Release Notes for Cisco CMX Release 10.6.x

First Published: January 30, 2019
Last Modified: July 22, 2022

Introduction

Cisco Connected Mobile Experiences (Cisco CMX) Release 10.6.0 and later is a high-performing scalable software solution that addresses the mobility services requirements of high-density Wi-Fi deployments. Unless otherwise noted, Cisco Connected Mobile Experiences is referred to as Cisco CMX in this document.

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

- Detect and Locate
- Analytics
- Hyperlocation
- FastLocate
- Federal Information Processing Standard (FIPS) deployment
- Integration with Cisco Prime Infrastructure Release 3.4 or later
- Integration with Cisco Digital Network Architecture (DNA) Center Release 2.1 or later
- Single sign-on through Security Assertion Markup Language (SAML)

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

- Cisco Adaptive Wireless Intrusion Prevention System (aWIPS) feature

Cisco Systems, Inc.
www.cisco.com

What's New

What's New in Cisco CMX Release 10.6.2-89

This is a mandatory security patch which addresses CVE-2021-45105, CVE-2021-44228 and CVE-2021-45046 vulnerability issues in Apache log4j. This patch works for Cisco CMX Release 10.6.2-89.

You must download Cisco CMX Release 10.6.2-89 patch *cmx-log4j-vulnerability-patch-10.6.2-2.cmxp* available at Software Download page and copy the patch file to **/home/cmxadmin** directory.

Note If the *cmx-log4j-vulnerability-patch-10.6.2-1.cmxp* patch file is previously installed, ensure that you run the **cmxos patch remove** command to remove the patch before installing the new patch.

To apply this patch on Cisco CMX High Availability, you must break High Availability and rebuild it.

To install Cisco CMX Release 10.6.2-89 patch:

Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX) through SSH.

Step 2 Enter the **cmxos patch list** command to check if a patch file is installed.

Step 3 Enter the **cmxos patch remove** command to remove any installed patch.

Run the command and provide the patch name that needs to be removed.

Step 4 Enter the **cmxctl restart** command to restart Cisco CMX services.

Step 5 Download Cisco CMX Release 10.6.2-89 patch *cmx-log4j-vulnerability-patch-10.6.2-2.cmxp* available at Software Download page.

Step 6 Copy the patch file to **/home/cmxadmin** directory.

Step 7 Enter the **cmxos patch install** command to install the patch.

Run the command and provide the patch name as *cmx-log4j-vulnerability-patch-10.6.2-2.cmxp*.

Note This patch restarts all Cisco CMX services and might take few minutes to complete. We recommend that you wait until the installation process is complete.

Table 1 Cisco CMX Release 10.6.2-89

Critical bug fixes	Provides critical bug fixes.

Table 2 What's New in Cisco CMX Release 10.6.2-72

New device support	Cisco Catalyst 9130AX-E Series Access Points
Critical bug fixes	Provides critical bug fixes.

Table 3 What's New in Cisco CMX Release 10.6.2

Single sign-on with SAML	Cisco CMX supports Security Authentication Markup Language (SAML) to allow for configuration of single sign-on (SSO) authentication. You can configure Cisco CMX to allow authentications from users configured outside of the system.
Cisco DNA Center multisite (Network Hierarchy) maps	Cisco CMX supports importing network hierarchy maps (**Country > State > City > Campus > Building > Floor > Zone**) from Cisco DNA Center.
Validate SSL certificate for Northbound notifications	This feature ensures that a valid HTTPS packet is created when webhooks are sent from Cisco CMX.
Data backup and restore support	Cisco CMX supports data backup and restoration using either SSH File Transfer Protocol (SFTP) or Secure Copy Protocol (SCP).
Removed the Cisco Operational Insights option from the Cisco CMX Cloud Apps window under the Manage tab	Cisco Operational Insights support is now available from Cisco DNA Spaces.
New device support	• Cisco Catalyst 9800-L Wireless Controllers Release 16.12 and later • Cisco Catalyst 9130AX-I Series Access Points • Cisco Catalyst 9120AX Series Access Points with Cisco FastLocate
Critical bug fixes	Provides critical bug fixes.

