Release Notes for Cisco CMX Release 10.4.x

First Published: November 27, 2017
Last Modified: December 12, 2017

This document describes what is new and important in Cisco Connected Mobile Experiences (Cisco CMX) Release 10.4.0 and later, and provides the system requirements and caveats. Unless otherwise noted, Cisco Connected Mobile Experiences is referred to as Cisco CMX in this document.

Contents

Cisco Systems, Inc.
www.cisco.com

Introduction to Cisco CMX Release 10.4.x

Cisco CMX Release 10.4.x is a high-performing scalable software solution that addresses the mobility services requirements of high-density Wi-Fi deployments.

This release is suitable for deployments where the following features are required:

- Detect & Locate
- Analytics
- Presence Analytics
- Connect
- Hyperlocation
- FastLocate

This release is *not* suitable for deployments where the following are required:

- Cisco Adaptive Wireless Intrusion Prevention System (aWIPS) feature
- Federal Information Processing Standard (FIPS) FIPS deployment
- Cisco Prime Infrastructure integration, specifically the ability to see Wi-Fi clients and other devices and Cisco CleanAir information in Cisco Prime Infrastructure.

What's New

Table 1   What's New in Cisco CMX Release 10.4.0

Rogue access point and rogue client support	Cisco CMX now detects and tracks rogue access points and rogue clients.
Cisco Hyperlocation mixed-mode support	Cisco CMX now supports a mixed deployment of Cisco Hyperlocation access points (AP) and non-Hyperlocation AP on the same floor map. All Cisco Hyperlocation APs must be within a contiguous area. Increased accuracy on the floor is only within the convex hull of the Hyperlocation contiguous area.
Cisco CMX FastLocate support on Cisco 2800/3800 access points	Cisco CMX FastLocate is now supported on Cisco Aironet 2800/3800 access points running Cisco Release 8.6 or later.
Notification enhancements	For the LocationUpdate notification, Cisco CMX provides a new **Status** option for the **Client** device type. Use this option to filter notifications to either associated or probing devices. If the **Status** option is not selected, the default option (**All**) is considered, and then notifications are sent for both associated and probing clients.
API version 3 support	Cisco CMX has a new active clients API version 3. Active clients API version 2 has been deprecated in this release.
Cisco CMX Cloud integration	You can now access Cisco CMX Cloud applications from Cisco CMX. Click the **Cloud Apps** option from the **Manage** tab.
Change in Cisco CMX Base License	The Cisco CMX Base License no longer provides access to Cisco CMX Hyperlocation or Partner Stream. The Cisco CMX Advanced License is required to access these services.

Table 1   *What's New in Cisco CMX Release 10.4.0*

Disabled support for CleanAir-based BLE Management	The **BLE Beacons** management page is no longer available on the Cisco CMX user interface. Beacon notifications are no longer provided. BLE beacons detected by Cisco CleanAir are displayed on Cisco CMX as interferers. BLE-related information is no longer available on the apidocs file.
Support for the Cisco Aironet 1800i Access Point and the Cisco Aironet 1800s Wireless Network Sensor	Cisco CMX now supports the Cisco Aironet 1800i Access Point and the Cisco Aironet 1800s Wireless Network Sensor.

Supported Platforms

Cisco CMX Release 10.4.x can be installed on these platforms:

- Cisco MSE 3365
- Cisco MSE 3355

Cisco CMX Release 10.4.x can be installed as a Virtual Cisco MSE appliance, which requires either VMware ESXi 5.1 to ESXi 6.5 versions, or Microsoft Hyper-V. For information about installing a Cisco MSE Virtual Appliance, see the Cisco MSE Virtual Appliance Installation Guide at:

https://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/products-installation-guides-list.html

Table 2 lists the Cisco CMX Release 10.4.x hardware guidelines for a virtual Cisco MSE appliance, such as VMWare or Microsoft Hyper-V. For complete requirements, see the *Cisco Connected Mobile Experiences Data Sheet* at:

https://www.cisco.com/c/en/us/solutions/enterprise-networks/connected-mobile-experiences/white-paper-listing.html

Table 2   *Hardware Guidelines*

Hardware Platform	Low-End Appliance	Standard Appliance	High-End Appliance
CPU	8 vCPU \ 4 physical cores	16 vCPU \ 8 physical cores	20vCPU \ 10 physical cores
RAM	24 GB RAM	48 GB RAM	64 GB RAM
HDD	500 GB HD	500 GB HD	1TB HD

Requirements

> **Note**
> - Before you deploy Cisco CMX, we strongly recommend that you refer to the VM sizing guidelines described in the *Cisco CMX Dimensioning Calculator* at:
> http://calculator.cmxcisco.com/aspnet_client/system_web/2_0_50727/CMX_calculator_v2.07/CMX_calculator_v2.07.aspx
>
> - For information about system scaling, see the *Cisco Connected Mobile Experiences Data Sheet* at:
> https://www.cisco.com/c/en/us/solutions/enterprise-networks/connected-mobile-experiences/white-paper-listing.html

- Cisco CMX Release 10.4.x (which includes Cisco CMX Location, Connect, and Configuration APIs) has been tested using Google Chrome 50 to 56.

- Cisco CMX supports input and output only in English.

- For compatibility information, see the "Cisco Connected Mobile Experiences (CMX) Compatibility Matrix" section in the *Cisco Wireless Solutions Software Compatibility Matrix* at:
https://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html

- (CSCvf91346) Cisco CMX Release 10.4 feature parity with Cisco Prime Infrastructure and Cisco MSE:

> **Note** By default, Cisco Prime Infrastructure maps—including client location and client counts—refresh every 2 minutes. To manually refresh, click **Refresh** on the user interface.

