bin
```

Step 5 Manually stop the Cisco MSE service by entering this command:

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

Step 6 Use the **/opt/installers/**<*.bin-image-name*> command to install the new Cisco MSE image. For example, for Cisco MSE Release 8.0.140.0:

```
/opt/installers/CISCO-MSE-L-K9-8-0-140-0-64bit.bin
```

Note The installation process takes a minimum of 30 minutes. The actual installation time depends on the amount of data present in your system. After the installation, reboot the system before starting Cisco MSE.

Step 7 After exiting the installer, enter the **reboot** command to reboot Cisco MSE.

See "Upgrading Cisco MSE High Availability" section on page 11 for details on upgrading Cisco MSE high availability.

Restoring an Old Cisco MSE Backup to Cisco MSE Release 8.0.140.x

Note **Before you begin**: If high availability is configured, delete the secondary Cisco MSE ***before*** restoring the historical data on the primary Cisco MSE. You can add the deleted Cisco MSE after restoration on the primary Cisco MSE successfully completes.

Note The regular restore option on the Cisco Prime Infrastructure cannot be used to restore a backup from an earlier Cisco MSE Releases such as 6.0, 7.0.105.0, or 7.0.110.0 to Cisco MSE Release 8.0.140.x.

To restore an old database to Cisco MSE Release 8.0.140.x, follow these steps:

Step 1 Stop the Cisco MSE service: /etc/init.d/msed stop

Step 2 Uninstall the software and select the option to delete the database.

Step 3 To restore backup data, you must first install the appropriate version of Cisco MSE software. Use the table below to determine the correct version of Cisco MSE to install.

Table 1 Release Matrix

Version of Database to be Restored	New Version to be Installed
5.2.0	6.0, 7.0
6.0	6.0, 7.0

Step 4 After you have installed the software, restore the desired database backup to the new Cisco MSE by using the regular procedure from Cisco Prime Infrastructure.

Step 5 To migrate data to 7.x.x.x, follow the steps provided in the "Upgrading from Cisco MSE Release 7.4.x to Cisco MSE 8.0.120 through 8.0.140.9" section on page 7.

Restoring an Old Cisco MSE Backup to Cisco MSE Release 8.0.150.x

Note A backup from Cisco MSE Release 8.0.140.9 or earlier cannot be restored directly to Cisco MSE Release 8.0.150.0.

To restore an old database to Cisco MSE Release 8.0.150.x, follow these steps:

Step 1 Restore backup data, as described in the "Restoring an Old Cisco MSE Backup to Cisco MSE Release 8.0.140.x" section on page 10.

Step 2 Upgrade Cisco MSE to Cisco MSE Release 8.0.150.x, as described in the "Upgrading from Cisco MSE Release 8.0.120.0 through 8.0.140.9 to Cisco MSE to 8.0.150.x" section on page 5.

Updated Software Version Shown in the Cisco Prime Infrastructure After Polling

After a software update, the new Cisco MSE software version does not immediately appear in Cisco MSE queries on the Cisco Prime Infrastructure. Up to 5 minutes are required for the new version to appear. By default, Cisco Prime Infrastructure queries the Cisco MSE for status every 5 minutes.

Upgrading Cisco MSE High Availability

To upgrade for Cisco MSE high availability, follow these steps:

Step 1 Ensure that the HA pair that needs to be upgraded is in normal mode and not in Failover mode. In normal mode, the Primary Cisco MSE is active and the Secondary is in standby mode. The output of the **gethainfo** command on primary MSE will show PRIMARY_ACTIVE and the secondary MSE will show SECONDARY_ACTIVE.

Step 2 Log in to Cisco Prime Infrastructure and delete the Cisco MSE HA pair.

Step 3 Perform a full backup of the primary Cisco MSE.

Step 4 Stop the primary Cisco MSE and the secondary Cisco MSE by using the **service msed stop** command.

Step 5 Perform the upgrade on the Primary and Secondary Cisco MSE servers by following the instructions described in Upgrading from Cisco MSE Release 7.4.x to Cisco MSE 8.0.120 through 8.0.140.9, page 7.

Step 6 Start both the primary and secondary Cisco MSE instances by using the **service msed start** command.

Step 7 Recreate the Cisco MSE HA pair using Cisco Prime Infrastructure.

Configuring History Pruning Parameters

The History Pruning parameters are configured from the Cisco Prime Infrastructure or Cisco MSE user interface. This interface is used to:

- Enable/Disable History tracking for clients/tags/rogue APs/rogue clients/interferers.
- History Retention period—How long (in days) to retain history data.
- Time at which to prune history records.

Starting in Cisco MSE Release 8.0.130.0, the Cisco Prime Infrastructure and Cisco MSE user interface is used to enable/disable History tracking for clients/tags/rogue APs/rogue clients/interferers. The pruning of History data takes place every hour automatically. This hourly pruning task computes the number of history records that must be deleted to bring the record count to the platform limit. After the computation, the pruning task deletes the oldest history records so that the record count matches the platform limit. The history pruning task does not perform anything if the history record count is below the platform limit. The Cisco MSE Administrator cannot change the pruning interval or the history retention duration.

The history record count for various Cisco MSE platforms is as follows:

- MSE-3355—7.5 million records
- MSE-3365—25 million records
- Virtual MSE—15 million records

Cisco MSE Licensing Information

Cisco MSE Licensing Overview

Client and wIPS licenses are installed from the Cisco 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 8.0, Cisco Wireless Intrusion Prevention System, Release 8.0*, and *Cisco Location Analytics Configuration Guide, Release 8.0*.