Table 4 What's New in Cisco CMX Release 10.6.1

Critical bug fixes	Provides critical bug fixes.

Table 5 What's New in Cisco CMX Release 10.6.0

Cisco DNA Spaces integration	Cisco DNA Spaces is a cloud-based location platform that provides a single pane for all location services. From Cisco CMX, you can configure location updates on the services enabled on Cisco DNA Spaces. For information about Cisco DNA Spaces, see https://dnaspaces.cisco.com/.
Enhanced traffic notifications	When Cisco CMX and Cisco DNA Spaces have an established connection, Cisco CMX provides traffic-related notifications, such as the destination of the traffic and the amount of traffic sent to Cisco DNA Spaces.
Restricted CLI	On Cisco CMX, Linux commands are restricted to prevent unauthorized users from inadvertently modifying the system configuration. For more information, see the "Restricted CLI" section in the Chapter "Getting Started" of the *Cisco CMX 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.
Federal Information Processing Standard (FIPS)	Cisco CMX implements software changes that are required for FIPS 140-2 security standard compliance. This standard is used to validate cryptographic modules. This feature is disabled by default, but FIPS mode can be configured on Cisco CMX.
Common Criteria (CC)	Cisco CMX implements software changes required for the CC certification process. This is a testing standard to verify that a product provides security functions. CC is enabled when FIPS mode is enabled on Cisco CMX. This feature is disabled by default.
U.S. Department of Defense (DoD) Unified Capabilities Approved Product List (UCAPL) compliance	Cisco CMX implements the software changes required for the U.S. DoD UCAPL compliance. The compliance certification is in progress. This feature is disabled by default, but UCAPL can be configured on Cisco CMX.
New device support	• Cisco Catalyst 9117AX-I Series Access Points • Cisco Catalyst 9115AX Series Access Points • Cisco Aironet 1840 Series Access Points • Cisco USB BLE Beacon (AIR-BLE-USB)

System Information

Supported Hardware

- Cisco CMX Release 10.6.x and later can be installed on the Cisco 3375 Appliance for Cisco Connected Mobile Experiences and Cisco Mobility Services Engine (MSE) 3365 Appliance. For Cisco 3375 appliance hardware and software installation information, see the *Cisco 3375 Appliance for Cisco Connected Mobile Experiences Installation Guide* for this release at: https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-installation-guides-list.html.
- Cisco CMX can be installed as a virtual Cisco MSE appliance, which requires a version from VMware ESXi 6.0 to ESXi 6.7. For information about installing a virtual Cisco MSE appliance, see the *Cisco MSE Virtual Appliance Installation Guide* for this release at: https://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/products-installation-guides-list.htm.

Note Cisco CMX does not support VMware tools.

Table 6 lists the Cisco CMX Release 10.6.x hardware guidelines for a virtual Cisco MSE appliance on VMware. For complete requirements, see the *Cisco Connected Mobile Experiences Data Sheet* at: https://www.cisco.com/c/en/us/products/wireless/mobility-services-engine/datasheet-listing.html.

Table 6 Hardware Guidelines [1]

Hardware Platform	Standard Appliance	High-End Appliance
CPU	16 vCPU 8 physical cores	20 vCPU 10 physical cores
RAM	48-GB RAM	64-GB RAM
HDD	550 GB	1 TB

1. For Cisco CMX OVA installation, 160 GB is the default hard disk drive (HDD) on standard and high-end virtual machines. We strongly recommend that immediately after deploying the OVA file and before powering on the VM, you increase the disk space to the recommended amount specified in this table, so that the HDD resource does not run low while using Cisco CMX. If you do not know how to increase the disk space before powering on the VM, see the VMWare 6.7 guidelines on how to increase disk space at: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.vm_admin.doc/GUID-79116E5D-22B3-4E84-86DF-49A8D16E7AF2.html

- 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.

Software Requirements

Before you deploy Cisco CMX, we strongly recommend that you see the following documents:

- 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 documents:
  - *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 Release 10.6.0 and later is required to support Cisco DNA Spaces.
- Cisco CMX (which includes Cisco CMX Location, Connect, and Configuration APIs) has been tested using Google Chrome up to Version 63.