Table 3   Cisco CMX Release 10.4 Feature Parity with Cisco Prime Infrastructure and Cisco MSE

Feature	Cisco CMX-Cisco Prime Infrastructure	Cisco MSE-Cisco Prime Infrastructure
Supported releases	• Cisco CMX Release 10.4 and later • Cisco Prime Infrastructure Release 3.2 and later	• Cisco MSE Release 8.0.x • All Cisco Prime Infrastructure releases
High Availability (HA)	Not supported	Supported
RFID tags, wireless-connected clients, interferers	• RFID tags i are not displayed. • Wireless-associated clients are supported.[1] • Probing clients are supported.[1] • Rogue API clients are not supported. • Interferences on Cisco Prime Infrastructure Release 3.2 is supported.	• RFID tags are displayed. • Wireless-associated clients are supported. • Probing clients are supported. • Interferences on Cisco Prime Infrastructure Release 3.2 is supported.

Table 3 *Cisco CMX Release 10.4 Feature Parity with Cisco Prime Infrastructure and Cisco MSE*

Feature	Cisco CMX-Cisco Prime Infrastructure	Cisco MSE-Cisco Prime Infrastructure
Cisco CMX APIs used by Cisco Prime Infrastructure	• Use the /api/config/v1/version/image API to display the Cisco CMX version. • Use the /api/config/v1/campuses/import API to import a map file to Cisco CMX.	• Use the /api/config/v1/version/image API to display the Cisco CMX version. • Use the /api/config/v1/campuses/import API to import a map file to Cisco CMX.
Cisco Prime Infrastructure performs the Cisco CMX API query when the Cisco Prime Infrastructure Map page is displayed.	Supported	Supported

1. Requires Cisco CMX Release 10.4 or later and Cisco Prime Infrastructure Release 3.2 or later.

Licensing Information

Cisco CMX License	Features
Base	• RSSI Location Calculation • GUI access to DETECT, MANAGE, and SYSTEM Tabs
Advanced	• Cisco CMX Base License features • Cisco Hyperlocation • Full GUI access • Connect Services, Presence Analytics Services, Location Analytics Services, and exposed raw RSSI for Wi-Fi tags only • Access to Partner Stream

- The Cisco CMX Evaluation License provides full functionality for a period of 120 days. The countdown starts when you start Cisco CMX and enable a service.

  Two weeks before the evaluation license expires, you will receive a daily alert to obtain a permanent license. If the evaluation license expires, you will not be able to access the Cisco CMX GUI or APIs. Cisco CMX will continue to run in the background and collect data until you add a permanent license and regain access to it.

- The Cisco CMX Base License no longer provides access to Cisco CMX Hyperlocation or Partner Stream. The Cisco CMX Advanced License is required to access these services.

- Cisco CMX now includes license changes that warn that the use of Cisco Hyperlocation capabilities requires the Cisco CMX Advanced License. If you have any questions about licensing, contact your Cisco account team.

- The High-Availability feature on Cisco CMX Release 10.4.x is part of the Cisco CMX Release 10.4.x "CMX Base" license, which you would install on the primary HA server. The secondary HA server automatically receives a copy of the Cisco CMX license during sync up. There is no HA-specific license to install.

- You can add any license file from Cisco CMX Release 10.0 or later to Cisco CMX Release 10.4.x.

- For information about procuring Cisco CMX licenses, see the *Cisco Connected Mobile Experiences (CMX) Version 10 Ordering and Licensing Guide* for this release at:
https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/connected-mobile-experiences/guide-c07-734430.html

- For information about adding and deleting licenses, see the "Managing Licenses" section in the *Cisco Connected Mobile Experiences Configuration Guide* for this release at:
https://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/products-installation-and-configuration-guides-list.html

Upgrading Information

⚠️

Caution (CSCvf71126) When you upgrade to Cisco CMX Release 10.4.x, the old InfluxDB database is deleted.

- Downgrading from Cisco CMX Release 10.4.x to any release is not supported.

- Anticipate an increase in the client count if you upgrade from Cisco CMX Release 10.2.1 to Cisco CMX Release 10.3.0 (CSCux31137) or if you upgrade from Cisco CMX Release 10.2.3 to Cisco CMX Release 10.3.0 (CSCvd15253). This is due to the way Cisco CMX Release 10.3.0 counts visits to different areas. For more details, see the Analytics Documentation that is available from the UI on Cisco CMX Release 10.3.0.

- There are three ways to upgrade from Cisco CMX Release 10.x to Cisco CMX Release 10.4.x:

  – Option 1: Copy the Cisco CMX image to the Cisco CMX node, and then use the **cmxos upgrade** *<cmx-file>* command from the command line to perform the upgrade.

  – Option 2: Use the web installer on port 1984, and choose **Remote File** to download the Cisco CMX image from a hosted site, for example, the Cisco CMX image could be placed on an internal web server for the download.

  – Option 3: Use the web installer on port 1984, and choose **Local File** to upload the Cisco CMX image from your local machine through the web browser.

  ✎

  Note We recommend that you use Option 1.

  With Option 3, the upload of the Cisco CMX image might fail. This is due to a memory leak in a third-party library used in the installer. However, this library is fixed in subsequent versions of the installer.

  However, if you chose Option 3 and the upload fails, restart the installer program by using the **cmxos adminui stop** command and then the **cmxos adminui start** command. Option 3 might succeed after several tries.

