Release Notes for Cisco CMX Release 10.5.x

First Published: July 9, 2018
Last Modified: June 16, 2020

This document describes what is new and important in Cisco Connected Mobile Experiences (Cisco CMX) Release 10.5.0 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 10.5.x

Cisco CMX Release 10.5.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
- Integration with Cisco Prime Infrastructure Release 3.4 or later
- Integration with Cisco Digital Network Architecture (DNA) Center Release 2.1 or 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

What's New

Table 1 What's New in Cisco CMX Release 10.5.1

New device support	• Cisco 3375 Appliance for Cisco Connected Mobile Experiences • Cisco Catalyst 9800 Series Wireless Controller
Critical bug fixes	This release provides critical bug fixes. No features were added. We recommend this release to all Cisco CMX users.

Table 2 What's New in Cisco CMX Release 10.5.0

Data Privacy—General Data Protection Regulation (GDPR)-compliant	The Cisco CMX Data Privacy feature complies with General Data Protection Regulation (GDPR). GDPR is intended to strengthen and unify data protection for individuals. The Data Privacy feature ensures data protection by not disclosing the client identity details such as MAC address, username, and IP address.
Cisco CMX Connect Opt-In/Opt-Out	On Cisco CMX, if data privacy with MAC hashing is enabled, Cisco CMX Connect Services will have opt-in enabled by default. This means that client location is tracked and client data is stored and maintained in Cisco CMX. To disable this, the client must specifically select to opt-out.
Cisco CMX Grouping	The Cisco CMX Grouping feature enables Cisco CMX to form an Access Point (AP) group, consisting of all Cisco APs learned from maps imported from Cisco Prime Infrastructure. The Cisco WLC would then only report data for the APs in that group to Cisco CMX.

Table 2 What's New in Cisco CMX Release 10.5.0 (continued)

Enhanced History API	Cisco CMX supports the new Client History API, which allows you to collect and download history data to a file and use it offline. For additional information, see the "APIs for Exporting Large Dataset from CMX Cassandra Database" section in the *Cisco CMX REST API Guide* for this release.
OS Upgrade: CentOS 7 (1708)	Cisco CMX Release 10.5 has upgraded the OS environment to CentOS 7 (1708).
New device support	Cisco Aironet 4800 Access Points

Supported Platforms

Cisco CMX Release 10.5.x can be installed on the Cisco 3375 Appliance for Cisco Connected Mobile Experiences and the Cisco MSE 3365 platform.

Note Cisco CMX Release 10.4.x or later does not support the Cisco MSE 3355 platform.

The Cisco 3375 Appliance requires Cisco CMX Release 10.5.1 or later. For hardware and software installation information, see the *Cisco 3375 Appliance for Cisco Connected Mobile Experiences Installation Guide* at: https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-installation-guides-list.html.

Cisco CMX Release 10.5.x can be installed as a Virtual Cisco MSE appliance, which requires VMware ESXi 5.1 to ESXi 6.5 versions. 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

Note Cisco CMX does not support VMWare tools.

Table 3 lists the Cisco CMX Release 10.5.x hardware guidelines for a virtual Cisco MSE appliance, such as VMWare. 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 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	550 GB	550 GB	1TB

Requirements

Note Before you deploy Cisco CMX, we strongly recommend that you refer to the following:

- For VM sizing guidelines, see 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. Note that the calculator applies to Cisco CMX Release 10.3 or later, even though the calculator refers only to Cisco CMX Release 10.3.
- For scaling information, see the following:
  - *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 Connected Mobile Experiences (CMX) 10 Ordering and Licensing Guide* at: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/connected-mobile-experiences/guide-c07-734430.html

- Cisco CMX (which includes Cisco CMX Location, Connect, and Configuration APIs) supports Google Chrome 50 or later.

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

- 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
- Cisco Prime Infrastructure, when paired with Cisco CMX, displays client information and location but not client history.