  Note If you are using Google Chrome Version 72 or later, we recommend that you use Mozilla Firefox as your browser, or downgrade to Google Chrome Version 63.

- Cisco CMX supports only English input and output.
- Cisco Prime Infrastructure, when paired with Cisco CMX, displays client information and location, but not client history.

  For more information about Cisco CMX feature parity with Cisco Prime Infrastructure and Cisco MSE appliance, see the "Cisco CMX Feature Parity" section in the Chapter "Getting Started" in the *Cisco CMX 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.
- SSL mode is mandatory with Cisco CMX Release 10.5.0 and later. Use https:// to access the Cisco CMX Connect portal page. http:// is no longer supported.
  - 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 available, Cisco CMX Analytics might not work as expected.

  For information on installing a certificate, see the "Importing Certificates" section in the *Cisco CMX 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.

- See Table 7 and Table 8 when backing up and restoring Cisco CMX data between the Cisco 3375 appliance, Cisco MSE appliance, and Cisco vMSE appliance.

Table 7 System Memory for Cisco MSE and Cisco 3375 Appliances

Cisco MSE Appliance Model	RAM Allocated
Standard vMSE	48 GB
High-end vMSE	64 GB
Cisco 3375 and Cisco MSE 3365 appliances	64 GB

Table 8 Recommendations for Backup and Restore

Restore From...	Restore To...	Supported
Same machine specifications	Same machine specifications	Yes
Cisco MSE 3365 appliance	Cisco 3375 appliance	Yes
Cisco MSE 3365 appliance	High-end MSE virtual (vMSE) appliance	Yes
High-end vMSE appliance	Cisco 3375 and Cisco MSE 3365 appliances	Yes, unless the high-end machine has more RAM allocated than the recommended specifications
Standard vMSE appliance	Cisco MSE 3365 appliance	Yes
Standard vMSE appliance	High-end vMSE appliance	Yes
Cisco 3375 appliance	Cisco MSE 3365 appliance	Not supported
Cisco 3375 appliance	High-end vMSE appliance	Not supported
Cisco MSE 3365 appliance	Standard vMSE appliance	Not supported
High-end vMSE appliance	Standard vMSE appliance	Not supported

Note HA pairing checks are done for software versions and hardware specifications. 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 databases.

- 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.

License Information

Cisco CMX License	Features
• Cisco CMX Base • Cisco DNA Spaces SEE	• Cisco CMX RSSI-based location calculation of clients, interferers, and rogues for Cisco products such as Cisco DNA Center, Cisco Prime Infrastructure, and Cisco Identity Services Engine • Use of Cisco CMX location data in Cisco DNA Center • Use of Cisco CMX location data in Cisco Prime Infrastructure • Tethering of Cisco CMX to Cisco DNA Spaces • Use of Business Insights and other capabilities of Cisco DNA Spaces as and when available • Use of Basic Detect and Locate capabilities of Cisco DNA Spaces as and when available • Use of Basic Location Analytics capabilities of Cisco DNA Spaces as and when available • Access to the DETECT, MANAGE, and SYSTEMS tabs in the Cisco CMX or Cisco DNA Spaces user interface
• Cisco CMX Advanced • Cisco DNA Spaces ACT/EXT	• Cisco CMX advanced location calculations capabilities, including Cisco FastPath and Cisco Hyperlocation • Use of Captive Portal capability of Cisco DNA Spaces as and when available • Use of Profile and Engagement capability of Cisco DNA Spaces as and when available • Use of Advanced Location Analytics capability of Cisco DNA Spaces as and when available • Use of Operational Insights capability of Cisco DNA Spaces as and when available • Use of Advanced Detect and Locate capability of Cisco DNA Spaces as and when available

- 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 for obtaining 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.
- A Cisco DNA Spaces license (SEE or ACT/EXT) is required to connect Cisco CMX to a cloud. The cloud license includes the Cisco CMX license required to enable Cisco CMX.
- 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 should install on the primary HA server. The secondary HA server automatically receives a copy of the Cisco CMX license during synchronization. There is no HA-specific license to install.
- When a third-party certificate is installed in an HA setup, the certificate needs to be installed separately on both the primary and secondary Cisco CMX servers. For additional information and procedures, see the “Installing a CA-Signed Certificate for High Availability in Cisco CMX” section in the *Cisco CMX Configuration Guide* at https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmx_config/b_cg_cmx106/getting_started_with_cisco_cmx.html#id_122557.

