Release Notes for Cisco CMX Release 10.2.0 and Later

First Published: September 25, 2015
Last Modified: March 28, 2016

This document describes what is new in Cisco Connected Mobile Experiences (Cisco CMX) Release 10.2.0 and later, and the system requirements, upgrade scenarios, and caveats. Unless otherwise noted, Cisco Connected Mobile Experiences is referred to as Cisco CMX in this document.

Contents

This document contains the following sections:

- Introduction, page 2
- What's New, page 2
- System Scaling, page 13
- System Requirements, page 13
- Solution Compatibility Matrix, page 14
- Upgrading Cisco CMX, page 14
- Licensing Information, page 14
- Software Release Recommendations, page 16
- Important Notes, page 16
- Caveats, page 17
- Documentation Errata, page 22
- Troubleshooting, page 29
- Related Documentation, page 29
- Obtain Documentation and Submit a Service Request, page 30

Cisco Systems, Inc.
www.cisco.com

Introduction

Cisco CMX Release 10.2.x is a high-performing scalable software solution that addresses the mobility services requirements of high-density Wi-Fi deployments.

What's New

- What's New in Cisco CMX Release 10.2.3, page 2
- What's New in Cisco CMX Release 10.2.2, page 4
- What's New in Cisco CMX Release 10.2.1, page 6
- What's New in Cisco CMX Release 10.2.0, page 6

What's New in Cisco CMX Release 10.2.3

- Cisco Aironet 1800, 2800, and 3800 Series Access Points Support, page 2
- Portal Login Frequency, page 2
- Analytics Report Filtered for Associated Devices, page 2
- SSID Filtering in the Location Service, page 3
- Inclusion/Exclusion Region, page 3
- Northbound Notifications Improvements, page 3
- Feature Flag and UI Responsiveness, page 3
- Hyper–V Support, page 3
- Real-Time Analytics Reports, page 4

Cisco Aironet 1800, 2800, and 3800 Series Access Points Support

Cisco CMX Release 10.2.3 supports the Cisco Aironet 1800, 2800, and 3800 Series Access Points.

Portal Login Frequency

You can define how often your login page is displayed to a visitor each time their device associates with the SSID in your network. By default, a repeat visitor does not need to go through the portal login process for 180 days from the day the visitor associated with the SSID. For the configuration procedure, see the "Changing the Portal Login Frequency" section on page 23.

Analytics Report Filtered for Associated Devices

You can create filtered analytics reports based on all visitor devices connected to the network (regardless of SSID) and on all visitor devices detected by the network. These are categorized as CONNECTED and DETECTED devices. In addition, any devices filtered by the Location service is also excluded from analytics reports. For the configuration procedure, see the "Creating an Analytics Report Based on Connected or Detected Devices" section on page 24.

SSID Filtering in the Location Service

You can configure filtering in the Cisco CMX Location Service to exclude all visitor devices that are associated to a particular SSID. For the configuration procedure, see the "Configuring SSID Filtering in the Location Service" section on page 24.

Inclusion/Exclusion Region

The Create Inclusion/Exclusion feature allows you to create inclusion and exclusion regions on a floor.

- Inclusion regions define areas within a floor where wireless devices will be either inside or snapped on the boundary (due to weak coverage). There will be one inclusion region per floor only. When there is no inclusion region defined in the floor maps, Cisco CMX creates a default inclusion region that is the same as the floor dimension. We recommend having one inclusion region on a floor to correctly bound the clients on floor area.
- Exclusion regions define areas within a floor which are inside an inclusion region. In an exclusion region, wireless devices will be ignored. There could be multiple exclusion regions per floor.

Defining inclusion and exclusion regions can help you focus Cisco CMX processing to just those areas of the map where you want to manage your wireless devices, and ignore others.

For the configuration procedure, see the "Creating an Inclusion or Exclusion Region" section on page 24.

Northbound Notifications Improvements

You can now view northbound notifications from the Cisco CMX UI and CLI. For the procedure, see the "Viewing Northbound Notifications" section on page 25.

Feature Flag and UI Responsiveness

You can use the **cmxctl config featureflags** command to enable and disable Cisco CMX Analytics features. For example, the CMX system includes an ALERT tab, to have these alerts configured you need to set the feature flag to enable alerts. This tab also displays hashtags and statistics information.

For more information about the **cmxctl config featureflags** command, see the "cmxctl config featureflags" section on page 27.

Hyper–V Support

You can now run Cisco CMX on Microsoft Hyper-V virtualization hosts. This enables you to use Cisco CMX on virtual machines using any Hyper-V capable host running Windows Server 2008 R2 or later. You can create a new virtual machine using Hyper-V Manager application. Ensure to specify 24 GB of memory or higher when creating the virtual machine in Hyper-V manager, and to subsequently increase the processor count for the virtual machine to 8 vCPU or higher before starting the new virtual machine.

If you are running Windows Server 2012 or later, we recommend you to convert the Cisco CMX .vhd disk image to .vhdx format before adding it to the new virtual machine. For the configuration procedure, see the "Creating New Virtual Machines Using Hyper-V Manager" section on page 25.

Real-Time Analytics Reports

You can now view real-time analytics reports in the Cisco CMX GUI. This is a new tab that shows you a WIFI adoption widget based off of the REAL TIME information. The **NOW** parameter for Analytics has been removed.

What's New in Cisco CMX Release 10.2.2

The Cisco CMX Release 10.2.2 underwent extensive validation to improve quality and includes these feature enhancements:

- License Enforcement, page 4
- Property Management System Integration, page 4
- Policy Plans, page 5
- User Opt-Out Option, page 5
- Hyperlocation Diagnostics, page 5
- Queue Analytics, page 5
- Presence Notification, page 5

License Enforcement

Cisco CMX displays an alert when the 120-day Cisco CMX evaluation license expires. The alert includes a link to add a permanent license. You must upload a permanent license to CMX before the evaluation license expires. Otherwise, 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.

After the evaluation license expires, only users with admin privileges can log in to add additional licenses.

Property Management System Integration

Using the Cisco CMX Connect service in Cisco CMX Release 10.2.2, you can integrate a Property Management Systems (PMS) solution (for example, a PMS solution used by a hospitality industry). The PMS solution in Cisco CMX:

- Provides a guest WiFi portal at a hotel
- Provides flexibility to assign different WiFi plans to different portals at different locations

Currently, the Cisco CMX Connect service only integrates with the Nevotek Property Management System accounts. The Nevotek Property Management System is a paid service for which the customer must establish their own account or subscription.

Policy Plans

The Cisco CMX Policy Plans feature gives you the option to specify location-specific bandwidth and to control the bandwidth assigned to the client as they move from one location to the next. Use the **CMX Policy Plans** window to configure this feature.