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

Cisco MSE provides a wide variety of location-based services. To enable these services, the following are required:

- Cisco MSE hardware or software appliance
  - Physical Appliance—An activation license is not required.
  - Virtual Appliance—Requires a Cisco MSE Virtual Appliance Activation license (L-MSE-7.0-K9). It is not sufficient to simply have a service or feature license on an Cisco MSE Virtual Appliance.
- Licenses
- Support

Three types of Cisco MSE licenses are available:

Table 2 Cisco MSE License Types

Cisco MSE Service License	Features
Base Location License	Provides advanced spectrum capability, with the ability to detect, track, and trace rogue devices, Cisco CleanAir interferers, Wi-Fi clients, and RFID tags. The Base Location license also enables customers and partners to use standard Cisco MSE APIs.
Cisco CMX License	Provides Base Location license capabilities and the Cisco CMX features: • Cisco CMX Analytics, a user-friendly location analytics platform to view and analyze how, where, and when visitors move through a venue. • Cisco CMX Connect and Engage for a customizable and location-aware captive portal to on-board guest users to Wi-Fi including: • Cisco CMX for Facebook Wi-Fi, helping guests connect to Wi-Fi and use the Internet. Enterprises or merchants gain social demographic data via Facebook Insights. • Cisco CMX SDK for enabling organizations to integrate Wi-Fi-based indoor navigation with push notification and auto-launch capabilities into mobile applications.

Table 2 Cisco MSE License Types (continued)

Cisco MSE Service License	Features
wIPS License	Provides complete wireless threat detection and mitigation in the wireless network infrastructure: • Rogue Detection, Classification, and Mitigation • Over-the-Air Attack Detection • Security Vulnerability Monitoring • Performance Monitoring, and Auto-Optimization • Management, Monitoring, and Reporting Requires a separate Cisco MSE running the wIPS service. There are 3 deployment options: • Enhanced Local mode–Number of wIPS licenses required equals the number of access points in local mode (data serving) deployed in the network. • Monitor mode–Number of wIPS licenses required equals the number of access points configured in the full-time monitor mode. • Wireless Security Module (WSM) or Monitor module–Number of wIPS licenses required equals the number of wireless security and spectrum intelligence modules deployed in the network.

Cisco CMX License

The Cisco CMX license, called Advanced Location license in release 7.4, supports new features, such as:

- Cisco CMX Analytics
- Cisco CMX Connect
- Cisco CMX for Facebook Wi-Fi

The CMX license includes the Base Location license features used for device tracking and the new additional features of Cisco CMX.

The part number format of this license is L-AD-LS-100AP. Here 'AD-LS' refers to Advanced Location services license and '100AP' gives the AP count supported.

Table 3 Cisco CMX License

Cisco MSE Release	License Name	Based On
After 7.4	Cisco CMX license	Number of APs
7.4	Advanced Location Services license	Number of APs
Earlier than 7.4	Nonexistent	—

Cisco wIPS License

All Cisco wIPS licenses come with the license name wIPS license

There are three deployment options:

- Enhanced Local mode–Number of wIPS licenses required equals the number of access points in local mode (data serving) deployed in the network.
- Monitor mode–Number of wIPS licenses required equals the number of access points configured in the full-time monitor mode.
- Monitor module–Number of wIPS licenses required equals the number of wireless security and spectrum intelligence modules deployed in the network.

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

Table 4 Cisco wIPS License

Cisco MSE Release	License Name	Based On
All releases	wIPS license	Number of APs.

Cisco MSE License Product Numbers and SKUs

Ordering Support for Physical and Virtual Appliance

The Cisco MSE Virtual Appliance activation license is required for every instance of a Cisco MSE Virtual Appliance. 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 CMX or wIPS license.

Table 5 Ordering Support for Physical and Virtual Appliance

Cisco MSE Model	SKU	Service SKU	Description
Cisco MSE 3365 (Physical Appliance)	AIR-MSE-3365-K9	CON-SNT-AIRMSE3K	Hardware and software support
Cisco MSE 3355 (Physical Appliance)	AIR-MSE-3355-K9	CON-SNT-MSE3355	Hardware and licenses support
Cisco MSE Virtual Appliance	L-MSE-7.0-K9	CON-SAU-LMSE7K	Software and licenses support

Table 5 Ordering Support for Physical and Virtual Appliance (continued)

Cisco MSE Model	SKU	Service SKU	Description
Cisco MSE Release 8.0 Base License	L-LS-xAP	CON-SAU-LLS1APSW	Software support (only if ordering Cisco 3365 MSE appliance).
Cisco MSE Release 8.0 Cisco CMX License	L-AD-LS-xAP	CON-SAU-LADLA1AP	Software support (only if ordering Cisco 3365 MSE appliance).

Licenses Summary

Table 6 License Summary

Base Location License SKU	Cisco CMX License SKU	Cisco wIPS Monitor Mode/Monitor Mode SKUs	Cisco wIPS Enhanced Local Mode SKUs	Description
L-LS-1AP	L-AD-LS-1AP	L-WIPS-MM-1AP	L-WIPS-ELM-1AP	Supports 1 AP[1]
L-LS-100AP	L-AD-LS-100AP	L-WIPS-MM-100AP	L-WIPS-ELM-100AP	Supports 100 APs[2]
L-LS-1000AP	L-AD-LS-1000AP	L-WIPS-MM-1000AP	L-WIPS-ELM-1000AP	Supports 1000 APs[3]

1. 1 AP license gives 10 elements for evaluation license.