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 CMX 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.

Installation and Upgrade Information

- (CSCvp04706) Use the CLI, not the GUI, to upgrade to Cisco CMX Release 10.6.1 or later.
- You cannot upgrade to Cisco CMX Release 10.6.x or later from Cisco CMX Release 10.4.x or earlier until you install and deploy the latest Cisco CMX 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 or later.

  For complete information about the relevant procedures, see the *Cisco Mobility Services Engine Virtual Appliance Installation Guide* for this release at: https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-installation-guides-list.html.
- Downgrading from any Cisco CMX release is not supported.
- Inline upgrade from Cisco CMX Release 10.5.x to Cisco CMX Release 10.6.x is supported.
- We recommend that you run Cisco CMX Release 10.5.x or later in parallel with the existing Cisco MSE appliance Release 8.0 or earlier, and utilize the evaluation license for 120 days. After the evaluation period, the earlier Cisco MSE appliance release can be decommissioned.
- No database migration or inline upgrade is supported from Cisco MSE appliance Release 8.0 or earlier to Cisco CMX Release 10.5.x or later.
- (CSCvn98931) The Cisco 3375 appliance supports Cisco CMX Release 10.5.1 and later. Do not upgrade the Cisco Integrated Management Controller (CIMC) software.

For information about upgrading from an earlier Cisco CMX release to this release, see the Chapter "Upgrading" in the *Cisco Mobility Services Engine Virtual Appliance Installation Guide for Cisco CMX* for this release 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 appliance 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.

Limitations, Restrictions, and Important Notes

Tip To clean up long queues and long-running processes, we recommend that you schedule a full restart of Cisco CMX once a month during a low activity time, such as late at night or early in the morning. The restart takes approximately 5 minutes to complete.

To restart Cisco CMX services, follow these steps:

1. Enter the **cmxctl stop -a** command.
2. Enter the **cmxctl start -a** command.

Note Contact Cisco Customer Support (https://www.cisco.com/c/en/us/support/index.html) for the patch file.

Note If a Cisco CMX CLI or GUI user account is inactive for 60 days or more, the account is locked. A Cisco CMX admin user (cmxadmin) can unlock the account and use the applicable command:

- **cmxctl users unlock gui** <*userID*> command to unlock the user's Cisco CMX GUI account.
- **cmxctl users unlock cli** <*userID*> command to unlock the user's Cisco CMX CLI account.

If the Cisco CMX admin user account is locked out, the admin user must connect directly to the console and use the applicable command: **cmxctl users unlock gui** <*userID*> or **cmxctl users unlock cli** <*userID*>.

- You can use the **cmxctl config auth settings** command to set the expiration period for the password. The default expiration period is 9999 days.
- (CSCvo95518) Cisco CMX Release 10.6.2 and later with FIPS mode enabled can establish a Network Mobility Services Protocol (NMSP) connection with Cisco Catalyst 9800 wireless controllers running Release 16.12, with FIPS and CC mode enabled.

  In contrast, Cisco CMX Release 10.6.2 and later with FIPS mode enabled cannot establish an NMSP connection with Cisco WLCs running Release 8.x.

  Note Before enabling FIPS mode on Cisco CMX, remove all the non-FIPS compliant controllers from Cisco CMX. Otherwise, establishing NMSP connectivity after restarting Cisco CMX services will require an extensive amount of time.

- For support in using APIs, including the GitHub version of API Version 3, contact the Cisco DevNet Community at: https://developer.cisco.com/site/cmx-mobility-services/.
- Cisco CMX supports the Cisco Mobility Express wireless network solution.
- The Cisco FlexConnect feature does not support DNS ACL, and as such, you cannot use DNS ACLs when configuring Cisco CMX Connect and Engage.

- (CSCve28851) The following error message is displayed because MATLAB only counts heavy walls for location calculation, while Java counts all the obstacles on the floor map. Ignore this message because the heat maps are now correctly generated and stored:

  ```
  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.
  ```

- (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 Chapter "Wireless Quality of Service" 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.

