Release Notes for Cisco CMX Release 10.3.x

First Published: April 1, 2017
Last Modified: August 22, 2018

This document describes what is new and important in Cisco Connected Mobile Experiences (Cisco CMX) Release 10.3.0 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.

Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience. Do provide feedback about your experience with the Content Hub.

Contents

Cisco Systems, Inc.
www.cisco.com

Introduction to Cisco CMX Release 10.3.x

Cisco CMX Release 10.3.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 (available in Cisco CMX Release 10.2.1 and later)
- FastLocate (available in Cisco CMX Release 10.2.1 and later)

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 3.0 Infrastructure integration, specifically the ability to see Wi-Fi clients and other devices and Cisco CleanAir information in Cisco Prime 3.0. Ability to view clients will require Prime 3.2 or later

What's New

Table 1 What's New in Cisco CMX Release 10.3.1

Enhanced Cisco Hyperlocation support	Cisco Hyperlocation now supports up to 10,000 tracked devices—1000 Cisco access points (APs) with up to 10 connected clients per AP—on Cisco 3365 Mobility Services Engine (MSE) and Cisco high-end MSE Virtual Appliances (vMSE) running Cisco CMX Release 10.3.1 and later.
Northbound Notification improvements	Cisco CMX now supports absence events for RFID tags and partner streaming for up to five different receivers. This feature is further documented in the *Cisco Connected Mobile Experiences (CMX) Command Reference Guide* and *Cisco Connected Mobile Experiences REST API Guide* for this release.
Cisco 802.11ac Wave 2 Access Points support	Cisco Aironet 1540, 1552H, 1560, 1800, 1800i, 1800s, 1810, 1815, 1830, 1850, 2800, and 3800 series access points are now supported.

Table 2 What's New in Cisco CMX Release 10.3.0

Support for Cisco Aironet 1815I, 1560I, 1560E, and 1560D Access Points	Cisco CMX now supports the Cisco Aironet 1815I, and 1560 (1560I, 1560E, 1560D) Series access points.
High Availability	Cisco CMX now supports the High Availability feature. This feature involves two synchronized servers, one operating as the primary (active) server and the other operating as the standby server. If the primary server becomes unavailable, the standby server becomes the active server so that Cisco CMX services are minimally impacted. **Note** Both the primary and standby servers must have the same virtual machine size and the same Cisco MSE Virtual Appliances. **Note** Cisco CMX Release 10.3.0 supports Cisco MSE 3355. However, the HA feature in Cisco CMX Release 10.3.0 is not supported on the Cisco MSE 3355.
Repeat Visitor API	Cisco CMX now includes the Repeat Visitor API. Using this API, you can create a report displaying a 6-month history for the repeat devices.
Enhanced Licensing	When you install a Cisco CMX license for Release 10.3.0 and later, the terms and conditions are displayed. Provide your name and specifically accept the license.
Stationary Device Filtering	Cisco CMX now helps you filter out stationary devices from your analytics reports.
Enhanced Display of Status Page	Cisco CMX now supports the display of the number of heterarchy elements, access points, and active clients, as well as high-availability configuration information.
Updated Detect & Locate Window	The **Detect and Locate** window now displays GPS markers and thick walls.
GUI Configuration of Opening Hours	The **Analytics** tab now includes a screen to configure different opening hours. Up to 10 different opening hour buckets can be created.

Supported Platforms

Cisco CMX Release 10.3.x can be installed on these platforms:

- Cisco MSE 3365
- Cisco MSE 3355

Cisco CMX Release 10.3.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: http://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/products-installation-guides-list.html

Table 3 lists the Cisco CMX Release 10.3.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: http://www.cisco.com/c/en/us/solutions/enterprise-networks/connected-mobile-experiences/white-paper-listing.html

Table 3 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: http://www.cisco.com/c/en/us/solutions/enterprise-networks/connected-mobile-experiences/white-paper-listing.html

- Cisco CMX Release 10.3.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: http://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html

Upgrading Information

- Downgrading from Cisco CMX Release 10.3.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.
- (CSCvd22768) There are three options to upgrade from Cisco CMX Release 10.x to Cisco CMX Release 10.3.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 Cisco CMX Release 10.1.x or 10.2.x to Release 10.3.x, see: http://www.cisco.com/c/en/us/td/docs/wireless/mse/10-2/installation/guide/installation_guide/MSE_Installation_Using_Vsphere_Client.html#task_4139404649859663872979444825113 31
- For information about upgrading from Cisco MSE Release 8.x to Cisco CMX Release 10.3.x, see: http://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
  – We recommend that you run Cisco CMX Release 10.3.x in parallel with the existing Cisco MSE 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 8.0 or earlier to Cisco CMX Release 10.3.x.

Licensing Information

- 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 High-Availability feature on Cisco CMX Release 10.3.x is part of the Cisco CMX Release 10.3.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 10.3.x.
- For information about procuring Cisco CMX licenses, see the *Cisco Connected Mobile Experiences (CMX) Version 10 Ordering and Licensing Guide*
- 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/connected-mobile-experiences/products-installation-and-configuration-guides-list.html

Important Notes

- Cisco CMX Release 10.3.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/connected-mobile-experiences/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/connected-mobile-experiences/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/connected-mobile-experiences/products-installation-and-configuration-guides-list.html
- 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.