- For information about upgrading from an earlier Cisco CMX release to a later release, see the applicable to *Cisco Mobility Services Engine Virtual Appliance Installation Guide for Cisco CMX* at:
https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-installation-guides-list.html

- For information about upgrading from Cisco MSE Release 8.x to Cisco CMX Release 10.x, see the applicable *Release Notes for Cisco Mobility Services Engine, Release 8.0.x* at:
  https://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/products-release-notes-list.html

  – We recommend that you run Cisco CMX Release 10.4.x in parallel with the existing Cisco MSE Release 8.0 or earlier, and utilize the evaluation license for 120 days. After the evaluation period, the older Cisco MSE release can be decommissioned.

  – No database migration or inline upgrade is supported from Cisco MSE Release 8.0 or earlier to Cisco CMX Release 10.4.x.

Important Notes

- Cisco CMX Release 10.4.x supports the Cisco Mobility Express wireless network solution.

- Cisco CMX requires interaction with Cisco Prime Infrastructure only during the initial installation stage. After the maps and controllers are imported, Cisco CMX and Cisco Prime Infrastructure do not have any run-time dependencies.

- Do not use Internet Explorer 8.0 to edit the Cisco Wireless Controller's (WLC) SNMPv3 credentials. Use Google Chrome 50 to 56.

- The Cisco FlexConnect feature does not support DNS ACL and as such you cannot use DNS ACLs when configuring Cisco CMX Connect and Engage.

- The SSL mode is enabled by default.

  – To use the Cisco CMX Connect portal page in HTTP, disable the SSL mode by entering the **cmxctl node sslmode disable** command.

  – If SSL is enabled and you enable HTTPS for Cisco CMX Analytics (generally, Cisco CMX as a whole), make sure that a valid SSL certificate is installed. Otherwise, slower UI performance will occur.

    If you do not have a valid SSL certificate to install, you need a self-signed certificate.

    If neither a valid SSL certificate nor a self-signed certificate is present, Cisco CMX Analytics might not work as expected.

  For information on installing a certificate, see the "Importing Certificates" section in the *Cisco Connected Mobile Experiences Configuration Guide* for this release at:
  https://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/products-installation-and-configuration-guides-list.html

- Observe disk space utilization by going to the **Overall Disk Usage** section in **Metrics** from the **Systems** tab. For information about increasing hard disk space, see the "Increasing the Hard Disk Space" section in the "Performing Administrative Tasks" chapter in the *Cisco Connected Mobile Experiences Configuration Guide* for this release at:
  https://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/products-installation-and-configuration-guides-list.html

- When more than 85 percent of the disk space is consumed, all the Cisco CMX services shut down. For information about how to care of this issue, see the "Troubleshooting Cisco CMX Server Shutdown Problems" section in the "Performing Administrative Tasks" chapter in the *Cisco Connected Mobile Experiences Configuration Guide* for this release at: https://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/products-installation-and-configuration-guides-list.html

- (CSCuw73675) For security reasons, Cisco CMX Release 10.3.0 blocks a list of ports, such as port 5555.

- (CSCuz66192) The Cisco CMX Release 10.3.1 provides an **ftp** command to transfer files to and from a Cisco CMX server.

- (CSCva36827) Instead of the /api/location/v2/clients API or /api/location/v2/clients/ API, use the /api/location/v1/clients API to get a report on the number of active clients.

- (CSCvc36715) We recommend that you monitor your northbound notifications by clicking **Details** from the **Notifications** window. Make sure that the value in the **Send Rate (per sec)** column does not exceed 500. This value represents the number of notifications sent per second.

  A value that exceeds 500 can cause network latency and you might observe a drop in notifications. To reduce this value, configure the notification to send fewer updates (for example, send updates for only specific floors) or use a movement notification that only sends updates when a device moves a certain distance.

- (CSCvc44074) Cisco CMX tracks up to 100,000 devices. Tracking beyond this recommended limit can cause an outage of the Cisco CMX Analytics service. If this occurs, restart Cisco CMX after the number of tracked devices decrease to less than 100,000 devices.

- (CSCvc89944) If the hostname of Cisco CMX is changed using the **cmxos reconfigure** command, and then changed back to localhost.localdomain, the following error is displayed:

  ```
  1 assert/signal failures have occurred;  MATLAB will abort in 10 seconds.
  ```

  This is because the Cisco CMX agent cannot start the Matlab package. Use the following commands to resolve this:

  cmxctl stop -a

  cmxctl agent start

  cmxctl start

- (CSCvc94895) Cisco CMX supports Google Earth coordinates on imported maps from Cisco Prime Infrastructure. Use the Cisco CMX **/api/config/v1/maps/** REST API to verify the GPS coordinates on Cisco CMX floor maps, and then use the Cisco CMX **/api/location/v2/clients** REST API to check that the GPS coordinates are available for the devices. For information about adding GPS markers, see the Cisco Prime Infrastructure documentation.

- (CSCvd17090) In Cisco CMX Release 10.3.0, the dwell-time calculation is improved to provide a more accurate total duration value. The dwell time is now based on the median values of the different types of visits (repeat or new, and associated or probing). For more information, see the Analytics Documentation and Definitions Online Help available in the Cisco CMX user interface. Choose **Documentation** from the **admin** drop-down list, and then click **Analytics Documentation and Definitions**.

- (CSCvd17114) Cisco CMX uses the Apache Cassandra database to store location history, raw visits for the Analytics service, and user statistics for the Connect service. Cassandra provides fast read and write performance by writing its data to a memcache, which is periodically written to disk. When the memtable contents exceed a configurable threshold, the memtable data, which includes indexes, is put in a queue to be flushed to disk. If the data to be flushed exceeds the queue size, Cassandra blocks writes until the next flush succeeds. Note that the timing of such memtable flushes would vary from installation to installation.