For example, the bandwidth provided to clients in a hotel room is higher than the bandwidth provided in a hotel lobby. If the CMX Policy Plans feature is active, the bandwidth to the client is automatically increased when the client moves from the lobby to their hotel room. In addition, if the **Keep Highest Bandwidth** check box on the **CMX Policy Plans** window is selected, the client retains the higher bandwidth when returning to the lobby.

Note To use the Cisco CMX Policy Plans feature, make sure the Cisco CMX Property Management System (PMS) feature is disabled. In addition, adding a PMS server disables the Cisco CMX Policy Plans feature. By default, the Cisco CMX PMS feature is disabled.

User Opt-Out Option

The Cisco CMX Connect service allows the user to opt-out from having their mobile device location history maintained and used by CMX.

Hyperlocation Diagnostics

The Hyperlocation Diagnostics tool executes a set of tests to verify common issues found on the Cisco WLC, Cisco AP, and Cisco CMX when deploying Cisco HyperLocation. These tests are executed against an existing Cisco Hyperlocation setup on a floor. The floor should have clients associated to Cisco Hyperlocation access points to validate complete functionality. Execution of the full set of tests requires credentials for the Cisco WLC and the HyperLocation-enabled Cisco APs.

Queue Analytics

A specialized analytics widget that calculates Queue Time instead of Average Dwell Time is available when an instance is configured with the airport vertical.

Presence Notification

The CMX Presence Notifications feature provides notifications when the presence of passersby is detected, when passersby become visitors, when visitors have left the network, and when the site entry changes.

What's New in Cisco CMX Release 10.2.1

- Cisco Hyperlocation, page 6
- Cisco CMX FastLocate, page 6

Cisco Hyperlocation

The Cisco Hyperlocation solution is a suite of technologies that enable advanced location capabilities through a mix of software and hardware innovations. Cisco CMX Release 10.2.1 supports Angle of Arrival (AoA) technology available on Cisco Aironet 3600/3700 access points with a Hyperlocation module and a Hyperlocation antenna. Cisco CMX uses advanced location algorithms to extract phase differences to accurately locate associated wireless clients within 1 meter accuracy.

Note Cisco Aironet 3600/3700 APs Release 8.1.131.20 or later support CMX Hyperlocation. In addition, Hyperlocation is not supported on the Cisco Virtual Wireless LAN Controller (vWLC).

The Cisco Hyperlocation module with advanced security also integrates Bluetooth Low Energy (BLE) Beacons with the module. Customers can take advantage of hassle-free BLE Beacon deployment powered over Ethernet and centrally managed from the convenience of a data center. This eliminates the need for local IT engineers to perform an inspection walk of BLE beacon health, using an app on their Smart devices. Cisco Hyperlocation brings configurable BLE beacon technology since a single Hyperlocation module can be configured to beacon out five different BLE beacons to enable applications.

Cisco CMX FastLocate

Cisco CMX FastLocate technology enables quick location refresh for connected WiFi clients. RSSI from data packets and probe frames when available are used for calculating location. It is available with both centrally switched WLANs as well as FlexConnect (locally switched WLANs).

Note Cisco Aironet 700, 1700, 2600/2700, and 3600/3700 APs support Cisco CMX FastLocate when used with Cisco WLC Release 8.1.131.18 or later, and with Enhanced Local Mode enabled. Cisco 3600/3700 APs also support Cisco CMX Fastlocate with dedicated radio modules.

These are the recommended AP modes:

- Enhanced Local Mode: APs scan opportunistically on-current channel and off-channel with up to ~15 percent performance impact to data serving radios.
- Monitor Mode AP: APs scan on 2.4 and 5 GHz bands.
- Modular AP: Cisco 3600/3700 APs with Hyperlocation Module or Wireless Security Module (WSM) scan on 2.4 and 5 GHz bands with no impact to data serving radios.

What's New in Cisco CMX Release 10.2.0

- Presence Analytics, page 7
- Social Analytics, page 8
- Verticalization, page 8

- Detect and Locate Features, page 9X
- Connect Features, page 9
- Analytics Features, page 10
- Platform Features, page 11

Presence Analytics

Note You cannot run both the Location and Presence Analytics services on the same Cisco CMX instance.

The Presence Analytics service uses the received signal strength indicator (RSSI) along with the duration of the RSSI from a client device to determine whether a client device is in the site or is a passer-by. Presence Analytics takes input directly from the Network Management Services Protocol (NMSP) load balancer in the form of a MAC address and observed RSSI values for the MAC address.

There are two RSSI threshold values defined for a site, low (default of -95 dBm) and high (default of 65 dBm).

- Clients with RSSI below the low threshold are discarded.
- Clients with RSSI above the low threshold are classified as *passer-by*.
- Clients with RSSI above the high threshold plus *x* minutes (default of 5) in the past 20 minutes are classified as visitors.

Note Clients associated with an access point (AP) in a site are classified as visitors at the site.

Presence Analytics does not require APs to be placed on a map; they should only be associated with a site. The Presence Analytics feature neither uses nor requires maps. Therefore, all the configurations are accomplished from the Dashboard rather than the Manage tab.

Table 1 lists the Presence Analytics features.

Table 1 Presence Analytics Features

Feature Name	Benefits
Dashboard— Key Performance Indicators (KPIs)	Allows users to view the Presence Analytics Dashboard for a site for a day, week, or month and displays (KPIs).
Dashboard—Proximity count and distribution	Shows a break-up of passersby, visitors, and connected devices hourly, for a site for a day, week, or month.
Dashboard—Dwell time count and distribution	Shows a break-up of dwell time based on five predefined intervals, for a site for a day, week, or month. Dwell Time buckets of 5-30 min, 30-60 min, 1-5 hour, 5-8 hour, and 8 hour+ are hard coded and nonuser configurable.
Dashboard—Repeat visitors - count and distribution	Shows a break-up of daily, weekly, occasional, first time, and yesterday's visitors, for a site for a day, week, or month.
Dashboard—Insights and weather	Shows weekly and monthly insights of busiest day, peak visitors, and peak first-time visitors.

Social Analytics

Cisco CMX provides the ability to use data collected from social media to provide analytics, which can be used to enhance decision-making capabilities. Business organizations can analyze their online reputation and view trends relating to positive and negative comments about their events or services.

Social Analytics is currently limited to interaction with Twitter only, with Cisco CMX making API calls to Twitter servers. Cisco CMX establishes a connection to the Twitter server public search API filtered for the configured tags.

The Social menu option on the Analytics service provides access to the collected data. Tweets are collected using a background process. The process starts every hour and collects for 90 percent of the hour (nonconfigurable). The process stops at the end of the hour and a new process starts.

In the Social Analytics window, you can perform the following operations:

- Use the Filter options to select the locations to analyze.

