



Cisco CMX Configuration Guide, Release 10.4

First Published: 2017-03-31

Last Modified: 2018-04-05

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017 Cisco Systems, Inc. All rights reserved.



Preface

- [Audience, on page iii](#)
- [Conventions, on page iii](#)
- [Related Documentation, on page iv](#)
- [Obtaining Documentation and Submitting a Service Request, on page iv](#)

Audience

This document is for network administrators who configure Cisco Connected Mobile Experiences (Cisco CMX) services.

Conventions

This document uses the following conventions:

Table 1: Conventions

Convention	Indication
bold font	Commands and keywords and user-entered text appear in bold font .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[]	Elements in square brackets are optional.
{x y z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string. Otherwise, the string will include the quotation marks.
<code>courier font</code>	Terminal sessions and information the system displays appear in <code>courier font</code> .
<>	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.

Convention	Indication
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.



Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.



Tip Means the following information will help you solve a problem.



Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Related Documentation

For more information on coding and specific assistance, see <https://developer.cisco.com/site/cmx-mobility-services/>

For more information about Cisco Mobility Services Engine and related products, see:

<http://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/tsd-products-support-series-home.html>

For more information about Cisco Connected Mobile Experiences (Cisco CMX), see:

<http://www.cisco.com/c/en/us/solutions/enterprise-networks/connected-mobile-experiences/index.html>

For more information about Cisco CMX Cloud, see:

<https://support.cmx.cisco.com/hc/en-us>

Obtaining Documentation and Submitting 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 . RSS feeds are a free service.



CONTENTS

PREFACE

Preface iii

Audience iii

Conventions iii

Related Documentation iv

Obtaining Documentation and Submitting a Service Request iv

CHAPTER 1

Getting Started 1

Introduction to Cisco Connected Mobile Experiences 1

Overview of Cisco CMX Services 1

Importing Maps and Cisco Wireless Controllers 4

Exporting Cisco Prime Infrastructure Maps 4

Copying the Exported Maps 4

Importing Maps 4

Adding Cisco WLCs 5

Logging In to the Cisco CMX User Interface 5

Using the Evaluation License 6

Enabling or Disabling Cisco CMX Services 6

Importing Certificates 7

Installing Self-signed and Third Party SSL Certificate in Cisco CMX 8

Installing a self-signed certificate 8

Installing a Third Party Signed Certificate 10

Installing the Certificate 12

Instructions for CMX build 324: (10.2.2 beta) or 10.2.2 CCO and Later 13

Adding Users and Managing Roles 13

Using the Cisco CMX Setup Assistant 14

Supporting Active Clients Version 3 API 14

Getting APIs	14
Changing Time Zones and NTP Server	15

CHAPTER 2

The Cisco CMX Detect and Locate Service	17
Overview of the Detect and Locate Service	17
Initial Configurations	17
Viewing or Tracking Devices	18
Viewing Device Details	21
Customizing Client Refresh Rates	22
Customizing Device Views Using Filters	22
Adding and Deleting Filters	23
Searching for a Device	23
Client Playback	24
Enabling Hyperlocation and FastLocate in Cisco CMX	24
Hyperlocation Mixed Mode Support	26
Running Hyperlocation Diagnostics	27
Configure Hyperlocation Groupings	33
Controlling the Probing Client Expiry Time	36
Measuring Client Location Accuracy Using the Location Accuracy Test	37
Analyzing Location Accuracy Results	41
Understanding Client Diagnostics	41
Analyzing Location Accuracy Log Files	44
Location Accuracy for Hyperlocation Deployments	46

CHAPTER 3

The Cisco CMX Analytics Service	49
Overview of the Analytics Service	49
The Analytics Dashboard	49
Accessing the Analytics Dashboard	50
Filtering the Data Displayed in the Analytics Dashboard	50
Viewing a Device Count and Average Dwell Time Report	51
Analytics Reports	52
Creating and Managing Customized Reports	53
Create a Custom Report	53
Edit a Report	56

Create a Scheduled Custom Report	56
Configure Custom Time Ranges for an Analytics Report	57
Download a Customized Report	59
Delete a Customized Report	59
Creating an Analytics Report Based on Associated or Probing Only Devices	60
Viewing Global Alerts for Critical Services	60
Customized Widgets	61
The Visitors Widget	61
The Dwell Time Widget	62
The Correlation Widget	63
The Path Analysis Widget	64
The Wi-Fi Adoption Widget	64
The Dwell Time Breakdown Widget	65
Creating Customized Widgets	67
Create a Realtime Report	67
Performing Heatmap Analysis	68
Using the Schedule Manager	69
Verticalization	69
Set SSID Filter Parameters for Analytics Service	69

CHAPTER 4

The Cisco CMX Connect Service	71
Overview of the Connect Service	71
Comparison of Facebook Wi-Fi and Custom Portal	72
Preparatory Tasks	73
Adding a Connect or ConnectExperience User	73
The Connect Dashboard	74
Summary Information	74
Historical Information	74
Visitor Search	75
Additional Information	75
Connect Experiences	75
Overview	75
Facebook Wi-Fi	75
Custom Portal	76

Setting Up a Facebook Wi-Fi Portal	76
Configuring Access Control Lists on Cisco Wireless Controller	76
Configuring WLAN for Web Passthrough Authentication	78
Creating a Facebook Page for Your Organization	79
Assigning a System Default Facebook Page	79
Assigning a Location-Specific Facebook Page	80
Setting Up a Custom Portal	80
Creating a Default Custom Portal Page	82
Assigning Location-Specific Custom Portal Page	82
Enabling Multi-language Support in Custom Portals	82
Configuring Connect Portal Pages for Sites	83
Viewing Connect Clients with Sites	83
Device-Browser Matrix	84
Offering Opt-Out and Opt-In Options for Cisco CMX Services	85
Configuring Elements for Custom Portal Navigation	86
Configuring URLs for Custom Portal Navigation	86
FlexConnect AP Support on Cisco CMX	87
Configuring FlexConnect ACLs	88
Setting Up a Controller with FlexConnect ACLs	90
Offering Portal Pages on HTTP from Cisco CMX Connect	90
Disabling HTTPS	90
Adjusting ACLs on Cisco WLC	91
SMS Authentication	91
Customizing a Policy Plan	92
Using the Connect Library	93
Using Content Elements for Creating Portals	94
Authentication with Social Network Accounts	95
Configuring OAuth with Facebook	95
Facebook Data Collection	98
Configuring OAuth with Instagram	98
Configuring OAuth with Foursquare	99
Connect Settings	99
Connect Settings	99
Changing the Portal Login Frequency	100

Using the CMX Connect Debugging Tools	100
Configuring the Property Management System	101
Prerequisites for the Property Management System	102
PMS Policy Enforcement	102
Configuring the FreeRADIUS on Cisco CMX	102
Customizing the FreeRADIUS Server	103
Cisco WLC Configurations	104
Configuring a PMS User's Account and Wi-Fi Plan	106
Using the Visitors Search to Find PMS Information	108
Configuring Connect Services in Cisco CMX High Availability	110

CHAPTER 5**The Cisco CMX Presence Analytics Service 111**

Overview of the Presence Analytics Service	111
Installing the Presence Analytics Service	112
Benefits of the Presence Analytics Service	112
Initial Configurations	112
Presence Analytics Dashboard	113
Adding Sites	114
Adding Sites Individually	114
Adding Sites in Bulk	115
Viewing Available Sites	116
Editing an Existing Site	116
Deleting an Existing Site	116
Searching for a Site	117
Adding APs	117
Adding an AP to a Site	117
Adding APs in Bulk	118
Deleting an AP	119
Viewing Site Details for a Specified Period	119
Viewing KPI Summary	120
Viewing Device Proximity, Count, and Distribution for a Specific Site	120
Emailing a Report	121
Printing a Report	121
Generating a PDF Report	121

Managing Reports	122
Specifying Filter Parameters	123
Enabling a Global Site	123
Creating a Site Group	123
Changing the Presence Analytics Theme	124

CHAPTER 6

Managing Cisco CMX Configuration	125
Overview of the Manage Service	125
Managing Perimeters and Zones on Location Maps	126
Viewing Campus, Building, Floor, and Zone Details	126
Managing Tags	126
Creating an Inclusion or Exclusion Region	127
Creating a Perimeter	127
Deleting a Perimeter	128
Editing a Perimeter	129
Creating a Zone	129
Deleting a Zone	130
Editing a Zone	131
Managing Licenses	131
Add a License	133
Deleting a License	134
Managing Users	134
Adding a User	134
User Roles	134
Changing the Default Admin Password	135
Editing User Information	136
Deleting a User	136
Managing Notifications from Applications	136
Create a New Notification	137
Making Changes to Notifications	140
Enabling and Disabling a Notification	141
Editing a Notification	141
Viewing Northbound Notifications	141
Viewing Northbound Notification Attributes	141

Managing Proxy Settings for Notifications	143
Deleting a Notification	145
Managing Cisco CMX Cloud Apps	145
Setting Up Outbound Proxy	148
Managing Verticalization	149
Queue Analytics	151
Customizing Verticals	151
Configuring Basic CMX Settings	152
Root User Changes	153

CHAPTER 7

Managing Cisco CMX System Settings	155
Overview of the System Service	155
Viewing the Overall System Health	155
Understanding the Node Table	156
Understanding the Coverage Details Table	157
Understanding the Controllers Table	158
Managing Dashboard Settings	158
Setting Device Tracking Parameters	158
Setting Filtering Parameters	160
Setting Location Calculation Parameters	161
Configuring the Mail Server for Notifications	163
Importing Maps and Controllers into Cisco CMX	163
Importing Maps and Adding Controllers	164
Upgrading Cisco CMX	165
Enabling High Availability for Cisco CMX	166
Pre-requisites for HA	167
Enabling High Availability for Cisco CMX Using the Web UI	167
Enabling High Availability Using CLI	168
Viewing Live System Alerts	169
Viewing Patterns	169
Understanding the Metrics Tab	170
Viewing System Summary Metrics	170
Viewing System Summary Metrics Using the Dashboard	171
Viewing CMX Node Metrics	171

- Viewing CMX Node Metrics Using the Dashboard 172
- Viewing Database Metrics 172
 - Viewing Database Metrics Using the Dashboard 173
- Viewing Cache Metrics 173
 - Viewing Cache Metrics Using the Dashboard 173
- Viewing Location Metrics 174
 - Viewing Location Metrics Using the Dashboard 174
- Viewing Analytics Notification Metrics 175
 - Viewing Analytics Notification Metrics Using the Dashboard 175
- Viewing Presence Metrics 176

CHAPTER 8 Performing Administrative Tasks 177

- Cisco CMX User Accounts 177
- Unlocking Users 178
- Recovering Password 178
- Using FTP Commands for Cisco CMX 179
- Backing Up Data 179
 - Increasing the Hard Disk Space 181
- Restoring Data 183
- Troubleshooting Cisco CMX Server Shutdown Problems 184

APPENDIX A Guidelines for Managing Zones in Cisco CMX 185

APPENDIX B Cisco CMX Alerts 189

APPENDIX C Cisco CMX Network Protocols and Port Matrix 201



CHAPTER 1

Getting Started

- [Introduction to Cisco Connected Mobile Experiences, on page 1](#)
- [Overview of Cisco CMX Services, on page 1](#)
- [Importing Maps and Cisco Wireless Controllers, on page 4](#)
- [Logging In to the Cisco CMX User Interface, on page 5](#)
- [Using the Evaluation License, on page 6](#)
- [Enabling or Disabling Cisco CMX Services, on page 6](#)
- [Importing Certificates, on page 7](#)
- [Installing Self-signed and Third Party SSL Certificate in Cisco CMX, on page 8](#)
- [Adding Users and Managing Roles, on page 13](#)
- [Using the Cisco CMX Setup Assistant, on page 14](#)
- [Supporting Active Clients Version 3 API, on page 14](#)
- [Getting APIs, on page 14](#)
- [Changing Time Zones and NTP Server, on page 15](#)

Introduction to Cisco Connected Mobile Experiences

Cisco Mobility Services Engine (Cisco MSE) acts as a platform to deploy and run Cisco Connected Mobile Experiences (Cisco CMX). Cisco MSE is delivered in two modes—the physical appliance (box) and the virtual appliance (deployed using VMware vSphere Client). Using your Cisco wireless network and location intelligence from Cisco MSE, Cisco CMX helps you create personalized mobile experiences for end users and gain operational efficiency with location-based services.

For more information about Cisco CMX features for this release, see the *Release Notes for Cisco CMX*, at: <https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-release-notes-list.html>

Overview of Cisco CMX Services

Cisco CMX enables you to access the following services:

- **DETECT & LOCATE**—The Detect & Locate service uses the data provided by Cisco WLCs to calculate the X,Y location (based on 0,0 at the top left hand side of the map) of wireless devices that are detected by the access points that support the wireless LAN (WLAN) to a high degree of precision (generally +/-5 to 7M, 90% of the time with standard location technologies and +/-1 to 3M, 50% of the time with Hyperlocation technologies). Given the proper physical environment with access points deployed in

accordance with Cisco best practices for a location ready environment. The CMX GUI will be able to display the physical location of:

- Associated Wireless Devices (shown as green dots in default view)
- Unassociated Wireless Devices (shown as red dots in default view)
- RF Interferers (Lightning icon)
- Access Points (Circles)
- Rogue Access Points
- Rogue Clients
- BLE Tags (Bluetooth Icon)
- Active Wi-fi RFID Tags (Tag icon)

The background map can display:

- Inclusion and Exclusion Zones imported from Cisco Prime Infrastructure
- Analytics Zones created in Cisco CMX
- Thick Walls
- GPS Markers

Additionally when passed to the CMX Analytics service, this location information provides visibility into customer movements and behavior throughout the venue and throughout the day. The Cisco CMX Analytics service determines device parameters and can display this information as part of six different unique widgets.

If you choose Location during installation, you will see the following services in Cisco CMX GUI.

- DETECT & LOCATE—Active for 120 day trial period unless either a CMX base or advanced license is added.
- ANALYTICS—Active for 120 day trial period unless a CMX advanced license is added.
- CONNECT—Active for 120 day trial period unless either a CMX base or advanced license is added
- MANAGE
- SYSTEM

For more information, see [Overview of the Detect and Locate Service, on page 17](#).

- **ANALYTICS**—This service provides a set of data analytic tools packaged for analyzing Wi-Fi device locations. It functions as a data visualization engine that helps organizations use their network as a data source for business analysis to understand behavior patterns and trends, which can help them take decisions on how to improve visitor experience and boost customer service.

The ANALYTICS service allows for the creation of six different type of widgets.

- Device count
- Dwell time
- Dwell time breakdown

- Associated User Report
- Path
- Correlation

For more information, see [The Cisco CMX Analytics Service, on page 49](#).

- **CONNECT**—This service provides intuitive, simple, highly customizable, and location-aware guest services in the form of a captive portal that offers two types of guest on-boarding experiences:
 - Facebook Wi-Fi
 - Custom Portal

For more information, see [The Cisco CMX Connect Service, on page 71](#).

- **PRESENCE ANALYTICS**—Cisco Presence Analytics service is a new analytics engine that detects the presence of visitors via their mobile devices interactions with even a single network access point. The probe requests which are transmitted from the wireless devices provide information, which is used to identify the general location of a client, in respect to the location of even a single access point which hears the clients probing activity. The information available from even a single AP allows the Presence Analytics service to develop valuable business intelligence. Presence Analytics uses Received Signal Strength Indication (RSSI), along with the duration of high signal strength to determine whether a client device is in the site or just passing by. Even if a device is not connected to the access point, its presence is still detected if the device is within the signal range and the wireless is turned on. Given that Presence Analytics develops location information with respect to a given set of APs it has a simpler management overhead in that it does not require the importation or configuration of any maps into the CMX instance. By simply knowing the association of a given AP, or set of APs, to a physical location, Presence Analytics allows a business insight into the number of visitors to a location, whether these are first time or repeat visitors, the average amount of time each visitor spent in physical proximity to the AP, and the ability to ascertain whether a device was just passing by a location or if they were actually within the location serviced by the AP. For more information, see [Overview of the Presence Analytics Service, on page 111](#).

If you choose Presence during installation, you will see the following services in the Cisco CMX GUI.

- PRESENCE ANALYTICS
 - CONNECT
 - MANAGE
 - SYSTEM
- **MANAGE**—This service enables you to manage licenses, users, zones, beacons, and notifications. For more information, see [Managing Cisco CMX Configuration, on page 125](#).
 - **SYSTEM**—This service enables you to verify the health of the system and view patterns and metrics. For more information, see [Managing Cisco CMX System Settings, on page 155](#).

For a complete list of new features supported by Cisco CMX for this release, see the *Release Notes for Cisco CMX*, at:

<http://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/products-release-notes-list.html>



Note The installation methods for Location and Presence are different. If you want to change the service, you must perform a fresh installation.

Importing Maps and Cisco Wireless Controllers

Cisco CMX relies on incoming Network Mobility Service Protocol (NMSP) data from any of the Cisco Wireless Controllers (Cisco WLCs) added to the system. The following sections describe the process to follow.

Exporting Cisco Prime Infrastructure Maps

To obtain maps for Cisco CMX, you have to export maps from Cisco Prime Infrastructure.

Procedure

- Step 1** Log in to Cisco Prime Infrastructure.
- Step 2** Choose **Site Maps** from the Maps menu.
- Step 3** Choose **Export Maps** and click **Go**.
- Step 4** Select the map to be exported and click **Export**.

The selected map is downloaded to a compressed tar file named `ImportExport_XXXX.tar.gz`, for example, `ImportExport_4575dcc9014d3d88.tar.gz`, in your browser's download directory.

Copying the Exported Maps

Use Secure Copy Protocol (SCP) to copy the exported maps to a directory of a server accessible by Cisco CMX.

Importing Maps

You can import maps from Cisco Prime Infrastructure into Cisco CMX using either GUI or CLI.

When you import maps, they are appended to the existing ones in Cisco CMX. When Cisco CMX finds that a campus whose name already exists in Cisco CMX has a different AesUID in the import map file, Cisco CMX performs a map sync operation under this campus if the override option is set to **Yes**.

To import maps using the CLI, use the `cmxctl config maps import --type FILE --path path to .tar.gz file` command.

For more information about Cisco CMX commands, see the *Cisco Connected Mobile Experiences (CMX) Command Reference Guide*, at:

<https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-command-reference-list.html>



Note When importing the maps from Prime Infrastructure using CLI, you also can import the zones. To import zones, set the import zone option as **Yes** and import the maps. After importing maps from Cisco Prime Infrastructure, you can update them in Cisco CMX by drawing new zones. However, these changes are not synchronized back to Cisco Prime Infrastructure.

Adding Cisco WLCs

You can add Cisco WLCs using CLI or the CMX user interface. If you want to import controllers to Cisco CMX from Prime Infrastructure, you must provide SNMP RW credentials for the WLCs after your import them to successfully add them to Cisco CMX. Otherwise, controllers will display as "Inactive."

To add Cisco WLCs from the Cisco CMX CLI, run one of these commands:

- **cmxctl config controllers add**
- **cmxctl config controllers import [PI/FILE]**

For more information about Cisco CMX commands, see the *Cisco Connected Mobile Experiences (CMX) Command Reference Guide*, at:

<https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-command-reference-list.html>



Note After adding Cisco WLCs, you must verify if the controller status is up and running. Using the CLI, you can run the command **cmxctl config controllers show** to display the list of controllers with the status. An **Active** status indicates a established connection.

To validate the controller status using user interface, you need to navigate to the **System** tab. The controllers list is displayed in the tab and the new controller should appear in green.