  Blocked writes to the Cassandra database can result in errors in Cisco CMX, such as this analytics error message:

  ```
  2017-02-14T20:27:26,258 [Thread-57] ERROR
  com.cisco.mse.analytics.aggregation.processing.AggregationProcessor - AP-009: Error
  updating visits: RVP-005: Could not merge redis + db data: Error while accessing
  database....
  ```

  You can prevent untimely memtable flushes by scheduling the flush during off-peak hours and running the **/opt/apache-cassandra-2.1.13/bin/nodetool flush** command.

- (CSCvd21695) Image tiling can take a few seconds to complete if images need to first be converted to RGB. Once the tiling completes, the image properly displays on the user interface.

  If an imported floor map image is not an RGB/Truecolor image, Cisco CMX might take longer to prepare its image tiles, causing the floor map image to not display immediately after being imported. While the tiling process is in progress, the **Detect and Locate** window displays this warning message: `This image is currently being processed, it will be ready for viewing shortly.`

- (CSCvd29399) In Cisco CMX Release 10.3.1, the **Compare Data to** and the **Hourly Trend** views shown on **Analytics > Realtime** were removed.

- (CSCvd31309) If you have the High Availability feature configured on Cisco CMX Release 10.3.x and you initiate a failback, the following message is displayed in the Cisco CMX Location service /opt/cmx/var/log/location/error.log file:

  ```
  2017-04-26T12:54:31,646
  [location:post.calculation.persistence:PostCalcPersistence:479] ERROR
  com.cisco.mse.location.intf.PostCalcPersistence - Failed to add history exception
  {}com.datastax.driver.core.exceptions.UnavailableException: Not enough replica
  available for query at consistency ONE (1 required but only 0 alive)
  . . .
  ```

  This message is non-fatal and correlates to the period of time when Cisco CMX is configuring the primary server to take control again.

- Initial HA configuration is dependent on data size. For example, for 5 GB of data, initial configuration could take up to 1 hour to complete.

  The average time for a failover condition is 7 minutes, depending on your systems.

  The failback time is dependent on the amount of data to resynchronize. For example, for 5 GB of data, the expected time for failback to complete is 1.5 hours.

- (CSCvd35578) When you import a new or existing map containing zones from Cisco Prime Infrastructure to Cisco CMX Release 10.3.0, make sure that you check the **Delete & replace existing zones** check box. Even if you are updating a map that was previously imported, check the **Delete & replace existing zones** check box.

- (CSCvd41641) Data loss will occur with the Cassandra database when restoring data with Cisco CMX Release 10.2.3 and earlier. We recommend upgrading to and using Cisco CMX Release 10.3.0 to successfully restore data from a previously made backup.

  For backup and restore information, see the "Performing Administrative Tasks" chapter in the *Cisco Connected Mobile Experiences Configuration Guide* for this release at:
  https://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/products-installation-and-configuration-guides-list.html

- (CSCvd53632) Restoring Cisco CMX data must be done on a device that has the same local time as the device from which the data is collected. Otherwise, you will not be able to correctly access the analytics data. In addition, the data will result in errors or zero values on reports.

- (CSCvd70133) To turn off Analytics SSID filtering from the **SSID Filter** window (**Analytics > Settings > SSID Filter**), make sure no SSIDs are in the **Excluded SSID** list.

- (CSCvd73907) In certain situations, such as high traffic for the day, all visitors for that day, including new ones, are added to the collection of repeat visitors before the data for that day has been aggregated completely. This results in the visitor count showing 100% repeat visitors for that day.

- (CSCvd78913) Starting from Cisco CMX Release 10.3.1, you can use the **Tab** key to auto complete any Cisco CMX command in the command line interface. For example, if you enter **cmxos** and then click the **Tab** key, the CLI displays the available keywords. If you enter a partial string and then click the **Tab** key, the CLI then displays the complete string.

- (CSCvd80519) Starting from Cisco CMX Release 10.3.1, you can use the **cmxctl config analytics setNumMonthsRepeatHistory** *<number>* command to change the number of months of repeat history used and maintained by the Cisco CMX Analytics service. You do not need to restart Cisco CMX for the change to take effect.

  ✎ **Note**   If you change the repeat history setting, existing history will be deleted.

- (CSCve05677) Cisco CMX Release 10.2.x and later uses the default Cisco 3365 Mobility Services Engine (MSE) power and fan settings displayed from the Cisco Integrated Management Controller (CIMC) interface. The default power and fan settings can vary, based on the installed Cisco MSE firmware. The current firmware version has these default power and fan settings:

  – Power setting is **Power On**

  – Fan setting is **Balanced**

- (CSCve09739) The time ranges used as parameters with Analytics REST APIs must be from the list of predefined values displayed from **Analytics > Settings > Global TimeRanges**. Time ranges use the 24-hour format (HH:mm-HH:mm).

- (CSCve13731) Use the **System > Presence Metrics** window and the **System > Metrics > System Summary** window to understand the overall Cisco CMX system health. Changes in normal patterns, such as unusual spikes, could indicate network issues.

  – The P**resence Metrics** window displays the number of clients being tracked and the number of clients reported with locally administered MAC addresses.

  – The **System Summary** window displays metrics that mainly describe the incoming message rate, data persistence rate, and so on.

- (CSCve15152) If the Analytics report uses the **Summary** view with the **This Week** time frame option, the **Daily Trend** chart will only show data points for the days of the week that have been completed. For example, on Monday, no data points will appear on the **Daily Trend** chart because Monday is considered the first day of the week and the day has not yet completed. If you want to display a breakdown of the data for the day, use the **Chart** or **Table** view to display details by a different granularity.

