Release Notes for Cisco Connected Mobile Experiences (CMX) Release 10.6.3

First Published: 2020-12-02

Last Modified: 2022-11-08

Release Notes for Cisco CMX Release 10.6.3

Introduction

Cisco Connected Mobile Experiences (Cisco CMX) Release 10.6.3 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

What's New in Cisco CMX Release 10.6.3-146-Patch Release

This is a patch release for Cisco CMX Release 10.6.3-146, which addresses the issues you might encounter while creating notifications for devices with the DeviceType as **RFID Tag**, **Client** or any option other than **All**.

Note

- This patch release is supported only on Cisco CMX Image Version: 10.6.3.-146.
- This patch release addresses the bug: CSCwc99232.

To install the Cisco CMX Release 10.6.3-146 patch, follow these steps:

1. Download the cmx-notification-patch-10.6.3-1.cmxp file available on the Software Download page.
2. Use the Secure Copy Protocol (SCP) and copy the cmx-notification-patch-10.6.3-1.cmxp file to the Cisco CMX `/home/cmxadmin/directory`.
3. Use Secure Shell (SSH) to connect to the Cisco CMX console as **`cmxadmin`**.
4. Navigate to `/home/cmxadmin/directory`.
5. (Optional) To view the currently installed patches, run the **cmxos patch list** command.
6. To install the patch, run the **cmxos patch install** command.
7. At the `Please enter the patch file name:` prompt, enter the patch name as cmx-notification-patch-10.6.3-1.cmxp

   After successful installation, the following message is displayed:

   ```
   Patch installed successfully
   ```
8. To restart the configuration service, run the **cmxctl restart configuration** command
9. (Optional) To view the installed patches again, run the **cmxos patch list** command.

What's New in Cisco CMX Release 10.6.3-146

This release requires you to upgrade from Cisco CMX Release 10.6.3-105 to the latest version Cisco CMX Release 10.6.3-146.

You must break the High Availability pairing before upgrading Cisco CMX.

To break the High Availability, run the **cmxha disable** command on the primary Cisco CMX server.

To upgrade Cisco CMX, follow these steps:

1. Download the CISCO_CMX-10.6.3-146.cmx file available on the Software Download page.
2. Perform upgrade of the primary Cisco CMX VMs from Cisco CMX Release 10.6.3-105 to Cisco CMX Release 10.6.3-146.
3. To upgrade Cisco CMX, run the **cmxos upgrade** command. For example: **cmxos upgrade** CISCO_CMX-10.6.3-146.cmx.
4. After the upgrade is complete, to verify the updated version, run the **cmxctl version** command.
5. To verify that all services are operational, run the **cmxctl status** command.
6. (Mandatory) To repeat the Cisco CMX upgrade process to the same version, run the **cmxos upgrade** command again. For example: cmxos upgrade CISCO_CMX-10.6.3-146.cmx.

Note This is a mandatory step to address the vulnerabilities.

7. After the upgrade is complete, to verify the updated version, run the **cmxctl version** command.

8. To verify that all services are operational, run the **cmxctl status** command.
9. Perform a fresh installation (CISCO_CMX-10.6.3-146.ova) on the secondary server.
10. Perform the High Availability pairing and verify if both units are actively synchronizing.

To install Cisco CMX OVA, follow these steps:

1. Download the CISCO_CMX-10.6.3-146.ova file available on the Software Download page.
2. Install Cisco CMX Release 10.6.3-146 OVA build on the primary and secondary servers.
3. Perform the High Availability pairing and verify if both units are actively synchronizing.

To install a Cisco CMX ISO (on appliance only), follow these steps:

1. Download the CISCO_CMX-10.6.3-146.ISO file available on the Software Download page.
2. Install Cisco CMX Release 10.6.3-146 ISO build on the primary and secondary servers.
3. Perform the High Availability pairing and verify if SSH is functional on secondary box.

What's New in Cisco CMX Release 10.6.3-105 Patch Release

This is a patch release for Cisco CMX Release 10.6.3-105, which addresses the SSH failure issue on the secondary Cisco CMX server. You must install the patch on both the primary and the secondary Cisco CMX servers. You do not have to restart the Cisco CMX server for this patch install.

Note This patch release does not intend to fix an impacted Cisco CMX secondary server. You must perform a fresh install or rebuild of the Cisco CMX secondary server before installing the patch.

To install the Cisco CMX Release 10.6.3-105 patch, follow these steps:

1. Download the cmx-ha-sshd-patch-10.6.3-1.cmxp file available on the Software Download page.
2. Use the Secure Copy Protocol (SCP) and copy the cmx-ha-sshd-patch-10.6.3-1.cmxp file to the Cisco CMX `/home/cmxadmin/ directory`.
3. Use Secure Shell (SSH) to connect to the Cisco CMX console as **`cmxadmin`**.
4. Navigate to `/home/cmxadmin/ dir`.
5. To view the currently installed patches, run the **cmxos patch install** command.
6. To install the patch, run the **cmxos patch install** command.
7. At the *Please enter the patch file name:* prompt, enter the patch name as cmx-ha-sshd-patch-10.6.3-1.cmxp.