  The sources of interference are:

  - 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-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 802.15.4vAn 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)

- (CSCve56353) End users using Android devices are unable to open the Cisco CMX landing page URL configured from the **Connect & Engage > Connect Experiences** window. In addition, the Guest Portal might also close after an 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 addition, special configuration changes can be made to increase this rate. Contact Cisco Technical Support for more information on these recommendations.

- (CSCvg10317) Cisco MSE virtual machine (VM) appliance running Cisco CMX might not function properly after being powered on after a power outage. If this occurs:
  1. Use the **cmxos date** command to make sure that the Cisco CMX system date matches the current date. If the dates do not match, use the NTP server to synchronize the dates.
  2. Enter the **cmxctl stop –a** command to shut down Cisco CMX services.
  3. Enter the **cmxctl start** command to restart the services.
- (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.
- (CSCvg79749) In Cisco CMX Release 10.4.0, the v3 client API was introduced, and the v2 client API was deprecated. We recommend that you use the v3 API instead of the v2 API. High CPU usage by the Cisco CMX Location service occurs when the v2 API is used for a long duration. Restart the Cisco CMX Location service to correct the condition.
- (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.
- (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.
- (CSCvi84935) High CPU usage of the Cisco CMX Analytics and Location services might occur during initial HA synchronization, causing the synchronization to not complete. If this occurs, remove the Cisco WLC from the system to decrease the CPU usage of the Cisco CMX Analytics service. This provides enough memory for the initial HA synchronization to complete.
- (CSCvj52515) There is significant overhead in maintaining the compact history, which allows you 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 From 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:

  a. `cmxctl config featureflags location.compactlocationhistory false`

  b. `cmxctl agent restart`

  c. `cmxctl location stop`

  d. `cmxctl location start`
- (CSCvn33059) When you click the **Client movement history playback** icon on the **Detect & Location** > **Activity Map** window, you can select a day—up to 30 days from the current date—to track the history of a client. This window of 30 days is independent of the Data Retention - Client History Pruning Interval.

- (CSCvn98927) We recommend that you assign an IP address to a single interface (ens32). Assigning IP addresses to two interfaces allows data to go to both the interfaces, which causes Cisco CMX to drop packets, and creates issues related to client tracking.
- (CSCvo14248) Generating scheduled reports in PDF format is not supported on Cisco CMX Release 10.5.0 and later. Use the **PrtSc** option instead. This feature set will be removed from the product.
- (CSCvo60319) On Cisco CMX, using OAuth with Instagram might not always display the Log In portal. If the portal is not displayed, refresh your browser.
- (CSCvp00432) As of Cisco CMX Release 10.6.0, Cisco CMX no longer supports the **Historylite** (/api/location/v1/historylite) API. The API requires collecting compact location history, which causes performance issues.
- (CSCvp11685) If FIPS mode is enabled on Cisco CMX, the Maps online sync (Import from Cisco Prime Infrastructure) fails for Cisco Prime Infrastructure Release 3.5.

  To import maps from Cisco Prime Infrastructure Release 3.5 to Cisco CMX with FIPS mode enabled, you must download the tar file of Cisco Prime Infrastructure, and then upload the tar file to Cisco CMX, as described in the "Importing Maps" section in the *Cisco CMX Configuration Guide* at: https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-installation-and-configuration-guides-list.htm.
- (CSCvp19413) If you need to use round brackets (such as parentheses) in a Cisco CMX API regex expression, use a backslash (\) to escape the next character. For example, instead of this string:

  ```
  Global->System Campus>1212 Deming Way (TTD)>Floor 1
  ```

  use this string:

  ```
  Global->System Campus>1212 Deming Way \(TTD\)>Floor 1
  ```
- (CSCvp31400) Cisco CMX in FIPS mode does not support the aes128-ctr and aes256-ctr ciphers (while Cisco CMX in non-FIPS mode supports them). If a Cisco Catalyst 9800 wireless controller is using either of these ciphers, it will not be able to communicate with Cisco CMX in FIPS mode.