  Data can be evaluated:

  - From either a single location or multiple locations combined
  - Daily, weekly, monthly, or yearly
  - For a predefined portion of the day
- Click the Configure icon to open the Term Definition window.
- Define the hash tags or terms to look for.

The upper half of the Social Analytics UI provides the current statistics gathered from the tweets matching the currently configured hashtags. The lower half of the UI provides a day-to-day detail comparison.

Verticalization

The Verticalization capabilities provide the ability to change the names or terms associated with each level of the hierarchy used in the Analytics report generation.

Although you can change the names of the hierarchy levels, the names of the existing elements, if any, cannot be changed once they are created. The renaming process is global and will impact all users.

To configure verticalization, perform the following procedure:

1. Log in to Cisco CMX.
2. Choose **Manage > Verticalization**.
3. Choose one of the five available verticals:
   - **Retail**
   - **Mall**
   - **Hospitality**
   - **Education**
   - **Healthcare**
   - **Airport**
4. Click **Run Setup Wizard**.

Detect and Locate Features

Cisco CMX uses advanced RSSI-based trilateration algorithms to locate Wi-Fi and non-Wi-Fi assets.

Connect Features

Table 2 Cisco CMX Connect Features

Feature Name	Benefits
Portal and Image Libraries	The new user interface of the portal and image libraries simplify portal and image management. Image library—Allows the same image to be used more than once while uploading multiple copies. The new image library allows an imported image to be used for multiple portals. There is no size limit on uploaded images because they are scaled during the upload. After being uploaded, they can be rotated, cropped, or have their aspect ratio changed using the built-in image editor. Portal library—Allows you to: • Copy and edit an existing portal. • Create a new portal without assigning it. • Save a design, which is in progress, as a draft. • Preview a design before assigning it. The Portal editor now provides preview options for laptops and tablets along with phones.
Support for Multiple Languages	Provides venue owners with an option to serve portal splash pages in different languages. The languages supported by a splash page must be added to the page library before they can be enabled for the page. **Note** Cisco CMX does not contain any language translation engines. The administrator must edit each language page individually and manually translate all text entries.
SMS Authentication	In order to prevent the Cisco Connect service from not meeting the requirement of providing proof of identity of a connected individual, Cisco CMX offers the ability to add SMS-based authentication to a custom portal. Currently, Cisco CMX only integrates with Twillio accounts for SMS authentication. Users must procure their own Twillio account. **Note** You can have only one Twillio account. However, since that account can have many phone numbers associated with it, you can use the same account with multiple portals, but each portal can only have a single number associated with it. Also, this feature requires users to have an SMS-capable device to gain access to the network. Users can either edit an existing portal or use a template to create a new portal to use this feature.
Reports and API Enhancements	Connect reports provide the following additional capabilities: • Number of visitors on the current day and their load on the network. • Pages Served vs Submitted. • SMS Sent vs Authenticated. • Languages Used.

Analytics Features

Cisco CMX has three new widgets that can be added to a custom Analytics report:

- Path Analysis
- Associated Status
- Dwell Time Breakdown

Table 3 Cisco CMX Analytics Features

Feature Name	Benefits
Path Analysis	This widget brings back the concept of Most Popular Path analysis. The green (left) side represents where a device is coming from, for example, immediately before entering the focus zone. The blue (right) side represents where a device goes to, for example, immediately after exiting the focus zone. Hovering your cursor over the focus displays a break-up of: • Percentage of paths that either started or ended in the focus zone. • Percentage of paths that either arrived at or departed from the focus zone. Hovering your cursor over a green section shows how many paths that entered the focus zone originated from this zone. Hovering your cursor over a blue section shows how many paths that originated in the focus zone ended from this zone.
Associated Status (also known as Connected vs Detected)	This widget provides comparison between connected and detected devices by time or areas. Detected—Seen probing. Connected—Associated to an AP. This widget can be configured to show this relationship on an hourly, daily, or weekly basis. Hover your cursor to reveal the actual numbers for each interval.
Dwell Breakdown	This new widget displays dwell-time distribution for selected areas, for example: 20 percent of the visitors stayed less than an hour. 50 percent stayed for 1-2 hrs. 30 percent stayed for more than 2 hrs. You can configure this widget to show dwell-distribution on an hourly, daily, or weekly basis for the selected area.
Client Playback	Shows up to 24 hours of movement of a device on the floor. The following are the features of this widget: • Limited to displaying a single device at a time. • Shows movement one floor at a time. • Provides the ability to jump to previous or next floor.

Platform Features

Table 4 lists the Platform features.

Table 4 Platform Features

Feature Name	Benefits
New User Accounts	Cisco CMX Release 10.2.0 introduces two new user accounts to prevent any potential misuse of the root user account. The new user accounts are: • cmx—A no-login account that includes all the Cisco CMX processes, with the exception of postgress. • cmxadmin—A primary account used to perform all administrative tasks. Users can use sudo from this account to perform tasks requiring root-level access.
Software Packaging	The installation process uses an open source configuration and management tool called SaltStack. This enables standardization, such as International Organization for Standardization (ISO), Open Virtualization Archive (OVA), cloud virtual machines (VMs), and upgrade packages. The Salt-base installation model consists of the following components and packaged in a single file named CISCO_CMX$$$.cmx: • The base operating system, which is a minimal installation of CentOS 6.6. • The Cisco CMX repository, which contains both the necessary cmx rpm files and other files to install and upgrade any mandatory operating system or third-party dependencies. • The Salt configuration. The Cisco CMX software is packaged as follows: • .iso—File for initial install on a physical appliance such as Cisco MSE 3365. • .ova—File for use with the VMware vSphere client for initial installation of a virtualized Cisco MSE appliance on customer-provided hardware. • .cmx—New installation and upgrade package that contains a mountable CD image (mounted at /mnt/cmx), which contains the Cisco CMX repository, Salt configuration information, and an .md5 file to verify the integrity of the repository. **Note** Users do not have to make changes to the operating system manually beyond the network configuration and node type choice.