   After successful installation, the following message is displayed:

   Patch installed successfully
8. To view the installed patches again, run the **cmxos patch list** command.

Note (Optional) To remove the patch, run the **cmxos patch remove** *cmx-ha-sshd-patch-10.6.3-1.cmxp* command.

What's New in Cisco CMX Release 10.6.3

Cisco CMX Release 10.6.3 Security Patch Release

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 Releases 10.6.3-105 and 10.6.3-70.

You must download Cisco CMX Release 10.6.3 patch *cmx-log4j-vulnerability-patch-10.6.3-2.cmxp* available on the Software Download page and copy the patch file to `/home/cmxadmin` directory.

Note

- If the *cmx-log4j-vulnerability-patch-10.6.3-1.cmxp* patch file is previously installed, ensure that you run the **cmxos patch remove** command and remove the patch before installing the new patch.
- To apply this patch on Cisco CMX High Availability, you must break the HA and rebuild it.

To install Cisco CMX Release 10.6.3 patch, follow these steps:

1. Log in to Cisco Connected Mobile Experiences (Cisco CMX) through SSH.
2. To check if a patch file is installed, run the **cmxos patch list** command.
3. To remove any installed patch, run the **cmxos patch remove** command and provide the patch name that needs to be removed.
4. To restart Cisco CMX services, run the **cmxctl restart** command.
5. Download Cisco CMX Release 10.6.3 patch *cmx-log4j-vulnerability-patch-10.6.3-2.cmxp* available on the Software Download page.
6. Copy the patch file to `/home/cmxadmin` directory.
7. To install the patch, run the **cmxos patch install** command.
8. Enter the patch name as *cmx-log4j-vulnerability-patch-10.6.3-2.cmxp* at the prompt.

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: What's New in Cisco CMX Release 10.6.3-137

Support for Proxy with Basic Authentication	Cisco CMX Release 10.6.3 now includes support for proxy with basic authentication is added. For more information, see Support for Proxy with Basic Authentication.

New device support	• Cisco Catalyst Wireless 9166I Wi-Fi 6E Series Access Points • Cisco Catalyst Wireless 9164I Wi-Fi 6E Series Access Points
Critical bug fixes	Provides critical bug fixes.

Table 2: What's New in Cisco CMX Release 10.6.3-105

New device support	• Cisco Catalyst 9105AX Series Access Points • Cisco Catalyst 9124AX Series Access Points • Cisco Catalyst 9130AXE Series Access Points • Cisco Catalyst 9136I Series Access Points
Critical bug fixes	Provides critical bug fixes.

Table 3: What's New in Cisco CMX Release 10.6.3

Smart License support	• Cisco CMX Release 10.6.3 now supports Smart Licensing for Cisco DNA Spaces. • Cisco CMX Release 10.6.3 is supported on Cisco Connected Mobile Experiences (Cisco CMX) using the classic licensing model. Smart Licensing Satellite (on-premise) is under evaluation. Smart License support in Cisco CMX helps to maintain the licensing information with CSSM central repository and helps you to manage licensed software easily. Smart License functionality helps you to eliminate storing of Product Activation Keys (PAK) and to reduce the efforts in gathering information during license renewal process.
Cisco CMX tethering enhancements	The following enhancements are made to Cisco CMX tethering: • Cisco CMX version information is also included in the healthcheck api. • In the location notifications sent to Cisco DNA Spaces, statistics notification information is also included. • When a map sync event is triggered in Cisco CMX, calibration model is also sent along with maps data to Cisco DNA spaces.

IP Address and Username Hashing	Cisco CMX hashes the IPv6 address in northbound notifications to comply with privacy regulations as per General Data Protection Regulation (GDPR).
V3 API support	Cisco CMX supports REST Version 3 APIs. With this enhancement, V3 APIs support the following: • Wi-Fi RFID Tags • Rogue Clients • Rogue APs • Interferers
Northbbound Notification subscription limitation	This feature limits adding northbound notifications if active notification count is five.
MAC Randomization for associated devices	Cisco CMX will not filter random MAC when devices are associated with it.
Support Radius Authentication without FIPS	In Cisco CMX Release 10.6.3, the External Authentication (AAA) feature is enabled without the Federal Information Processing Standard 140-2 (FIPS) or the U.S. Department of Defense Unified Capabilities Approved Products List (UCAPL) mode.
System at a Glance > Time display	This feature ensures that Cisco CMX recommends a restart when system update time reaches the configured threshold.
Cisco CMX GUI Login information display	To comply with the US Department of Defense Information Network Approved Products List (DODIN APL) requirements, Cisco CMX GUI displays the last login details of the logged in GUI user if user has admin privileges. Cisco CMX CLI displays the last logged in cmxadmin user.
Syslog over TCP	Cisco CMX supports Rsyslog server configuration using TLS or IPSec protocol.
New device support	Cisco Catalyst 9105AX Series Access Points
Critical bug fixes	Provides critical bug fixes.