  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 4 Cisco CMX 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 or later • Cisco Prime Infrastructure Release 3.2 or later	• Cisco MSE Release 8.0.x • All Cisco Prime Infrastructure releases
High Availability (HA)	Supported	Supported
RFID tags[1], wireless-connected clients, rogue APs, rogue clients, and interferers	• Wireless-associated clients are supported.[2] • Probing clients are supported.[2] • Rogue clients and access points are supported. • Interferers on Cisco Prime Infrastructure Release 3.2 or later is supported.	• RFID tags are displayed. • Wireless-associated clients are supported. • Probing clients are supported. • Interferers on Cisco Prime Infrastructure Release 3.2 is supported.
Client history	• Not supported. This feature is available on Cisco CMX and Cisco DNA Center Release 1.2 or later.	• Supported.
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.	—
Cisco Prime Infrastructure performs the Cisco CMX API query when the Cisco Prime Infrastructure Map page is displayed.	Supported	Supported

1. BLE tags are supported only on high-end appliances.
2. 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 for clients, tags, rogue APs, rogue clients and interferers • Data privacy opt-in/opt-out • GUI access to DETECT, MANAGE, and SYSTEM Tabs
Advanced	• Cisco CMX Base License features • Cisco Hyperlocation • Full GUI access • Cisco CMX Connect Services, Presence Analytics Services, and Location Analytics Services • Expose raw RSSI for tags through partner streaming • BLE support

- 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.
- 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 is part of the Cisco 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 or later.
- 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/connected-mobile-experiences/products-installation-and-configuration-guides-list.html

Upgrading Information

Note

- You cannot upgrade to Cisco CMX Release 10.5.x from Cisco CMX Release 10.4.x and earlier. You must install and deploy the Cisco CMX Release 10.5.x OVA or ISO file on your system.
- Before installing and deploying the Cisco CMX OVA or ISO file, back up your existing system to a safe location. After OVA or ISO deployment, you can restore your data to your system running Cisco CMX Release 10.5.x.

For complete information and procedures, see the *Cisco Mobility Services Engine Virtual Appliance Installation Guide for Cisco CMX Release 10.5*.

- Downgrading from any Cisco CMX 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.

- For information about migrating from an earlier Cisco CMX release to a later release, see the applicable *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 transitioning 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 10.5.x or later 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 10.5.x.

Important Notes

- For support on getting a Cisco CMX Beacon Management Cloud account and on using the Cisco CMX Cloud Beacon Management Service, contact beaconmanager-support@external.cisco.com.
- For support on using APIs, including the GitHub version of API version 3, contact the Cisco DevNet Community: https://developer.cisco.com/site/cmx-mobility-services/.
- The Cisco FlexConnect feature does not support DNS ACL and as such you cannot use DNS ACLs when configuring Cisco CMX Connect and Engage.
- SSL mode is mandatory with Cisco CMX Release 10.5.0 or later.
  - Use https:// to access the Cisco CMX Connect portal page. Use of http:// is no longer supported.
  - For Cisco CMX Analytics (generally, Cisco CMX as a whole), make sure that a valid SSL certificate is installed. Otherwise, slower UI performance can 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.

- Refer to the following information when backing up and restoring Cisco CMX data between the Cisco 3375 Appliance, Cisco MSE, and Cisco vMSE platforms.

Table 5 System Memory for Cisco MSE and Cisco 3375 Platforms

Cisco MSE Model	RAM Allocated
Low-end MSE virtual appliance (vMSE)	24 GB
Standard vMSE	48 GB
High-End vMSE	64 GB
Cisco 3375 Appliance and Cisco MSE 3365 (physical appliance)	64 GB

Table 6 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

Table 6 Recommendations for Backup and Restore (continued)

Restore from...	Restore to...	Recommendations
High-end vMSE	Cisco 3375 Appliance and 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.

- (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.

- (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/v3/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 was 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.`

- 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.

- (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.

- (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.
- (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 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.
- (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.