  Cisco CMX in FIPS mode supports only the aes128-cbc, aes256-cbc, aes128-gcm@openssh.com, and aes256-gcm@openssh.com ciphers.
- (CSCvp25049) The **Repeat Devices** API does not provide all the required information because it requires information from history location data, which is managed by the **compacthistory** feature flag. The feature flag causes performance issues and is disabled by default.
- (CSCvp92688) Cisco CMX might not be able to process a large amount of history data from the Cassandra database if the duration between locatedAfterTime and locatedBeforeTime for the **All Client History** API is either 1 hour or 20 minutes. We recommend that you use the Cassandra export tool to extract history data.
- (CSCvq81962) When the Cisco CMX session idle timeout period is reached, users are logged out of their Cisco CMX UI session whether the session is idle or is actively being used. Users must then log in to Cisco CMX again.

  Use the **cmxctl config auth settings** command to configure the **Session idle timeout in minutes** setting. The time range is 1 to 720 minutes. The default value is 30 minutes.

  This timeout period does not apply to Cisco CMX CLI sessions.
- (CSCvq82147) Cisco CMX supports VMware Snapshot.
- (CSCvq82305) Location data is poor when too few Angle of Arrival (AoA) measurements are reported in a network, with both hyperlocation and nonhyperlocation access points.

- (CSCvr16016) The issue of the Cisco CMX Analytics Service not processing data is now fixed in Cisco CMX Release 10.6.2-72 but for the fix to come into effect, you must reboot Cisco CMX.
- (CSCvr26395 and CSCvr26398) The Cisco CMX Troubleshooting Tool supports only Cisco Hyperlocation-capable access points.
- (CSCvs57713) With Cisco CMX Release 10.5 and later and Cisco WLC Release 8.7 and later, the Cisco CMX Group Subscription feature allows one Cisco Hyperlocation-enabled wireless controller to connect to multiple Cisco CMX servers.
- (CSCvs68618) When collecting client data from the Cisco CMX v3 Location API, the last seen time stamp is different from the time stamp displayed on the Cisco CMX GUI.
- In Cisco CMX Release 10.6.2-89, the floorRefId component is replaced with floorId.
- (CSCvs89951) If your network has a Cisco Catalyst 9800 wireless controller, do not check the **Exclude Probing Only Clients** check box located in the **Settings > Filtering** section on the **System > Dashboard** window on Cisco CMX. Checking the **Exclude Probing Only Clients** check box causes all the clients (probing and associated clients) to be excluded from the controller, and hence will not be displayed on Cisco CMX.
- (CSCvt83715) We recommend that you disable the Cisco CMX Analytics service if you are not using the service.
  - If you are running Cisco CMX Release 10.6.2-72 or earlier, install the **cmx-disableanalytics-patch-10.6.2-1.cmxp** patch file. Contact Cisco Customer Support (https://www.cisco.com/c/en/us/support/index.html) for the patch file.
  - If you are running Cisco CMX Release 10.6.2-89 or later, use the **cmxctl disable analytics** command.

  Note The **cmxctl disable analytics** command is supported only on Cisco CMX Release 10.6.2-89 and later.

- (CSCvt83902) Cisco CMX displays an authentication error during SSO login if the SAML response from the IDP does not include the **User.email**, **User.FirstName**, and **User.LastName** attributes.
- (CSCvu18413) Due to FIPS/CC/UCAPL compliance, root access is no longer available as of Cisco CMX Release 10.6.0. Only Cisco Customer Support has access to a root patch for troubleshooting. Contact Cisco Customer Support (https://www.cisco.com/c/en/us/support/index.html) for assistance.

Caveats

Cisco Bug Search Tool

The Cisco Bug Search Tool (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 BST is designed to improve the effectiveness in network risk management and device troubleshooting. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

- To view the details of the software bugs pertaining to your product, click the Caveat ID/Bug ID number in the table.
- To view the details of caveats whose IDs you do not have, access the BST using your Cisco user ID and password.

For more information about the Cisco Bug Search Tool, including how to set email alerts for bugs and to save bugs and searches, see Bug Search Tool Help & FAQ.