Logging In to the Cisco CMX User Interface

Procedure

- Step 1** Launch the Cisco CMX user interface using Google Chrome 50 or later.
- Step 2** In the browser's address line, enter `https://ipaddress`, where *ipaddress* is the IP address of the server on which you installed Cisco CMX.
- The Cisco CMX user interface displays the Login window.
- Step 3** Enter your username and password.
- (The default username is admin and the default password is admin.)
-

Using the Evaluation License

Cisco Connected Mobile Experiences (CMX) ships with a fully functional 120-day evaluation license, which is activated after Cisco CMX is installed and started for the first time. The evaluation license is based on Cisco CMX usage, not calendar days (meaning, days when Cisco CMX is not used are not counted).

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.

CMX provides multiple reminders that the evaluation license is about to expire:

- For two weeks before the evaluation license expires, a daily alert is displayed on the Cisco CMX **System > Alerts** window.
- An alert email is sent, if you have configured email settings.
- An alert is displayed when you log in to Cisco CMX.

To add a license, click **Add new license** from the alert. You can also add a license from the Cisco CMX **Manage > Licenses** window. For information about adding permanent licenses, see [Managing Licenses, on page 131](#).



Note

The license file has an .lic extension. Make sure it is the .lic file that you install on Cisco CMX. The .lic file is available as part of your licensing package and is sent as an email attachment from licensing. Extract the .lic file to your system and upload to Cisco CMX when adding a new license.

For details about procuring licenses, see the [Cisco Connected Mobile Experiences \(CMX\) Version 10 Ordering and Licensing Guide](#).

Enabling or Disabling Cisco CMX Services

- To enable a Cisco CMX service using the CLI, run the following command:

```
cmxctl enable {consul | qllesspyworker | cassandra | iodocs | cache_6382 | cache_6380 | cache_6381 | cache_6383 | cache_6385 | influxdb | metrics | confd | cache_6379 | cache_6378 | haproxy | database | analytics | connect | location | configuration | matlabengine | hyperlocation | nmsplb | agent}
```

- To disable a Cisco CMX service using the CLI, run the following command:

```
cmxctl disable {consul | qllesspyworker | cassandra | iodocs | cache_6382 | cache_6380 | cache_6381 | cache_6383 | cache_6385 | influxdb | metrics | confd | cache_6379 | cache_6378 | haproxy | database | analytics | connect | location | configuration | matlabengine | hyperlocation | nmsplb | agent}
```

For detailed information about these commands, see the *Cisco Connected Mobile Experiences (CMX) Command Reference Guide*, at:

<https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-command-reference-list.html>

Importing Certificates

Cisco CMX requires certificates for serving the user interface over SSL. You can import self signed certificates or certificate authority (CA) signed certificates to Cisco CMX. Before initiating the import process, ensure that you have a self signed or a CA signed certificate and the key file. We recommend you to consult your CA authority to generate certificate signing requests (CSR) and certificates.

The certificate should be in the PEM format (with .pem extension) as shown below:

```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: your_domain_name.key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: your_domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----
```



Note Cisco CMX has multiple internal servers that work with SSL certificates. If these certificates use passphrase, after a Cisco CMX restart, the passphrase must be manually entered to use the certificates. As the internal servers within Cisco CMX do not directly interact with the user, there is no interface to input the required passphrases. Hence, at this point, Cisco CMX cannot support certificate with passphrases.

To work around this issue, remove the passphrase from the certificates, by running the following command:
openssl rsa -in <OriginalKeyfile> -out <NewKeyfileWithoutPassphrase>.

Procedure

-
- Step 1** Run the following **scp** command to copy the PEM certificate into Cisco CMX system.
scp cert.pem cmxadmin@10.10.10.10:~/
- Step 2** Run the following **scp** command to copy the key file into Cisco CMX system.
scp host.key cmxadmin@10.10.10.10:~/
- Step 3** Log in to Cisco Connected Mobile Experiences (Cisco CMX) as cmxadmin user.
 The PEM certificate and the key file must be in the home directory of the cmxadmin user.
- Step 4** Ensure that the certificate and key files have minimum global read permissions (0644).
- Step 5** Run the following command to verify whether the certificate is valid.
openssl verify -CAfile /home/cmxadmin/cert.pem /home/cmxadmin/cert.pem
 A valid certificate returns an OK message.
- Step 6** To install the new certificate in Cisco CMX, run the following command:
cmxctl node sslmode enable --pem /home/cmxadmin/cert.pem --key /home/cmxadmin/host.key

Step 7 Run the following commands to restart the agent and haproxy services:

```
cmxctl restart agent
```

```
cmxctl restart haproxy
```

Step 8 Navigate to Cisco CMX URL in your web browser and then use the browser tools to confirm the new certificate.

Installing Self-signed and Third Party SSL Certificate in Cisco CMX

This section describes the installation of self-signed and 3rd party signed certificates in CMX.

Installing a self-signed certificate

Procedure

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

Step 2 Run the following command:

```
[root@cmx]# cd /opt/haproxy/ssl/
[root@cmx]# mkdir newcert
[root@cmx]# cd newcert
[root@cmx newcert]# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/opt/haproxy/ssl/newcert/private.key -out /opt/haproxy/ssl/newcert/cert.crt
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/opt/haproxy/ssl/newcert/private.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:BE
State or Province Name (full name) []:Brussels
Locality Name (eg, city) [Default City]:Brussels
Organization Name (eg, company) [Default Company Ltd]:Cisco
Organizational Unit Name (eg, section) []:TAC
Common Name (eg, your name or your server's hostname) []:cmx.example.com
Email Address []:cmx@example.com
[root@cmx newcert_byserge]# ls
cert.crt private.key
[root@cmx newcert_byserge]# cat cert.crt private.key | tee cert.pem
```

Step 3 The following example shows the certificate:

```

-----BEGIN CERTIFICATE-----
MIID8TCCAtmgAwIBAgJAOWdn/1xqQKNMA0GCSqGSIb3DQEBBQUAMIGOMQswCQYD
VQQGEwJCRTERMA8GA1UECAw1QnJ1c3NlbHMxeTAPBgNVBACMCEJydXNzZWxzMQ4w
DAYDVQQKDAVDaXNjbzEMMAoGA1UECwwDVVEFDMRgwFgYDVQQDDA9zZXJnZWNh0B0
ay5jb20xITAfBgkqhkiG9w0BCQEWEnN5YXNtaW51QGNpc2NvLmNvbTAeFw0xNTEw
MjYxMDU0MzlaFw0xNjExMjUxMDU0MzlaMIGOMQswCQYDVQQGEwJCRTERMA8GA1UE
CAw1QnJ1c3NlbHMxeTAPBgNVBACMCEJydXNzZWxzMQ4wDAYDVQQKDAVDaXNjbzEM
MAoGA1UECwwDVVEFDMRgwFgYDVQQDDA9zZXJnZWNh0B0ay5jb20xITAfBgkqhkiG
9w0BCQEWEnN5YXNtaW51QGNpc2NvLmNvbTCCASIdDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAKOWDC5Y/dRCTSp8mnL40M0QXvrLjzsb2U9++oUsB+e7g0pYITqp
PaPK9KEem17WhoYMqFJ4+AXvuRxsY8EIT/cEs0BfM38QDzDxc42X6TBe7eiFX+MH
WODwk3p3sGLbdVWckWViz99b3eMnPoRdlXPQhQS/LVZcCiNdoHQdwwyPQ32107Gf
x1FVHcjLpUE4FmqhvIttePypwEMoq/3s1tOP3OiJkB9Doy7wrEF+bKHEi6b8N453
jwY70QG7wLrKBRz7QFxxWwurb3PBOtQohWJ16e2aABUDBq9Ata02BVxPaw+dfiC
XCq5Yc8mmDxqc+B7THOPdN9jLzhenMiRJRcAwEAaANQME4wHQYDVR0OBBYEFgQu
ZDeZNoTENM4cO8NNzEdU421cMB8GA1UdIwQYMBaAFGQuZDeZNoTENM4cO8NNzEdU
421cMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAAGL7U4Ls/3bj11dd
500IluEbxPF+SPId+C+dM7BWEf6deeb+yb2KwjmsV0k9CFw9Hs0lqOen5LbnqtzN
3rDwqpkAiaXxKUR34oUONgdnjuCQZwRaTpzQmB0CzwGqu5JuoNSHNtvtOfTtErKRH
oNt6ZlDtpoPTdoj2cUWFrPs7FTkre+ITmKXPORPYoq/vteYtjde5geW6dAV98QC
3HL+FDewGmQDSwnDQcnANUhh88cR3HQge5hx5rLof/xHExrKx/e19Jmw+ft92AC1
sbPb6dR/svR7G1jRyzoO4AMaqlZlOhgiXq3Su8OqcV9MP6k3ArOkUjHzhGX+flw
8wIsYX8=
-----END CERTIFICATE-----
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCCKYwgwSiAgEAAoIBAQCjsAwuWP3UQk0q
fjpy+NDNEF76y487G9IPfvqFLAfnu4NKWJU6qT2jyvShHpte1oaGDKhSePgF77kc
bGPBJU/3BLNAXzN/EA8w8XONI+kwXu3ohV/jB1jg8JN6d7Bi23VVnJF1Ys/fW93j
Jz6EXZVz0IUEvy1WXAojXaB0HcMMj0N9tTu4BcdRVR31y6VBOBZqobyLbXD8qcBD
KKv97Nbtj9zoiZAFq6Mu8KxBfmyhxlum/DeOd48GozkBu8C6ygUc+0BV8VlRq8W9
zwTrUKIVidentmgAAwAvQLWtNgVcT2sPnX6wlvquWHPJpg8anPge0xzj3Tfy84
XpzIkSaxAgMBAAECggEAYIO2fYDnuUG6qPMAf/SzdwvseflulQYTjCwvJ6egQ2a
6GYd/ob7iBC6sq54Fpg3Zv7jfec8lhQS1oglxDhtuK0SIHEPthwng/cGut+uLGHZ
8XttBiu7sCPT85VCV6AM88iBbq3UwQ+mUnWYkFrHFDMGNLvCuEXBsUzkvdc9x+C
GvtXBLERJmLbGh4kyEPFUiTYzXBOTsh+oRaZ5gh4YLicV6a5Cjwu8wm/xZILwbZ
NKCD1RYxAZ7vxASU5Lagi72hIZM5r9kDIDj2zhzdPGo/+R5fIPN92UWjur9r5QM0
9+LU+qeTbjdNojOnYrckBstGySx2+r22FLkWBKcqIQKBgQDSibalRqpMxgZENBfo
RsgHP532AB7cufaDkjEV+vmLupExZ9yRRlWIrqZ7XYkdFRCHTCFt5zrzN8bz5nO5
OdigOZ1Ae7yACmwsSmyBACbNrcVpwE4geckVzw/V2xT+c331rCEd2tzDivlC7Dr0
7s8D3J4zq+KwGEguCYXiPCUUh3wKBgQDHCiH7as1RGQzizVQkN+rDvzo8+TjOHZSF
9BYXQqknCSYuT2d3bFqOdAhqxRL8zKn5qvUOSSr8TvLh4aowVR4ZSO0HMVChjs1W
QZ9PLKkaVyz3Awqvw+UFF0SG7SROjJM8YSMI9qp1rgPY3jrotgZZ02I/TJ8wn9m2
NBsx5s1pbwKBgGf0FVm/7YBg2mE8s309zbA+ihkX8CuEMQi/2zq2JBcI9H3HgZG8
ncP/sDYDdhsE9pdHUM46ONi0fSiaZhNT65EZQXrAXc9+1fb8gtjyHYW6wlm32RuN
8zKwfWojdVc54Ty3U9aw5QYsCdjFmUqsy0xl1zs+KHy4UJNioloVSORTAoGAaA+5
rhLsId+hrh8+o+UceJXNxD1lhtaOZe71cdnniMJO1R2s8hKT0jE2iWRahhQXtrK8
h2iX8ezxLkqHadfG8d9gFkehZoOmNjf/LC0hIuL7XnaXq0vZWO0OziEsv2jePk5n
O/ODsh12Y3flgvBQp7xOfNv5yzl4Ybwij9elhD8CgYAr1K7aM6YznlHaIL0my37Y
cqYE5/EUaL5ng33Rk65krS6k1xFKwRXbq0Nmzln7iWnWA5EMr5WWDKASqJ35niYm
9Plqda0jCDcjTBlib9SVmQ8E016A7WRrqDc9CLY2JjY8KnB1RC9sJ936AErcKiOj
cudhWiCshs6n9Tmfsw6LJQ==
-----END PRIVATE KEY-----

```

Step 4 Run the following commands:

```

[root@cmx newcert]# ls
cert.crt  cert.private.key

```

```
[root@cmx newcert]# cmxctl node sslmode enable --pem /opt/haproxy/ssl/newcert/cert.pem
enabling ssl
ssl enabled
[root@cmx newcert]#reboot
```

Installing a Third Party Signed Certificate

Procedure

Step 1 Generate the certificate signing request.

Step 2 Run the following commands:

```
[cmxadmin@cmx]$ su -
Password:
[root@cmx]# cd /opt/haproxy/ssl/
[root@cmx]# mkdir newcert
[root@cmx]# cd newcert

[root@cmx newcert]#openssl req -nodes -days 365 -newkey rsa:2048 -keyout
/opt/haproxy/ssl/newcert/private.key -out /opt/haproxy/ssl/newcert/cert.crt
```

Step 3 Get the certificate signed by the third party CA.

Step 4 Create the certificate chain for import into CMX.

The following example shows the format for signed SSL certificate:

```
-----BEGIN RSA PRIVATE KEY----- < Your Private Key
MIIEpAIBAAKCAQEA2gXgEo7ouyBfWwCkteYo8ABwFw3d0yG5rvZRHvS2b3FwFRw5
...snipped
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE----- < Your CMX server signed SSL certificate
MIIFeZCCAvugAwIBAgIBFzANBgkqhkiG9w0BAQsFADCBIDELMAkGA1UEBhMCVVMx
...snipped
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < Your intermediate CA certificates
...snipped
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < The root CA certificate that signed your certificate above
MIIGqjCCBJKgAwIBAgIJAPj9p1QMdTgoMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYD
...snipped
-----END CERTIFICATE-----
```

```
-----BEGIN RSA PRIVATE KEY-----

MIIEpAIBAAKCAQEAuRPbZqm6JITR6FCvWF8PejHF+HpTTrwgypty4mviw78gC2G
TGrIYdA2eErpj1UCYVc/0rm5OU68Qr0X2DUm1lukopXgTF3dWtg8FZ77sj8+RN8L
YAaHySHJc9tRF8QUDB8zyHryXSM/5aw1z1F+4DSMP5nVYoZroiM+WXhP3BYFvyHm
nBbgOKZ8Zmln0idJMu8qI53/Hfh3pNsuFjR9sCh+jbIEpUh9Jt54jifeFFUY+7Xt
GJ7GVjyCsGKFHWx6EgrCOb4uqS1crEUjO9/vDlp6M559F1hMQRHkAY5sSFDq5qY+
XEPY7mopyQmNBRZxWgOogtQ2fsK1XFDZ4ZBW0QIDAQABAoIBAQCkIWv+1+DaRYOF
PHsx8xcoayrKFL4QvmvKwFLdNcvNtb4FnnZXbn5TvX0y7CtXMxmyxowTMOXueH4i
```

```

O1YBBwNKjKSTkQSt5Kr8Jl8IOyFJGcSeKltLQYNU8YTcaqRqpgvN29GI7wyolrgz
3jib7HUPnKs7w+lmfHMq9Hx1w/AAnm/Fb7/sXUww80cdfGFHIYfqBvC5FJKe3N/f
sg5Npjhaqrvs9bsd7MUKu5LjcdUN9nVWU604NWaMJHUQPoHmf3vwNND41YDbsG7
Aj8exOW4+2WKYz9c9Ry1qivkIgneGUval3mR4Z0Rc+Ijckie+UhfHx4DmO4M
pEw5wjIhAoGBAPEQfmDSme8Ur9V6zNaXtcaAL77JozNuSyEzpvSduUf4HLTJBY34
U4V6AWyQR2koSZON2tBbuC8s/D2cas2A1htoD8ffl/dWefoJmNzOTyyjQNKepf0
NfEOvGKQdOpI/DG62ngxbT5zkUpV/qSxdQw9xZoYV7FkPrst+7kv8gLAoGBAMSL
XA7aVSkFmrBDsag6YNsmOaBp8geEAll/N3dazXulIHUCnpUpY//Cgeb+LBrKQmWA
Fuf5gcb7GR4oFmu4jaTpXvKz8eqnsNeDmzVKMoB31wd9QTrYMc+SBuyX3nHldRFF
CXU1UIAj/ujomZ+wYuyE/qtOISZ2FITkZQvjRjoTAoGBALa76QDeRB/uj4eFCeeV
ow5wt0CputPOxJbL8CoGv5KPwBv7Yz789wXayLv6JQDs4SVw9gp5LjR+YwPum+
ww6NaID7o9d5JKDd4tO6UWYId0pKV/n9/jHYGMeid23tm3bbDKbV2NjhY/8UvQNN
5TZ/U54hy8W6f7cmYBtwPUyXAoGAC1bS79Ru11glBaTqKf98OQiCiJu0J/TYwdsS
EyO8+SY0sit9hLOHnmjVX8NIPh9vJzX1nFqLvzQbZd8ANCTInzwL0sQaO5VyILC
OhfWxAYl7juuuLiXExbc+jrH30SfPWTrxtbEw3V66VzIXZzzV5D98JEP9aRFY
NxBeq9sCgYBSIZfEKW9DTuPAHFYLTQpDRLM/1sT2K9CcASHlj4jmV+7CfJggKY
TQnshZuvArjIYUCjrSubwt6FYmP+O6hbnHEBHo6RTCc2qnvS7J+GGk8C/CH/iTO
PbXaW7rcUuX6hEFdZQQ8OOJBstnKjZn2sI+OIX+VBrqnDOYWIFwIEA==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIEFjCCAvqgAwIBAgIBGDANBgkqhkiG9w0BAQsFADCBIDELMAkGA1UEBhMCVVMx
CzAJBgNVBAGTAk5DMQwwCgYDVQQHEwNSVFAxHDAaBgNVBAoTE0Npc2NvIFN5c3Rl
bXMsIEluYy4xMjE5MjE5MjE5MjE5MjE5MjE5MjE5MjE5MjE5MjE5MjE5MjE5MjE5
Y29tMSEwHwYJKoZIhvcNAQkBFhJzc2NobWlkdEBjaXNjby5jb20wHhcNMjE5MjE5
MTQ0MDAeWWhcMTcwNTA1MTQ0MDAeWjCBhjELMAkGA1UEBhMCVVMxMzAJBgNVBAGM
Ak5DMRwwGgYDVQQKDBNDaXNjbyBTeXN0ZW1zLmJmMmMwCgYDVQLDANUQUXUMx
GzAZBgNVBAMMEmxhdWodGvYlMnNpc2NvLmNvbTEhMB8GCSqGSIb3DQEJARYScmFt
a3JpczJAY2lzY28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEa
uRpbZqm6JlTR6FCvWF8PejHF+HpTTrwgypty4mviw78gC2GTGriYdA2eErpj1UC
YVc/0rm5OU68QrOX2DUM1lukopXgTF3dWtg8F77sj8+RN8LYAaHySHJc9tRF8QU
DB8zyHryXSM/5aw1z1F+4DSMP5nVYoZroiM+WXhP3BYFvyHmnBbgOKZ8Zmln0idJ
Mu8q153/Hfh3pNsuFjR9sCh+jbIEpUh9Jt54jfcFFUY+7XtGJ7GVjyCsGKFWHx6
EgrCOB4uqS1crEUj09/vDlp6M559F1hMQRHkAY5sSFDq5qY+XEPY7mopyQmNBRZx
WgOogtQ2fsK1XFDZ4ZBW0QIDAQABo3sweTAJBgNVHRMEAjAAMCwGCWCGSAGG+EIB
DQQFh1PcGVuU1NMIEdlbmVyYXRIZCBZDZXJ0aWZpY2F0ZTAeBgNVHQ4EFgQUeKxp
ACe19Jpz6QUXGALJik41DjcwHwYDVR0jBBgwFoAUUPGERegtBFb+1WJ+1ZLqRpWK
G84wDQYJKoZIhvcNAQELBQADggIBAzykVSWLvNuFk/Q1PRFU7pdX5z8g5K0aQjo
4erS148m1WoM7vJNXjqjHD6JdcOMINGeuxEli1Vd7prpARhE+Qj7xSMfDMilzSfy
mKvPtNQzT/9yHytAycVsvbGYJDh8R3jTpxJXWPBcvErE8OuaxkCbePNzQD56KqFC
Sjibw2GqWLa8GaHZdL0IGQ9dJdfsQwriqphBX9Dkd9qeMPnxYCXVSE4SsLbUWC
n0tasfJ4pergRqEi6OBw8zh3twcy6vEBJvp0tA3/z3yPdvG0sZ5x5WCTCCOMlvUE
BswbZusCMQFCHg14wbEoNo/I3GDoqRHzw1j0hA887r4AWnMOeXjkHjA7YxtrSzJ4
cQL5WEXj8di6UqwQA+dNBCLv488huLFecEL8YjMLV4Z6nfaXzNF2FLJZByaD4/sP
TcZ2BkKS53YKKE7LUalbUH3ymdfejQuIvabtBnc/of5bw7WODlyBZlhd4MW3eFJK
puoXXxp0xqmS3/VMnefyVqBz3eV4KXkg0Z6w6KbCxs9aTP+NtSGEBEXgm36TvR
2SIVCwKH/RIDQp+vk1QykQdj6JSMJUrI6fdRAtpAZssMGIT2KsreRVnJ8ig7VAKp
17ES4FZ/7rg87GoUYfmAl+AhvZCCu2SjJBdW6/IO1rHHkB+1UkU+yswY85Cq7Wj
+9TmdHX8
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIGqjCCBJKGAwIBAgIJAPj9p1QMdtgoMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYD
VQQGEwJVUzELMAkGA1UECBMCTkMxDDAKBgNVBAcTA1JUUEEcMBoGA1UEChMTQ2lz
Y28gU3lzdGVteywgSW5jLjEMMAoGA1UECXMdVEFDMRswGQYDVQQDEwJsaW51eGxh
Yi5jaXNjby5jb20wITAfBgkqhkiG9w0BCQEWEnNzY2htaWR0QGNpc2NvLmNvbTAe
Fw0xNjA1MDUxMzQ5MTIaFw0zNjA0MzAxMzQ5MTIaMIGUMQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCTkMxDDAKBgNVBAcTA1JUUEEcMBoGA1UEChMTQ2lzY28gU3lzdGVt
eywgSW5jLjEMMAoGA1UECXMdVEFDMRswGQYDVQQDEwJsaW51eGxhYi5jaXNjby5j