- (CSCve19090) If you perform an online backup of a Cisco CMX server, the backup might fail if a change to the system occurs during the backup. If a backup fails, try again during an off-peak period when there is low activity on the server. If the backup still fails, turn off the Cisco CMX services and then perform the backup offline.

  Note If HA is configured, first disable HA and then turn off the Cisco CMX services.

- (CSCve24919) When generating a map report, we recommend that the number of floors that you select not exceed **100**. Use tags to restrict the data gathered by the report. If you exceed the recommended amount, the report might not generate and an error message might be displayed.

- (CSCve28851) Ignore this error message:

  ```
  ERROR com.cisco.mse.matlabengine.heatmap.BaseMatlabHeatmapBuilder -
  MatlabHeatmapBuilder#createApInterfaceHeatmap Number of heavy walls used by Matlab:
  <nn> not equal to count reported by Java: <nn> during heatmap calculation for AP
  Interface: 88:f0:31:08:06:70-5.0-2.
  ```

  The heatmaps are correctly generated and stored.

  This error occurs because MATLAB only counts heavy walls for location calculation, while Java counts all obstacles on the floor map.

- (CSCve35205) Cisco CMX continuously updates the client count; therefore each time you call the /api/location/v2/clients/count GET REST API, the API returns a different result.

- (CSCve37513) Cisco CMX detects the same sources of interferences as the Cisco CleanAir system. For more information, see the "Configuring Cisco CleanAir on the Cisco Wireless LAN Controller (GUI)" section in the "Wireless Quality of Service" chapter of the *Cisco Wireless Controller Configuration Guide, Release 8.4* at: https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-4/config-guide/b_cg84/wireless_quality_of_service.html#ID51

  – Bluetooth Paging Inquiry—A Bluetooth discovery (802.11b/g/n only)

  – Bluetooth Sco Acl—A Bluetooth link (802.11b/g/n only)

  – Generic DECT—A digital enhanced cordless communication (DECT)-compatible phone

  – Generic TDD—A time division duplex (TDD) transmitter

  – Generic Waveform—A continuous transmitter

  – Jammer—A jamming device

  – Microwave—A microwave oven (802.11b/g/n only)

  – Canopy—A canopy bridge device

  – Spectrum 802.11 FH—An 802.11 frequency-hopping device (802.11b/g/n only)

  – Spectrum 802.11 inverted—A device using spectrally inverted Wi-Fi signals

  – Spectrum 802.11 non std channel—A device using nonstandard Wi-Fi channels

  – Spectrum 802.11 SuperG—An 802.11 SuperAG device

- Spectrum 802.15.4—An 802.15.4 device (802.11b/g/n only)

- Video Camera—An analog video camera

- WiMAX Fixed—A WiMAX fixed device (802.11a/n/ac only)

- WiMAX Mobile—A WiMAX mobile device (802.11a/n/ac only)

- XBox—A Microsoft Xbox (802.11b/g/n only)

• (CSCve39234) Use the **cmxos sysproxy** command to configure proxy settings. Do not edit the /etc/profile.d/cmxprof.sh file to configure proxy settings, because those settings will be overwritten when you upgrade Cisco CMX.

• (CSCve47829) On Cisco CMX, Redis memory is allocated based on system memory. If you try to restore data from a 64 GB machine onto a low-end 24 GB machine, downstream failures might occur.

Cisco MSE Model	RAM Allocated
Low-end MSE virtual appliance (vMSE)	24 GB
Standard vMSE	48 GB
High-End vMSE	64 GB
Cisco MSE 3365 (physical appliance)	64 GB

Table 4   Recommendations for Backup and Restore

Restore from...	Restore to...	Recommendations
Cisco MSE 3365 (physical appliance)	Standard MSE virtual appliance (vMSE)	Not recommended
Cisco MSE 3365	Low-end vMSE	Not recommended
High-end vMSE	Standard vMSE	Not recommended
High-end vMSE	Low-end vMSE	Not recommended
Standard vMSE	Low-end vMSE	Not recommended
Same machine specs	Same machine specs	OK
Low-end vMSE	Standard vMSE	OK
Low-end vMSE	High-end vMSE	OK
Low-end vMSE	Cisco MSE 3365	OK
Standard vMSE	High-end vMSE	OK
Standard vMSE	Cisco MSE 3365	OK
High-end vMSE	Cisco MSE 3365	OK unless the high-end machine has more RAM allocated than the recommended specs
Cisco MSE 3365	High-end machine	OK

Note   HA pairing checks are done for software versions and hardware specs. HA pairs should have matching CPU count, memory size, and hard drive size. They should also have the same software versions for Cisco CMX, Redis, Cassandra, and Postgres.

- (CSCve51867) The **Dwell Threshold** setting affects the **Visitors** widget but does not affect the **Dwell Time Breakdown** widget. The **Dwell Time Breakdown** widget always uses the **0 Minutes To 24 Hours** setting, and always includes stationary devices regardless of the report settings. Thus, the data in **Visitors** widget and the **Dwell Time Breakdown** widget might not match.

  For the data to match, set the **Dwell Threshold** filter either to **0 Minutes To 24 Hours** or to **No filter**, and then check the **Include stationary devices** check box.

- (CSCve56353) End users using Android devices are unable to open the landing page URL (Success Page) configured from **Connect & Engage > Connect Experiences**. In addition, the Guest Portal might also close after the end user registers. This is a known 'Redirection to Success Page' Android bug from Google. For more information, see https://support.cmxcisco.com/hc/en-us/articles/115007357987.