2. 100 AP license gives 1000 elements for evaluation license.
3. 1000 AP license gives 10000 elements for evaluation license.

Base Location Services Licenses

Table 7 Base Location Services Licenses

License SKU	Description
L-LS-1AP	1 AP Base Location Services license
L-LS-100AP	100 AP Base Location Services license
L-LS-1000AP	1000 AP Base Location Services license

Cisco CMX Licenses (Previously Known as Advanced Location Services)

Cisco CMX licenses include the Base Location Service licenses. There is no need to purchase a separate Base Location Service license when purchasing a Cisco CMX license.

Table 8 Cisco CMX Licenses

License SKU	Description
L-AD-LS-1AP	1 AP CMX license (Advanced Location Services)
L-AD-LS-100AP	100 AP CMX license (Advanced Location Services)
L-AD-LS-1000AP	1000 AP CMX license (Advanced Location Services)

Base Location Services to Cisco CMX Upgrade License

Table 9 Base Location Services to Cisco CMX Upgrade License

License SKU	Description
L-UPG-LS-1AP	1 AP Upgrade from Base Location to Cisco CMX license.

wIPS Enhanced Local Mode License

Table 10 wIPS Enhanced Local Mode License

License SKU	Description
L-WIPS-ELM-1AP	1 AP wIPS-Enhanced Local Mode License
L-WIPS-ELM-100AP	100 AP wIPS-Enhanced Local Mode License
L-WIPS-ELM-1000AP	1000 AP wIPS-Enhanced Local Mode License

wIPS Monitor Mode/Monitor Module License

Table 11 wIPS Monitor Mode Licenses

License SKU	Description
L-WIPS-MM-1AP	1 AP wIPS Monitor Mode License
L-WIPS-MM-100AP	100 AP wIPS Monitor Mode License
L-WIPS-MM-1000AP	1000 AP wIPS Monitor Mode License

Cisco MSE Virtual Appliance Product Specifications

Table 12 Cisco MSE Virtual Appliance Product Specifications

Feature	Cisco MSE Virtual Appliance
Virtual appliance versions	VMware ESX or ESXi version 5.5 and 6.0.

Table 12 Cisco MSE Virtual Appliance Product Specifications (continued)

Feature	Cisco MSE Virtual Appliance
Minimum Server Requirements	Cisco MSE High-End Virtual Appliance • Base location license–5000 access points • Cisco CMX license–5000 access points • wIPS license–10,000 access points • Maximum number of tracked devices: 50,000 (regardless of the number of AP licenses). Note that the end-device scaling guidelines differ if your are using FastLocate or Presence as a method for determining device location. See the *Cisco MSE ordering and licensing* guide for more details. • Minimum RAM: 24 GB • Minimum hard disk space allocation: 500 GB with SAS drivers and 1600 I/O operations per second (IOPS) • Processors: 16 vCPUs at 2.0 GHz or faster and a passmark (cpubenchmark.net) no less than 4000 • Cisco UCS ® ref: Cisco UCS C240 M3 Rack Server or C460 M2 High-Performance Rack Server
	Cisco MSE Standard Virtual Appliance • Base Location license–2500 access points • Cisco CMX license–2500 access points • wIPS license–6000 access points • Maximum number of tracked devices–25,000 (regardless of number of access point licenses). Note that the end device scaling guidelines differ if you are using FastLocate or presence as a method for determining device location. See the *Cisco MSE ordering and licensing* guide for more details. • Minimum RAM: 16 GB • Minimum hard disk space allocation: 500 GB with SAS drivers and 1000 IOPS • Processors: 8 vCPUs at 2.0 GHz or faster, and a passmark (cpubenchmark.net) no less than 4000 • Cisco UCS ref: Cisco UCS C240 M3 Rack Server
	Cisco MSE Low-End Virtual Appliance Base Location license: 200 access points • Cisco CMX license: Does not support Cisco CMX license • wIPS license: 2000 access points • Maximum number of tracked devices: 2000 (regardless of number of access point licenses). Note that the end device scaling guidelines differ if you are using FastLocate as a method for determining device location. See the Cisco MSE ordering and licensing guide for more details. • Minimum RAM: 8 GB • Minimum hard disk space allocation: 250 GB with SAS drives and 900 IOPS • Processors: 4 vCPUs at 2.0 GHz or faster and a passmark (cpubenchmark.net) no less than 4000

Important Notes

This section describes the operational notes and navigation changes for Connected Mobile Experiences, wIPS, and the Cisco MSE for Release 6.0.103.0 and later releases.

Features and operational notes are summarized separately for the Cisco MSE, Connected Mobile Experiences, and wIPS.

This section contains the following topics:

Operational Notes for Cisco MSE High Availability

VIP and Prime Infrastructure Configuration

(CSCvb61125) When configuring High Availability on the Cisco MSE, make sure that the virtual IP address (VIP) is assigned first, and then set the Prime Infrastructure password through the setup.sh file.

If you change the VIP after setting the Prime Infrastructure password, you will need to reset the password through the setup.sh file. Otherwise, HA configuration cannot be completed.

Swapping HA Roles

(CSCvb59484) We do not recommend swapping HA roles. If the role or the VIP needs to be changed, follow these steps:

Step 1 Run the setup script.