Table 4 Platform Features (continued)

Feature Name	Benefits
Initial Installation	Cisco CMX Release 10.2.x software can be installed on a Cisco MSE 3365 that is currently running 8.0 code, using the .iso image. file (CISCO_CMX-10.2.0-213-3365.iso). **Note** All data on the MSE 8.0 system will be erased and no data migration is supported. **Note** Cisco CMX Release 10.2.x is supported on the MSE 3355 but on a limited scale in terms of number of tracked clients and number of WLCs synchronized. Cisco Hyperlocation is not be supported on the MSE 3355. Scale numbers for Location and Presence Analytics will be published at a later date. Cisco WLC Release 8.1.131.0 or later is required to use with CMX Hyperlocation. The .iso image can be loaded on a USB stick or mounted as a virtual drive using the Cisco Integrated Management Controller (CIMC). For more information, see the "Installing the CIMC Firmware Update Utility" chapter in the *Cisco CIMC Firmware Update Utility User Guide*. Cisco CMX Release 10.2.x software is deployed on a new Cisco MSE Virtual Appliance (vMSE) by using the VMware vSphere client to deploy the .ova file available on Cisco.com. A new first-boot script determines if the initial configuration has been completed or not. If it is not completed, the script prompts for a default login or a normal login. **Note** Initial login requires password configuration for both the root and new cmxadmin user.
Changing Network Configuration	The Network configuration information can be changed after deployment by issuing the **cmxos reconfigure** command from the Cisco CMX CLI. This feature allows you to change the IP address, netmask, default gateway, and Domain Name System (DNS) server information. The Network Time Protocol (NTP) server information can be changed by using the vi editor to manually edit the etc/ntp.conf file to change the server line to reflect the new NTP server fully qualified domain name (FQDN).
Password Recovery	Cisco CMX uses a *single user mode* to reset the root or cmxadmin user password. Entry into the single user mode requires: • A non-SSH console connection to the Cisco MSE. • A power cycle of the Cisco MSE appliance. The GUI admin user password can be reset to the default admin password from the Cisco MSE CLI with the **cmxctl reset ui-password** command. CLI access requires that you to know the password of the cmxadmin user.
Upgrading Cisco CMX Release 10.2.x to Future Releases Using Cisco CMX Web UI	After you install Cisco CMX Release 10.2.x, future updates can be performed through the Cisco CMX GUI or by using the **cmxos upgrade** command and the .cmx file, while you are logged in as cmxadmin, for example, **cmxos upgrade** *<CISCO_CMX$$$.cmx>*

System Scaling

For information, see the *Cisco Connected Mobile Experiences Data Sheet*: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/connected-mobile-experiences/datasheet-c78-734648.html.

System Requirements

Cisco CMX Release 10.2.x can be installed on a physical or virtual Cisco MSE appliance. Virtual Cisco MSE appliances require either VMware ESXi 5.1 or later, or Microsoft Hyper-V.

Note Cisco CMX Release 10.2.x is supported on the MSE 3355 and 3365 but on a limited scale in terms of number of tracked clients and number of WLCs synchronized. Cisco Hyperlocation is not be supported on the MSE 3355. Scale numbers for Location and Presence Analytics are included in the *Cisco Connected Mobile Experiences Data Sheet*: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/connected-mobile-experiences/datasheet-c78-734648.html.

Cisco WLC Release 8.1.131.20 or later is required to use with CMX Hyperlocation.

- Computing Requirements, page 13
- Browser Support, page 14

Computing Requirements

Table 5 lists the Cisco CMX Release 10.2.x hardware guidelines for a virtual Cisco MSE appliance, such as VMWare or Microsoft Hyper-V.

For complete requirements, see the *Cisco Connected Mobile Experiences Data Sheet*: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/connected-mobile-experiences/datasheet-c78-734648.html.

Table 5 Hardware Guidelines

Hardware Platform	Basic Appliance	Standard Appliance	High-End Appliance
CPU	8 vCPU \ 4 physical cores	16 vCPU \ 8 physical cores	20vCPU \ 10 physical cores
RAM	24 GB RAM	48 GB RAM	64 GB RAM
HDD	500 GB HD	500 GB HD	1TB HD

Browser Support

Cisco CMX Release 10.2.x has been tested using the following browser:

- Google Chrome 50 and later

Cisco CMX Location, Connect, and Configuration APIs have been tested using the following browser:

- Google Chrome 50 and later

Solution Compatibility Matrix

For information, see the "Cisco Connected Mobile Experiences (CMX) Compatibility Matrix" section in the *Cisco Wireless Solutions Software Compatibility Matrix*: http://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html.

Upgrading Cisco CMX

Cisco CMX Release 10.2.x is available as software that can be run on physical or virtual Cisco MSE appliances. No database migration or inline upgrade is supported from Cisco MSE 8.0 or earlier to Cisco CMX Release 10.2.x. You can upgrade from Cisco CMX Release 10.1.x to Cisco CMX Release 10.2.x. We recommend that you run Cisco CMX Release 10.2.x in parallel with the existing Cisco MSE 8.0 or earlier, and utilize the evaluation license for 120 days. After the evaluation period, the older Cisco MSE can be decommissioned.

- For information about upgrading from Cisco CMX Release 10.2.0 to 10.2.1 or later, see http://www.cisco.com/c/en/us/td/docs/wireless/mse/10-2/installation/guide/installation_guide/MSE_Installation_Using_Vsphere_Client.html#pgfId-1255361
- For information about upgrading from Cisco CMX Release 10.1.x to 10.2.x, see http://www.cisco.com/c/en/us/td/docs/wireless/mse/10-2/installation/guide/installation_guide/MSE_Installation_Using_Vsphere_Client.html#pgfId-1291078

Note Information related to Cisco CMX Release 10.2.x upgrades is described in the *Cisco MSE Virtual Appliance Installation Guide for CMX Release 10.2*.

Note In Cisco CMX Release10.2.2, the analytics client count trend was corrected to reflect the actual counts. After upgrading from Cisco CMX Release 10.2.1 to 10.2.2, the analytics client count trend is higher.

Licensing Information

Note For information about procuring Cisco CMX licenses, see the *Cisco Connected Mobile Experiences (CMX) Version 10 Ordering and Licensing Guide*.

For information about adding and deleting licenses, see the "Managing Licenses" section in the *Cisco Connected Mobile Experiences Configuration Guide, Release 10.2*.

- Cisco CMX Release 10.2.x continues to use two-tier licensing—Cisco CMX Base and Cisco CMX Advanced. (The Connect service is now included as part of the Cisco CMX Base license.)

  The CMX Base license provides the following services:

  - Detect and Locate —The ability to determine the location of Wi-Fi clients, Bluetooth Low Energy (BLE) beacons, devices, and Radio Frequency Identification (RFID) tags
  - Connect—Visitor Wi-Fi onboarding platform
  - APIs—Third-party integration using standard REST APIs
  - Location, Connect, and Configuration APIs

  The CMX Advanced license provides the following services:

  - Includes all the Cisco CMX Base services—Detect and Locate, APIs, Connect
  - Location Analytics\Presence Analytics
  - Analytics APIs
- The Evaluation License of Cisco CMX Release 10.2.x provides full functionality for a period of 120 days. Evaluation of Cisco CMX Base and Cisco CMX Advanced licenses are built in with every Cisco CMX Release 10.2.x instance. There are no limitations with regard to the functionalities when you use the Evaluation License in a current release.
- Every Cisco CMX Release 10.2.x box or image ships with a 120-day evaluation license for all the services. The countdown starts when you start Cisco CMX and enable a service.