- (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.

- (CSCve76843) For scheduled PDF reports, there are limitations for viewing tables that have a large number of rows. These limitations do not occur for direct PDF reports that are directly downloaded.

  Note these considerations about Analytics PDF reports on Cisco CMX:

  - Scheduled PDF reports, which have widgets that use the table view and have a large number of rows, do not display long tables. Pages containing long tables appear blank.

    To view a PDF report with long tables, we recommend that you use the direct PDF download instead of a scheduled PDF report.

  - Adobe Acrobat Reader DC has a limit of pages being 200 in. and does not display tables that go over this limit. If a table in the report is larger than this limit, you will not be able to view it using Adobe Acrobat Reader DC. Other viewers without this limit, such as Chrome, do not have this problem.

  - Large tables, even if they do not reach the 200 in. limit might not be immediately viewed on Adobe Acrobat Reader DC. This can be remedied by enabling the **Show large images** and **Show art, trim, & bleed** settings. To do this, select to **Edit > Preferences > Page Display > Page Content and Information**. Check the check boxes next to **Show large images** and **Show art, trim, & bleed** settings. Click **Confirm**. You will sometimes need to uncheck the check boxes, confirm, go back, check them again, and confirm.

- (CSCve76843) Note these considerations about PDFs on Cisco CMX:

  - Download the PDF to view extremely long tables.

  - Adobe Acrobat Reader DC has a limit of pages being 200 inches, and does not display tables that go over this limit. This does not occur with other viewers such as Chrome.

  - With Adobe Acrobat Reader, sometimes if you check the **Show large images** check box and the **Show art, trim, & bleed** check box on **Edit > Preferences > Page Display > Page Content and Information**, the changes are not saved. If this occurs, uncheck the check boxes, save, and confirm. Then, check the check boxes, save, and confirm. This problem occurs in scheduled PDF reports if you change a widget to a table view and it has a lot of rows.

- (CSCve85988) **Minimum Physical APs Detection Filter**. Cisco CMX detects devices through the use of probe signals. Information sent to Cisco CMX might contain RSSI measurements from a collection of Cisco access points (APs) detecting the device. An AP is defined by a MAC address. The Minimum Physical APs Detection Filter enforces a constraint on the number of unique APs, which must detect the device with an RSSI value greater than the RSSI cutoff value. If the constraint is met, Cisco CMX considers the device detected. The default setting for the filter is 1.

  This is an example for setting the AP detection minimum to 4:

  ```
  curl -X POST -H "Content-Type: application/json" -d '{"minapwithvalidrssi":4 }'
  http://localhost/api/config/v1/filteringParams/1
  ```

- (CSCve86596) Cisco CMX Release 10.3.x does not support certificates with passphrases. If your certificate has a passphrase, use the **openssl rsa -in** *<original key file>* **-out** *<new key file>* command to remove the passphrase from the key file. Use this new key file in the procedure described in the "Importing Certificates" section in the *Cisco Connected Mobile Experiences Configuration Guide* for this release at:

  https://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/products-installation-and-configuration-guides-list.html

- (CSCvf21552) (related to CSCvf77237, CSCvf93122) Follow these best practices for integrating Cisco CMX and Cisco Prime Infrastructure Release 3.2:

  - With Cisco Prime Infrastructure Release 3.2, you can assign floors (for showing clients count and RFID tags count) one at a time to Cisco MSE Release 8.x or to Cisco CMX Release 10.3.1 and higher.

  - When importing floor maps from Cisco Prime Infrastructure Release 3.2 to Cisco CMX Release 10.3.1 and higher, either:

    – From Cisco Prime Infrastructure, select the **Delete & replace existing maps & analytics data** option to override the existing maps in Cisco CMX. Do not select this option if the existing maps are needed.

    – From Cisco Prime Infrastructure, select the **Delete & replace existing zones & analytics data** option on Cisco Prime Infrastructure to override the existing zones in Cisco CMX. Do not select this option if the existing zones are needed.

  - Make sure that no Cisco CMX campus is assigned to two or more Cisco Prime Infrastructure instances. Distinct campuses can be assigned to the same Cisco Prime Infrastructure instance or to multiple instances.

  - From Cisco Prime Infrastructure, make sure the **Include Calibration Information** option is selected before you export maps from Cisco Prime Infrastructure to Cisco CMX. Otherwise, Cisco CMX will not be able to compute the location of network elements (such as clients and interferers) on maps that have no calibration information.

- (CSCvf25629) Due to the nondeterministic nature of Wi-Fi signals from mobile devices, Cisco CMX makes a best effort in calculating and updating the location of probing wireless clients. The Wi-Fi probing behavior of each client can be different, therefore no guarantee can be made with respect to the accuracy of the client's location. For more guidance, see the "CMX Solution Components" chapter in the *Cisco Connected Mobile Experiences (CMX) CVD*:

  https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/CMX/CMX_Components.html

- (CSCvf26272) If Cisco CMX is running on a low-end machine and incoming NMSP messages exceed the queue size on the low-end machine, this message might be displayed:

```
Received AesServerMsg, BUT EXCEEEDED QUEUE SIZE LIMIT Current msg queue size: 415182
maximum msg quque size: 415181 total dropped msg count: 13622000 msg Id:
AES_NMS_INFO_MSG_sender module : NMSP service module
```

We recommend that you migrate to a high-end machine with a bigger CPU to avoid this problem.

Restarting Cisco CMX only temporarily resolves the issue.

- (CSCvf41345) Cisco CMX Connect does not maintain histories. Therefore, if you download the CSV file from Cisco CMX, information in the CSV output and the UI might not match for past dates.