Step 2 Change the HA role.

Step 3 If the new role is **Primary**, assign the VIP.

Step 4 Select the **Verify and apply** option to apply the changes.

Step 5 Restart the Cisco MSE services.

Step 6 Reboot the Cisco MSE, if needed.

Step 7 Run the setup script again.

Step 8 Change the Prime Infrastructure password of the Cisco MSE.

Step 9 Select the **Verify and apply** option to apply the changes.

Step 10 Restart the Cisco MSE services.

Step 11 From Prime Infrastructure, edit the Cisco MSE configuration so that the primary Cisco MSE uses the new Prime Infrastructure password.

Step 12 Verify that the reachability status for the primary Cisco MSE shows as **Reachable**.

Step 13 Continue with HA configuration from Prime Infrastructure.

Changing Cisco MSE HA Role from Primary to Secondary

(CSCve63054) If you need to change the Cisco MSE HA role from Primary to Secondary:

- Make sure the HA pair is no longer configured on Cisco Prime Infrastructure.
- Make sure the Cisco MSE services are stopped on the Primary Cisco MSE server. Use the **service msed stop** command to stop the services.
- Use the **/opt/mse/setup/setup.sh** command from the Primary Cisco MSE server to change the HA role from Primary to Secondary.

If you need to change the Cisco MSE HA role from Secondary to Primary:

- Make sure the Cisco MSE services are stopped on the Primary Cisco MSE server. Use the **service msed stop** command to stop the services.
- Use the **/opt/mse/setup/setup.sh** command from the Primary Cisco MSE server to change the HA role from Secondary to Primary.

Deleting HA Mode MSE from Prime Infrastructure

To delete the Cisco MSE in HA mode from Prime Infrastructure, follow these steps.

Step 1 From Prime Infrastructure, go to the HA configuration of the primary Cisco MSE and click **Delete** to break the HA pair.

Step 2 After the secondary Cisco MSE is deleted from Prime Infrastructure, delete the primary Cisco MSE from Prime Infrastructure.

Operational Notes for Cisco MSE

This section lists the operational notes for the Cisco MSE and contains the following topics:

Synchronizing Maps with Cisco MSE

- (CSCve02624) Cisco Prime Infrastructure Release 3.1.6 or earlier displays incorrect information when unsupported access points attempt to associate with Cisco Wireless LAN Controllers (WLCs). Ensure that only supported Cisco access points are associating with the WLCs.
- We recommend that you synchronize maps and floors on Cisco MSE and Cisco Wireless LAN Controllers (WLCs) by using the **Network Designs** sidebar menu from Cisco Prime Infrastructure instead of just synchronizing the WLCs by using the **Controllers** sidebar menu.

Synchronizing Floor Maps in Location Service

While synchronizing floor maps in location service, we recommend that you synchronize floor maps in batches of 1000 APs at a time.

Enabling TLS Version 1.0 for NMSP Connections

From Cisco MSE Release 8.0.150.0 and later, Transport Layer Security (TLS) version 1.0 is, by default, disabled for all types of connections. Cisco MSE uses only TLS versions 1.1 and 1.2 for all connections.

Cisco wireless controllers running releases 8.0.72.140 and earlier do not support TLS version 1.1 and above, causing Network Mobility Services Protocol (NMSP) connections to become inactive.

To make NMSP connections active again, enable TLS version 1.0 (only for NMSP connections) through the **setup.sh** script by following these steps:

1. From the Cisco MSE shell prompt, enter the **/opt/mse/setup/setup.sh** command.
2. Enter the **Menu** mode.
3. Select the **23) Configure TLSv1.0 for NMSP** option.
4. Follow the prompts to enable TLSv1.0.
5. Select the **25) ## Verify and apply changes ##** option to apply the changes. Note that this restarts Cisco MSE services.

Resolution to NMSP/SHA2 Keyhash Mismatch Issue

By default, Cisco MSE Release 8.0 supports SHA-2 keyhash algorithm for peer authentication with Cisco WLC Release 8.0 during the SSL handshake. Cisco Prime Infrastructure 1.4.2 and 2.1 supports only SHA-1 AP (or Cisco MSE) Authorization template when synchronizing Cisco WLC with the Cisco MSE. This causes keyhash mismatch issue because the Cisco Prime Infrastructure and Cisco MSE use different keyhash algorithm on Cisco WLC Release 8.0. An option is added to the Advanced Parameters page in the Cisco MSE user interface (UI) to allow the user to force Cisco MSE Release 8.0 to use SHA-1 keyhash algorithm.

Follow these instructions to configure SHA-1 Cipher:

Step 1 Launch the Cisco MSE admin UI by typing **https://mseip/mseui** in a web browser.