The following features are removed from Cisco CMX Release 10.6.3:

- **Connect** and **Presence** services: In Cisco CMX Release 10.6.3, **Connect** and **Presence** services are removed. When installing Cisco CMX, the installer window does not show **Presence** node as an option starting from CMX Release 10.6.3. The **Connect** tab is also removed from Cisco CMX.
- BLE support from Cisco CMX (BLE related features/APIs/CLIs): In Cisco CMX Release 10.6.3, BLE support is removed. BLE tracking is not supported in Cisco CMX 10.6.3. The BLE Management Cloud Application connection support from Cloud Application is not avaliable anymore.

- Client V1/V2 API support: In Cisco CMX Release 10.6.3, all V2 location client APIs are deprecated. V2 API support is disabled from this release onwards.
- **Analytics > Schedule Report**: In Cisco CMX Release 10.6.3, the **Analytics Schedule Report** is deprecated. The **Schedule** and **Download** options are removed from the **Analytics > Dashboard**.
- **Analytics > Correlation and Path Widget**: The **Correlation** and **Path** widgets are deprecated in **Analytics** service.
- **Analytics > Repeat Visitor History**: In Cisco CMX Release 10.6.3, the support for tracking repeat visitor history is disabled.

System Requirements

Supported Hardware

- Cisco CMX Release 10.6.3 supports Cisco Catalyst IW9167E Heavy Duty Access Point and Cisco Catalyst IW9167I Heavy Duty Access Point.
- 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, that 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.html.

Note Cisco CMX does not support VMware tools.

The following table 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 4: 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 6.7 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 and Cisco 3375 Appliance for Cisco Connected Mobile Experiences. By default, Cisco Hyperlocation is disabled on Low-End appliances.

- 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/products/collateral/wireless/mobility-services-engine/datasheet-c78-734648.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 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.
- See the following tables when backing up and restoring Cisco CMX data between the Cisco 3375 appliance, Cisco MSE appliance, and Cisco vMSE appliance.

Table 5: 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 6: 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

Restore From...	Restore To...	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.

Licensing Information

Table 7: 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 License	Features
• 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 11.0.0 is a new OVA installation for Cisco CMX. Inline upgrade from Cisco CMX Release 10.6.3 to Cisco CMX Release 11.0.0 is not supported.
- Database migration is supported only from Cisco CMX Release 10.6.3-146 to Cisco CMX Release 11.0.0. You must install the Cisco CMX Release 10.6.3-146 Patch Release on the primary server running Cisco CMX Release 10.6.3-146 to migrate data.
- (CSCvp04706) Use the CLI, not the GUI, to upgrade to Cisco CMX Release 10.6.1 or later.
- After upgrading to Cisco CMX Release 10.6.3, the Cisco Prime Infrastructure stops displaying clients on the Cisco Prime Infrastructure map. This is due to the deprecation of V1 and V2 client API calls in Cisco CMX Release 10.6.3. Cisco Prime Infrastructure Release 3.8 and earlier versions use V1and V2 API calls to Cisco CMX to get the client information, and hence, fails. To work around this issue, in the Cisco Prime Infrastructure Release 3.9, there is an option to specify the Cisco CMX V3 API credentials while adding Cisco CMX in Cisco Prime Infrastructure, resulting in Cisco CMX Release 10.6.3 working with Cisco Prime Infrastructure Release 3.9.
- 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.
- Backups from Cisco CMX Release 10.4.x can be restored in Cisco CMX Release 10.5.x and later.
- Backups from Cisco CMX Release 10.3 or earlier cannot be restored in Cisco CMX Release 10.5.x and later.
- 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.
- Cisco CMX Release 10.6.3 - 105 and 10.6.3 - 146 are supported on an ESXi-7.0.2 - 17630552-standard (VMware) device. However, Cisco CMX Release 10.6.3 - 70 is supported on ESXi 6.0 through 6.7 only.

For information about upgrading from an earlier Cisco CMX release to the latest 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

- (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.

Caveats

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

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

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, on page 17.