```

```

b20xITAfBgkqhkiG9w0BCQEWEEnNzY2htaWR0QGNpc2NvLmNvbTCCAiIwDQYJKoZI
hvcNAQEBBQADggIPADCCAgOCggIBALDXzffE4YyvCakwDop2gKcfOAOgn96hzbVC
OvVGDNwYE/070u9Rh8Tf4yCX8tknrkN2QnqZVarWgUPYvc0zSVqXiT6bxWkuvGYL
nO+PiXFKAfMIF+BjF0L8Fdm0B+ZowSULrFwLCX7yOsemn62NfwVH0MUImJogIF0
JW+8pJrxrfoWG78AgRUsKFi5R4IuTPWV1PSWiD1nDEEkxn1JKNmwtnc7iAUHWMS
gKK64VBpoSTNwpiyHCD0B4Col2x+R9NNWOQ9X7NnmhtR16AYKm60ElkMYvP1Zjrl
aZFfzkZXLmsxluxjbU9mv4IUhGzeJxbcBUPuvLbM6WoOYp6/YoSdd5PtfX9Ixim
7zO/uL7w2vyI4+kJYm7HHtFVHuhEcWEhyEdW0JcvT61L68F/iB79WezJd0VbPCel
gFSJFhx5F2jhyYlZq2bbjOdzf0RC+U053W+xfqQUt17BDnb6n+UvPSDFwDpnKMH
RbZlis0nC7YfqscDnrpBETRPnvNfRsQznoBgqqPWrfJ/RVU+CnjxZB+SiEWhV2ei
WlaP8iB+MmMBYoHXbk1pBf0BkZEXd2uGk74o7a3rj1MAIzdppoGYAW2hfvYYqNW
kDGOgkHLf1KzawB9gaiWNHo6UujaHZNi/jKL6FQlor+HQ/EggWtflTLI1YBTz4cB
iNIK3wQ7AgMBAAGjgfwgfkWgHQYDVR0OBByEFFDxhEXoLQRW/tViftWS6kaVihvO
MIHJBgNVHSMEEgcEwgb6AFFDxhEXoLQRW/tViftWS6kaVihvOoYGapIGXMIGUMQsw
CQYDVQQGEwJVUzELMAkGA1UECBMCTMxDDAKBgNVBACeTA1JUUEDEcMBoGA1UEChMT
Q2lzY28gU3lzdGVtcywgSW5lLjEMMAoGA1UECXMdVEFDMRswGQYDVQQDEwJsaW51
eGxhYi5jaXNjby5jb20xITAfBgkqhkiG9w0BCQEWEEnNzY2htaWR0QGNpc2NvLmNv
bYlJAPj9p1QMdTgoMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggIBAD0R
CmpKKygd3oRip8NaRssHYndwm6t3Add4+BM/wZ5TbNi5POg5JZIDgV2qT6elJlux
dLTTTCJcHaoeITWW/CTpYrve+Q3NAPTImmXTX2swN7zVX3GXNoBQWhIuZh4A9YMVb
tAST307qCQq+6NU1LKBJtdnc6qw/VLe2WD9vvhDcq+i5HyHJWJqsTcO8iU8fyTGv
Q1i8MFZ7VPgnr2RGalki8yCsFG+bSKuiVQgylQLMKSkqCtWww+eBj1bPr/MecgC
1bO5OJ+id08UalM6KhlRQYY9o5q7lRIFVgUvHyhsNdvmsa15kpWLeKqsNrf5A
jipNPJW4Cf2HLutZZZGGIDNc9kQID7XyPXIV41n/4uoYuKjea6RgcJYR/IFh0rTo
nUp3LbZkpRQksWrhKfO7BoFOif7s9K06YDuOu2o/dzU1XUf937ovNmGqvOPRPrV2
5cUrQKEXeTsGubxvxxkEFv39BZsefc0tiSMRkpN84FOBoYUkc0zioiURQa8gs6Eo
w5CuB/DH65uxQ2yowV4KvktHA5az5j0ZUoayLX0vOktr54g+z3+li+QN2yftIOOS
zvz4k6Ylu4ySosg4BdWVmPXbLLkTpb+AEHPK+IZF6I6qMVPU5wz6VMAVKhilaEkN
o1d/c05RYSTy8/SIROa4ms68xqCpQIdaWg10VIDQ
-----END CERTIFICATE-----

```

Installing the Certificate

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX) as cmxadmin user.
- Step 2** Run the following command to make a directory on CMX to hold the new certificate: `[root@cmx ~]#mkdir /opt/haproxy/ssl/newcert/`
- Step 3** Copy your properly formatted signed certificate to the new directory.
- Step 4** Run the following commands on Cisco CMX to ensure that everything is property built: `openssl verify`

```
[root@cmx newcert]#cd /opt/haproxy/ssl/newcert
```

```
[root@cmx newcert]#openssl verify -CAfile /opt/haproxy/ssl/newcert/localhost.pem
/opt/haproxy/ssl/newcert/localhost.pem
```

```
/opt/haproxy/ssl/newcert/localhost.pem: OK
```

You must get an OK message.

Instructions for CMX build 324: (10.2.2 beta) or 10.2.2 CCO and Later

In CMX 10.2.1-219 there is a bug that will not allow the install to work properly ([CSCux30499](#) Need exact steps in the config guide for certificates). The issue will be fixed in CMX 10.2.2 which will be out May 2016. If there is a business need to continue with CMX 10.2.1-219, please contact the TAC for the workaround.

Procedure

Run the following command:

```
[root@cmx newcert]#cmxctl node sslmode enable --pem /opt/haproxy/ssl/newcert/localhost.pem
enabling ssl
ssl enabled
```

```
[root@cmx newcert]#reboot
```

Adding Users and Managing Roles

Using the **MANAGE** service in Cisco CMX, you can create new users and assign roles to them based on the tasks they have to perform, that is, enabling role-based access control.

The following list displays the types of users:


- Admin users—An admin user can access all the services and functionalities (based on the license type) of Cisco CMX.
- Others—An admin user can create other users and assign roles to them.

The following is a list of roles that can be assigned to users:

- System
- Manage
- Analytics
- Read Only
- Location
- Admin
- ConnectExperience
- Connect

For more information about the creation of users and assignment of roles, see [Managing Users](#), on page 134.

Using the Cisco CMX Setup Assistant

The Cisco CMX Setup Assistant pop-up helps you through the basic steps before you start using your system. The Cisco CMX Setup Assistant is automatically displayed when you log in to Cisco CMX. To relaunch the Cisco CMX Setup Assistant, click the Help () icon.

Supporting Active Clients Version 3 API

Cisco CMX release 10.4 supports new active clients version 3 API under Location REST API. The new Active Clients v3 API allows frequent requests without impacting other services such as location service. The new **Node.js** processes API requests in the API v3. The location service sends the local notifications to the API server and active clients are tracked in the API server memory.

The Active Clients v3 API has its own user ID and password for accessing the REST APIs. Use the **cmxos apiserver** command to define the unique user ID and password. The Cisco CMX web UI username and passwords will not work for API v3.



Note Active Clients v3 API under Location API documentation section includes better parameter testing. Active Clients Version 2 API has been deprecated in Cisco CMX 10.4 release.

Active Clients v3 API supports these additional parameters:

- mapHierarchy
- manufacturer
- macAddressSearch
- associated/probing

The following log files are located in the directory `/opt/cmx/var/log/apiserver` for troubleshooting:

- `cmxapiserver.pid`—Processes ID file for the top process.
- `server.log`—Log file for messages and errors
- `stdout.log`—Standard output messages

Getting APIs

To obtain the following APIs, use the `https://cmx-ip-address/apidocs/` URL:

- Configuration REST APIs for configuring different aspects of Cisco CMX.
- Location-based REST APIs for finding location-specific details about visitors.
- Analytics-based REST APIs for finding analytical data on visitors.

- Connect-based REST APIs for finding user session information.
- Presence-based REST APIs for finding presence data on visitors.

Changing Time Zones and NTP Server

After the initial CMX configuration, you can change the time, time zone, and NTP server details using the CLI. You can edit the `ntp.conf` file to change the NTP server. Ensure that you are logged in as root user to change the NTP settings.

To change time zones and NTP server after initial configuration using CLI, perform the following task:

Before you begin

- Ensure that your server has a valid hostname before making any NTP changes. If not, some of the `ntp` commands will fail, for example, `ntpstat`.
- Ensure that incoming and outgoing UDP port 123 for NTP communication is open in your configuration setup.
- Ensure to manually edit `/etc/ntp.conf` as admin user and appropriate time zone is selected using `/opt/cmx/bin/tzselect` before restarting `ntpd` using **service ntpd restart**.

Procedure

- Step 1** To stop all the services on the CMX, run the **cmxctl stop** command.
 - Step 2** To change the current user to admin root user, run the **su** command.
 - Step 3** In the `/opt/cmx/bin/tzselect` path, run the time zone script.
 - Step 4** To log out from the configuration setup, run the **exit** command.
 - Step 5** Log in again and verify the time, time zone, and date settings.
 - Step 6** To restart the services, run the following commands:
 - **cmxctl start agent**
 - **cmxctl start**
-



CHAPTER 2

The Cisco CMX Detect and Locate Service

- [Overview of the Detect and Locate Service, on page 17](#)
- [Initial Configurations, on page 17](#)
- [Viewing or Tracking Devices, on page 18](#)
- [Viewing Device Details, on page 21](#)
- [Customizing Client Refresh Rates, on page 22](#)
- [Customizing Device Views Using Filters, on page 22](#)
- [Adding and Deleting Filters, on page 23](#)
- [Searching for a Device, on page 23](#)
- [Client Playback, on page 24](#)
- [Enabling Hyperlocation and FastLocate in Cisco CMX, on page 24](#)
- [Controlling the Probing Client Expiry Time, on page 36](#)
- [Measuring Client Location Accuracy Using the Location Accuracy Test, on page 37](#)

Overview of the Detect and Locate Service

The Cisco Connected Mobile Experiences (Cisco CMX) **DETECT & LOCATE** service enables you to view and track devices in your deployment.

Using the **DETECT & LOCATE** service, you can either view all the access points (APs) deployed in all the buildings of a campus or view the APs deployed on the individual floors of each building. You can also locate Wi-Fi tags, Wi-Fi interferers, and Bluetooth low energy (BLE) Tags.

Initial Configurations

In order to use the **DETECT & LOCATE** service, the following initial configurations have to be performed:

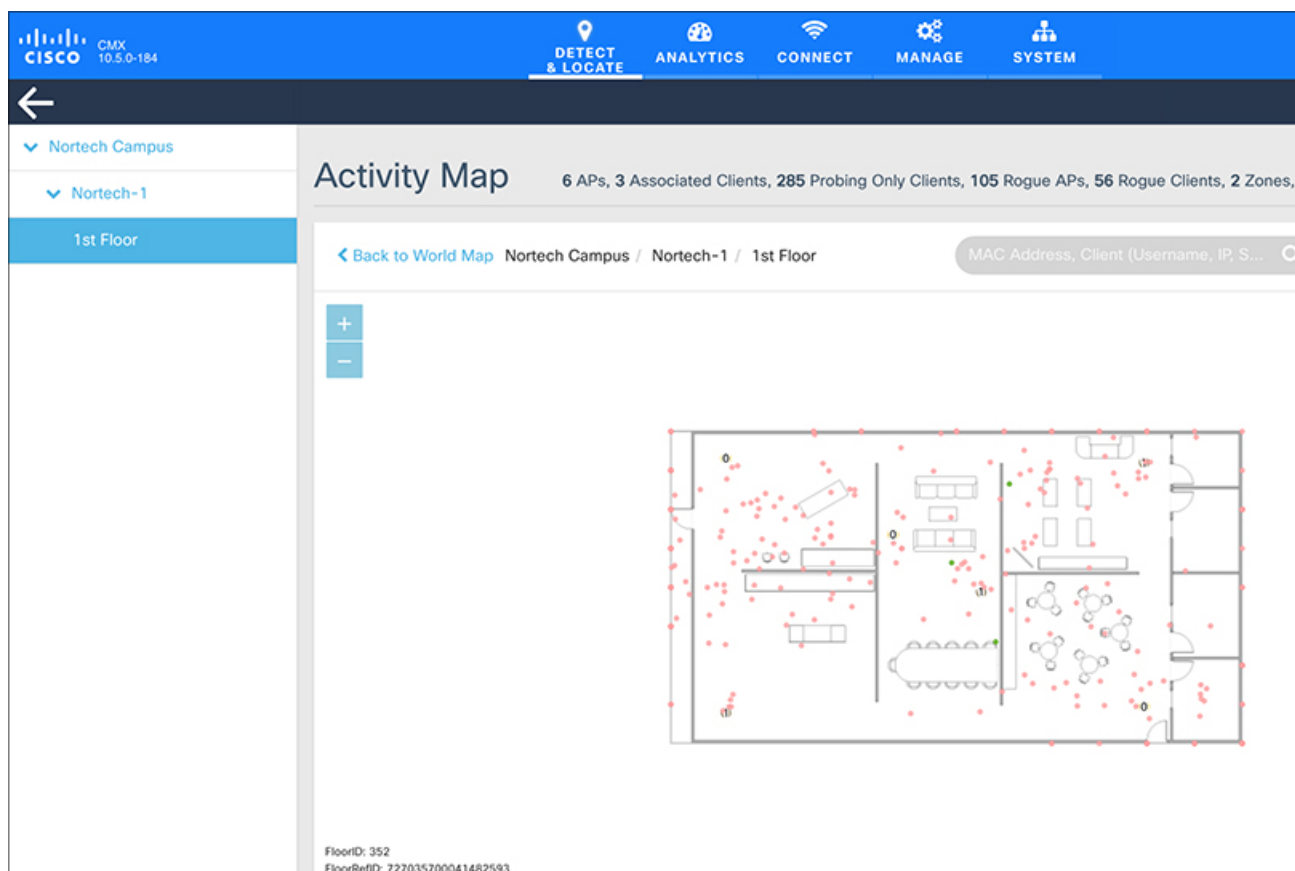
- Import maps—For information about this, see [Importing Maps and Cisco Wireless Controllers, on page 4](#).
- Add controllers—For information about concept, see [Adding Cisco WLCs, on page 5](#).


Viewing or Tracking Devices

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Click **DETECT & LOCATE**.
- Step 3** Using the left pane of the **Activity Map** window, navigate to the desired building and floor. The **Activity Map** window displays a list of icons to the right.


Figure 1: Activity Map Window

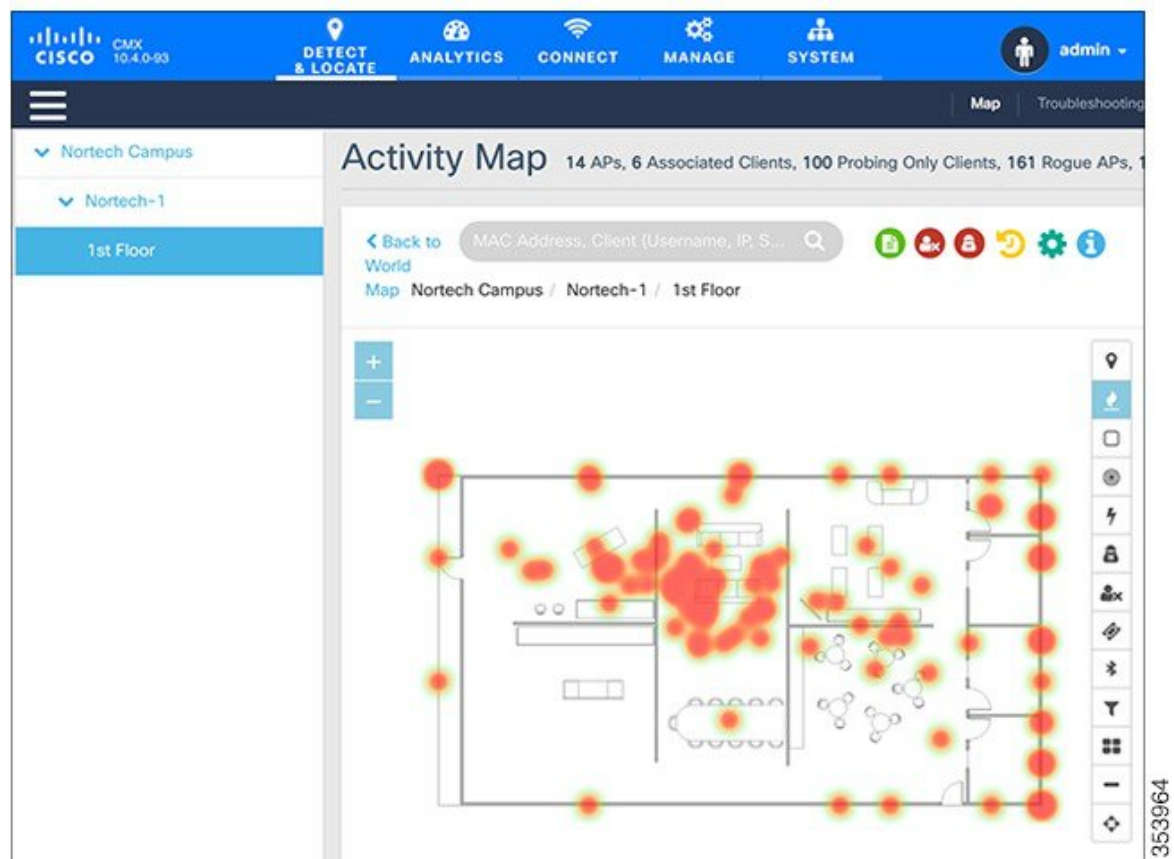




- Step 4** Choose any combination of the following icons to customize your view of the devices:
- **Clients**—Click the **Clients**  icon to show or hide all the client devices (connected and detected) that are being tracked by your Cisco CMX. Client devices are displayed either as red dots (probing clients) or green dots (connected clients). Clicking on connected clients show the AP that the client is associated with (blue lines) and the APs that are participating in the location calculation (red lines), and while clicking on a probing of unassociated client displays the APs that are being used to detect the clients (red lines).