- (CSCvf41362) Make sure the **Track Probing Clients** option is enabled on Cisco CMX Connect. If the number of tracked clients is more than what your machine can handle, migrate to a high-end machine. To enable this option, choose **System > Settings > Filtering**, and then check the **Exclude Probing Only clients** check box.

- (CSCvf60571) Cisco CMX does not support VMWare tools.

- (CSCvf61201) If the **Enable Location SSID Filtering** option (**System > Settings > Filtering**) is enabled, all mobile clients associated to filtered SSIDs are displayed with the **Global** location in the CSV file that you can download by selecting **Presence > Manage > Export CSV**.

Cisco CMX cannot calculate the location of clients associated to a filtered SSID and thus cannot track them. The **Global** location indicates that Cisco CMX is not able to determine the client's location.

- (CSCvf69877) If you upgrade from Cisco CMX Release 10.2.x to a later release of Cisco CMX, you might not be able to add tags to zone maps that you imported from Cisco Prime Infrastructure. If this occurs, recreate the tags for the zone maps by following these steps:

  1. From Prime Infrastructure, remove all zones from the maps that you want to export to Cisco CMX.

  2. Import the updated zone maps from Cisco Prime Infrastructure to Cisco CMX.

  3. From Cisco CMX, select **Manage > Locations**, and then click the **Tags** icon located at the top right corner of the window. This displays the **Location Tag Manager** window.

  4. From the **Location Tag Manager** window, create tags for the zone maps.

- (CSCvf77237, CSCvf93122) (related to CSCvf21552) The following are considerations when using Cisco Prime Infrastructure:

  – Cisco Prime Infrastructure Release 3.2 supports either Cisco CMX or Cisco MSE, but it does not support both at the same time.

  – Cisco Prime Infrastructure Release 3.2 synchronizes to either the Cisco CMX or Cisco MSE, but not to both at the same time.

  – Cisco Prime Infrastructure Release 3.2 directly receives data from either Cisco CMX or Cisco MSE.

  – Only data is synchronized between Cisco Prime Infrastructure and Cisco CMX. Changes to maps are not synchronized.

- If a map is modified in Cisco Prime Infrastructure, you must import the modified map to Cisco CMX. Similar with Cisco MSE.

- Cisco Prime Infrastructure Release 3.2 does not support Cisco CMX High Availability but it does support Cisco MSE High Availability.

- Cisco Prime Infrastructure Release 3.2 does not display RFID tags. Cisco CMX displays RFID tags

- (CSCvg10317) Cisco MSE virtual machine (VM) running Cisco CMX might not function properly after being powered on after a power outage. If this occurs,:

  1. Enter the **cmxctl stop –a** command to shutdown the Cisco CMX services.

  2. Enter the **cmxctl start** command to start the services.

- (CSCvg23023) Cisco Hyperlocation cannot be enabled from two Cisco CMX sessions on the same Cisco WLC.

- (CSCvg27539) When Cisco Hyperlocation is enabled on Cisco CMX Release and Cisco CMX is not receiving the Hyperlocation data (AoA packets), no alert is displayed on the user interface to indicate this condition.

- (CSCvg28274) If NMSP tunnel flapping occurs, ping an external address to check if the DNS resolution is slow. If it is slow, delete all the external DNS server entries in the **/etc/resolv.conf** file, except for the entry that maps to the localhost.

- (CSCvg31522) The Client Playback feature applies only to associated devices (clients). This feature is not applicable to RFID tabs because they are not associated devices.

- (CSCvg37621) The BLE beacon has the same characteristics as a wireless client. Thus, on Cisco CMX, the device appears to move around the map even though the device is considered stationary. The movement should be the same as a wireless client.

- (CSCvg48564) Note that due to CSCvg70464, synchronization problems can occur after changing the IP address and reenabling the High Availability (HA) feature. Refer to the CSCvg70464 bug details for further information.

  If you need to change the IP addresses of your primary or secondary Cisco CMX servers configured with the High Availability (HA) feature, follow these steps:

  1. From the Cisco CMX CLI on the primary server (as cmxadmin user), enter the **cmxha config disable** command to disable HA on servers.

  2. Enter the **cmxctl stop -a** command to shut down the Cisco CMX services.

  3. Enter the **cmxctl status** command to verify that the Cisco CMX services are not running.

     If the services are still running, enter the **cmxos kill** command to shut down the services, and then enter the **cmxctl status** command to verify the services are not running.

  4. Edit the Cassandra YAML files to update the seeds information with the correct IP address:

     /opt/cmx/sw/confd/templates/cassandra.template.yaml

     /opt/cmx/etc/cassandra/cassandra.yaml

  5. Verify the changes to the YAML files by using these command:

     egrep -i "listen_address|seeds" /opt/cmx/etc/cassandra/cassandra.yaml

     egrep -i "listen_address|seeds" /opt/cmx/sw/confd/templates/cassandra.template.yaml

  6. Enter the **cmxctl start** command to start the Cisco CMX services.

  7. From the Cisco CMX CLI on the primary server (as cmxadmin user), enter the **cmxha config enable** command to re-enable HA on the servers.

- (CSCvg68045) Cisco CMX Release 10.4.0 UI and API do not display the zone of impact for a rogue access point.

- (CSCvg72780) The **Cloud Applications** window displays BLE notifications only if you log in to Cisco CMX as an admin user. Otherwise, the **Notifications** area on the window displays as blank.