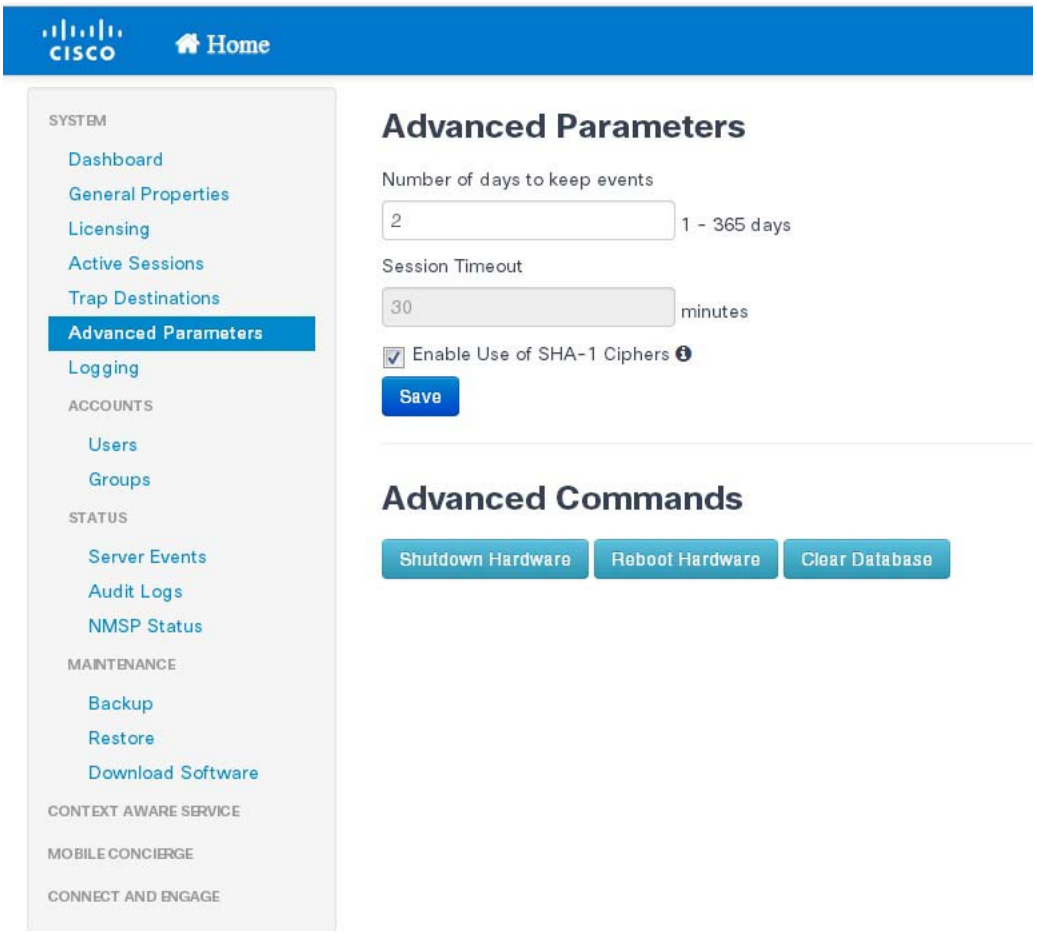
Step 2 Click **Configuration**.

Step 3 Choose **System > Advanced Parameters** from the left menu.

Step 4 Check the **Enable Use of SHA-1 Ciphers** check box (see Figure 1).

Step 5 Click **Save**.

Figure 1 Advanced Parameters



Step 6 Unsynchronize Cisco WLC from Cisco MSE, and then resynchronize Cisco WLC with Cisco MSE from Cisco Prime Infrastructure.

Step 7 The NMSP status should change to active state.

Note If the FIPS mode (also known as Root Access Control) is enabled on the Cisco MSE, then this option will not be available to the users as FIPS mode requires all operations in SHS-2.

DNS Server

Use a valid DNS sever as CAS and Analytics service to use nslookups.

Rebooting Cisco MSE After Fresh Installation or Upgrade

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

Automatic Installation Script for Initial Setup

An automatic setup wizard is available to help you initially set up the Cisco MSE.

An example of the complete automatic setup script is provided in the *Cisco Mobility Services Engine Getting Started Guide*:
https://www.cisco.com/en/US/products/ps9742/prod_installation_guides_list.html

Mapping Controller and Associated Cisco MSE Must be Mapped to the NTP and Cisco Prime Infrastructure Server

Communication between the Cisco MSE, the Cisco Prime Infrastructure, and the Cisco WLC 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 Cisco WLC, Cisco Prime Infrastructure, and the Cisco MSE.

The Cisco MSE and its associated controllers must be mapped to the same NTP server and the same Cisco Prime Infrastructure server.

Local time zones can be configured on a Cisco MSE to assist the network operations center personnel in locate 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 https://www.cisco.com/en/US/products/ps9742/prod_installation_guides_list.html

Default Root Password

You must change the default root password of the Cisco MSE while running the automatic installation script to ensure optimum network security.

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

Note During 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 Cisco Prime Infrastructure Communication Username and Password by Using Cisco MSE setup.sh

You can configure the Cisco Prime Infrastructure communication password by using the Cisco MSE setup.sh script file.

The scenarios which you might encounter while configuring the Cisco Prime Infrastructure password are as follows:

- By default, the username used by Cisco Prime Infrastructure to communicate with Cisco MSE is “admin”.
- The username/password used by Cisco Prime Infrastructure to communicate with Cisco MSE can be updated from the Prime user interface only. The setup.sh script only allows changes to the Cisco Prime Infrastructure communication password associated with the username “admin”. If you change the username that is used by Cisco Prime Infrastructure to a username other than “admin” then the password changes made via setup.sh are not effective.
- If you configure a new Cisco Prime Infrastructure password, the password provided is applicable for the Cisco Prime Infrastructure username: admin.

Note The Cisco Prime Infrastructure communication users are API users, and they do not have corresponding operating system users on the Cisco MSE appliance.