Note Two weeks before the evaluation license expires, you will receive a daily alert to obtain a permanent license. If the evaluation license expires, you will not be able to access the Cisco CMX GUI or APIs. Cisco CMX will continue to run in the background and collect data until you add a permanent license and regain access to it. For information about adding and deleting licenses, see the "Managing Licenses" section in the *Cisco Connected Mobile Experiences Configuration Guide, Release 10.2*.

- Accounting starts from the day you start using the Cisco CMX Release 10.2.x software. Each day, the evaluation license is decremented by one.
- The license page shows a summary of the current licenses and their state. If a service is running and its license has expired, an `Out of Compliance` message is displayed. However, the service is still allowed to run.

Note Out-of-compliance licenses running in Cisco CMX Release 10.2.x will not receive any support from the Cisco Technical Assistance Center.

- You can add any license file from Cisco MSE 8.0 or earlier to Cisco CMX Release 10.2.x.

Note For information about adding and deleting licenses, see the "Managing Licenses" section in the *Cisco Connected Mobile Experiences Configuration Guide, Release 10.2*.

- In Cisco CMX Release 10.2.x, the licenses are not node-locked to a box.

Software Release Recommendations

Table 6 lists the recommended Cisco CMX software releases and their benefits.

Table 6 Software Release Recommendations

Cisco CMX/Cisco MSE Release	Benefits
Cisco MSE Release 8.0.130.0	This release should be used in production environments that require the full suite of Cisco MSE features.
Cisco CMX Release 10.2.2 and later	This release is suitable for deployments where the following features are required: • Detect & Locate • Analytics • Presence Analytics • Connect • Hyperlocation (Release 10.2.1 or later) • FastLocate (Release 10.2.1 or later) This release is *not* suitable for deployments where the following features are required: • aWIPS • CMX SDK • FIPS deployment • Cisco CMX Release 10.2.x supports RTLS tag integration (such as Aeroscout). Check with the third-party vendor on the availability of CMX-supported software. • Cisco Prime Infrastructure integration, specifically the ability to see WiFi clients and other devices and Cisco CleanAir information in Prime.

Installing a Cisco MSE Virtual Appliance

For information about installing a Cisco MSE Virtual Appliance, see the *Cisco MSE Virtual Appliance Installation Guide, CMX Release 10.2* at:

http://www.cisco.com/c/en/us/td/docs/wireless/mse/10-2/installation/guide/installation_guide.html

Important Notes

- From Cisco CMX Release 10.1.x, Cisco CMX, Cisco Wireless LAN Controller (Cisco WLC) and Cisco Prime Infrastructure will be independently version numbered. See the "Solution Compatibility Matrix" section on page 14 to identify release numbers of individual components for your deployment.
- Cisco CMX Release 10.2.x requires interaction with Cisco Prime Infrastructure only during the initial installation stage. After the maps and controllers are imported from Cisco Prime Infrastructure, the two do not have run-time dependencies.
- Unlike in releases earlier than Cisco CMX Release 10.1.x, zones are created in Cisco CMX Release 10.1.x or Cisco CMX Release 10.2.x after the maps are imported from Cisco Prime Infrastructure.

- Changing the hostname through command line is not supported. Use the **cmxos reconfigure** command to change a hostname, IP address, or any of the network parameters.
- The Analytics service supports input and output only in English.
- Do not use Internet Explorer 8.0 to edit the wireless LAN controller (WLC) SNMPv3 credentials. Use Chrome 40 or later ("Browser Support" section on page 14).
- The device name must start with a letter (for example, cmx01). The setup script fails if the device name starts with a numeric (for example, 01cmx).
- In Cisco CMX Release 10.1, the SSL mode is disabled by default. In Cisco CMX Release 10.2, the SSL mode is enabled by default and therefore to offer Cisco CMX Connect portal page in HTTP, you should disable the SSL mode by entering the following command:

  cmxctl node sslmode disable
- To observe the disk space utilization, refer to the Memory details from the Systems tab. For details on increasing hard disk space, see the "Increasing the Hard Disk Space" section in the "Performing Administrative Tasks" chapter in the *Cisco Connected Mobile Experiences Configuration Guide, Release 10.2*.

  When more than 85 percent of the disk space is consumed, all CMX services shut down. For details, see the "Troubleshooting Cisco CMX Server Shutdown Problems" section in the "Performing Administrative Tasks" chapter in the *Cisco Connected Mobile Experiences Configuration Guide, Release 10.2*.
- After installing the ISO file on the Cisco MSE 3355 or 3365, use the **cmxctl status** command to check if the CMX services are running. If they are not running, use the **cmxctl start** command.
- The following information applies only if you have SSL enabled: If you enable HTTPS for Cisco CMX Analytics (generally Cisco CMX as a whole), make sure a valid SSL certificate is installed. Otherwise, slower UI performance will occur and reporting will not work as expected.

  If you do not have a valid SSL certificate to install, you need at least a self-signed certificate.

  If neither a valid SSL certificate or self-signed certificate is present, Cisco CMX analytics might not work as expected.
- (CSCvb64651) If you have HTTPS enabled and if you do not have a valid certificate (meaning, a screen was displayed where you accepted the risk to continue), reports do not work. This is a limitation from the Google Chrome browser, not from Cisco CMX.

  If you do not need HTTPS, disable it so that reports work.If you need HTTPS, install a valid SSL certificate on the box. Note that having a valid SSL certificate also improves the interface speed.
- (CSCvb24320) In Cisco CMX Release 10.2.2 and 10.2.3, changes were made related to Cisco CMX Analytics device count. For detailed information, see the *CMX 10.2.2 and CMX 10.2.3 - Changes in Analytics Numbers* document: https://communities.cisco.com/docs/DOC-69845.
- (CSCva36827) Instead of the /api/location/v2/clients API or /api/location/v2/clients/count API, use the /api/location/v1/clients API to get a report on the number of active clients.
- (CSCuw73675) For security, Cisco CMX Release 10.3.0 blocks a list of ports, such as port 5555.

Caveats

- Cisco Bug Search Tool, page 18
- Open Caveats, page 18
- Resolved Caveats in Cisco CMX Release 10.2.3, page 20

- Resolved Caveats in Cisco CMX Release 10.2.2, page 20
- Resolved Caveats in Cisco CMX Release 10.2.1, page 21
- Resolved Caveats in Cisco CMX Release 10.2.0, page 21

Cisco Bug Search Tool

The Bug Search Tool (BST), which is the online successor to the Bug Toolkit, is designed to improve the effectiveness of network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The tool has a provision to filter bugs based on credentials. Perform the following task:

1. Access the BST (using your Cisco user ID and password) at:

   https://tools.cisco.com/bugsearch/

2. Enter the bug ID in the **Search For:** field.

Note Using the BST, you can also find information about the bugs that are not listed in this document.