Open Caveats

Bug ID	Description
CSCvq81962	CMX UI session timeout forces log out at set time while setup is in use
CSCvs85182	CMX filters out locally administered MAC addresses
CSCvt85105	Show certs command in FIPS CMX is displaying non-cert related output messages

Resolved Caveats in Cisco CMX Release 10.6.2-89

Bug ID	Description
CSCwa47312	Evaluation of cmx for Log4j RCE (Log4Shell) Vulnerability vulnerability
CSCvr37865	FIPS: Large java heapdump files getting created daily on a FIPS enabled CMX
CSCvr80298	FREERadius on CMX-10.6.x is not working
CSCvs61111	Timezone setting is not reflected during initial wizard, causing DB stopped
CSCvs64361	Controllers do not show in CMX 10.6 GUI
CSCvs79217	Incorrect timezone conversion in syslog message
CSCvs90116	API call returns Null values for individual RFID tags. Issue seen on Random tags.
CSCvs96925	CMX10.6.2: Excessive Exception Errors found in both configuration and location error.log
CSCvt01326	CMX is reporting incorrect geo-coordinates for some of the clients
CSCvt14774	Using POSIX TZ format prevents HA formation
CSCvt32460	CMX is reporting -999 geo-coordinates for some clients

Resolved Caveats in Cisco CMX Release 10.6.2-72

Bug ID	Description
CSCvj69166	10.5-183 : Restore failing in Presence setup
CSCvn04814	10.6.0-UCAPL Encryption of /var/log partition (SRG-APP-000126-NDM-000242)
CSCvp51131	CMX 10.6-177 Running unsecure version of OpenSSH 7.5p1 (dating back to 2017)
CSCvr16016	Analytics service not processing data
CSCvr27467	CMX fails to import certificates as cmxadmin user does not have the right permissions
CSCvr32448	Correct floorId in Maps and v3 clients APIs response.
CSCvr33343	CMX 10.6.2-53 Cassandra Connection Failed Alert. Port 9042 not responding
CSCvr47013	Customer getting "Website not trusted" screen when redirected to cmx portal page.
CSCvr47389	CMX user after successfully importing the servercert is not able to perform Reboot
CSCvr53419	10.6.2 Password Change asked on first login in UCAPL mode with RADIUS server configured
CSCvr82898	CMX 10.6.2-57 -Over time AP Client dont show up on CMX Error-nmspdata
CSCvr86743	CMX 10.6.2 - Redis check failed for Primary
CSCvs02267	CMX 10.6.2 Influx DB Verification Failure

Resolved Caveats in Cisco CMX Release 10.6.2

Bug ID	Description
CSCvn92422	CMX realtime report doing wrong calculation of associated devices
CSCvo11605	On Detect and Locate page, Maps image were not seen.
CSCvo15147	APIs for Exporting Large Dataset from CMX Cassandra Database not working
CSCvo43574	cmxos verify command is wrong about HDD min requirements
CSCvo56226	Analytics view not getting synced from Primary to Secondary
CSCvo60319	CMX 10.5.1 - CMX Oauth not working with Instagram
CSCvp13117	MSE3375-10.6.0 request to enter username or password during Resetting Root Password procedure
CSCvp13182	Rogue AP status keep being 'Initializing'
CSCvp39346	SAN field being added to the CSR file
CSCvp41845	CMX 10.6 - Presence Analytics managed tabs not loading (except the \"Sites\" tab)
CSCvp42740	cmxloc based commands not working
CSCvp46421	HA failover from Redis non response
CSCvp51797	CMX Network Port Matrix lists incorrect port for upgrades
CSCvp60337	CMX Maps showing Campus off the coast of Africa when importing from Prime
CSCvp88854	CMX 10.6.X, running cassandraexport command throws Java exception errors "NoHostAvailableException"
CSCvp89626	Support for polling Connected Clients fields periodically.
CSCvp92122	cmxos techsupport dump throws error on CMX 10.6.1