Configuration Changes for Greater Location Accuracy

In some RF environments, where location accuracy is around 60 to 70 percentage or where incorrect client or tag floor location map placements occur, you might have to modify the moment RSSI thresholds in the **Context Aware Service > Advanced > Location Parameters** page on the Cisco 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

Contact Cisco TAC for assistance in modifying these parameters.

Wireless Security Module with Cisco Aironet 3600 and 3700 Series Access Points

If you are attempting to deploy Wireless Security Module (WSM) with Cisco Aironet 3600 and 3700 Series APs, then APs should be placed in monitor mode with both submode wIPS and advanced wIPS engine enabled on the Cisco Prime Infrastructure.

AeroScout Engine Module Changes

Starting Release 7.5, the AeroScout engine module is removed from both the Cisco CMX 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 AeroScout engine is removed and by default, the Cisco Tag Engine is started as part of Cisco CMX. If you do not agree to remove the AeroScout engine, the installation will exit.

Ports to be Opened for High Availability Between Cisco MSEs

The following is the list of ports to be opened for High Availability between Cisco MSEs:

- tcp 22
- tcp 80
- tcp 443
- tcp 1411
- tcp 1521
- tcp 1522
- tcp 1523
- tcp 1524
- tcp 1525
- tcp 1621
- tcp 1622
- tcp 1623
- tcp 1624
- tcp 1625
- tcp 8001
- tcp 8080
- tcp 8081
- tcp 9006
- tcp 15080
- tcp 59000
- tcp 61617
- udp 12091

Northbound Notification Name Issue

- (CSCvd80611) When adding a Northbound Notification, do not include a period in the notification name (for example, *Northbound.Msg* or *notification.aeroscout.1*). Notification names with a period cannot be deleted.

Operational Notes for Context-Aware Service

This section lists the operational notes for a Cisco MSE and contains the following topics:

Synchronization Required When Upgrading to Release 8.0.130.0 or Later, or When Importing CAD Floor Images

When upgrading to Release 8.0.130.0 or later from Release 7.x, you must synchronize after the software upgrade and when CAD-generated floor images are imported into the Cisco Prime Infrastructure.

Floor Change or Minimum Distance for Location Transitions to Post to 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

The Cisco MSE does not support non-Cisco CX Wi-Fi tags. Additionally, these non-compliant tags are not used in location calculations or shown on the Cisco Prime Infrastructure maps.

Cisco Compatible Extensions Version

Only Cisco CX Version 1 or later tags can be used in location calculations and mapped in the Cisco Prime Infrastructure.

Monitoring Information

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

Calibration Models and Data

Calibration models always apply 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 8.0* for more information about 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 8.0*.

See **Services > Mobility Services >** D**evice Name > Context Aware Service > Advanced > Location Parameters**.

Location History Time Stamps

The Cisco Prime Infrastructure time stamp is based on the browser location and not on the Cisco MSE settings. Changing the time zone on the Cisco Prime Infrastructure or on the Cisco MSE does not change the time stamp for the location history.

Tablets and Smartphones with Limited Probe Requests

Many tablets, 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 devices by using RSSI readings is not always optimal.

Repeat Use of FloorIDs

In the relevant CAS API, the use of the parameter FLOORID is not guaranteed to return the same value on consecutive calls. It may get changed by such activities as resynchronizing the Cisco MSE. Instead, the parameter FLOORAESUID should be used. The API call getStationHistoryListByArgs can use both parameters in Cisco MSE Release 8.0.

Operational Notes for wIPS

A wIPS profile cannot be pushed to Cisco Wireless Controller (WLC) 7.5 or earlier by using the Cisco Prime Infrastructure 1.4.x or 2.x with Cisco MSE Release 7.6.

Operational Notes for Upgrading Cisco MSE from CAS Licenses to wIPS Licenses

After converting the Context-Aware Services (CAS) licenses to Wireless Intrusion Prevention System (wIPS) licenses on the Cisco MSE, run the **chown nobody:nobody /opt/mse/logs/framework/mse-framework.log** command before restarting the Cisco MSE services.

Operational Notes for Cisco CMX Analytics

Firefox Browser

While using the newer version of Firefox browser to connect to the Cisco MSE user interface or Cisco CMX Analytics user interface, an error message appears saying “Peer’s certificate has an invalid signature”. For more information on how to fix this, see https://support.mozilla.org/en-US/questions/776144.

To fix this, follow these steps:

Step 1 Open Firefox browser.

Step 2 Enter **`about:config`** in the address bar.

Step 3 Enter **`browser.xul`** in the Filter field.

Step 4 Verify if the **`browser.xul.error_pages.expert_bad_cert`** property exists with a value of false.

Step 5 Right-click **`browser.xul.error_pages.expert_bad_cert`** and select **Toggle**. The value will change to true.

Step 6 Exit from Firefox.

Step 7 Launch Firefox again and try the Cisco CMX Analytics user interface. You will be asked to add the exception.

WebGL Compatibility

The Cisco CMX Analytics in Release 8.0 the provides ability to view the analytic results in both 2D (Open Street Maps) and 3D Web Graphics Library (WebGL) environments. This provides improved understanding of results on multiple floor paths or when dwell times are calculated throughout a multistory building. The 3D environment presents the same information as the 2D environment.

WebGL is an advanced feature that provides graphic capabilities. All browsers 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.

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

If your browser does not support WebGL, perform the following actions:

Step 1 Update your latest drivers for video card.

Step 2 For Google Chrome, follow the instructions given for WebGL and 3D Graphics in the Google Chrome support website.