- Note** The maximum number of clients (connected and detected) that can be displayed at a given time is 2000. If this limit is exceeded, only connected clients are displayed, again up to a maximum of 2000 (see the figure below). However, if the number of total connected clients also exceeds 2000, no clients are displayed. In such a scenario, we recommend that you use the Analytics service to view the client information.




- **Heatmap**—Click the **Heatmap**  icon to show or hide areas with varying concentrations of client devices. Areas with a high concentration of client devices are marked bright red, as shown in this figure.




- **Zones**—Click the **Zones**  icon to show or hide the zones on a specific floor.
- **Access Points**—Click the **Access Points**  icon to show or hide all the APs that have been deployed on a specific floor. APs are displayed as circular objects, with a number in the center. This number indicates the number of clients connected to that specific AP. Inactive access points (red circle with a hyphen) are also detected.

Cisco CMX shares Access Points grouping information to Cisco WLC every time when a NMSP connection is established. To get a list of APs connected to the Cisco WLC, Cisco CMX performs a SNMP get action on the Cisco WLC. Based on the list of APs received from the Cisco WLC and the APs on the map, identify the subset of APs and prepare a grouping request to send to the controller. You can store the AP grouping information on the datastore.

- Note**
- 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.
 - Clicking an AP shows the clients connected to it (blue lines), the probing clients that are detected by the AP (red lines), and additional information such as height, orientation, and X,Y location of the AP.
 - If you have a Cisco Hyperlocation module that is attached to the back of your Cisco Aironet 3700 and 3600 Series APs, you can track the location of customers, visitors, or assets to about one meter in an ideal environment. Currently, the Hyperlocation solution works for the associated clients only.


- **Interferers**—Click the **Interferers**  icon to show or hide all the RF interferers that have been detected by the wireless network, and their zone of impact.

Note In Cisco CMX release 10.4, the BLE Beacons management page is no longer available on the Cisco CMX user interface. Beacon notifications are no longer provided. BLE beacons detected by Cisco CleanAir are displayed on Cisco CMX as interferers. BLE-related information is no longer available on the apidocs file.

- **Rogue APs**—Click the **Rogue APs**  icon to show or hide the rogue access points. Rogue access points are those access points that are not part of the Cisco CMX infrastructure access points and not managed by Cisco CMX. They are classified as Unclassified, Malicious, Friendly, and Custom and indicated by different colors on the Activity Map.




- **Rogue Clients**—Click the **Rogue Clients**  icon to show or hide rogue clients. Rogue clients are clients connected to rogue access points.

Note To track rogue access points and clients, enable the tracking parameters **Rogue Access Points** and **Rogue Clients** in the **Network Location Service** window under the **System** tab. For more information, see [Setting Device Tracking Parameters, on page 158](#).

- **BLE Tags**—Click the **BLE Tags**  icon to show or hide BLE-transmitting devices that have been detected by the wireless network.

Note A beacon is detected as an interferer. A common problem faced in the context of beacons is tracking not being enabled. In such a scenario, you can modify the tracking configurations using the System service. For more information, see the [Viewing or Tracking Devices, on page 18](#).

Click **Beacons** to view the beacon attributes related to the selected beacon profile.

- If the beacon is chirping with iBeacon profile, Cisco CMX displays the properties such as UUID, Major and Minor number.
 - If the beacon is chirping with Eddystone-UID profile, Cisco CMX displays the properties such as Namespace and Instance-Id.
 - If the beacon is chirping with Eddystone-URL profile, Cisco CMX displays the HTTP resource URL being broadcasted by that beacon.
- **Tags**—Click the **Tags**  icon to show or hide Wi-Fi tags. The vendor specific information related to the tags are displayed in raw format.
 - **Filters**—Click the **Filters**  icon to filter the display of devices based on parameters such as Connection Status, Manufacturer, and Service Set Identifier (SSID).
 - **Inclusion & Exclusion Regions**—Click the **Inclusion & Exclusion Regions**  icon to view the inclusion and exclusion regions on a floor. The inclusion and exclusion regions are created in Cisco Prime Infrastructure. In Cisco CMX, you can view these regions, but you cannot modify them. The inclusion regions are shown in green, and the exclusion regions are shown in gray.
 - **Thick Walls**—Click the **Thick Walls** icon to view any thick walls that have been created on prime infrastructure and included on the floor. Thick wall improves location by modeling areas of high RF signal attenuation with more accuracy.
 - **GPS Markers**—Click the **GPS Markers** to view any GPS markers that are placed on the floor. When at least three GPS markers are placed on a floor, the system can use these to provide GPS co-ordinates, in addition to X, and Y co-ordinates in client location API requests.

Viewing Device Details

Procedure

-
- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
 - Step 2** Click **DETECT & LOCATE**.
 - Step 3** Using the left pane of the **Activity Map** window, navigate to the desired building and floor.
The **Activity Map** window displays a list of icons to the right.
 - Step 4** Click the corresponding icon to show the desired devices, for example, client devices, APs, beacons, and so on.

- Step 5** Click the corresponding device on the map.
A pane displaying details of the device, such as MAC address, IP address, status, and so on is displayed.
-

Customizing Client Refresh Rates

The DETECT & LOCATE service enables you to configure the refresh rate for clients' position on a floor map. The refresh interval can be used to configure how frequently a client's positions will be polled to determine their positions. The default refresh rate is five seconds. The refresh rate gets automatically reset when you navigate to another tab or log in again. The client refresh rates are temporary and is not stored in the CMX.

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX) either as an admin user or a user with Location role.
- Step 2** Click **DETECT & LOCATE**.
- Step 3** Using the left pane of the **Activity Map** window, navigate to the desired building and floor.
The **Activity Map** window displays a list of icons to the right.
- Step 4** Click the **Gear** icon to configure the client refresh rate.
A pane indicating the client refresh intervals is displayed.
- Step 5** Use the + or - icon to increase or decrease the client refresh rates. The refresh rates are in seconds. The range is one to 30 seconds.
- Step 6** Click **OK**.
The client, represented by dots on the map, will be refreshed with the new configured rate.
-


Customizing Device Views Using Filters

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX) either as an admin user or a user with Location role.
- Step 2** Click **DETECT & LOCATE**.
- Step 3** Using the left pane of the **Activity Map** window, navigate to the desired building and floor.
The **Activity Map** window displays a list of icons to the right.
- Step 4** Click the corresponding icon to show the desired devices, for example, client devices, APs, beacons, and so on. The more icons you click, the more filtering options are enabled.
-

Adding and Deleting Filters

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Click **DETECT & LOCATE**.
- Step 3** Using the left pane of the **Activity Map** window, navigate to the desired building and floor.
The **Activity Map** window displays a list of icons to the right.
- Step 4** Click the corresponding icon to show the desired devices, for example, client devices, APs, beacons, and so on. The more icons you click, the more filtering options are enabled.
- Step 5** Click the **Filter**  icon.
- Step 6** In the **Filters** dialog box that is displayed, you can add or remove client filters based on the following parameters:
- **Connection Status**—Unassociated or Connected
 - **Device Manufacturer Type**—Name of the device manufacturer, for example, Apple, Samsung, and so on
 - **SSID**—Device's SSID
-

Searching for a Device

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Click **DETECT & LOCATE**.
- Step 3** Using the left pane of the **Activity Map** window, navigate to the desired building and floor.
- Step 4** In the **Search** field of the **Activity Map** window, enter any of the following parameters to search for or filter a desired device:
- **MAC Address**—Enter the corresponding client's MAC address in lowercase, colon delimited, for example, 00:a0:22:bc:e2:00.
 - **Device IP Address**—Enter the client's IPv4 or IPv6 address in dotted format, for example, 10.22.12.212.
 - **SSID**—Enter the client's SSID in free-form text.
 - **Device Manufacturer**—Enter specific manufacturer names, for example, Apple, Samsung, and so on in free-form text.
 - **Username**—Enter the client's username in free-form text.

Note When performing a device search based on MAC address, if a device is not located on the specific floor that you are on, a dialog box is displayed that shows the floor in which the specific device is currently on. In addition, you can search based on MAC address for a specific date.

Client Playback

The Client Playback feature enables you to locate and track the movement of clients in a venue. You can track the activity of one client at a time.

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Click **DETECT & LOCATE**.
- Step 3** Using the left pane of the **Activity Map** window, navigate to the desired building and floor.
- Step 4** Search the client you want to track using the its MAC ID.

For more information about how to search client devices, see [Searching for a Device, on page 23](#).

- Step 5** Click the **Client Movement History Playback** icon .

The Client Playback (see the image below) pane is displayed .



- Step 6** Click the **Play** icon to start client playback.
You can also change the date in order to view the playback on a specific date, by clicking the **Calendar** icon. You can increase the speed of the playback by clicking the **2x** button.

Enabling Hyperlocation and FastLocate in Cisco CMX

The Cisco Hyperlocation solution is a suite of technologies that enables advanced location capabilities through a mix of software and hardware innovations. Cisco CMX Release 10.2.1 supports the Angle of Arrival (AoA) technology available on Cisco Aironet 3600 and 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 up to one meter accuracy in an optimal deployment.

The Cisco Hyperlocation module with advanced security also integrates Bluetooth Low Energy (BLE) beacons with the module. Customers can take advantage of 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 virtual BLE beacon technology so that a single Hyperlocation module appears as five different BLE beacons to consumer applications.

Cisco CMX FastLocate technology enables quick location refresh for connected Wi-Fi clients. RSSI from data packets and probe frames, when available, are used for calculating a location. This technology is available with both centrally switched WLANs and FlexConnect (locally switched WLANs). Cisco Aironet 700, 1700, 2600, 2700, 3600, and 3700 APs support Cisco CMX FastLocate when used with Cisco WLC Release 8.1.123.0 or later.

Accuracy results for the Cisco FastLocate feature are reflected in the Cisco CMX Accuracy Tool under the **50% and 75% Error Distance** columns. Accuracy is considered good if the distance displayed under those columns is 10 meters or less, meaning the client will be detected less than 10 meters from its actual position. For information about configuring Cisco FastLocate, see “FastLocate for Cisco Wave 2 Access Points” section in the *Cisco Wireless Controller Configuration Guide, Release 8.6* at:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-6/config-guide/b_cg86/location_services.html#ID2048

**Note**

- The above result is only valid for smart devices.
- We recommend that you have all the APs in the same group on a particular floor. If you cannot have APs in the same group, then plan to include nearby APs in the same group. All AP groups available on the same floor must be synchronized to the same NTP server.
- Ensure that you disable the global **Hyperlocation** option and enable **Hyperlocation** option specific for AP group. We recommend that you do not set the XOR radio to monitor mode manually. When you enable Hyperlocation in the AP group, the XOR radio settings are taken care by default.

The following 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—APs scan on 2.4 and 5 GHz bands.
- Modular Mode—Cisco 3600 and 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.

**Note**

- The FastLocate and Hyperlocation features are supported in Cisco CMX 10.2.1 and later.
- In Cisco CMX Release 10.4, FastLocate feature is supported on Cisco Aironet 2800/3800 access points running Cisco Release 8.6 or later.
- In Cisco CMX Release 10.3.1, the Hyperlocation feature supports 10,000 tracked devices—1000 Cisco access points (APs) with up to 10 connected clients per AP—on Cisco 3365 Mobility Services Engine (MSE) and Cisco high-end MSE Virtual Appliances (v MSE) running Cisco CMX Release 10.3.1 and later.
- The Hyperlocation and FastLocate features are supported in Cisco WLC 8.1.123.0 and later.
- Currently, a Hyperlocation-enabled Cisco WLC can support only one Hyperlocation-enabled Cisco CMX.
- The Hyperlocation feature is not supported on a virtual Cisco WLC.

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Choose **SYSTEM > Dashboard**.
- Step 3** Click the **Gear** icon at the top-right corner of the window. The **SETTINGS** window is displayed.
- Step 4** Click the **Location Setup** tab.
- Step 5** In the **Location Calculation Parameters** window, check the **Enable Hyperlocation / FastLocate/ BLE Management** check box.
- Step 6** Add Cisco WLC to Cisco CMX.

Note If hyperlocation is enabled and one controller is in active status, and no data is received for almost 15 minutes an alert is generated with the following description "Hyperlocation is enabled on CMX, however no AOA data is received". The alert service type is Hyperlocation and alert type is Service_Status.

As a work around, maintain a one to one mapping between controller and Cisco CMX. Only one controller can serve one Cisco CMX box with hyperlocation enabled. If two hyperlocation enabled Cisco CMX boxes are using the same controller, disable hyperlocation service in one of the Cisco CMX box.

Hyperlocation Mixed Mode Support

Cisco CMX Release 10.4 now supports a mixed deployment of Cisco Hyperlocation access points (AP) and non-Hyperlocation AP on the same floor map. If the client is associated to a regular access point but has a hyperlocation enabled access point near by, AoA computation is performed to provide an acceptable accuracy. All Cisco Hyperlocation APs must be within a contiguous area. Increased accuracy on the floor is only within the convex hull of the Hyperlocation contiguous area

Hyperlocation groups are formed consisting both hyperlocation and regular access points. The floor mode is decided when generating the hyperlocation group. There following are the three supported modes:

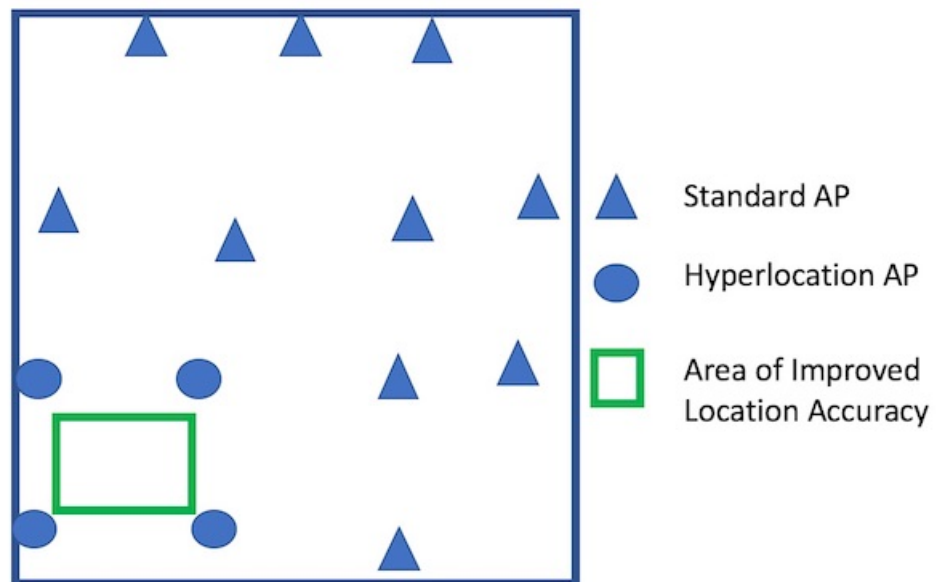
- RSSI mode-All access points on the floor are regular APs.
- Mixed mode: Few APs on the floor are Halo APs.



Note Use the `cmxctl config hyperlocation mixmodeFloor ID` command to enable hyperlocation mixed mode.

We recommend that you use this command in a deployment scenario where there are both Hyperlocation enabled APs and non Hyperlocation APs on the same floor map. The improved location accuracy that comes from the use of Hyperlocation AP will occur within the convex hull of the Hyperlocation APs. Outside of this convex standard location accuracy results will occur. At the edges of the convex hull there may also be lower accuracy than when clients are at least 10M inside of the convex hull. This command does not support the interspersion of Hyperlocation AP with non Hyperlocation AP. If this is type of deployment is used, then there will be no improvement in location over standard probe RSSI based location.

An example of an supported deployment is as follows:



- Halo mode: All APs on the floor are Halo APs.

Running Hyperlocation Diagnostics

Hyperlocation Diagnostics is a tool that can find common issues in a Hyperlocation deployment.

Hyperlocation Diagnostics executes a set of tests to verify any common issues with Hyperlocation. These tests are executed against an existing Hyperlocation setup on a floor. The floor should have clients associated to Hyperlocation access points to validate complete functionality.

Procedure

Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX) either as an admin user or a user with Location role.

Step 2 Choose **DETECT & LOCATE > Troubleshooting**.

The **Hyperlocation Diagnostics** window is displayed. As this is a floor-level test, select a building and floor. Note that only floors with hyperlocation access points are populated here.

Step 3 (Optional) Add the details and credentials of a controller and an access point for a more detailed report.

Step 4 Click **Run Diagnostics** and wait for a few minutes.

a) Click the **Troubleshooting guide** for a detailed description of each test.

Hyperlocation Diagnostics

Hyperlocation Diagnostics will execute a set of tests to verify any common issues with Hyperlocation. These tests are executed against an existing Hyperlocation setup on a floor. The floor should have clients associated to Hyperlocation access points to validate complete functionality.

Troubleshooting
Guide

Running Hyperlocation Diagnostics
Building: Nortech-1
Floor: 1st Floor

Test Can Take Several Minutes To
Complete



TROUBLESHOOTING GLOSSARY

Close window ✕

- 1) Check Hyperlocation calculation is enabled on CMX ▾
- 2) Check Hyperlocation enabled on wireless LAN controller ▾
- 3) Check wireless LAN controller AP radios are installed properly ▾
- 4) Check wireless LAN controller AP radios are operating properly ▾
- 5) Check wireless LAN controller added to CMX ▾
- 6) Check NMSP connection on wireless LAN controller ▾
- 7) Check NTP configuration on CMX ▾
- 8) Check NTP configuration on wireless LAN controller ▾
- 9) Check AP has correct time configuration ▾
- 10) Check CMX and wireless LAN controller time difference ▾
- 11) Check map has Hyperlocation APs ▾
- 12) Check for missing Hyperlocation APs ▾

Step 5 Observe a sample test result. The Test Type indicates which deployment component is being tested, and it can be CMX, WLC, or AP.