- (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
- (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.
- (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.
  - 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.
- (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 restart the services.
- (CSCvg23023) Cisco Hyperlocation cannot be enabled from two Cisco CMX sessions on the same Cisco WLC.
- (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 wireless clients (associated and probing). This feature is not applicable to other devices such as interferers, rogue devices, BLE beacons, and RFID tags.
- (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.
- (CSCvg69524) Cisco CMX displays incorrect IP address information for access points connected to a Cisco WLC with Network Address Translation (NAT) enabled.
- (CSCvg79749) In Cisco CMX Release 10.4.0, v3 Client API was introduced and v2 Client API was deprecated. We recommend that you use v3 API instead of v2 API. High CPU usage by the Cisco CMX Location service occurs when v2 API is used for a long duration, Restart the Location service to correct the condition.
- (CSCvg81107) Notification subscriptions—manually created in Cisco CMX Release 10.3.x through the **Manage** > **Notifications** window—for sending data to CMX Cloud applications need to be deleted and then recreated from the Cisco CMX **Cloud Applications** page in Cisco CMX Release 10.4.x or 10.5.x. Notification subscriptions created in Cisco CMX Release 10.3.x do not display on the **Cloud Applications** page.
- (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.
- (CSCvh82477) For Cisco CMX Release 10.5.x or later, all HTTP functions are no longer supported on Cisco CMX Connect Services.
- (CSCvi07385) With VMware vSphere ESXi 6.5 Update 2, you can successfully deploy the Cisco CMX OVA file. Update 2 displays the deployment options (**Low-end**, **Standard**, and **High-end**). Minor erroneous text such as `[object Object]` is also displayed.

  With VMware vSphere ESXi 6.5 and VMware vSphere ESXi 6.5 Update 1, the deployment options are not displayed.

- (CSCvi73412) Cisco CMX cannot connect to the Internet through the Cisco WLC Service port, because the service port does not support SNMP.
- (CSCvi84935) High CPU usage of the Cisco CMX Analytics and Location Services can occur during initial high-availability (HA) synchronization, causing the sync to not complete. If this occurs, remove the Cisco WLCs from the system to decrease the CPU usage of the Analytics Service. This provides enough memory for the initial HA sync to complete.

  We recommend that you also clean up Redis, if high memory usage occurs:

  1. **cmxctl analytics stop**
  2. **cmxctl config analytics cleanRedis**
  3. **cmxctl config qlesspyworker cleanRedis**
  4. **cmxctl analytics start**

- (CSCvj52515) There is significant overhead seen in maintaining the compact history, which allows to query the unique clients seen on a floor or zone per day. This does not affect the regular clients history that is stored in the Cassandra database.

  Note As of Cisco CMX Release 10.4.1-15, the feature flags setting is disabled by default. If your system is running an earlier release of Cisco CMX, we recommend that you disable the feature flags setting.

  To disable the feature flags setting, enter these commands:

  ```
  cmxctl config featureflags location.compactlocationhistory false
  cmxctl agent restart
  cmxctl location stop
  cmxctl location start
  ```

- (CSCvm09209) Before Cisco CMX Release 10.5.1, Cisco CMX performed the SNMP polling to populate the SSID list.

  With Cisco CMX Release 10.5.1 or later, Cisco CMX relies on WLC notification (INFO messages) to populate the SSID list. This means for an SSID to appear on Cisco CMX, the SSID must have clients associated to it. This new way of retrieving SSIDs is independent of maps on Cisco CMX. This behavior change is applicable for both Location and Analytics SSID filters on Cisco CMX.
- (CSCvm57237) In the “Clients V3 API Server User Management API” section of the online apidocs document, the **Try it** button to add a v3 user section does not work. However, the API is functional by using this curl command:

  ```
  curl -X POST -H "Content-Type:application/json" -d
  '{"username":<username>,"password":<password>}'
  http://localhost/api/config/v1/apiserver/add
  ```

- (CSCvm39027) The v3 User Management (Add, Delete) API requires the Cisco CMX Server to refresh, which could cause a minimal downtime. After the refresh completes, the v3 APIs become available.
- (CSCvn33059) When you click the **Client movement history playback** icon on the **Detect & Location > Activity Map** window, you can select up to the past 30 days to track the history of a client. This window of 30 days is independent of the Data Retention - Client History Pruning Interval.

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 17.

Bug ID	Description
CSCvj41126	CMX10.5: OI notification issues when cmx is upgraded
CSCvj93397	On demand report does not work on 10.5.
CSCvk07774	10.5 : cassandra does not start after restore for a large GB file occasionally
CSCvk66624	v3 Count API shows invalid number of clients
CSCvm39027	CMX API Server became unavailable after creating a user via POST /api/config/v1/apiserver/add
CSCvm57237	10.5.1:POST api under Clients V3 API Server User Management API doesn't work via API Documentation.
CSCvm88206	Controller edit flow overwrites the SNMP v3 details.
CSCvn33465	Hyperlocation troubleshooting tool does not work for C9800.
CSCvn35890	C9800 Controllers Stay Inactive after Importing from Prime.
CSCvn48283	CMX AP grouping with C9800 (16.x) release is not tested, hence not supported by CMX
CSCvn48300	CMX Connect portal with C9800 (16.x) is not tested, hence not supported by CMX

Resolved Caveats in Cisco CMX Release 10.5.1

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 17.