Step 3 Enable WebGL:

- For Firefox, follow these steps:
  1. Download the latest build of Firefox browser and launch Firefox on your computer.
  2. In the browser address bar, enter **about:config**.
  3. In the Search text field, enter **webgl** to filter the settings.
  4. Double-click **webgl.enabled_for_all_sites**.
  5. Set **webgl.enabled_for_all_sites=true**.
- For Safari, follow these steps:
  1. Choose **Safari** > **Preferences**.
  2. Click the **Advanced** tab.
  3. Check the **Show Develop menu in menu bar** check box.
  4. Choose **Enable WebGL** from the Develop menu.

JBoss Issue

Sometimes, the Cisco 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, perform the following actions:

Step 1 Stop Cisco CMX Analytics service from the Cisco Prime Infrastructure.

Step 2 Kill the Jboss process.

Step 3 Run the **chown -R nobody:nobody /opt/mse/analytics** command.

Step 4 Start Cisco CMX Analytics service from the Cisco Prime Infrastructure.

Operational Notes for Facebook Wi-Fi

When you try to pair a location with the Facebook page, it may fail with no notification in Connect and Engage user interface. One of the reasons could be due to Facebook site outage. You can check Facebook API health at: https://developers.facebook.com/status/

Operational Notes for Cisco CMX Connect and Engage

- (CSCve73287) The default setting of Cisco CMX Connect allows for a maximum of approximately two clients per second continuously, a higher number can be achieved at peak (for example 4,000 HTTP connections can be made during a 5-minute window). In additional, special configuration changes can be made to increase this rate. Contact Cisco Technical Support for these recommendations. The information in the *Cisco Mobility Services Engine Ordering and Licensing Guide (up to Release 8.0 software)* incorrectly states that Cisco CMX supports 45 logins per second.
- While upgrading the Cisco Prime Infrastructure server, the map IDs and the information also get updated. This results in new identifiers for maps. The new identifiers are not automatically synchronized with the Cisco CMX Connect and Engage. This causes the location updates to use the new identifiers, but the Cisco CMX Connect and Engage will not be aware of the new identifiers and cause the location updates to get ignored. To resolve this issue, you must update maps in the Cisco CMX Connect and Engage user interface. To update maps, log in to the Cisco CMX Connect and Engage user interface and choose **Maps** from the left sidebar menu and click **Update Maps from Cisco Prime Infrastructure**.

Operational Notes for Mobile SDK

Two different venues with the same Cisco MSEs receiving location updates result in the device location bouncing from one venue to another venue. The Mobile Application Server (MAS) receives updates and changes the location to the most recent update received. The client location then changes from the most recent location update, which can be from either venue.

Operational Notes for Cisco Access Points

- (CSCvf27150) Cisco MSE provides the following access point support:

Cisco MSE Model	Location	wIPS
MSE 3365 (physical appliance)	5000 APs	10000 APs
MSE 3355 (physical appliance)	2500 APs	6000 APs
High-End MSE virtual appliance (vMSE)	5000 APs	10000 APs
Standard vMSE	2500 APs	6000 APs
Low-End vMSE	200 APs	2000 APs

For more information, see the *Cisco Mobility Services Engine Ordering and Licensing Guide (up to Release 8.0 software)*:
https://www.cisco.com/c/en/us/products/collateral/wireless/mobility-services-engine/data_sheet_c07-473865.html

- (CSCvf04279) The Cisco MSE internal-3800-5GHz antenna pattern is not compatible with the 2.4 Ghz band in Cisco 3800 access points, This combination results in this error message:

```
09:02:23.550 ERROR[location] [97]
AesLocationMathJavaBuilder#generateAlarmsAndEventForErrors Antenna Pattern:
Internal-3800-5GHz unknown, no heatmap generated for AP Interface:
28:6f:7f:32:e0:a0-2.4-0
```

The supported antenna patterns are:

- AIR-ANT-LOC-01
- AIR-ANT-LOC-01-2.4GHz
- AIR-ANT-LOC-01-5GHz

The supported band and antenna combinations are:

Slot	Band	Protocol Heatmap
0	2.4G	a/b/g/n Internal-Dual-2.4G
0	5G	a/n Internal-Dual-5G
1	5G	a/n Internal-3800-5G

- (CSCvd79048) Cisco MSE Release 8.0.x does not support Cisco Hyperlocation running on the Cisco 3800 access points.

Enabling Root Access Control in HA Mode

To enable Root Access Control (RAC) in HA mode, you need to enable RAC on both the primary and secondary Cisco MSEs. The RAC configuration is not synchronized across the primary and secondary servers. Therefore, you should enable it on both servers. This will enable the RAC configuration to work on the active server in case of a failover or failback.

Resynchronizing Cisco WLC to Cisco MSE After an Upgrade

After upgrading Cisco Prime Infrastructure or Cisco MSE, in some cases, the NMSP sync between the controllers and Cisco MSE may not work properly. Without performing the unsync and resync of the controllers to Cisco MSE, you may not able to push the wIPS profiles to Cisco WLC. We recommend that after you upgrade Cisco Prime Infrastructure or Cisco MSE, perform an unsync operation and then resync all the controllers with Cisco MSE.

DoD Mode Is Enabled by Default

(CSCuy95991) By default, the DoD mode is enabled on a newly installed or upgraded Cisco MSE.

When the DoD mode is enabled, the future restart date of the Cisco MSE cannot be later than 6 months.