Open Caveats

Use the BST to view the details of the caveats listed in this section. For more information about the BST, see the "Cisco Bug Search Tool" section on page 18.

Bug ID	Description
CSCup03264	Anchor WLC not appending client parameters for external webauth redirect
CSCuw56474	CMX shows incorrect WLC added and version
CSCux07724	Client location V2 API returns double the number of expected results
CSCux14701	Issues in CMX presence roles
CSCux68286	Non Admin Users get no indication of error when license expired
CSCux82505	Confidence factor for Hyperlocation client very high compared to RSSI
CSCuy00200	ConnectPMS- IE-browser client after auth redirect to visitor-login page
CSCuy12468	10.2.2: Duplicate location notifications
CSCuy54243	10.2 : System - > Pattern is empty for Incoming Rate
CSCuy64955	/api/location/v2/clients not returning correct connected AP
CSCuy91650	CMX do not have provision to add Controller using hostname over CLI
CSCuz18736	Halo - CMX Samsung S5 gets poor location accuracy
CSCuz19506	Success Page for CMX Connect does to support multiple languages
CSCuz19554	CMX should show rouge AP on the DETECT and ENGAGE screen
CSCuz21077	CMX Import of Controllers from PI
CSCuz25674	Import of WLC imports non WLC Switches
CSCuz28085	10.2.2: Beacon movement/absence notification not working as expected

Bug ID	Description
CSCuz28102	10.2.2:Placing a beacon to actual position ending beacon going misplaced
CSCuz28293	Hyperlocation client takes 20 seconds to settle after stopping to move
CSCuz30773	PDF Reports do not comply with ISO standard and cannot be read on iPhone
CSCuz36836	CMX new upgrade WLC image not reflected on CMX GUI and CLI
CSCuz41175	10.2.2:SMA Details Chart is showing UTC time for today's report
CSCuz48510	10.2.2: analytics now report gives inconsistent data
CSCuz51285	Patterns incorrect - Wording of IOS8 needs to change and blanks removed
CSCuz54861	10.2.2: Few attributes for In/Out notification payload are null
CSCuz60996	Notifications page always reverting to first page
CSCuz61423	10.2.2:scheduled reports are received after deleting from dashboard
CSCuz67458	CMX 10.2.2-332 GUI System Metrics all graphs fails to load with an error
CSCuz69078	/v1/history/clients API giving invalid response.
CSCuz74751	Presence is counting \"connected\" clients only based on new connected/hrs
CSCuz80928	10.2.2: LVCC Crossover widget - Unexpected system error occured
CSCuz82637	CMX upgrade will not cleanup old log files
CSCuz84769	Social Analytics show error when not configured
CSCuz84784	Heatmaps do not respect Inclusion Zones
CSCuz84801	Address validation Check box does not work
CSCuz84809	When a Analytics Report is deleted, it is not deleted from schedule and will result in a null report being sent
CSCuz84818	Line does not connect between BLE Beacon expected and true location.
CSCuz84833	Point 10 from the doc may not be a bug as on Presence Node, I could see the API returns sites info, BUT on Location node, it always returns NULL.
CSCuz84841	The Activity Map Filter does not work
CSCuz86119	Analytics Average Dwell Time is inaccurate
CSCva00869	Troubleshooting tool appears blank
CSCva02210	System error on CMX when sync with PMS
CSCvb18097	10.2.3: connect/detect filter not getting displayed after disabling both
CSCvb24932	Email Notification Counts are shown as success even for invalid email ID
CSCvb27904	Cannot email Troubleshooting tool test result
CSCvb56278	CMX Location Pause & Relaunch is broken
CSCvb56660	10.2.3-29: Dwell & WiFi adoption daily reports show system error
CSCvb71883	confd errors while installing services post ISO installation on 3355 model
CSCvc34851	Enhance SSID Filter for blocking hyperlocation clients
CSCvd15253	Probing only clients count is slightly less in 10.3 with compared to 10.2.3

Resolved Caveats in Cisco CMX Release 10.2.3

Use the BST to view the details of the caveats listed in this section. For more information about the BST, see the "Cisco Bug Search Tool" section on page 18.

Bug ID	Description
CSCuz29618	Map Resource API fail with Response Code 406
CSCuz80047	CMX 10.2 : changing scheduled reports title won't change much
CSCva22027	CMX 10.2 generates error when setting SNMP v3 auth or priv types to none
CSCva24776	Reduce the stalerssiinmins from default 3 mins to 1 min
CSCva39187	CMX client api call /api/location/v2/clients return invalid response
CSCva41729	CMX 10.2 : NTP services need to be restarted to sycn post install
CSCva46690	Analytics Repeat visitor count is empty on certain floors, days
CSCva52597	CMX 10.2.2: NMSP tunnel between wlc and cmx goes down intermittently
CSCva58843	Remove CMX Presence Timestamp showing end-user Laptop time
CSCva65320	CMX User with Role Manage can not create notifications
CSCva70314	MAC Filtering is not working as expected
CSCva70561	CMX Unable to create heatmap for Barbados AP
CSCva77202	Missing information in the PDF analytics report
CSCvb05478	CMX Location queue getting full on spike in client traffic
CSCvb12536	Redis Service Memory Handling Improvement

Resolved Caveats in Cisco CMX Release 10.2.2

Use the BST to view the details of the caveats listed in this section. For more information about the BST, see the "Cisco Bug Search Tool" section on page 18.

Bug ID	Description
CSCuw32543	MSE 3365: KVM Console does not permit ENTER during ISO recovery
CSCuw80659	CMX Active client V2 API throws 204 instead of bad req 400
CSCuw84275	CMX 10.2 - DNS reconfigure doesnt get updated and throws error messages
CSCuw86154	Getting traceback error while running command \"cmxctl debug\"
CSCuw86285	CMX: Presence memory issues
CSCuw92999	CCO 10.2.1 CMX - cmxos reconfigure returns permission error
CSCux13935	Mail server doesn't get initialized properly
CSCux24984	CMX10.2 BLE beacon changing it to Known from Rogue doesn't save
CSCux27531	CMX server stops at short intervals
CSCux30858	Layout API will overflow the data for the charts (Concurrency bug)
CSCux44949	BEAST Vulnerability on CMX (CVE-2011-3389)