- (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.
- (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.

  Note (CSCvi48997) Make sure to enable TCP acknowledgments (ACKs) on the receiving end for northbound notifications.

- (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.
- (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/connected-mobile-experiences/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 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 **Presence 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.
- (CSCve30747) We recommend not using the BLE Beacon Management (**MANAGE > BLE Beacons**) feature. This feature will be deprecated in a future release.
- (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*.
  - 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 so that the settings are retained when you upgrade Cisco CMX. Do not manually edit the /etc/profile.d/cmxprof.sh file to configure proxy settings. Any changes made to the file /etc/profile.d/cmxprof.sh are not retained 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.

Machine Type	RAM Allocated
Low-end machine	24 GB
Standard machine	48 GB
High-end machine	64 GB
Cisco MSE 3365	64 GB

Table 4 Recommendations for Backup and Restore

Restore from...	Restore to...	Recommendations
Cisco MSE 3365	Standard machine	Not recommended
Cisco MSE 3365	Low-end machine	Not recommended
High-end machine	Standard machine	Not recommended
High-end machine	Low-end machine	Not recommended
Standard machine	Low-end machine	Not recommended
Same machine specs	Same machine specs	OK
Low-end machine	Standard machine	OK
Low-end machine	High-end machine	OK
Low-end machine	Cisco MSE 3365	OK
Standard machine	High-end machine	OK
Standard machine	Cisco MSE 3365	OK

Table 4 Recommendations for Backup and Restore (continued)

Restore from...	Restore to...	Recommendations
High-end machine	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.

- (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 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/connected-mobile-experiences/products-installation-and-configuration-guides-list.html

- (CSCvh13119) On Apple MacBook Pro laptops: After accepting the terms and conditions and clicking **Submit**, the Cisco CMX Portal page with the Facebook icon keeps redisplaying and does not connect to the Internet. Opening a separate browser session results in connecting to the Internet but bypasses portal authentication.

  On Apple iPads, The custom portal page appears twice before authentication is successful.

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 13.

Bug ID	Description
CSCvc03870	Location metrics required for better analysis of issues
CSCvd37155	Tag Exciter Support - does not import exciters placed on map
CSCvd56943	Interface not shown when next hop address is an Mapped IPv4 address
CSCve48059	10.3.1: Influx DB corrupt due to CMX hostname or IP address change; 10.3.1-62
CSCve71327	CMX-Location: RedisConnectionPool exception from location messing up location accuracy test
CSCve76843	CMX PDF Reports - Only first page of multi page Report in included in PDF reports
CSCve78807	CMX 10.3-1.33 Probing and connected clients show up outside of map
CSCve89764	CMX 10.3.1-35 -- Overall client count mismatch between D&L and Metrics page

Resolved Caveats in Cisco CMX Release 10.3.1

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 13.

Bug ID	Description
CSCuw32543	MSE 3365: KVM Console does not permit ENTER during ISO recovery
CSCuz66192	FTP command on CMX 10.X
CSCva79431	CMX: Terms and Conditions mandatory before we login to facebook
CSCvc28608	WLC 8540 & ME show default build version CMX 10.3
CSCvb94247	CMX 10.2.3 Static IP address is not configurable during initial setup
CSCvc12880	CMX connect does not work with https proxy to contact Twilio
CSCvc50355	10.3: Upgrade failed for the setup which is having influxdb data corrupted
CSCvc58495	CMX UI not available after upgrade from 10.2.0 or 10.2.1 to 10.2.2 or above
CSCvc85061	Number of logins per second should be documented for 10.x
CSCvc85132	CMX install should not allow to change ethernet interface name - breaks afterwards
CSCvc92819	10.3: Analytics/Location unable to fetch SSIDs after deleting snmp string from WLC
CSCvc96122	CMX Connect does not keep Border and Padding for image elements when changing the theme
CSCvd04363	PC try to access internet when add new site into CMX
CSCvd05611	connect & agent need to be restarted after failover if proxy is used to work with sms,fbwifi portal.
CSCvd07358	Map import should fail if calibration model is missing in the floor map file
CSCvd09051	Location service is Overloaded. Nmsplb sending:616 Location processing:311
CSCvd09466	NMSP goes down Intermittently on 8.2 code
CSCvd10750	10.3: CLI add controller type option need to change to match with UI option.
CSCvd12782	Serviceability: apidocs lacks example on how to format JSON array of parameters
CSCvd12949	10.3: QlessException due to OOM after 5 days of longevity on L+A+C; 10.3.0-39
CSCvd15253	Probing only clients is slightly less in 10.3 with compared to 10.2.3
CSCvd23317	10.3: Path Analysis giving zero for reports other than Today and Yesterday
CSCvd35578	10.3: importing map(having zones) to cmx doesn't import the zones by default
CSCvd41579	CMX-Location: Heatmap failed to complete calculating after CMX Failback
CSCvd52707	Location tracking : Low sampling rate with Mac filter **Note** MAC filtering requires a few seconds of computation overhead when checking a given MAC address against the lists of allowed and disallowed MAC addresses.
CSCvd53632	CiscoLive! 2017 Berlin - did backup/restore but cannot see reports
CSCvd56343	CiscoLive! 2017 Berlin - Analytics heatmap not rendering consistently.
CSCvd56447	10.3: Cassandra Db corruption after Sec reboots in the middle of HA config enable ; 10.3.0-53
CSCvd56636	10.3: Cassandra data sync from primary to secondary indefinitely; 10.3.0-53
CSCvd70133	CMX 10.3.0-50: Analytics SSID filter can't be turned off
CSCvd73907	With high number of raw visits from new visitors, analytics reports 100% repeat visitors
CSCvd73991	Same map import to CMX from PI resulting change in floorRefId/aesIdString and floor ID

