Release Notes for Cisco Connected Mobile Experiences (CMX) Release 11.0.1

First Published: 2024-04-12

Introduction

Cisco Connected Mobile Experiences (Cisco CMX) Release 11.0.1 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.

What's New in Cisco CMX Release 11.0.1

This release includes deployment of a new image version of Cisco CMX 11.0.1-129. This release is packed with an Alma Linux operating system upgrade.

You can upgrade from the previous releases of Cisco CMX 11.0.0-154.

Cisco CMX Release 11.0.1 supports migration of your data from Cisco CMX Release 10.6.3-146 to the latest Cisco CMX Release 11.0.1-129. Use the **cmxos upgrade** command to migrate data from CMX 11.0.0-154.

Note Cisco CMX Release 11.0.1 is not supported on Cisco 3375 Appliance for Cisco Connected Mobile Experiences and Cisco Mobility Services Engine (MSE) 3365 Appliance.

To install Cisco CMX OVA, follow these steps:

1. Download the CISCO_CMX-11.0.1-129.ova file available on the Software Download page.
2. Install the Cisco CMX Release 11.0.1-129 OVA build on the primary and secondary servers.
3. Migrate data from Cisco CMX Release 10.6.3-146 to Cisco CMX Release 11.0.1-129. For detailed instructions, see Data Migration.

Table 1: What's New in Cisco CMX Release 11.0.1

Feature	Description
AlmaLinux Upgrade	This release supports the upgrade from AlmaLinux 8.4 to AlmaLinux 8.7 Stable.
FIPS Support	This release includes FIPS recertification and supports CSM Toolkit/FIPS toolkit with FOM v7.2a.
Data migration	Data migration from Cisco CMX Release 10.6.3-146 to Cisco CMX Release 11.0.1 is supported. For more information, see Data Migration.

Feature	Description
TLS 1.3 Support	In this release, all TLS connections (haproxy, influxdb, postgres, nodejs) support TLS Version 1.3 protocol.
Customer Success Management Software (CSM) Toolkit support	The CSM toolkit supports erstwhile CiscoSSL, CiscoSSH, and other tools repackaged under csm-toolkit (using FOM 7.2a).
Critical issue fixes	Includes critical issue fixes.

System Requirements

Supported Hardware

- Cisco CMX can be installed as a virtual Cisco MSE appliance, that requires a version VMware ESXi 7.0. The OVA deployment using a VMware vCenter is supported on VMware ESXi 7.0 and above. The VMware vCenter version must be 7.x or above and earlier versions are not supported.

Note The vSphere Hypervisor ESXi 6.0 is End of General Support.

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.html.

Note

- Data migration support is only available from Cisco CMX Release 10.6.3-146 to Cisco CMX Release 11.0.1.
- If you are on Cisco CMX releases earlier than Release 10.6.3-146, you need to upgrade to Cisco CMX Release 10.6.3-146 and then install the cmx-11-migration-readiness-patch patch release, and then migrate the data.
- Cisco CMX does not support VMware tools.

The following table lists the Cisco CMX 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 2: Hardware Guidelines

Hardware Platform	Low-End Appliance	Standard Appliance	High-End Appliance
CPU	8 vCPU 4 physical cores	16 vCPU 8 physical cores	20 vCPU 10 physical cores
RAM	24 GB RAM	48-GB RAM	64-GB RAM

Hardware Platform	Low-End Appliance	Standard Appliance	High-End Appliance
HDD[1]	550 GB	550 GB	1 TB

[1] For Cisco CMX OVA installation, 250 GB is the default hard disk drive (HDD) on all virtual machines. We strongly recommend that immediately after deploying the OVA file and before powering on the VM, you should 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 guidelines on how to increase disk space.

If you do not select the recommended disk space, the basic installation defaults to 160 GB of the disk space.

Note Cisco Hyperlocation is only supported on the High-End Cisco CMX appliances for Cisco Connected Mobile Experiences. By default, Cisco Hyperlocation is disabled on Low-End appliances.

- Cisco CMX Release 11.0.1 is not supported on Cisco 3375 Appliance for Cisco Connected Mobile Experiences and Cisco Mobility Services Engine (MSE) 3365 Appliance.
- 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 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 *Cisco Connected Mobile Experiences Data Sheet* at:

  https://www.cisco.com/c/en/us/products/collateral/wireless/mobility-services-engine/datasheet-c78-734648.html
- Cisco CMX Release 10.6.0 and later is required to support Cisco Spaces.
- Cisco CMX (which includes Cisco CMX Location 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.
- 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.
- See the following table for system memory details:

Table 3: System Memory for Cisco MSE

Cisco MSE Appliance Model	RAM Allocated
Standard vMSE	48 GB
High-end vMSE	64 GB

Note High Availability pairing checks are done for software versions and hardware specifications. High Availability 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.

Licensing Information

Table 4: Cisco CMX License

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

- Cisco CMX Release 11.0.1 is a new OVA installation for Cisco CMX.
- Inline upgrade from Cisco CMX Release 11.0.0 to Cisco CMX Release 11.0.1 is supported.
- Inline upgrade from Cisco CMX Release 10.x.x to Cisco CMX Release 11.0.1 is not supported.
- Data migration is supported only from Cisco CMX Release 10.6.3-146 to Cisco CMX Release 11.0.1-129.
- You must install the cmx-11-migration-readiness-patch Patch Release on the primary server running Cisco CMX Release 10.6.3-146 to migrate data.
- Downgrading from any Cisco CMX release is not supported.

Limitations, Restrictions, and Important Notes

- (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)

- (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.

- (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 incomplete synchronization. If this occurs, remove the Cisco controller from the system to decrease the CPU usage of the Cisco CMX Analytics service. This provides enough memory for the initial HA synchronization to get completed.

- (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 for compact location history 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:

1. **cmxctl config featureflags location.compactlocationhistory false**
2. **cmxctl agent restart**
3. **cmxctl location stop**
4. **cmxctl location start**

- (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, which in turn, leads to 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 he collection of the 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.html.

- (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.

Issues

Issues describe unexpected behavior in the Cisco CMX application. The Open Issues and Resolved Issues sections list the issues in this release.

Open Issues

This section lists the open issues in this release of Cisco CMX 11.0.1.

Table 5: Cisco CMX 11.0.1 Open Issues

Bug ID	Description
CSCwf31042	CMX11 on IPv6 most services not shown as running after initial configuration
CSCwf36900	CMX-11: Hostname change is not sticky as it does not get saved
CSCwf36890	CMX-11: Authenticated ntp not supported

Resolved Issues

This section lists the issues that have been resolved in this release of Cisco CMX 11.0.1.

Table 6: Cisco CMX 11.0.1 Resolved Issues

Bug ID	Description
CSCwc99232	Cannot create notification when Device Type is RFID Tag, clients or anything other than all.
CSCwh60064	CMX11 OVA doesn't allow to bring up the GUI services for standard and high-end deployment.

Documentation and Support

Related Documentation

- Cisco Spaces product information:

  https://www.cisco.com/c/en/us/solutions/enterprise-networks/connected-mobile-experiences/index.html
- Cisco Spaces documentation:

  https://www.cisco.com/c/en/us/support/wireless/dna-spaces/tsd-products-support-series-home.html
- Cisco CMX documentation:

  https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/tsd-products-support-series-home.html
- Cisco CMX Cloud documentation:

  https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences-cmx-cloud/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'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 DevNet.
- 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 gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.