Test No	Test Type	Test Name	Results	Actions
1)	CMX	Check Hyperlocation calculation is enabled on CMX	Passed ▾	
2)	WLC	Check Hyperlocation enabled on wireless LAN controller	Passed ▾	
3)	WLC	Check wireless LAN controller AP radios are installed properly	Failed ▾	Fix Issue
4)	WLC	Check wireless LAN controller AP radios are operating properly	Passed ▾	
5)	CMX	Check wireless LAN controller added to CMX	Passed ▾	
6)	WLC	Check NMSP connection on wireless LAN controller	Passed ▾	
7)	CMX	Check NTP configuration on CMX	Failed ▾	Fix Issue
8)	WLC	Check NTP configuration on wireless LAN controller	Passed ▾	
9)	AP	Check AP has correct time configuration	Passed ▾	
10)	WLC	Check CMX and wireless LAN controller time difference	Passed ▾	

Step 6 If a test has failed, click **Fix Issue** for instructions on how to resolve the issue.

Close window ▾

Test: Check wireless LAN controller AP radios are installed properly

Test Description:
Check wireless LAN controller AP radios are installed properly

How to fix this issue:

1. Restart the access point
2. Restart the NMSPLB service

Step 7 Expand a passed test result to see further details of the test.

1)	CMX	Check Hyperlocation calculation is enabled on CMX	Passed
2)	WLC	Check Hyperlocation enabled on wireless LAN controller	Passed
<p>Hyperlocation is enabled on the wireless LAN controller</p> <pre> show advanced hyperlocation summary Hyperlocation..... UP Hyperlocation NTP Server..... 10.22.243.24 Hyperlocation pak-rssi Threshold..... -90 Hyperlocation pak-rssi Trigger-Threshold..... 3 Hyperlocation pak-rssi Reset-Threshold..... 1 Hyperlocation pak-rssi Timeout..... 3 AP Name Ethernet MAC Slots Hyperlocation ----- CMX-AP02-6509.8990 3c:08:f6:d9:08:a0 3 UP CMX-AP06-6193.96e4 b8:38:61:a8:ba:a0 3 UP CMX-AP01-6193.9720 b8:38:61:a8:bc:60 3 UP CMX-AP04-61a6.84ac b8:38:61:b1:c8:d0 3 UP CMX-AP05-61af.42c4 b8:38:61:b4:53:60 3 UP CMX-AP03-61af.42cc b8:38:61:b4:53:70 3 UP </pre>			
3)	WLC	Check wireless LAN controller AP radios are installed properly	Failed Fix Issue


Step 8 If the **Check AoA messages increasing for access points** test has failed, expand the test.

This may happen if there aren't clients to communicate with the access point, and hence the message count does not increase.

1)	CMX	Check Hyperlocation calculation is enabled on CMX	Passed
2)	WLC	Check Hyperlocation enabled on wireless LAN controller	Passed
<p>Hyperlocation is enabled on the wireless LAN controller</p> <pre> show advanced hyperlocation summary Hyperlocation..... UP Hyperlocation NTP Server..... 10.22.243.24 Hyperlocation pak-rssi Threshold..... -90 Hyperlocation pak-rssi Trigger-Threshold..... 3 Hyperlocation pak-rssi Reset-Threshold..... 1 Hyperlocation pak-rssi Timeout..... 3 AP Name Ethernet MAC Slots Hyperlocation ----- CMX-AP02-6509.8990 3c:08:f6:d9:08:a0 3 UP CMX-AP06-6193.96e4 b8:38:61:a8:ba:a0 3 UP CMX-AP01-6193.9720 b8:38:61:a8:bc:60 3 UP CMX-AP04-61a6.84ac b8:38:61:b1:c8:d0 3 UP CMX-AP05-61af.42c4 b8:38:61:b4:53:60 3 UP CMX-AP03-61af.42cc b8:38:61:b4:53:70 3 UP </pre>			
3)	WLC	Check wireless LAN controller AP radios are installed properly	Failed Fix Issue

a) Expand the test for a further look, and ensure that there is a significant difference for the first and second reading for access points that are connected to clients.

18)	CMX	Check AoA messages are increasing for access points	Passed																												
<p>All access points have increasing AoA messages</p> <table border="1"> <thead> <tr> <th>AP Name</th> <th>AP MAC</th> <th>AP IP</th> <th>Result</th> </tr> </thead> <tbody> <tr> <td>CMX-AP01-6193.9720</td> <td>b8:38:61:a8:bc:60</td> <td>10.22.243.128</td> <td>Message count is increasing</td> </tr> <tr> <td>CMX-AP02-6509.8990</td> <td>3c:08:f6:d9:08:a0</td> <td>10.22.243.164</td> <td>Message count is increasing</td> </tr> <tr> <td>CMX-AP03-61af.42cc</td> <td>b8:38:61:b4:53:70</td> <td>10.22.243.113</td> <td>Message count is increasing</td> </tr> <tr> <td>CMX-AP04-61a6.84ac</td> <td>b8:38:61:b1:c8:d0</td> <td>10.22.243.123</td> <td>Message count is increasing</td> </tr> <tr> <td>CMX-AP05-61af.42c4</td> <td>b8:38:61:b4:53:60</td> <td>10.22.243.141</td> <td>Message count is increasing</td> </tr> <tr> <td>CMX-AP06-6193.96e4</td> <td>b8:38:61:a8:ba:a0</td> <td>10.22.243.126</td> <td>Message count is increasing</td> </tr> </tbody> </table> <p>Message count for AP-CMX-AP01-6193.9720</p> <pre> Message count for first reading 1700336 Message count after 10 second interval 1700348 </pre> <p>Message count for AP-CMX-AP02-6509.8990</p> <pre> Message count for first reading 1706098 Message count after 10 second interval 1706110 </pre> <p>Message count for AP-CMX-AP03-61af.42cc</p>				AP Name	AP MAC	AP IP	Result	CMX-AP01-6193.9720	b8:38:61:a8:bc:60	10.22.243.128	Message count is increasing	CMX-AP02-6509.8990	3c:08:f6:d9:08:a0	10.22.243.164	Message count is increasing	CMX-AP03-61af.42cc	b8:38:61:b4:53:70	10.22.243.113	Message count is increasing	CMX-AP04-61a6.84ac	b8:38:61:b1:c8:d0	10.22.243.123	Message count is increasing	CMX-AP05-61af.42c4	b8:38:61:b4:53:60	10.22.243.141	Message count is increasing	CMX-AP06-6193.96e4	b8:38:61:a8:ba:a0	10.22.243.126	Message count is increasing
AP Name	AP MAC	AP IP	Result																												
CMX-AP01-6193.9720	b8:38:61:a8:bc:60	10.22.243.128	Message count is increasing																												
CMX-AP02-6509.8990	3c:08:f6:d9:08:a0	10.22.243.164	Message count is increasing																												
CMX-AP03-61af.42cc	b8:38:61:b4:53:70	10.22.243.113	Message count is increasing																												
CMX-AP04-61a6.84ac	b8:38:61:b1:c8:d0	10.22.243.123	Message count is increasing																												
CMX-AP05-61af.42c4	b8:38:61:b4:53:60	10.22.243.141	Message count is increasing																												
CMX-AP06-6193.96e4	b8:38:61:a8:ba:a0	10.22.243.126	Message count is increasing																												

3) WLC Check wireless LAN controller AP radios are installed properly Indeterminate  [Fix Issue](#)

Wireless LAN controller credentials were not provided. The test can be run manually.

1. On the wireless controller run the command 'show ap module summary all'
2. Check each Hyperlocation access point for the module 'Hyperlocation Module w/Antenna'

If you haven't provided the optional controller and access point details, the corresponding tests will not be executed, and the result is marked INDETERMINATE for your reference.

Configure Hyperlocation Groupings

The Hyperlocation deployment calculates location in the following manner. During the time period of a slot, the respective master emits bar packets. Bar responses are sent by client devices in the vicinity. The slaves access point listen to these response packets. The master and slaves then use the collected information to calculate the location of a client, as a collective activity. This process is repeated, with the master and slaves of the next slot. If a floor is too large, there maybe more than one masters. The master and slaves form groups, and a floor may have more than one such group.



Procedure

Step 1 Open the CMX Dashboard, **Detect and Locate>Troubleshooting**. As this is a floor-level test, select a building and floor. Note that only floors with hyperlocation access points are populated here.

Step 2 Click **View Hyperlocation Groupings** to configure a different master for a slot.


Note You can observe that each slot has an allocated time which is listed below the slot. There are also two frequency bands, 2.4 and 5 GHz, each with scan times. Scan time is the total time allocated to scan every slot of a band at least once. Since there are two such bands, 2.4 and 5 GHz, the total Refresh time is the sum of these two, and is the time taken to scan all slots of all bands.

Location (Please select building & floor)

Nortech-1[6]  1st Floor [6 APs] 


Please Provide Controller Credentials:

Credentials are optional. Tests requiring credentials will be skipped if not provided.
 Controller IP: 10.22.243.56
(Credentials are not saved and only used during diagnostics)

username password SSH  [Verify Credentials](#)

Please Provide Access Point Credentials:

(These credentials will be applicable for all APs of the floor)

username password SSH  [Verify Credentials](#)

Run Diagnostics
View Hyperlocation Groupings

Step 3 Click a frequency band, and select a slot. You can observe the master access point for the site marked by M, and the slaves marked by S. You can also change the master to a more appropriate one in this page.

The screenshot displays the 'HYPERLOCATION GROUPINGS' interface. At the top, there are tabs for '2.4 GHz' (Scan Time: 1.5s) and '5 GHz' (Scan Time: 1.5s). Below these are seven 'Slot' tabs: Slot 1 (250ms), Slot 2 (250ms), Slot 3 (250ms), Slot 4 (250ms), Slot 5 (250ms), and Slot 6 (250ms). A 'Refresh All' button with a 3s timer is located below the slot tabs. The interface is divided into two main sections: 'Master:' and 'Slaves:'. The 'Master:' section shows details for access point 'M', including its MAC Address (b8:38:61:b4:53:60), Name (CMX-AP05-61af.42c4), Scan Slot (1), Bandwidth (3), Channel (6), Client Count (2), and Refresh Time (3s). The 'Slaves:' section lists three slave access points: S2 (MAC: b8:38:61:a8:bc:60, Name: CMX-AP01-6193.9720, AP Distance: 59.31 FEET), S3 (MAC: b8:38:61:b4:53:70, Name: CMX-AP03-61af.42cc), and S4. To the right of the text is a floor plan diagram with orange circles representing access points: 'M' (Master) in the bottom left, 'S2' in the bottom right, 'S3' in the center, 'S4' in the top right, and 'S6' in the top left.

Step 4 Observe details of the master access point of a slot, like bandwidth, channel and client count.

HYPERLOCATION GROUPINGS

2.4 GHz 5 GHz Slot 1 Slot 2 Slot 3 Slot 4 Slot 5 Slot 6

Scan Time 1.5s Scan Time 1.5s 250ms 250ms 250ms 250ms 250ms 250ms

Refresh All 3s

Master:

M

MAC Address b8:38:61:b4:53:70
 Name CMX-AP03-61af.42cc
 Scan Slot 4
 Bandwidth 3
 Channel 1
 Client Count 0
 Refresh Time 3s

Slaves:

S1

MAC Address b8:38:61:b4:53:60
 Name CMX-AP05-61af.42c4
 AP Distance 41.02 FEET

S2

MAC Address b8:38:61:a8:bc:60
 Name CMX-AP01-6193.9720

Step 5 Observe the distance of a slave AP from the respective master.

HYPERLOCATION GROUPINGS

2.4 GHz 5 GHz Slot 1 Slot 2 Slot 3 Slot 4 Slot 5 Slot 6

Scan Time 1.5s Scan Time 1.5s 250ms 250ms 250ms 250ms 250ms 250ms

Refresh All 3s

Master:

M

MAC Address b8:38:61:b4:53:70
 Name CMX-AP03-61af.42cc
 Scan Slot 4
 Bandwidth 3
 Channel 1
 Client Count 0
 Refresh Time 3s

Slaves:

S1

MAC Address b8:38:61:b4:53:60
 Name CMX-AP05-61af.42c4
AP Distance 41.02 FEET

S2

MAC Address b8:38:61:a8:bc:60
 Name CMX-AP01-6193.9720

- Step 6** Observe that each slot has an allocated time which is listed below the slot. There are also two frequency bands, 2.4 and 5 GHz, each with scan times. Scan time is the total time allocated to scan every slot of a band at least once. Since there are two such bands, 2.4 and 5 GHz, the total Refresh time is the sum of these two, and is the time taken to scan all slots of all bands.

The screenshot displays the Cisco CMX interface. At the top, it shows 'Client Count 0' and 'Refresh Time 3s'. Below this, there are tabs for Slot 1 through Slot 6, each with a '250ms' value. A red box highlights the 'Slaves:' section for Slot 2, which lists six clients (S1 through S6) with their respective MAC addresses, names, and AP distances. To the right of this list is a floor plan diagram with six red circular markers labeled S1 through S6, corresponding to the clients listed. A mouse cursor is visible over the S5 marker on the floor plan.

Client	MAC Address	Name	AP Distance
S1	b8:38:61:b4:53:60	CMX-AP05-61af.42c4	59.31 FEET
S3	b8:38:61:b4:53:70	CMX-AP03-61af.42cc	29.47 FEET
S4	3c:08:f6:d9:08:a0	CMX-AP02-6509.8990	39.00 FEET
S5	b8:38:61:b1:c8:d0	CMX-AP04-61a6.84ac	44.98 FEET
S6	b8:38:61:a8:ba:a0	CMX-AP06-6193.96e4	71.36 FEET

Controlling the Probing Client Expiry Time

Probing clients count is usually more visible on CMX than compared to Wireless LAN Controller (WLC). WLC tracks the clients until the client no longer probes for more than five minutes, whereas CMX maintains the probing client for 10 minutes.

Connected Clients do not have this behavior because, WLC notifies CMX when the clients are disconnected from the network. You can perform additional configuration changes on CMX, if you want to minimize the probing client count on CMX.



Caution

We do not recommend to set the value less than five minutes because some clients may not send probe and in that case CMX will lose such clients. This configuration change could also increase the Analytics service processing time.

Procedure

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

Step 2 Click **DETECT & LOCATE**.

Step 3 Choose **SYSTEM > Settings > Filtering**.

Step 4 Specify the **RSSI Cutoff** value as **-75**.

Note Setting the RSSI cutoff to **-75** affects the probing clients only. This allows Cisco CMX to filter out weak probing clients in the initial stage.

Step 5 Navigate to **/opt/cmx/etc/** and open the **node.conf** file.

Step 6 To set the expiry time, at the end of the Location Services section, add **user_options=-Dredis_ttl=5**.

Note Cisco CMX maintains the default age out for clients as 10 minutes and when the client leaves the network, CMX usually takes 10 to 15 minutes to clean up the stale client details. If you set the age out to five minutes, Cisco CMX will perform the clean up in five to 10 minutes. Together, the RSSI cutoff and age-out settings, help Cisco CMX to narrow down the probing client count with respect to the WLC count.

Step 7 To restart the CMX agent, run the command **cmxctl agent restart**.

Step 8 To restart the Location Services, run the command **cmxctl location restart**.

Measuring Client Location Accuracy Using the Location Accuracy Test

From Cisco CMX 10.2, you can perform a location accuracy test for a single device with multiple location points. You can use the Location Accuracy Test tool to validate the placement and number of access points to ensure that the CMX deployment is giving the best location accuracy experience. The Location Accuracy tool provides an administrator the ability to quantify the location accuracy for a specific location by using a Wi-Fi device to measure the difference between the actual and calculated location of a device

To run a location accuracy test, perform the following task:

Procedure

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

Step 2 Click **DETECT & LOCATE**.

Step 3 Using the left pane of the **Activity Map** window, navigate to the desired building and floor.

Step 4 Use the search option on the **Activity Map** window to search for a device, for example, Client, RFID Tag, or BLE Tag. In this task, we will choose a client.


Step 5 Click the corresponding connected client, indicated by a green dot.



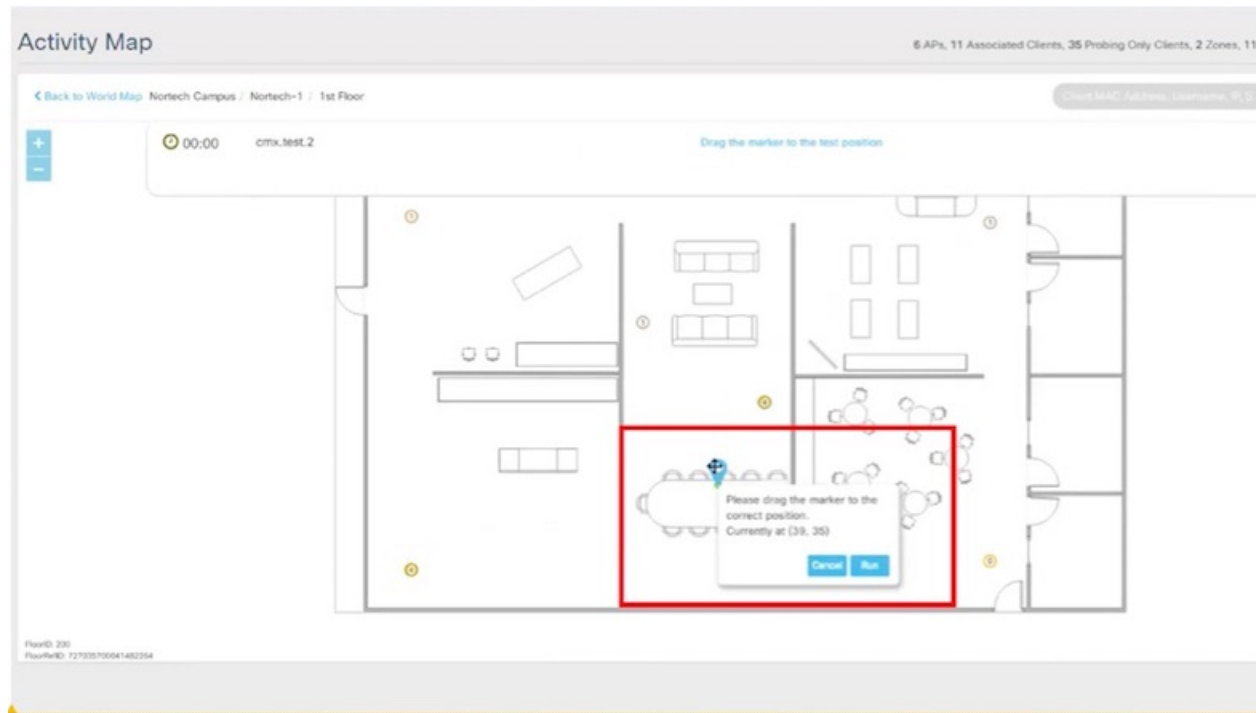
The **Client** dialog box is displayed.

Step 6 Click the **LOCATION ACCURACY TEST**  icon to start the location accuracy test.

Step 7 In the **Enter a test name** text box, type a name for the location accuracy test, and then press the **Enter**.

A dialog box, asking you to place the  marker at the client device's actual position on the map, is displayed.

Step 8 Drag the marker to the correct position.



Step 9 Click **Run**.

Observe the increasing samples. This indicates the number of times the client is detected at the pin-pointed location. You can run the test for any required amount of time. The elapsed time of the test is displayed.