Bug ID	Description
CSCvd74401	Could not edit controller if it's added using hostname
CSCvd83908	Disk size is not getting allocated to High End VM as mentioned in user guide
CSCve01572	Serviceability: CMX Client movement history time gaps
CSCve09739	Query for \"hourly\" data from the Dwelltime API does not run
CSCve16024	Special characters in analytics report title prevents job from running
CSCve27610	The excluded SSID on Location SSID filtering removed after modifying the other parameters.
CSCve34260	CMX 10 Database Exposes User Password For Mail Server
CSCve35783	CMX Connect: option to have a single checkbox needed
CSCve42950	CMX 10.3 cannot create zones for specific buildings
CSCve43973	Map import fails to handle special characters in the heterarchy string 'yw - cmx tests!@#$%^*()('
CSCve48281	CMX - Alert generated after upgrade to 10.3 - Too many elements in heterachy
CSCve43973	Map import fails to handle special characters in the heterarchy string 'yw - cmx tests!@#$%^*()('
CSCve48281	CMX - Alert generated after upgrade to 10.3 - Too many elements in heterachy
CSCve56	10.3: HA enabled failed with custom certificate used by customer; 10.3.0-62

Resolved Caveats in Cisco CMX Release 10.3.0

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 13.

Bug ID	Description
CSCux31137	10.2: CMX and WLC probing and associated client s not match
CSCuz17326	CMX 10.2.1 - Script to clear the unwanted files
CSCuz68222	CMX shouldn't use the wording NGWC
CSCva62398	UI order of hierarchy levels at Northbound Notification for Area Change
CSCva36583	/api/location/v1/history/clients API should sort in a date/time order
CSCva46690	Analytics Repeat visitor count is empty on certain floors, days
CSCva93880	CMX: 10.2.2-340 getting permission denied error for \"cmxctl debug\"
CSCvb64651	CMX email reporting unreliable
CSCvb80814	CMX get pink dots on map with Exclude Probing Clients Filter en-abled
CSCvb81056	CMX 10.2.3-34 upgrade from webgui fails
CSCvc11118	Location drops after a week of operation
CSCvc15143	Average DWELL time report not correctly displaying Daily and Weekly
CSCvc16450	CMX 10.2.3 - Cassandra issue where Analytic doesn't work after upgrade
CSCvc34851	Enhance SSID Filter for blocking hyperlocation clients
CSCvc41479	CMX 10.2.3 Scheduled One-Time Reports Do Not Show Up On Schedule Tab
CSCvc57938	CMX 10.2.3 import failed to copy image for map bundle
CSCvc61075	CMX Troubleshooting tool shows BLANK if you have empty Campuses

Bug ID	Description
CSCvc65932	Correlation chart missing devices
CSCvc70291	schedule email report take 15 hours to be received on CMX 10.2.2
CSCvc72639	CMX NMSPLB crash
CSCvc78860	Chrome cannot load campus maps because of Cross-Origin Resource Sharing
CSCvc79795	CMX Northbound Notification details have \"cisco.com\"
CSCvc83511	BLE Beacon support: Inaccurate/ incomplete data available
CSCvc88848	Filtering messages from AP not placed on the map
CSCvd06676	CMX 10.2.3 - dashboard UI analytics are not working
CSCvd09425	Client Information displaying as Blank for SSID, UserName and IP Address -41- (first seen in -29-)
CSCvd10730	CMX HA pre-pairing validation of memory, disk, etc. not appearing in UI
CSCvd11762	api to enable debug via curl for nmsplb does not work on CMX
CSCvd41641	10.3: Failed restore shows up as passed, without any error message; 10.3.0-50

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website: http://www.cisco.com/cisco/web/support/index.html.

1. Choose **Product Support > Wireless**.
2. Select your product.
3. Click **Troubleshoot and Alerts** to find information about the problem you are experiencing.

Related Documentation

For additional information on Cisco CMX, see:

- http://www.cisco.com/c/en/us/solutions/enterprise-networks/connected-mobile-experiences/index.html
- http://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/tsd-products-support-series-home.html
- http://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.