Bug ID	Description
CSCux51188	10.2 CMX Facebook login not working with SMS auth on captive portal
CSCux52492	Could not get Nmsp rate - Could not parse payload
CSCux72106	Missing presence notifications when clients move site
CSCux78723	HyperLocation Client Location is jumpy
CSCux92388	CMX 10.2 Not Reporting Live Client Location While Roaming
CSCuy37340	CMX Halo engine doesn't accept partial antenna phase values
CSCuy42159	10.2.2: Analytics service stopped processing data on BM w/ 426 zones
CSCuy59011	Clients falls outside the map
CSCuy64853	Visitor count incorrect in big zone
CSCuy67973	CMX face book Wifi does not support age restriction pages
CSCuy71687	CMX 10.2: Next button in location history intermittently fails
CSCuy81517	CMX SCheduled reports html format not showing the path graph
CSCuy92897	10.2.2: 'Location Tag Mgr' does not show details of ana. tag; 10.2.2-294
CSCuz05542	10.2.2: Hard disk usage is: 76% due to db growth & OOM; cmx-vmdev83
CSCuz09306	CMX NMSP Becomes Inactive
CSCuz09959	Analytics Accuracy Dwell time Breakdown should equal Visitors per floor
CSCuz21347	CMX 10.2: Beacons and Tags issues on CMX UI
CSCuz22657	CMX 10.2.1 maps import fails with 'CMX: System error'.
CSCuz24062	CMX enabling ssl mode breakes Zone and Custom Portal information
CSCuz63292	Analytics Reports will support upto 99 zones
CSCuz79200	Location sending Absence msg to Analytics for sleeping clients

Resolved Caveats in Cisco CMX Release 10.2.1

There were no resolved bugs in this release.

Resolved Caveats in Cisco CMX Release 10.2.0

Use the BST to view the details of the caveats listed in this section. For more information about the BST, see the "Cisco Bug Search Tool" section on page 18.

Bug ID	Description
CSCuv80878	Zones are overwrittend when a map is reimported after moving APs
CSCuv87924	Need some input from marketing. What is the expected use case around map import.

Documentation Errata

The following information will be incorporated in the applicable Cisco CMX Release 10.2 document at its next revision.

Configuration Guide

Node Details Window

(CSCuz67492) The “Viewing Cisco CMX Node Details” section in the configuration guide will be updated with this information:

In Cisco CMX Release 10.2.1, the **Node Details** window was changed to display this information: Node ID, IP Address, Hostname, and System Time.

Previously, the **Node Details** window displayed this information: Node ID, Name, Hostname, and Type.

Create New Notification Window

(CSCuz67492) The “Creating a New Notification” section in the configuration guide will be updated with this information:

In Cisco CMX Release 10.2.1, the **Device Type** field on the **Create New Notification** window was changed to provide these options: **All**, **Tag**, **Client**, and **Interferer**. The **Rogue Client** and **Rogue AP** options now have been removed.

In addition, if the **In** option is selected in the **Condition** field, this warning message is displayed: `Please make sure to add 'Out' condition with same Hierarchy`. Conversely, if the **Out** option is selected in the **Condition** field, this warning message is displayed: `Please make sure to add 'In' condition with same Hierarchy`.

Create New Report Window

(CSCuz67492) The “Creating and Managing Customized Reports” section in the configuration guide will be updated with this information:

In Cisco CMX Release 10.2.1, the maximum number of widgets you can include when creating a new report is 9. If you add more than 9 widgets, this message is displayed: **`Analytics only supports 9 widgets in a report. Please reduce the number of widgets.`**

Activity Map Window

(CSCuz67492) Step 4 in the “Viewing or Tracking Devices” section in the configuration guide will be updated with this information:

In Cisco CMX Release 10.2.1, when you select an access point icon from a floor map displayed on the **Activity Map** window, the **Access Point** information area includes **Angles** information.

Analytics Dashboard

(CSCuz67492) The “Analytics Reports” section in the configuration guide will be updated with this information:

Note In Cisco CMX Release 10.2.2, the Unique Device widget is no longer available for analytics reports.

Maps Window

(CSCuz67492) The “Importing Maps and Adding Controllers” section in the configuration guide will be updated with this information:

In Cisco CMX Release 10.2.2, these fields on the Maps window changed:

- The **Override Maps** check box is now the **Delete & replace existing maps** check box.
  - Select this option to delete existing maps by replacing them with the uploaded maps.
- The **Import Zones** check box is now the **Delete & replace existing zones** check box.
  - Select this option to delete existing zones by replacing them with the uploaded maps.

Changing the Portal Login Frequency

A new section about the Portal Login Frequency feature will be added to the configuration guide. See the “Portal Login Frequency” section on page 2 for the feature description. Below is the configuration procedure.

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

Step 2 Choose **Connect & Engage > Settings > General** to display the **Connect Settings** window.

Step 3 From the **Connect Settings** window, change the value in the **Visitor: Portal Frequency** field. The range is 0 to 1000 days. The default is 180 days.

Examples:

- If the login frequency is set to 0, the portal is displayed is each time the visitor’s device associates with the SSID.
- If the login frequency is set to 1, the portal is displayed when the visitor’s device first associates with the SSID and is not displayed again until after a 24-hour period. Within that 24-hour period, the portal is not displayed regardless of the number of times the visitor’s device disassociates and associate to the SSID.

Step 4 Click **Save**.

Creating an Analytics Report Based on Connected or Detected Devices

A new section about creating a filtered analytics report based on connected or detected devices will be added to "The Analytics Dashboard" section in the configuration guide. See the "Analytics Report Filtered for Associated Devices" section on page 2 for the feature description. Below is the configuration procedure.

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

Step 2 Choose **Analytics > Reports** to display the **Create New Report** window.

Step 3 From the **Connect/Detected Devices** widget, select **Connected** or **Detected**, or select both.

If both are selected, all connected and detected devices will be displayed (meaning, no filtering) in the **Visitor Count** area on the Analytics Dashboard.

Step 4 Click **Done**.

The Visitor Count information on the Analytics Dashboard reflects the following:

- If the **Connected** option is selected, a green WiFi icon appears next to the **Visitor Count** heading. The visitor count displayed is the number of devices connected to the SSID.
- If the **Detected** option is selected, a gray WiFi icon appears next to the **Visitor Count** heading. The visitor count displayed is the number of devices detected by the SSID.
- If both options are selected (meaning, no filtering), no icon appears.

Configuring SSID Filtering in the Location Service

See the "SSID Filtering in the Location Service" section on page 3 for the feature description. Step 4 in the "Setting Filter Parameters" section in the configuration guide will be updated to include the following bullet and procedure:

- **Enable SSID Filtering**—Check this check box to so that the Location service excludes all visitor devices associated to a particular SSID:

a. Click **Enable SSID Filtering**.

b. Click **Select SSID**, and select a particular SSID.

If no SSIDs appear in the list, make sure that a Cisco WLC is active, and then click **Fetch SSIDs** to refresh the list.

c. Click **Filter SSID** to add the selected SSID to the filter list.

Creating an Inclusion or Exclusion Region

A new section about creating inclusion and exclusion regions will be added to the "The Cisco CMX Detect and Locate Service" section in the configuration guide. See the "Inclusion/Exclusion Region" section on page 3 for the feature description.