Bug ID	Description
CSCwc85002	CMX 10.6.3-146: Reboot required to complete ISO installation via CIMC html option
CSCwb72268	CMX unable to form HA with Error running nodesetup; Degrades core services upon sync-failure

Resolved Caveats in Cisco CMX Release 10.6.3-146 Patch

Bug ID	Description
CSCwc99232	Cannot create notification when DeviceType is RFID Tag, clients or anything other than all

Resolved Caveats in Cisco CMX Release 10.6.3-146

Bug ID	Description
CSCwc09551	CMX-HA sync-failure prevents SSH login on Secondary CMX
CSCwc09547	CMX-HA man-in-the-middle/known_hosts exception breaks sync
CSCwc22845	CMX: Adding rsyslog server via TLS still shows the method to be IPSEC
CSCwa98899	CMX 10.6.3: Session Cookie Does Not Contain the "Secure" Attribute for TCP port 1948
CSCwb08580	nmsplb service is down
CSCwb19646	Multiple Vulnerabilities Found By Nessus on CMX 10.6.3(105)

Bug ID	Description
CSCwb55537	Vulnerability on CMX 10.6.3(105) when CBC ciphers on CMX appliance and CIMC is enabled
CSCwb72332	CMX showing MAPs incorrectly after import

Resolved Caveats in Cisco CMX Release 10.6.3-105 Security Patch

Bug ID	Description
CSCwa47312	Evaluation of cmx for Log4j RCE (Log4Shell) Vulnerability vulnerability

Resolved Caveats in Cisco CMX Release 10.6.3-105

Bug ID	Description
CSCvt95006	CMX 10.6.2-72: certificate installation gets stuck on CRL download.
CSCvx07554	CMX Smart Licensing with Proxy
CSCvx48497	Cisco CMX 10.6.3: Analytics service is throwing errors leading to Location process consuming CPU
CSCvx75593	Schedule backup fails due to file permission issues on CMX 10.6.3
CSCvz37414	CMX 10.6.3 Multiple Vulnerabilities Detected
CSCvw72659	Cisco Connected Mobile Experiences Strong Authentication Requirements Enforcement Bypass
CSCvw79801	CMX FIPS: RADIUS server credentials are stored in clear text in logs
CSCvw83235	Process classification field for Rogue AP from Type 25 message not shown
CSCvw96216	CMX 10.6.3 - QID 11827: HTTP Security Header Not Detected - missing “X-Conent-Type-Options” header
CSCvx44044	Clients outside the inclusion region showing on API as inside
CSCvx47832	CMX 10.6.-XX Hyperlocation diagnostic tool shows results as indeterminate for WLC and AP tests
CSCvx61490	CMX Campus address truncated
CSCvx93329	CMX 10.6.2 client device information may be reported under tagManufacturer in API responses
CSCvx93861	Unable to establish a nmsp connection from C9800 - > CMX (IPv6 deployment)
CSCvy31211	CMX Smart Licensing Error
CSCvy59628	v3 API enhancement for Rogue, Rouge AP, RFID tag and Interferer

Bug ID	Description
CSCvw52863	Process classification field for Rogue AP from Type 25 message

Resolved Caveats in Cisco CMX Release 10.6.3

Note Cisco CMX Release 10.6.3 includes all the bug fixes of the Cisco CMX Release 10.6.2-89. For more information about the resolved caveats in 10.6.2-89 build, see the "Resolved Caveats in Cisco CMX Release 10.6.2-89" section in the *Release Notes for Cisco Connected Mobile Experiences (CMX), Release 10.6.0 and Later* at:

https://www.cisco.com/c/en/us/td/docs/wireless/mse/release/notes/cmx_10_6_rn.html.

Bug ID	Description
CSCvv23233	CMX HA failure due to Postgres connection failed
CSCvv57203	CMX: Improper Privilege Management
CSCvt95006	CMX 10.6.2-72: cert installation stuck on CRL download
CSCvv57192	CMX: Insecure Direct Object Reference
CSCvv97836	CMX AAA integration with Cisco ISE not working
CSCvn45497	CMX sends SNMP getrequest without community string
CSCvv05994	Nmsplb service runs out of memory and hangs in CMX location
CSCvv53660	CMX 10.6: Users with location permission not able to see control panel (side bar)
CSCvo15147	APIs for Exporting Large Dataset from CMX Cassandra Database not working
CSCvp51131	CMX 10.6.0-177 Running unsecure version of OpenSSH 7.5p1 (dating back to 2017)
CSCvs28427	CMX shows \"Error exporting cassandra datajava.lang.RuntimeException\" when extracting database on CLI
CSCvv37334	CMX pam_limits misconfig floods syslogs
CSCvv57192	CMX: Insecure Direct Object Reference
CSCvv68542	Cannot deploy CMX HA after uploading
CSCvj58260	10.5 : \"cmxctl stop -a\" not stopping all services
CSCvq76301	CMXOS ntp type command is not intuitive
CSCvs93938	CMX Unable to Display Version Number for all User Roles

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 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.