You can disable the DoD mode, so that the future restart date of the Cisco MSE can be set up to 1 year later.

To disable the DoD mode:

1. Enter **echo “false” > /var/mse/certs/enabledod** command.
2. Restart the Cisco MSE.

Access to Cisco MSE UI

- The Cisco MSE UI can only be accessed by the users who are in the user group granted with Full Access permission. Users with only Read Access permission can use the REST APIs to pull data but cannot access the Cisco MSE UI.

Deleting Archive Logs

Do not manually delete the archive logs. Instead, use the /opt/mse/framework/bin/manualDeleteArchiveLogs.sh script to delete the archive logs.

Troubleshooting Errors While Installing Device Certificate on Cisco MSE

If you encounter the `Import Server Certificate failed.: Invalid input file` error while installing device certificate on Cisco MSE, perform the following steps:

Step 1 Combine all certificates in CA chain into single file by concatenating them (for example, ca-chain.pem).

Step 2 Combine the signed server certificate and server private key into single file by concatenating them (for example, server-cert-key.pem).

Step 3 Import the ca-chain.pem as the CA certificate.

Step 4 Import server-cert-key.pem as server certificate.

Adding New Iptables Rules to Cisco MSE

We recommend that you do not directly modify iptables, as those changes will not be retained when you restart the Cisco MSE services. Use the following procedure to add custom iptables rules.

Step 1 Create the f**older /var/mse/firewall** folder if it does not already exist:

g. Enter the **mkdir /var/mse/firewall** command.

h. Enter the **cp -f /opt/mse/framework/bin/msefirewall-dod /var/mse/firewall/** command.

i. Enter the **cp -f /opt/mse/framework/bin/msefirewall-no-dod /var/mse/firewall/** command.

j. Enter the **cp -f /opt/mse/framework/bin/msefirewall-no-dod-enablehttp /var/mse/firewall/** command.

k. Enter the **chown -R nobody:nobody /var/mse/firewall/** command.

l. Enter the **chmod -R 755 /var/mse/firewall/** command.

Step 2 In the **/var/mse/firewall/msefirewall-dod** file, add your new rule(s) just before the **DROP** rule (which is the last line in the file).

Step 3 Save the file.

Step 4 Restart the Cisco MSE services.

Caveats

Cisco Bug Search Tool

The Bug Search Tool (BST), which is the online successor to the Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat listed in this document:

1. Access the BST (use your Cisco user ID and password) at https://tools.cisco.com/bugsearch/.
2. Enter the bug ID in the **Search For:** field.

Open Caveats

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the "Cisco Bug Search Tool" section on page 33.

Identifier	Description
CSCvf61009	MSE not sending API response to PI for client location
CSCvf63223	wIPS Core Dumps in MSE 8.0.140.0
CSCvf84519	Controller cannot be added to MSE
CSCvf94799	The data on WIPS and AP not matching.
CSCvg05875	Exclude probing filter doesn't work with 50k clients causing db sluggishness
CSCvg22183	Evaluation of mse for Dnsmasq October 2017 vulnerabilities
CSCvg25734	Evaluation of mse for Apache Tomcat October 2017 Vulnerability
CSCvg26001	wIPS Report to Prime Infrastructure Defective
CSCvg38343	Archive log clean failure in HA setup on MSE 8.0.140.9
CSCvg40872	MSE affected by Linux kernel vulnerability

Resolved Caveats in Cisco MSE Release 8.0.150.0

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the "Cisco Bug Search Tool" section on page 33.

Identifier	Description
CSCut83666	BEAST Vulnerability on MSE (CVE-2011-3389)
CSCuz25921	wIPS profile push fails when a previously CAS box is re-used for WIPS
CSCvb48592	Evaluation of mse for Openssl September 2016
CSCvc94636	Evaluation of mse for OpenSSL Jan 2017
CSCvd72187	Evaluation of mse for NTP March 2017
CSCve01151	Unable to login to MSE GUI or add the MSE to Prime
CSCve27795	Logs in Oracle DB incident folder stall the MSE
CSCve33481	NG3K: NMSP for wired fails with SSL23_GET_CLIENT_HELLO:unknown protocol
CSCvf04279	MSE: 8.0.140.9 HEATMAP_CALCULATION_ERROR
CSCvf23034	MSE IPtable changes are not saved after services are restarted
CSCvf38803	3365 Fresh Installation hangs in Middle with 8.0 MSE builds.
CSCvf40800	MSE 3365 is not loading maps GET tile Image returns HTTP 404
CSCvf54746	Wireless client asset information is getting deleted from the DB
CSCvf58058	MSE loc table cleanup doesn't cleanup beyond 100000 records
CSCvf95213	MSE: CVE-2015-0204 observed on TCP Port 1621

Cisco Support Community

Cisco Support Community is a forum for you to ask and answer questions, share suggestions, and collaborate with your peers. Join the forum at https://supportforums.cisco.com/index.jspa.

Related Documentation

- Cisco MSE documentation: https://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/tsd-products-support-series-home.html
- Cisco CMX documentation: https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/tsd-products-support-series-home.html
- Cisco Prime Infrastructure Online Help is available with the Cisco Prime Infrastructure product.

Communications, Services, and Additional Information

To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

To get the business impact you're looking for with the technologies that matter, visit Cisco Services.

To submit a service request, visit Cisco Support.

To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.

To obtain general networking, training, and certification titles, visit Cisco Press.

To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.