- On Cisco CMX, the NMSP keepalive task runs every 15 secs. When the task runs, Cisco CMX checks the NMSP connection status. If the status is inactive, Cisco CMX generates an alarm/email alert. When the keepalive task runs again after 15 secs, Cisco CMX finds that the NMSP connection is still down; however, Cisco CMX does not generate another alert because it had already generated one earlier.

- The GitHub version of API version 3 is supported through the Cisco DevNet Community, not by Cisco Technical Support.

- We recommend not changing the Cisco CMX time zone setting after configuring it at initial setup. Changing the time zone setting causes gaps in the analytics data. Therefore, make sure to set the correct time zone at initial setup.

  If you must change the time zone setting—for example, it was incorrectly set or the Cisco CMX server is moved to a location in another time zone or is used to manage a new location in a different time zone—know that you will not be able to accurately view analytics data from the previous time zone. Therefore, change the time zone if you also do not need the previous analytics data.

  Note We strongly recommend using the Cisco CMX CLI, not Linux commands, to change the time zone setting.

  Note Do not change the time zone setting while Cisco CMX services are running. Shut down the Cisco CMX services before changing the setting.

  To change the time zone setting from the Cisco CMX CLI:

  1. Enter the **cmxctl stop –a** command to shutdown the Cisco CMX services.
  2. Enter the **su** command to become root user.
  3. Enter the **/opt/cmx/bin/tzselect** command, and then follow the prompts to set the new time zone.
  4. Enter the **exit** command to exit root user mode, and then enter the **exit** command again to exit cmxadmin mode.
  5. Log back in to the Cisco CMX CLI, and enter the **date** command to display the new time zone setting.
  6. Enter the **cmxctl start** command to restart the 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 of 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. Perform the following task:

1. Access the BST (using your Cisco user ID and password) at:

   https://tools.cisco.com/bugsearch/

2. Enter the bug ID in the **Search For:** field.

✎
Note   Using the BST, you can also find information about the bugs that are not listed in this document.

Open Caveats

Use the BST to view the details of the caveats listed in this section. For more information about the BST, see the "Cisco Bug Search Tool" section on page 18.

Bug ID	Description
CSCvg50124	v3 API calls over VIP fail with 503 Service unavailable error after Failover
CSCvg57042	CMX Failback via ssh times out as soon as ssh session on your laptop completes
CSCvg64819	Cisco Live Cancun: HA fails over due to keepalived state set to fault; 10.3.1 CCO build
CSCvg70464	CMX HA Failure after changing CMX IPs
CSCvg81225	Backup restore failing when disk usage reaching above 80% in cmx.

Resolved Caveats in Cisco CMX Release 10.4.0

Use the BST to view the details of the caveats listed in this section. For more information about the BST, see the "Cisco Bug Search Tool" section on page 18.

Bug ID	Description
CSCvc03935	Need an API to delete access points from CMX
CSCvc50355	10.3: Upgrade failed for the setup which is having influxdb data corrupted
CSCvc83511	BLE Beacon support: Inaccurate/ incomplete data available
CSCvd12949 1	0.3: QlessException due to OOM after 5 days of longevity on L+A+C; 10.3.0-39
CSCvd52707	Location tracking : Low sampling rate with Mac filter
CSCve30802	CMX API Server support in CMX
CSCve56206	Schedule Tab on CMX Analytics 10.3 does not show report type (PDF/EXCEL/HTML)
CSCve56255	CMX10.3 Analytics GUI Schedule Tab shows \"Invalid Date\" for Start From and cannot be modified.
CSCve69480	CMX 10.3 Analytics - Excel Reports show wrong Start and End dates on yesterday, last week reports
CSCve70958	API returns incorrect information

Bug ID	Description
CSCve73287	CMX connect service concurrent client sessions need to be documented
CSCve85988	DOC: AP RSSI Filter for CMX 10.3
CSCve86596	CMX doesn't work on certificates with passphrase
CSCve99900	10.3.1: An error occurred while merging bloom filter from day 2017-06-25@Cisco Live
CSCvf08330	CMX: 10.3 Location history doesn't give Zone information
CSCvf10773	CMX import from Prime 3.2 (maps and controllers) fails on Auth handshake
CSCvf16520	CMX presence hourly passerby counts dip at 4 pm
CSCvf21552	Need to document MSE & CMX integration restrictions for PI 3.2
CSCvf23970	Increase threshold for CPU alerts in CMX
CSCvf25629	Document Analytics using probing clients in CMX releases as best effort
CSCvf60571	Need information about VMware tools support on CMX
CSCvf69877	CMX 10.3.1 Can't save tag for location zone
CSCvf75090	CMX : consul irregularly shutdown
CSCvg10317	After a power outage, a CMX VM when powered on will not get the agent running
CSCvg23023	Should not be able enable hyperlocation from two CMX for same WLC
CSCvg26224	with 35 WLC NMSP is flapping
CSCvg27539	CMX Halo- Hyperlocation The system is not providing accurate location
CSCvg27585	CMX 10.3.1 - CMX performance issue when SSID filtering and exclude probing clients used together
CSCvg28274	NMSP Tunnel flapping when DNS server does not have a mapping to actual local hostname
CSCvg31522	Play back feature not supported for RFID tags

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.

Get Cisco CMX Cloud support at: https://support.cmxcisco.com/hc/en-us

Related Documentation

For additional information on Cisco CMX, see:

- https://www.cisco.com/c/en/us/solutions/enterprise-networks/connected-mobile-experiences/index.html
- https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/tsd-products-support-series-home.html
- https://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/tsd-products-support-series-home.html
- Cisco CMX documentation embedded in the product. From the Cisco CMX user interface, choose **admin > Documentation**.

Obtain Documentation and Submit a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.