Bug ID	Description
CSCvp99416	CMX on-prem pushing BLE AP config to wrong controller.
CSCvq03741	cmx 10.6.1.47: submit button in customer portal page doesn't redirect in connect and engage module
CSCvq05802	Import Nested sites from Cisco DNA Center
CSCvq14088	Enhance LocationUpdate notification for sending rssiEntries
CSCvq14236	CMX 10.6.0 coming up with some vulnerabilities
CSCvq14966	CMX UI Changes for SSID and AP interfaces.
CSCvq14991	cmxos CLI changes
CSCvq25953	Enabling Location SSID Filtering disables the exclusion of locally administered MACs and vice versa
CSCvq37294	\"Location Computation(per sec)\" section shows no data
CSCvq42343	RTLS Data Missing Issue in CMX
CSCvq44241	WLC attribute validation for SNMP v2c version needs improvement
CSCvq48489	Tracking Interferes enabled triggers \"The location service is not reporting health\"
CSCvq48782	CMX 10.6.1 // HSTS header configured shows for all URL except for https://< CMX_IP >
CSCvq55342	[10.6.2]:Rogue AP & Rogue Client count does not go to zero in system page after tracking is disabled
CSCvq63537	CMX 10.6.0-177 CleanupCassandra job always Failed
CSCvq64026	Enhance tethering to support zones and regions.
CSCvq67400	Fix collectd log file errors for python import issues
CSCvq67423	Display postgres and cassandra database sizes
CSCvq74080	Make SSID filter midnight cleanup job configurable.
CSCvq79596	admin password change is required on CMX10.6.1 after 60 days from initial setup
CSCvq86511	Enhance locationupdate notification for bletags to send ble info attributes.
CSCvq91381	Display Duty Cycle, Severity on Detect and Locate. Under Filtering, add a new field Severity Cutoff
CSCvr37803	Not all the cmx services pick up the SSL cert after successful cert import

Resolved Caveats in Cisco CMX Release 10.6.1

Bug ID	Description
CSCvk66624	v3 Count API shows invalid number of clients
CSCvn97729	evaluation of CVE-2018-5407 for CMX appliances of AIR-MSE-3365-K9
CSCvo00850	CMX 10.6.0 after WLC force switchover NMSP connection not coming active.
CSCvo07525	CMX10.4 does not reflect generated SSC Self-Signed Certificate
CSCvo08709	CMX Location API dropping RFID Tag information
CSCvo15106	Inclusion/Exclusion regions are not getting deleted from CMX after syncing with Prime Infrastructure
CSCvo19808	Import MAPs to CMX provokes NMSP to come down
CSCvp10496	CMX 10.x HA Floormaps folder get deleted as part of filesync OP causing the mount issues.
CSCvp24319	CMX GUI is blocked when SEE or ACT eval license is expired

Resolved Caveats in Cisco CMX Release 10.6.0

Bug ID	Description
CSCvj43002	No clients displayed in CMX API location map.
CSCvj84948	CMX 10.4.1 : The location service is not reporting health
CSCvk16626	CMX 10.4.1 - CMX Facebook wifi fails with \"Unable to obtain a gateway ID from Facebook\" error msg
CSCvk53552	Nodesetup service failed on Primary converted to Secondary
CSCvm29507	Notifications are not reaching cloud due to proxy compatibility with cmx libraries
CSCvn05152	CMX 10.5 Config Guide needs to be updated with correct steps of root password recovery
CSCvn33059	CMX 10.5 - Playback History Calendar does not allow to select date older than 30 days
CSCvn74143	CMX Base license file shows eval instead of perm or 3 years (only shows 120 days)

Documentation and Support

Related Documentation

Note 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.

- Cisco DNA Spaces product information: https://www.cisco.com/c/en/us/solutions/enterprise-networks/connected-mobile-experiences/index.html
- Cisco CMX documentation: https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/tsd-products-support-series-home.html
- Cisco CMX Cloud documentation: https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences-cmx-cloud/tsd-products-support-series-home.html

- Cisco DNA Spaces documentation: https://www.cisco.com/c/en/us/support/wireless/dna-spaces/tsd-products-support-series-home.html
- Cisco Mobility Services Engine documentation: https://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/tsd-products-support-series-home.html
- Cisco Aironet Access Point Modules documentation: https://www.cisco.com/c/en/us/support/interfaces-modules/aironet-access-point-modules/products-installation-guides-list.html

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 Cisco Community.

Communications, Services, and Additional Information

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

To get the business impact you are 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 applications, 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.