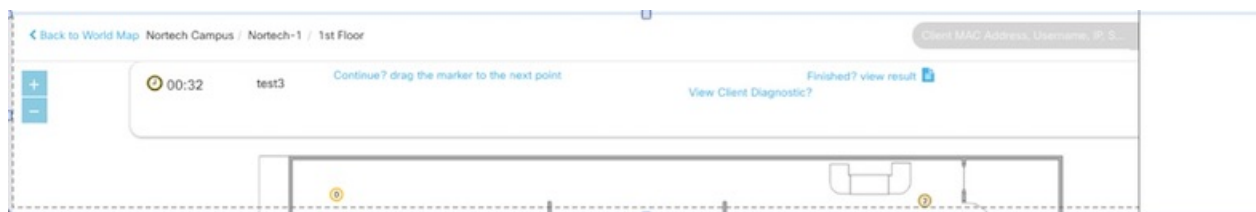
Step 10 Refresh your client frequently so that it exchanges information with the access points around it.

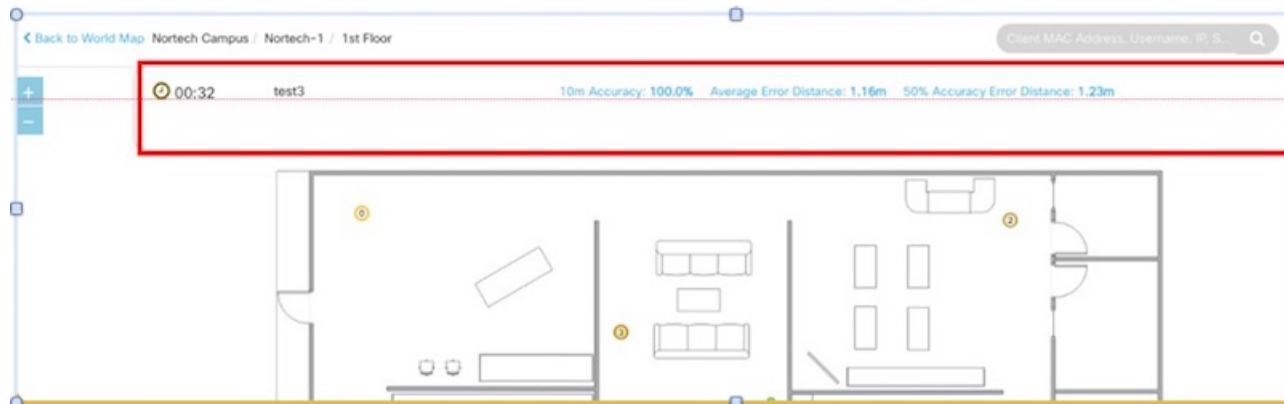
Step 11 Click **Pause** when you finish testing of the current location.


You can move your device to another location and continue testing (repeat Step 8 through Step 10). Wait for 30 seconds before resuming the test at a new spot, to eliminate any movement related discrepancies in the test result. Try to collect at least twenty samples at each spot, running the test at a spot for around five minutes.

Step 12 After you complete testing all the location points, click **Finished? View Result** to fetch the test results.

A dialog box, showing 10 m accuracy and Average Error Distance is displayed.



**Step 13**

Click **View accuracy test report**  icon on the top-right corner of the window to view the list of accuracy tests that you performed. This report enables you to restart a test, download the latest log or all logs, or email the test results.

The Location Accuracy Test window is displayed with the test details such as test name, status, MAC address, floor, start time, location computation frequency, measurements on correct floor (in percentage), accuracy and error distance. Click **Export All** to export the test results as CSV files.

Status	Mac Address	Floor	Start Time	Location Computation Frequency (s)	Measurements on Correct Floor (%)	10m Accuracy (%)	Average Error Distance (m)	90% Error Distance (m)
amel	f0:db:f8:4c:04:d9	Nortech Campus > Nortech-1 > 1st Floor	2017-07-26 01:43pm	0.0	100	0.0	0.00	0.00
Harvey Test 1	b8:e9:37:3c:69:d8	Nortech Campus > Nortech-1 > 1st Floor	2017-07-14 05:11am	5.6	100	100.0	0.49	1.37

Note Even when the test is in progress, you can click **View accuracy test report** to monitor all the tests. You can pause a running test by clicking **Pause**. You can continue a paused test by clicking **Relaunch**. To finish the test and get the results, click the **Report** icon.

To remove a report from the test report table, click **Delete**.

The Location Accuracy Test window is displayed. You can view all the previous test results in this window, not restricted to the selected floor, but includes all test runs. You also can download the log files, email the test results, and delete the tests.

Step 14

Analyze the test results.

What to do next

You can also perform the Location Accuracy Test using the Cisco CMX mobile application. The Cisco CMX mobile application complements the Cisco CMX product by providing a set of monitoring and testing tools for CMX deployments. The application enables users to monitor the status of CMX, monitor the number of

devices being tracked, receive alerts, test the location accuracy of the deployment, and test the latency of location updates. For more information, see <https://blogs.cisco.com/wireless/introducing-the-cisco-cmx-mobile-app-for-deployment-administrators>.

Analyzing Location Accuracy Results

Observe the test results in the figure below.



The test results displayed indicate that for 100% of the time, Cisco CMX locates the client within this many meters from where the client is actually located.

It also indicates that for 50% of the time, Cisco CMX locates the client within this many meters from where the client is actually located. A good location accuracy test result for an RSSI deployment is 10 meters, and 4 to 5 meters for FastLocate.

Observe the complete location-accuracy test below:

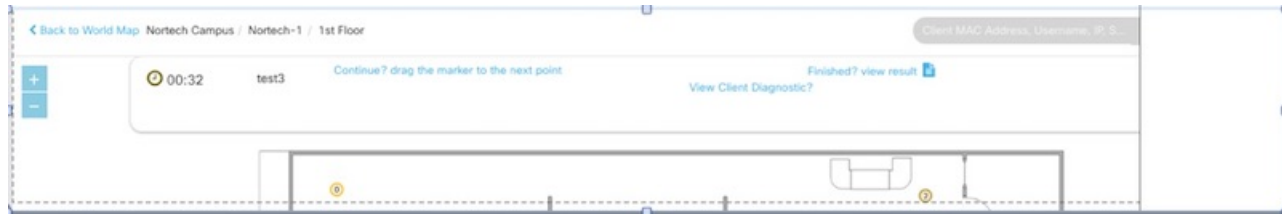
The screenshot shows a 'Location Accuracy Test' table. A 'Download options' dialog box is open, showing 'Latest' and 'All' buttons. The table has columns for Status, Mac Address, Floor, Start Time, Location Computation Frequency (s), Measurements on Correct Floor (%), 10m Accuracy (%), Average Error Distance (m), 90% Error Distance (m), 75% Error Distance (m), and 50% Error Distance (m). The first two rows are highlighted with a red box.

Status	Mac Address	Floor	Start Time	Location Computation Frequency (s)	Measurements on Correct Floor (%)	10m Accuracy (%)	Average Error Distance (m)	90% Error Distance (m)	75% Error Distance (m)	50% Error Distance (m)
amel	finished	f0:db:f8:4c:04:d9	Nortech Campus > Nortech-1 > 1st Floor	2017-07-26 01:43pm	0.0	100	0.0	0.00	0.00	0.00
Harvey Test 1	finished	b8:e9:37:3c:69:d8	Nortech Campus > Nortech-1 > 1st Floor	2017-07-14 05:11am	5.6	100	100.0	0.49	1.37	0.79

Ensure that **Measurements on Correct Floor** should be at 100%. This is an indicator of whether the client has been detected by the access points on the same floor, and not on a different floor. You can delete the test and the corresponding log files using the cross buttons here.

Understanding Client Diagnostics

Client diagnostics is a way to understand whether the tested client is sending messages to Cisco CMX for location-accuracy calculations. You can view Client Diagnostics during the location accuracy test.



Below is a sample test report.

Client Diagnostics			
Sr. No.	Test Description	Test Status	Actions
1.	Validate required location services are up.	Passed ▾	Details
2.	Check client history	Passed ▾	Details
3.	Check NMSP connection on CMX	Passed ▾	Details
4.	Check NTP configuration on CMX	Failed ▾	Details
5.	Check AoA messages are increasing for access points	Passed ▾	Details
6.	Check RSSI messages are increasing for access points	Failed ▾	Details
7.	Check nmsplb container, if it is receiving any data.	Passed ▾	Details
8.	Check for a client measurement.	Passed ▾	Details
9.	Check client location update.	Passed ▾	Details
10.	Validate connected AP.	Passed ▾	Details
11.	Check nearest detecting AP using last measurement.	Failed ▾	Details

It is best to ensure that all the tests here are in Passed status.

You can also email a summary of the messages to your Technical Support department for troubleshooting. Given below are some of the outputs of individual tests.

Figure 2: Sample Output: Check Client History

2. Check client history Passed ▾ Details

Client history for mac b8:e9:37:3c:69:d8 is available			
Time	Floor	X	Y
Jul 26,2017 15:20:23	Nortech Campus>Nortech- 1>1st Floor	49.130493	24.434755
Jul 26,2017 15:15:37	Nortech Campus>Nortech- 1>1st Floor	50.016193	23.615622
Jul 26,2017 15:14:54	Nortech Campus>Nortech- 1>1st Floor	52.579765	23.963598

Figure 3: Sample Output: Check Heatmaps are generated

14. Check Heatmaps are generated. Passed ▾ Details

Heatmaps are generated properly.		
AP MAC	Interface	Status
b8:38:61:a8:bc:60	IEEE_802_11_A	Pass
b8:38:61:a8:bc:60	IEEE_802_11_B	Pass
b8:38:61:a8:bc:60	IEEE_802_11_A	Pass
b8:38:61:a8:bc:60	IEEE_802_11_B	Pass
3c:08:f6:d9:08:a0	IEEE_802_11_B	Pass
3c:08:f6:d9:08:a0	IEEE_802_11_A	Pass
3c:08:f6:d9:08:a0	IEEE_802_11_B	Pass
3c:08:f6:d9:08:a0	IEEE_802_11_A	Pass
b8:38:61:b4:53:70	IEEE_802_11_A	Pass

Figure 4: Sample Output: Reasons for location failure

15. Reasons for location failure. Passed ▾ [Details](#)

No failuers messages found.	
Message	Value
Loc failed due to empty rssi list after failing to find corresponding AP	0
Loc failed due to empty RSSI lists	0
Loc failed due to empty rssi list after prune by time	0
Loc failed due to empty heatmap list afterpick floor	0
Loc failed due to empty rssi list after prune by value	0
Loc failed due to filtered APs	0
Loc failed due to pickFloor error	0
NOTE - Counts are cleared at	midnight
Loc failed due to invalid float value computation result	0
Loc failed due to empty heatmap list after prunerssi by time	0
Loc failed due to insufficient rssi measurements	0

Analyzing Location Accuracy Log Files

This task analyzes the Location Accuracy log files stored in `/opt/cmx/srv/location/accuracy`.

Procedure

- Step 1** Telnet into the CMX box and navigate to the `/opt/cmx/srv/location/accuracy` directory where location accuracy results are stored by default.


```

10.22.243.125 - cmxadmin@cmx-nortech:/opt/cmx/srv/loc...
File Edit Setup Control Window Help
[cmxadmin@cmx-nortech accuracy]$
[cmxadmin@cmx-nortech accuracy]$
[cmxadmin@cmx-nortech accuracy]$
[cmxadmin@cmx-nortech accuracy]$
[cmxadmin@cmx-nortech accuracy]$ ls
cmx.test.1 cmx.test.2 cmx.test.2-1499453064063 jun20-1
[cmxadmin@cmx-nortech accuracy]$ pwd
/opt/cmx/srv/location/accuracy
[cmxadmin@cmx-nortech accuracy]$

```

Step 2 Navigate to the folder named after your test.

```

10.22.243.125 - cmxadmin@cmx-nortech:/opt/cmx/srv/loc...
File Edit Setup Control Window Help
[cmxadmin@cmx-nortech accuracy]$ ls
cmx.test.1 cmx.test.2 cmx.test.2-1499453064063 jun20-1
[cmxadmin@cmx-nortech accuracy]$ pwd
/opt/cmx/srv/location/accuracy
[cmxadmin@cmx-nortech accuracy]$ cd cmx.test.2
[cmxadmin@cmx-nortech cmx.test.2]$ ls
aaaCoarseLocationProbability08:74:02:02:d7:ef.txt
aaaCoarseXyInfFtThThatBIn08:74:02:02:d7:ef.txt
aaaUnscaledHeatmapStore08:74:02:02:d7:ef.txt
clientDiag-08:74:02:02:d7:ef.txt
clientsFloor-08:74:02:02:d7:ef.txt
combinedLocationProbability08:74:02:02:d7:ef.txt
combinedXyInfFtThThatBIn08:74:02:02:d7:ef.txt
correlation08:74:02:02:d7:ef.txt
hyperlocationGroups-08:74:02:02:d7:ef.txt
locationSetup-08:74:02:02:d7:ef.txt
logs
mapInfo-08:74:02:02:d7:ef.txt
rsseLocationProbability08:74:02:02:d7:ef.txt
scaledHeatmapStore08:74:02:02:d7:ef.txt
[cmxadmin@cmx-nortech cmx.test.2]$ cd logs
[cmxadmin@cmx-nortech logs]$ ls
rf-08-74-02-02-d7-ef.log.temp
[cmxadmin@cmx-nortech logs]$

```

Step 3 Navigate into the logs folder, where the log files are stored.

- A good location accuracy result for a hyperlocation deployment has an Average Error Distance of around one meter.
- Convex hull is the perimeter formed by drawing lines connecting 3 or more APs in a AP group. Ensure that a test client is within the convex hull of an AP group.
- Do not choose a client that is in a spot between AP groups, or outside the convex hull of AP groups.
- You can use the Location Accuracy test to calculate latency in a Hyperlocation deployment. This is especially useful if you would like to know when clients visit your store in order to send personnel to greet them. You can find the latency by moving a test client, and observing how many seconds it takes for your Cisco CMX location accuracy dashboard to update itself with the new client location. Usually, it takes around 2-3 seconds to update its location. Ideally, latency should not be more than 5 seconds for a hyperlocation deployment.



CHAPTER 3

The Cisco CMX Analytics Service

- [Overview of the Analytics Service, on page 49](#)
- [The Analytics Dashboard, on page 49](#)
- [Customized Widgets, on page 61](#)
- [Create a Realtime Report, on page 67](#)
- [Performing Heatmap Analysis, on page 68](#)
- [Using the Schedule Manager, on page 69](#)
- [Verticalization, on page 69](#)
- [Set SSID Filter Parameters for Analytics Service, on page 69](#)

Overview of the Analytics Service

The Cisco Connected Mobile Experiences (Cisco CMX) Analytics service provides a set of data analytic tools for analyzing Wi-Fi device locations. The Analytics service helps organizations use the network as a data source to view visitors' behavior patterns and trends, which will in turn help businesses improve visitor experience and boost customer service.

The Analytics service enables you to:

- Analyze Wi-Fi device locations.
- Estimate the number of new visitors (visitors seen for the first time) and repeat visitors (recognized from an earlier visit), the amount of time they spend at a venue, and the frequency of their visits within a venue.
- Gain detailed insight into the behavior patterns of visitors moving and interacting within a venue.
- Analyze business performance by measuring the effect of in-venue marketing.
- Improve customer satisfaction through sufficient staffing during peak hours, proper signage, and making changes in underutilized areas.

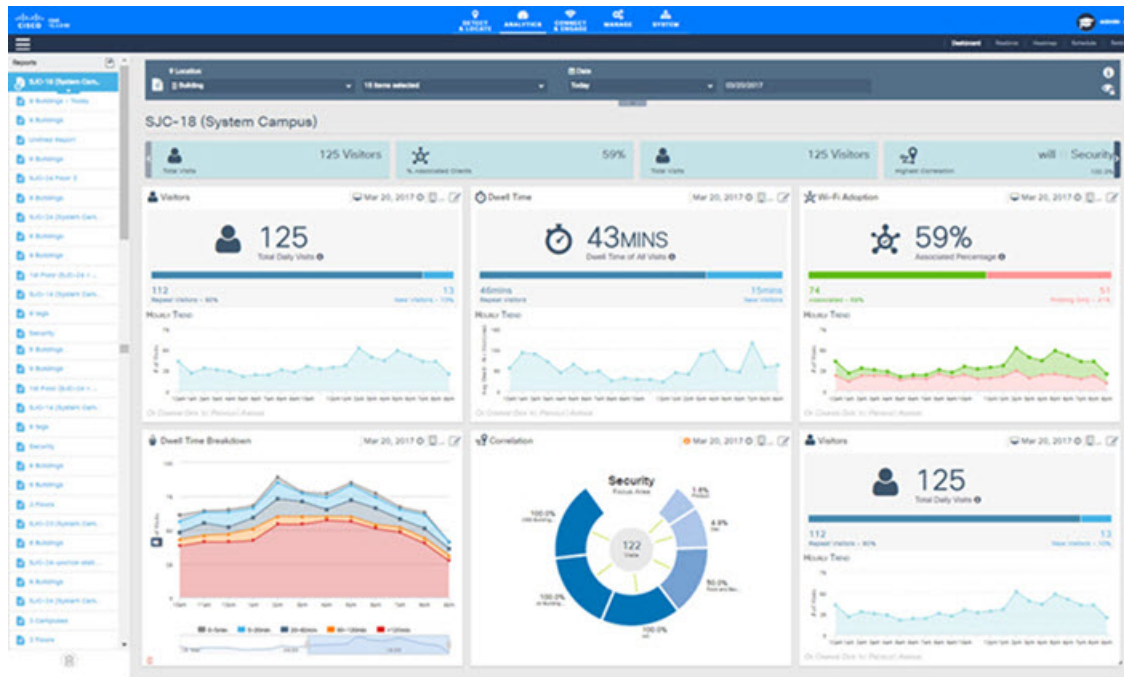
The Analytics Dashboard

The Analytics service's Dashboard is designed to help you visualize and understand various parameters associated with visitors' movement within a given zone. You can use the Dashboard on a daily basis to examine current trends or events. You can also customize the Dashboard with different widgets, as per your requirements.

Accessing the Analytics Dashboard

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
Step 2 Choose **Analytics > Dashboard**.



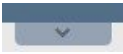
- Step 3** Using the left pane of the Dashboard, navigate to the desired report using the deployment hierarchy (heterarchy). The details pertaining to that report are displayed on the Dashboard.

Filtering the Data Displayed in the Analytics Dashboard

The data displayed in the Dashboard is filtered to include devices that are seen for more than 5 minutes and less than 8 hours.

To change the dwell time (the amount of time a visitor spends at a location):

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
Step 2 Choose **Analytics > Dashboard**.
Step 3 Click the Expander icon  below the **Location and Date** pane.

The **Edit Report** window is displayed. For more information, see [Edit a Report](#), on page 56.