Bug ID	Description
CSCvj87527	SNMP Timeout Alerts occur every 6 hours
CSCvk40719	API server stops responding to v3 calls when v1/v2 calls reach 200 per second approx.
CSCvk50849	CMX Connect Social Oauth feature fails with new Facebook App
CSCvk53552	Nodesetup service failed on Primary converted to Secondary
CSCvk58315	CMX adding zone will stuck on GUI(shown as \"saving\" forever)
CSCvk59861	Zone of impact of Rogue AP should have a maximum
CSCvk65473	CMX XLS Report show \"Invalid date\" when selecting a custom range date
CSCvk65492	CMX Reports \"Dwell Time Breakdown\" columns in XLS doesn't show the time ranges as it does in the GUI
CSCvk74832	Incorrect version displayed on CMX for C9800
CSCvk75736	CMX Connect API with sesstion start/end returns 404 code
CSCvm16726	CMX: 10.4.1 Realtime report Chart/Table shows wrong data
CSCvm33973	CMX root password initial setup rules should explicitly list allowed special characters
CSCvm36491	CMX 10.4.1 C&E custom portal Slovak language is saved as Saraiki.
CSCvm61420	CMX - Unable to integrate C9800 with TACACS auth.
CSCvm62527	CMX 10.5 Reimporting maps is required to detect 4800 AP as hyperlocation with WLC8.8.100
CSCvm70351	AP 4800: Add to Calibration file with ch 165 for 5GHz provided by AP HW team
CSCvm95417	Alpha HA 10.5-206 can't SSH on primary server and console also fail
CSCvn64747	CMX10.5.1 fresh install fails at Configuring Network step

Resolved Caveats in Cisco CMX Release 10.5.0

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 17.

Bug ID	Description
CSCve30802	CMX API Server support in CMX
CSCve56200	10.3: HA enabled failed with custom certificate used by customer; 10.3.0-62
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
CSCvf30659	CMX 10.3.1 Multiple SSL Vulnerabilities discovered with Nessus scan
CSCvg05393	CMX 10.3.1 - Ability to delete all controllers at once using CMX GUI/CLI
CSCvg14380	CMX runs over vulnerable CentOS version
CSCvg27539	CMX will generate alarm when Hyperlocation is enabled and AoA data is not received by CMX

Bug ID	Description
CSCvg48564	CMX - It should be documented how to change IP of HA pairs
CSCvg57042	CMX Failback via ssh times out as soon as ssh session on your laptop completes
CSCvg70464	CMX HA Failure after changing CMX IPs
CSCvg79749	CMX10.3: CPU usage increased and finally location service stopped
CSCvg86733	10.4 V3 API response slowness
CSCvh07962	Fix to address issues with leaks and extend timeouts for NSMP connections
CSCvh77152	Map Import in CMX leads to loss of random floors
CSCvi08023	CMX 10.4 license Documentation update
CSCvi08263	need commands to edit cmxos apiserver user account
CSCvi08269	cmxos apiserver user account password changes when upgrading OS
CSCvi12075	Enhancement for maps update and overwrite options
CSCvi23988	CMX Reports incorrect number of Associated and Probing Clients
CSCvi24579	Redis check failed for Primary even after a restart of the agent, causing HA failover in 10.4.1-2
CSCvi48997	ACKs to be enabled on the receiving end for Northbound Notifications to work in full capacity
CSCvi77477	CMX 10.4.1 - CMX Social Oauth feature doesn't work for Facebook App
CSCvi84935	Analytics and Loc service utilizes high CPU
CSCvi90183	CMX 10.4: Mandatory services are reconfigured to NOT run if CMX 10.3 backup is restored on 10.4
CSCvi93681	CMX 10.4: Notifications being sent with same to and from address causing mail server to drop

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**.

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.