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

Step 2 Choose **Manage > Locations**.

Step 3 In the left pane, click **Floor**.

Step 4 To go to the map view of the floor, click the arrow on the top right of the floor tile view. The **Zone Editor** window is displayed with a list of icons to the right.

Step 5 To add a new inclusion region:

a. Click the **+** icon to create an inclusion region on the map.

b. Double-click to finish creating the inclusion area. The inclusion region is displayed in green.

c. In the **Create a Inclusion** dialog box, click **Add**.

To add an exclusion region, click the **–** icon and draw the exclusion area on the inclusion area.

Viewing Northbound Notifications

The "Editing a Notification" section in the configuration guide will be updated to include viewing northbound notifications.

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

Step 2 Choose **Manage > Notifications**.

Step 3 Under the **Actions** column for an existing notification, click **Details** to view additional information about the notification.

You can also view the northbound notification details in the Edit Notifications window. Optionally, from the CLI, use the **cmxctl metrics notification** command to view the northbound notifications.

Creating New Virtual Machines Using Hyper-V Manager

Step 1 Download the CMX .vhd file to the location on the drive where it will reside.

Step 2 (Optional) Convert the .vhd file to .vhdx format.

Step 3 Open the Hyper-V Manager application and verify the Hyper-V virtual network switch configuration.

Note To configure a Hyper-V virtual network switch, click **Virtual Switch Manager** at the right side of the Hyper-V Manager screen.

Step 4 To create a new VM, choose **Action > New > Virtual Machine**.

Step 5 Enter the name for the new virtual machine.

Step 6 Select to store the virtual machine in a different location, browse to the folder containing the .vhd or converted .vhdx file, and then click **Next**.

Step 7 Choose **Generation 1** as the machine type, and then click **Next**.

Note Only certain Windows guests support Generation 2.

Step 8 Specify 8192 or greater for the VM memory, and then click **Next**.

Note Do not enable Dynamic Memory.

Step 9 Under **Connections**, choose the appropriate virtual network switch to connect the VM, and then click **Next**.

Step 10 Select **Use an existing hard disk**, and then navigate to the .vhd or .vhdx file on your hard disk.

Step 11 In the **Summary** screen, click **Finish**.

Step 12 Edit the new VM settings and change the processor count to a minimum of 4.

Adding and Deleting Perimeters Managing Perimeters and Zones on Location Maps

The “Managing Perimeters and Zones on Location Maps” section in the configuration guide will be updated with this information.

Note In Cisco CMX Release 10.2.3, the ability to create and delete a perimeter on location maps is no longer available.

Viewing Patterns

The “Viewing Patterns” section in the configuration guide will be updated with this information:

Note In Cisco CMX Release 10.2.3:

- The following pattern details are no longer available: Incoming Rate, Dropped Notifications, and NMSP LB Read Operations.
- In the **Select Criteria** drop-down list, the **iOS8 Devices** option is renamed to **Locally Administered MAC count**.

Viewing a Device Count and Average Dwell Time Report

The “Viewing a Device Count and Average Dwell Time Report” section in the configuration guide will be updated with this information:

Note In Cisco CMX Release 10.2.3, the **Now** option in the **Date & Time Filters** drop-down list is no longer available.

Command Reference

cmxctl debug

(CSCva94257) Usage guidelines for this command should state: This command should to be run using the cmxadmin (non-root) account.

In addition, the prompt in the CLI example should be `[cmxadmin@10.10.10.10:~]$`, not `[root@server]#`.

cmxctl config featureflags

The command reference will be updated with this information.

To list and toggle feature flags, use the **cmxctl config featureflags** command.

cmxctl config featureflags {*featurename*} {**true**|**false**}

Syntax Description

service.featurename	Name of the Cisco CMX service and feature. • analytics.areatransition • configuration.apimport: • analytics.sma • monit • container.influxdbreporter • halo • analytics.queuetime
true	Enables the feature of the service.
false	Disables the feature of the service.

Command Default

None

Usage Guidelines

To enable analytics social media analytics feature flag, use the **cmxctl config featureflags analytics.sma true** command, and then use the **cmxctl restart analytics** command to restart the Analytics service.

After making changes to any feature flag configuration, use the **cmxctl restart analytics** command to restart the Analytics service.

Command History

Release	Modification
Cisco CMX Release 10.2.2	This command was changed. The display default for analytics.sma was changed to false.
Cisco CMX Release 10.2.0	This command was introduced.

Examples

The following example shows how to list the feature flags:

```
[root@server]# cmxctl config featureflags
+----------------------------+-------+
| analytics.areatransition   | true  |
+----------------------------+-------+
| configuration.apimport     | true  |
+----------------------------+-------+
| analytics.sma              | false |
+----------------------------+-------+
| monit                      | false |
+----------------------------+-------+
| container.influxdbreporter | true  |
+----------------------------+-------+
| halo                       | true  |
+----------------------------+-------+
| analytics.queuetime        | false |
+----------------------------+-------+
```

cmxos backup

The prompt in the CLI example should be `[cmxadmin@10.10.10.10:~]$`, not `[root@server]#`.

cmxos monit

(CSCuy91949) The command reference will be updated with this information.

To manage the monitoring of Cisco CMX services, use the **cmxos monit** command.

cmxos monit {configure | start | stop | wipe}

Syntax Description

configure	Displays the default monitoring settings.
start	Enables monitored services.
stop	Disables monitored services.
wipe	Deletes the default monitoring settings. **Note** To reset to the default monitoring settings, use the **cmxos monit configure** command.

Command Default

Disabled.

Command History

Release	Modification
Release 10.2.0	This command was introduced.

Examples

The following example shows how to display the monitoring settings:

```
[cmxadmin]$ cmxos monit configure
Deleting all monit configurations....
Configuring monit mail settings...
```

```
Configuring monit OS settings...
Configuring monit CMX services settings...
```

The following example shows how to enable monitoring of Cisco CMX services:

```
[cmxadmin]$ cmxos monit start
Starting monit:
```

cmxos reconfig

(CSCuz95185) The following note will be added to the Usage Guidelines section for the **cmxos reconfigure** command:

Note Do not execute the **cmxos reconfigure** command when Cisco CMX services are not installed. This will prevent execution failures.

Importing Maps

(CSCvb31782) The Importing Maps section in the configuration guide will be updated with this information.

In Cisco CMX Release 10.2.2, overwriting an existing map with an imported map is no longer the default. If you want to overwrite your map during import, you must select the D**elete & replace existing maps and analytics data** check box on the **Settings > Advanced > Maps** window.

Note Previous data that existed before maps are overwritten can be only accessed through the API and not through UI.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at:

http://www.cisco.com/cisco/web/support/index.html

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

Related Documentation

For additional information on Cisco CMX, see:

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

Obtain Documentation and Submit a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.