- Step 4** Specify the **Dwell Threshold** values.
-

Viewing a Device Count and Average Dwell Time Report

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Choose **Analytics > Dashboard**.
- Step 3** Click the location you want to analyze, **Region, Building, Floor, Zone, or Tags**.
- Step 4** From the **Location** and **Date** pane, choose the timeframe for the report. The available options are:
- **Now**—The number of active devices in the last 15 minutes.
Note In Cisco CMX Release 10.2.3, the **Now** option in the **Date & Time Filters** drop-down list is no longer available.
 - **Today**—The report you specified is run for the current day and the generated results are displayed.
 - **Yesterday**—The report you specified is run using the previous day's values and the generated results are displayed.
 - **This Week**—The report you specified is run using the current week's values (Monday to Sunday) and the generated results are displayed.
 - **Last Week**—The report you specified is run using the previous week's values (Monday to Sunday) and the generated results are displayed.
 - **Last 2 Weeks**—The report you specified is run using past two weeks' values and the generated results are displayed.
 - **This Month**—The report you specified is run using this month's values and the generated results are displayed.
 - **Last Month**—The report you specified is run using the previous month's values and the generated results are displayed.
 - **Last 3 Months**—The report you specified is run using the past three months' values and the generated results are displayed.
 - **This Year**—The report you specified is run using this year's values and the generated results are displayed.
 - **Last Year**—The report you specified is run using the previous year's values and the generated results are displayed.
 - **Custom Range**—The report you specified is run using the date values you specified in the Start and End date fields.
- A report based on the chosen criteria is displayed in the Dashboard and contains the following widgets:
- Visitors widget

- In the Device Count report, information about the total number of visitors, along with percentage of repeat visitors and new visitors is displayed.
- In the Dwell Time report, the average dwell time of all the visitors, along with the dwell time of repeat and new visitors is displayed.
- Compared Data to widget—A comparative result of repeat visitors vs. new visitors is displayed. The available options are:
 - Previous
 - Average—The average value is calculated by averaging the current period and the previous period. If you select This Week in the Date pane, the previous to compared with is last week, and the average is over last week and this week.
- A line chart with a summary view and a detailed view of the criteria selected—You can customize the X-axis and Y-axis by applying the following filter criteria:
 - View Unique Devices or View Absolute Visits
 - Locations—Campus, Building, Floor, Zone, Zone Tag
 - Values—Ascending, Descending, Alphabetical

Analytics Reports

The Analytics Dashboard provides reports to understand and monitor the behavior pattern of visitors within a particular venue.

The Analytics service's report facility also provides a more regular and manager-oriented set of information through parameterized templates to measure various trends and patterns that occur over a period of time in a particular zone. You can create new reports as well as modify the existing reports. You can schedule a report at a customized frequency, print the reports, and download the reports in PDF, Excel, or HTML formats. You can either choose to auto-generate or customize a report.



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



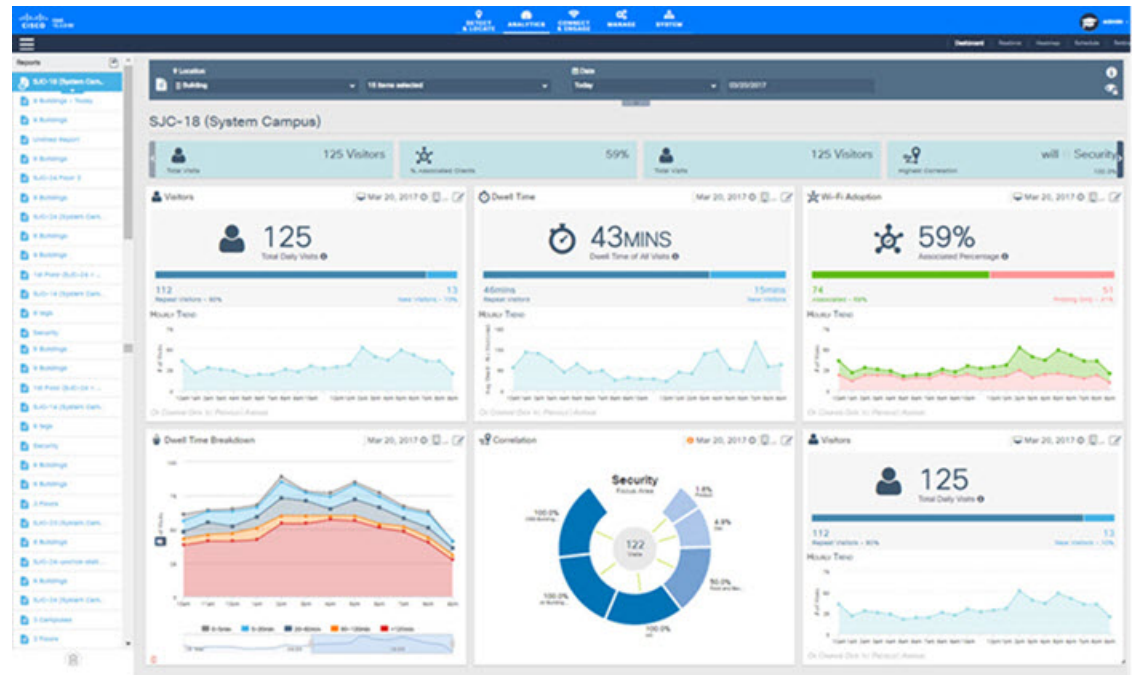
Note In Cisco CMX Release 10.2.2, reports where multiple zones and floors are selected can result in duplicate device counts when a device visits more than one zone or floor. So if a device visits zone 1 and zone 2, the device count is displayed as 2. However, this is not so in Cisco CMX Release 10.2. Hence a higher device count can be registered in a 10.2.2 report as opposed to 10.2.

A workaround for this is to tag multiple campus/building/floors/zone with the same TAG and create reports at the TAG level.

Creating and Managing Customized Reports

To create your own reports, pick the locations, date/time, and various widgets, and decide how they should be displayed in the Analytics Dashboard. Your reports will be listed in the left pane under **Reports**. Click a report name to view the corresponding details in the Dashboard.

Figure 5: Analytics Reports




Note 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.*




If there is no report present in the dashboard, the **Create New Report** window is automatically displayed.

The following is the list of custom report-related tasks that you can perform:

Create a Custom Report

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Choose **Analytics > Dashboard**.
- Step 3** In the left pane of the Dashboard, click  next to **Reports**. The **Create New Report** window is displayed.
- Step 4** To create a custom report, click **Customized** in the **Report Type** row in the right pane.

- Step 5** From the **Focus Area Filter** drop-down list, choose the locations that you want to analyze. The location types are **Building**, **Campus**, **Floor**, and **Zone**.
- Step 6** From the **Date & Time filters** drop-down list, choose the date and time range you want to run the report for.
- Step 7** In the Add Widgets  area, click **Add Widget to Report +** to include any of the following widgets to the report:
- **Visitors**—Shows the number of visitors detected in the network.
 - **Average Dwell Time**—Shows the amount of time visitors spent at a location.
 - **Correlation**—Shows the relationship between devices and visits between locations.
 - **Path**—Shows where visitors went before and after visiting a location.
 - **Wi-Fi Adoption**—Shows how many devices are connected to the Wi-Fi network.
 - **Dwell Time Breakdown**—Shows dwell-time distribution for selected areas, for example:
 - 20 percent of the visitors stayed less than an hour
 - 50 percent stayed for 1 to 2 hours
 - 30 percent stayed for more than 2 hours
- Note**
- The **Add Widget** is not available for the **Auto-Generate** report type.
 - For each widget in the report, you can click **Edit/View Options** to edit the display options. The options available are **Chart**, **Summary**, and **Table**. By default, the **Summary** option is selected.
- Step 8** From the **Advanced Widget Filter**  area, choose the devices that you want to filter in the report.
- Step 9** From the **Associated/Probing Devices** drop-down list, choose an option.
- Step 10** You can set a threshold for dwell time. This is the amount of time spent by a client device (visitor) at a given location. Select the minimum and maximum time from the corresponding drop-down lists in the **Dwell Threshold**  area.
- a) From the **Minutes To** drop-down list, choose the minimum time, in minutes.
 - b) From the **Hours** drop-down list, choose the maximum time, in hours.
 - c) Click **No Filters**, if filtering is not to be applied while generating the report. When you click this option, the dwell-time threshold values are automatically set in the range of 0 to 24.
 - d) Check the **Stationary Devices** check box if you want to include stationary devices while filtering.
- If stationary devices filtering must be included in the report, ensure that the dwell threshold maximum time is 24 hours. Stationary device filtering is only available for widgets with a count, such as **Visitors** and **Average Dwell Time**.
- Step 11** Click **Done**.
- Based on the **Focus Area and Date** filters that you specified, the report name is generated. The new report name is listed in the left pane under **Reports**.
- The following is a list of tasks that can be performed after a Custom report is created:
- Schedule a Report—To schedule a report:


1. Click the report for which you want to create a scheduled report.
2. Click the **Expander** icon that is displayed.
3. Click the **Clock** icon (Schedule) to schedule the report.
4. In the **SELECT REPORT OPTION** dialog box, choose **HTML**, **PDF**, or **Excel** and click **Next**.
 - **PDF Report**—Enables you to schedule a report in PDF format. You can customize the PDF report parameters.
 - In the **Header** text box, specify a Header for the PDF report.
 - Click **Select a Logo** to choose a logo for the PDF report. You can align the placement of the logo to left, center, or right.
 - If you want to provide comments, enter your comments in the **Add your comments here** field.
 - In the **Footer** field, specify a footer for the PDF report.
 - Enter the email address of the recipients to send the report to.
 - Enter the start date and time from which the report has to be generated.
 - Select the frequency of the report—**One Time**, **Daily**, or **Weekly**.
 - **Excel Report**—Enables you to schedule a report in excel format.
 - Enter the email address of the recipients to send the report to.
 - Enter the start date and time from which the report has to be generated.
 - Select the frequency of the report—**One Time**, **Daily**, or **Weekly**.
 - **HTML Report**—Enables you to schedule a report in HTML format.
 - Enter the email address of the recipients to send the report to.
 - Enter the start date and time from which the report has to be generated.
 - Select the frequency of the report—**One Time**, **Daily**, or **Weekly**.
5. Click **Schedule**.
 - **Print a Report**—To print a report:
 1. Click the report that you want to print.
 2. Click the **Expander** icon that is displayed.
 3. Click the **Print** icon to print the report.
 4. Click **Next**.
 - **View Scheduled Report Manager**—To view the scheduled reports, choose **Analytics > Schedule**. The **Scheduled Report Manager** page displays the following information:
 - **Report ID**—Shows the report ID.

- **Report Title**—Shows the report title.
- **Username**—Shows the name of the user who created the scheduled report.
- **Start From**—Shows the date and time from which the report is scheduled to run.
- **Recipients**—Shows the email addresses of recipients.
- **History**—Displays the history of the scheduled report.
- **Actions**—Modifies or deletes the scheduled report.

Edit a Report

You can use the **Edit Report** window to edit the report parameters and generate an updated report.

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Choose **Analytics > Dashboard**.
- Step 3** Click the Expander icon  below the **Location and Date** pane.
The window **Edit Report** window is displayed.
- Step 4** Edit the report parameters and then click **Done**.
The Dashboard window is refreshed and the updated report is displayed.

Create a Scheduled Custom Report

Besides creating customized reports, you can add a logo, text, header, and footer to a report to align it with your organization. The reports can be scheduled at a customized frequency for a targeted set of recipients.

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Choose **Analytics > Dashboard**.
- Step 3** In the left pane of the Dashboard, expand the report name, and click **Schedule**.
The **Select Report Option** dialog box is displayed. The following options are available:
- **HTML Report**
 - **PDF Report**
- Step 4** Click the radio button corresponding to the kind of report you require and click **Next**.

If you select the PDF option, the following customization options are available:

- **Header**—Add a header to the report and provide a name. You can customize the position of the header text by using the right, top, and left arrow keys.
- **Logo**—Add a logo to the report by clicking the **Logo** icon. A few default logos are available to choose from. You can also upload a logo by clicking **Upload a Logo**.
- **Comments**—Add comments about the report by entering the corresponding text in the **Add your comments Here** field. You can move the sections by clicking the **Up** or **Down** arrow keys on the left side of the different components present in the sections in the report.
- **Footer**—Add footer text at the bottom of the report.

- Step 5** Click **Next**.
The **Schedule Report** widget is displayed.
- Step 6** Enter the email addresses of the recipients to send the report to.
- Step 7** Enter the start date and time of the period for which the report has to be generated.
- Step 8** Select the frequency of the report, **One Time**, **Daily**, or **Weekly**.
- Step 9** Click **Schedule**.

Configure Custom Time Ranges for an Analytics Report

In Cisco CMX Analytics, the **Create New Report** window includes the date and time range option to select a specific period of time for creating Analytics reports. After creating or modifying these time ranges, you can proceed to select the corresponding range from the **Date and Time Filters** drop-down list, for example, Early Morning (12am -3:59am).

You can also modify the existing ranges or define custom time ranges for generating Analytics reports. You can configure the custom time using either the Cisco CMX GUI or CLI.

Add a New Time Range Using the Cisco CMX GUI

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Choose **Analytics > Settings**.
The **Analytics Settings** window is displayed with a list of the available time ranges.
- Step 3** To add a new custom time range, click **Add**.

The **Add Time Ranges** dialog box is displayed.

Step 4 In the **Annotation** field, enter a new name for the time range.

Step 5 Use the time range slide bar to pick a new time range.

Step 6 Click **Save**.

- Note**
- Any updates to the time range values will result in recomputation of the data.
 - The new time is displayed in the **Global TimeRanges** drop-down list.
 - By default, the interval time for a new time range is 15 minutes.

Add a New Time Range Using CLI

Procedure

Step 1 Log in to root through SSH.

Step 2 Use the CLI to edit the *analytics.params.json* file and change the time ranges. Optionally, you can use a third-party SFTP client to edit the file.

- Enter **cd /opt/cmx/etc/**
- Enter **vi analytics.params.json**

Step 3 (Optional) Delete all the older Analytics reports and reprocess the data with the new time ranges:

```
<USERNAME>:<PASSWORD> -X DELETE
"http://<IPADDRESS>:5556/api/analytics/v1/batch/daysProcessed/HistoricalVisitsJobProducer"
<USERNAME>:<PASSWORD> -X DELETE
http://<IPADDRESS>:5556/api/analytics/v1/batch/daysProcessed/TodayVisitsJobProducer
```

Step 4 To restart the Analytics services, use the **cmxctl analytics restart** command. This updates and displays all the new time ranges in the CMX UI. All the historical data will also be reprocessed using the new time ranges.

Note If the Analytics services are not restarted, only the unmodified time ranges will be available.

Download a Customized Report

You can use the Analytics service to download customized reports in PDF, Excel, or HTML formats.

Procedure

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

Step 2 Choose **Analytics > Dashboard**.

Step 3 In the left pane of the Dashboard, expand the corresponding report name, and click **Download**.

The **Select Report Option** dialog box is displayed. The following options are available:

- **PDF Report**
- **Excel Report**
- **HTML Report**

Step 4 Click the radio button corresponding to the format that you want the report to be downloaded in.

If you select the PDF option, the following customization options are available:

- **Header**—Add a header to the report and provide a name. You can customize the position of the header text by using the right, top, and left arrow keys.
- **Logo**—Add a logo to the report by clicking the **Select a Logo** icon. A few default logos are available to choose from. You can also upload a logo by clicking **Upload a Logo**.
- **Comments**—Add comments about the report by entering text in the **Add your comments** field. You can move the sections by clicking the **Up** or **Down** arrow keys on the left side of the different components present in the sections in the report.
- **Footer**—Add footer text at the bottom of the report.

If you select **Excel Report**, the data for all the Dashboard widgets will be exported as tables in the report. If you want to download reports with filtering options, choose the **Table** report option from the **Edit/View Options** for each widget.


Step 5 Click **Next**.

The customized reports are downloaded in the selected format.

Delete a Customized Report

You can delete any of the custom reports that you created.

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Choose **Analytics > Dashboard**.
- Step 3** In the left pane of the **Dashboard**, hover the cursor over a report, and click the **Delete**  icon.
-

Creating an Analytics Report Based on Associated or Probing Only Devices

You can create filtered analytics reports based on all visitor devices associated to the network (regardless of SSID) and on all visitor devices detected by the network. These are categorized as **Associated** and **Probing Only** devices. In addition, any devices filtered by the Location service is also excluded from analytics reports.

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 **Associated/Probing Only Devices** widget, select **Associated** or **Probing Only**, or select both.
- If both are selected, all associated and probing only 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 **Associated** option is selected, a green Wi-Fi icon appears next to the **Visitor Count** heading. The visitor count displayed is the number of devices associated to the SSID.
 - If the **Probing Only** option is selected, a gray Wi-Fi icon appears next to the **Visitor Count** heading. The visitor count displayed is the number of devices probing only by the SSID.
 - If both options are selected (meaning, no filtering), no icon appears.
-


Viewing Global Alerts for Critical Services

The Global Alerts window displays information for all Cisco CMX service. You can navigate to this window from the respective Cisco CMX service window.

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Choose **Analytics > Dashboard**.
- The **Dashboard** window is displayed.

Step 3

In the top-right corner of the window, click the **Alerts**  icon.

The **Live Alerts** window is displayed with the global alert details for critical and major alerts. For more information about alerts, see [Viewing Live System Alerts, on page 169](#).

Tip

For the Analytics service, Job Processor runs multiple jobs in the background. The Analytics service's Dashboard displays success alerts when the job processor completes all the jobs.

Customized Widgets

Customized widgets enable you to view and analyze specific activities to better suit the objective of your analysis. For example, you can create a widget that focuses on visitor (client) activity in a zone of interest. The customized widget will gather and present only the data pertaining to visitor activity, and enable the analysis and interpretation of this data. The information in the customized widgets enable you to take meaningful decisions based on client activity.



Note Customized widgets can be generated only by Advanced users.

The Visitors Widget

The Visitor widget provides a detailed summary of the visitor (client device) count in an area of focus.

The Visitor widget can be viewed in the following formats:

- **Summary**—This is the default view. This view consists of the **Visitors**, **Compare Data to**, and **Hourly Trend** charts. A breakup of new and repeat visitors is also provided. The **Compare Data to** chart presents comparative data for the current day and the previous day. You can also compare the current data with the average visitor count per day. A breakup distribution of repeat and new visitors is also shown as percentage. A graph shows the visitor count per hour from 12:00 a.m. to 12:00 p.m.
- **Chart**—A line chart with a summary view of the number of total visitors along the Y-axis and the activity at a given time of the day along the X-axis is displayed. You can configure the chart based on the following views:
 - **View Unique Devices or View Absolute Visits**
 - **Locations**—Campus, Building, Floor, Zone, By Hour
 - **Values**—Ascending, Descending, Alphabetical

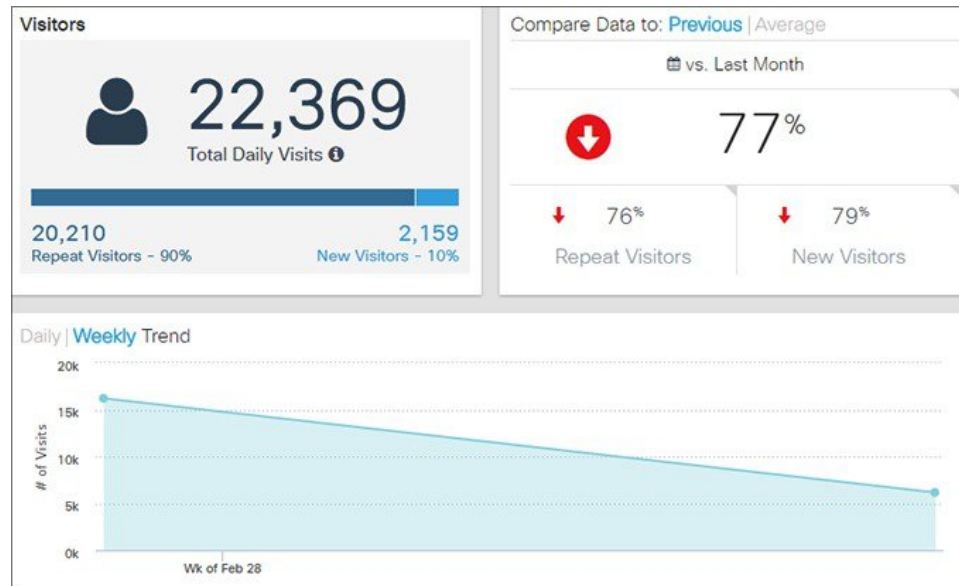
The Y-axis value provides alternate views of the number of visitors and percentage of total visitors. Hover your cursor at any point along the line to view the connected and probing data at that instance.

- **Table**—Visitor count attributes are presented in a tabular format.

The following trends are available for each view:

- **View Unique Devices**

- View Absolute Visits



The Dwell Time Widget

The Dwell Time widget presents detailed summary of the time spent by visitors (client devices) at a location.

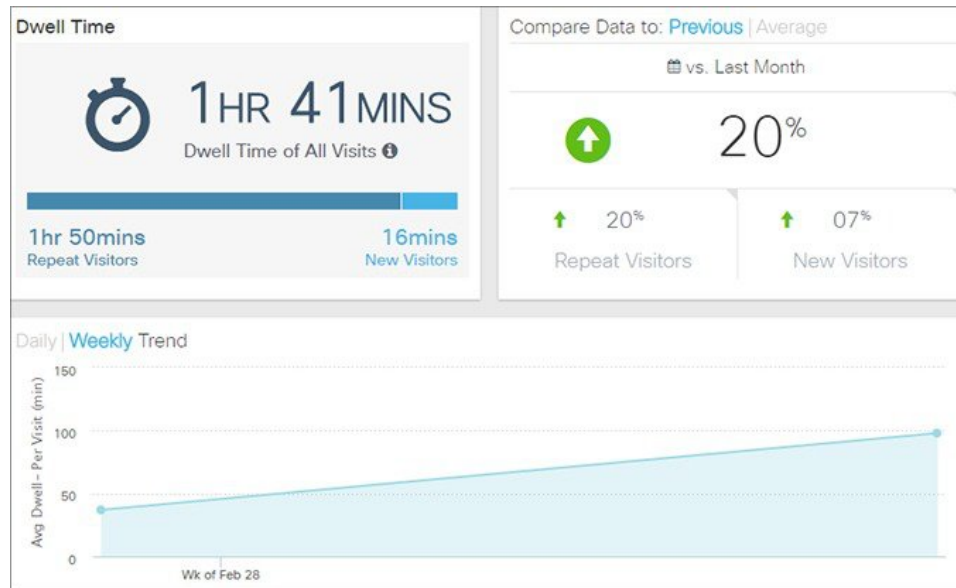
Average dwell time can be viewed in the following formats:

- **Summary**—This is the default view. The summary view consists of the **Average Dwell Time**, **Compare Data to**, and **Daily Trend** charts. A breakup of new and repeat visitors is also provided. The **Compare Data to** chart presents comparative data for the current day and the previous day. You can also compare the current data with the average visitor count per day. A breakup distribution of the repeat and new visitors is also shown as percentage. A graph shows the visitor count per hour from 12:00 a.m. to 12:00 p.m.
- **Chart**—A line chart with a summary view of the number of total visitors along the Y-axis and the activity at a given time of the day along the X-axis is displayed. You can configure the chart based on the following views:
- **Table**—Visitor count attributes are presented in a tabular format. You can view the following details:
 - Location
 - Parent Area(s)
 - Day
 - Time
 - Dwell Time

The following trends are available for each different view:

- View Unique Devices

- View Absolute Visits



The Correlation Widget



Note The Correlation widget of Cisco CMX 10.2 is referred to as Crossover widget in Cisco CMX Release 10.1.

The Correlation widget provides a detailed summary of correlation of client devices between two locations. Correlation data can be used to determine the relation between two zones. Low correlation between zones indicates lack of access between the two zones. For example, you can expect a high correlation between the food court and the cinema in a shopping mall. The Correlation widget can be viewed in the following formats:

- **Correlation**—Provides an interactive graphical representation of the correlation between zones. You can configure the correlation between zones by filtering according to the focus areas, building, or absolute versus unique devices.
- **Table**—The table format lists the data in a tabular format with the following columns:
 - **Area**—The zone around which correlation is configured.
 - **Grouping**—The focus area for which the correlation data is collected.
 - **Correlation**—The correlation data, in percentage, between the zone (Area column) and the focus area.

The following trends are available for each view:

- View Unique Devices
- View Absolute Visits

The Path Analysis Widget

The Path Analysis widget analyses the paths taken by visitors (or client devices) before and after visiting a focus location, and provides a graphical representation of the paths.

- 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 reveals a breakdown based on:

- Percentage of paths that either started or ended in the focus zone.
- Percentage of paths that either arrived or departed from the focus zone.

Hovering your cursor over a green section shows the number of paths that entered the focus zone originated in this zone.

Hovering your cursor over a blue section shows the number of paths that originated in the focus zone ended in this zone.



Note All paths are calculated based on the overall data set defined, but only the top 15 (by percentage) paths can be displayed in the widget due to space constraints.

In a generated report with **Path Analysis** widget, the **Focus on** drop-down displays the focus area with the correct floor level granularity.

The **Edit Widget** link allows you to define the heterarchy level from which the data pool is collected from, and then define the specific focus of this widget. That way, you can add more than one widget to the report and perform side-by-side comparisons of one zone with another.

The Wi-Fi Adoption Widget

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

The Wi-Fi Adoption widget displays a detailed summary of the number of clients that are associated with a network, and the clients that are probing the network:

- **Probing Only**—Refers to the client devices that are detected by APs in the network when they are probing the network.
- **Associated**—Refers to the client devices that have established a connection with an AP at least once during the time period selected in the report.

Associated status can be viewed in the following formats:

- **Summary**—This is the default view. The Summary view consists of the **Associated Status**, **Compare Data to**, and **Hourly Trend** charts.
- **Chart**—A line chart with a summary of associated and probing clients. The view can toggle to show associated clients in terms of percentage and total clients. The X-axis can be based either on location or

time. A line chart with a summary view and a detailed view of the criteria selected is also available. You can customize the X and Y axis by applying the following filter criteria:

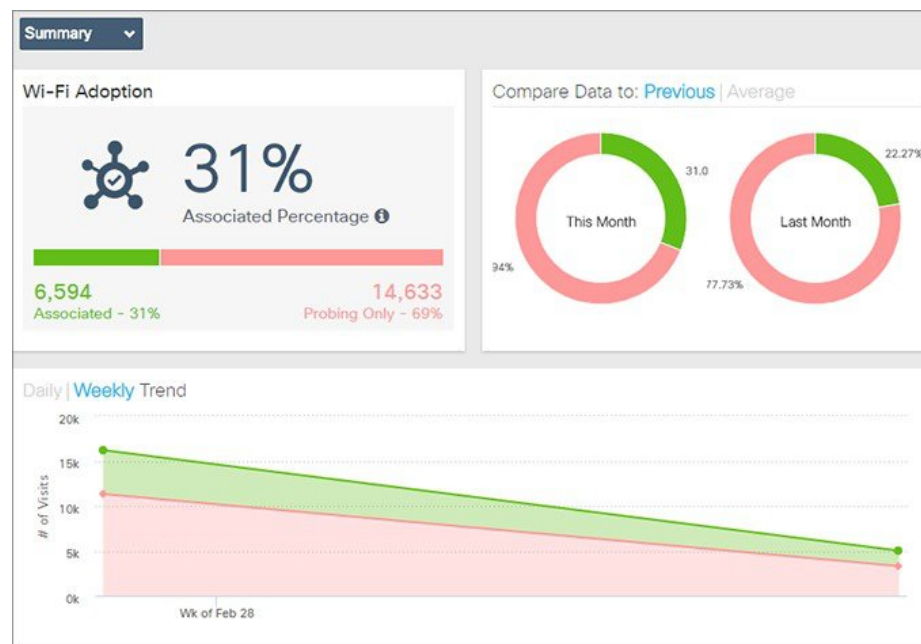
- View Unique Devices or View Absolute Visits
- Locations--Campus, Building, Floor, Zone, By Hour
- Values--Ascending, Descending, Alphabetical

Hover your mouse pointer at any point along the line to view the connected and probing data at that instance.

- **Table**—Connected and detected attributes of clients are presented in a tabular format.

The following trends are available for each different view:

- View Unique Devices
- View Absolute Visits



The Dwell Time Breakdown Widget

The Dwell Time Breakdown widget displays the dwell time distribution for selected areas.

Dwell Time Breakdown can be viewed in the following formats:

- **Summary**—This is the default view. The summary view consists of the **Dwell Time Breakdown**, **Compare Data to**, and **Daily Trend** charts. The dwell time breakdown is displayed in the following ranges:
 - **0-5 minutes**
 - **5-20 minutes**
 - **20-60 minutes**

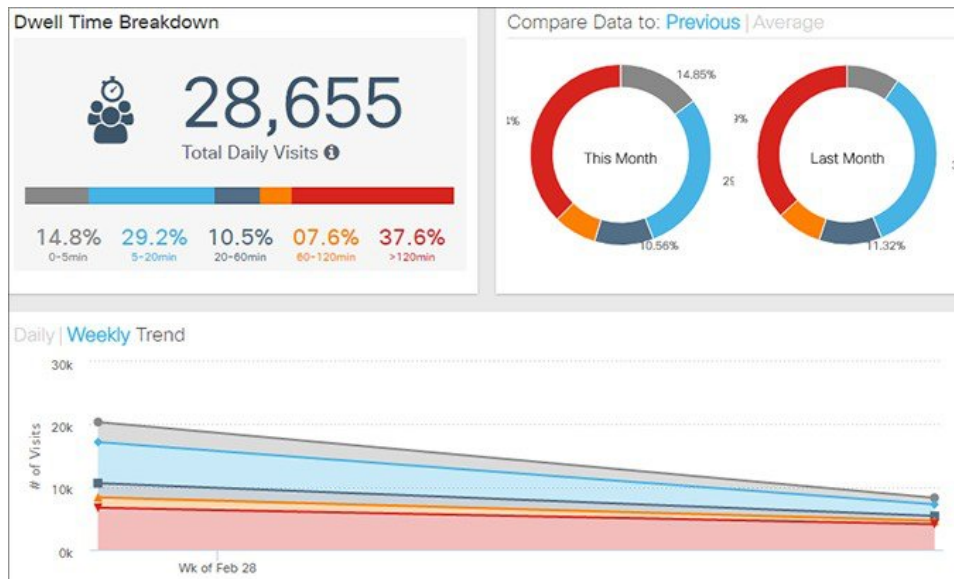
- **60-120 minutes**
- **>120 minutes**
- **Chart**—A line chart with a summary view of the dwell-time breakdown in the time ranges of **0-5 minutes**, **5-20 minutes**, **20-60 minutes**, **60-120 minutes**, and **> 120 minutes**. You can configure the chart based on the following views:
 - **View Unique Devices or View Visits**
 - **Locations**—Allows you to filter by any of these values: Campus, Building, Floor, Zone, Day, Hour of Day, Hour, Region, Building, Floor, Zone, Tag
 - **Sort order**—Ascending, Descending, Alphabetical
- **Table**—The tabular view provides information about the dwell-time breakdown in the time ranges of **0-5 minutes**, **5-20 minutes**, **20-60 minutes**, **60-120 minutes**, and **> 120 minutes**.



Note This view allows you to search for records within the table. The search text box is available above the table.





Note The Dwell Time filters are not available for the Dwell Time Breakdown widget.




Creating Customized Widgets


Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Choose **Analytics > Dashboard**.
- Step 3** In the left panel of the Dashboard, click the **Add** icon next to **Custom Reports**.
The **Create New Report** window is displayed.
- Step 4** Choose **Customized** from the Report Type widgets row in the right pane.
- Step 5** Choose the locations that you want to analyze from the **Focus Area Filter** drop-down list.
The location types are **Building, Campus, Floor, Zone**.
- Step 6** Choose the date and time range you want to run the report for from the **Date & Time filters** drop-down list.
Click the dot at the bottom of the **Add Widget** area to scroll to the next set of options. You can select multiple widgets to combine in one overall widget.
- Step 7** In the **Add Widgets**  area click the **Add+** icon to include any of the following widgets to the report:
Click the dot at the bottom of the **Add Widget** area to scroll to the next set of options. You can select multiple widgets to combine into one overall widget.
- Step 8** You can set a threshold for dwell time. This is the amount of time spent by a client device(visitor) at a given location. Select the minimum and maximum time from the drop-down options in the **Advanced Widget Filters**  area.
- Step 9** Click **Done**.
The widget is created.
- Step 10** Click the report title to name to your report.
- Step 11** Click **Save**.
-

Create a Realtime Report

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Choose **Analytics > Realtime**.
- Step 3** In the left pane of the Dashboard, click  next to **Now Reports**.
The **Create New Report** page is displayed.
- Step 4** From the **Focus Area Filter** drop-down list, choose the floor that you want to analyze.

- Step 5** In the Add Widgets  area, click the **Add Widget to Report +** to include any of the following widgets to the report:
- **Realtime Device Count**—Shows the number of devices currently detected on the Wi-Fi network. You can add a maximum of three Realtime device Count widgets to generate the report.
- Step 6** Click **Done**.
Based on the **Focus Area Filter** filters that you specified, the report name is generated. The new report name is listed in the left pane under **Now Reports**.
-

Performing Heatmap Analysis

A heatmap is a graphical representation of client movement, which shows areas having a large concentration of devices in red, and those with less activity in blue.



Note If you have an exclusion area, the heatmap will not consider that area for analysis.

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Choose **Analytics > Heatmap**.
- Step 3** In the **Activity Heatmap** window, click the **Date** icon and select the date.
- Step 4** Click the **Time** icon to show or hide the display of time.
- Step 5** Choose from the following options:
- From the **Campus** drop-down list, select the campus on which you want to run the heatmap analysis. The drop-down list contains all the campuses that are synchronized with Cisco CMX.
 - From the **Building** drop-down list, select the building on which you want to run this analysis. The drop-down list contains all the buildings that are synchronized with Cisco CMX.
 - From the **Floor** drop-down list, select the floor on which you want to run the analysis.
- Step 6** Click the **Heatmap** and **Zone** icons to display heatmap distribution and zones respectively.
- Step 7** Click the **Zoom in (+)** and **Zoom out (-)** buttons to increase or decrease the view of the map.
- Step 8** Click **Realtime** to view heatmap data.
- Step 9** Click **Playback** to play back the client movement for the selected date.
-

Using the Schedule Manager

To access the Schedule Manager window, log in to Cisco CMX, and choose **Analytics > Schedule**. The **Schedule Manager** window is displayed with the following information:

- **Report ID**—Shows the report IDs of scheduled reports.
- **Report Title**—Shows the titles of reports.
- **Username**—Shows the user who created the scheduled report.
- **Start From**—Shows the date from which reports will be emailed to recipients.
- **Recipients**—Shows the email addresses of recipients.
- **History**—Shows the status of past reports.
- **Action**—Click **Delete** to delete a scheduled report.

Verticalization

Verticalization capabilities provide the ability to change the names associated with each level of the hierarchy used in report generation. Although you can change the names of the hierarchy levels, names of any existing elements cannot be changed once created. Renaming through this process is global and will affect all users.

For more information about managing verticalization, see [Managing Verticalization, on page 149](#).

Set SSID Filter Parameters for Analytics Service

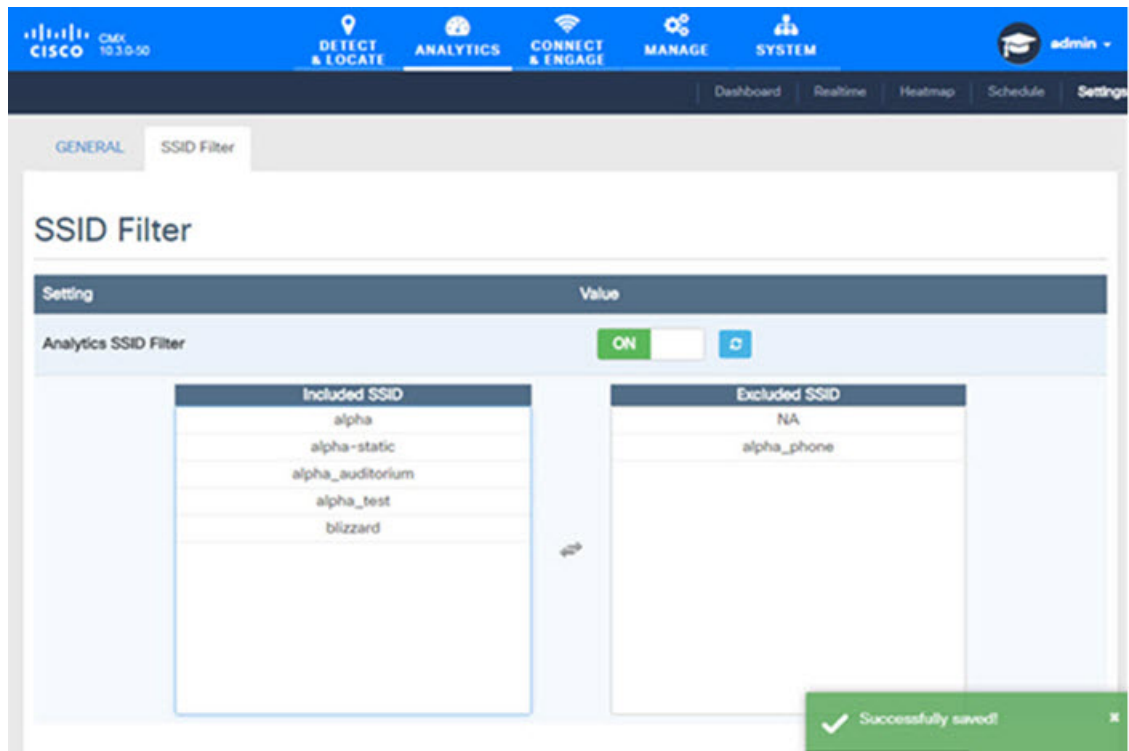
In the Analytics service, use the **SSID Filter** tab to exclude the SSIDs. You also can click the **Refresh** option to get any updates to the SSIDs.



Note If you filter out an SSID in the Location service, it will be automatically filtered out in the Analytics service too.

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Choose **Analytics > Settings**.
- Step 3** Click the **SSID Filter** tab.
- The **SSID Filter** window is displayed.



Step 4 To enable the SSID Filter, click **Analytics SSID Filter**.

Note A green **ON** option indicates that SSID filtering is on. The SSID Filter list displays the SSIDs from all the controllers. All duplicate instances of SSIDs are merged and displayed as a single ID. In the **Included SSID** list, the value **NA** indicates that SSID is not applicable. This option is available only for the **Analytics** service.

Step 5 To filter out an SSID, click the corresponding SSID in the **Included SSID** list. This SSID is moved to in the **Excluded SSID** list.



CHAPTER 4

The Cisco CMX Connect Service

- [Overview of the Connect Service, on page 71](#)
- [The Connect Dashboard, on page 74](#)
- [Connect Experiences, on page 75](#)
- [Customizing a Policy Plan, on page 92](#)
- [Using the Connect Library, on page 93](#)
- [Connect Settings, on page 99](#)
- [Configuring Connect Services in Cisco CMX High Availability, on page 110](#)

Overview of the Connect Service

CONNECT is a customizable and location-aware guest captive service that enables you to create customized, intuitive on-boarding experiences for your visitors. It enables you to provide two types of on-boarding experiences for your visitors:

- Facebook Wi-Fi:
 - Allows the administrator of a facility to enable the facility's Facebook page as a free Wi-Fi hotspot for visitors
 - Allows visitors to access free Wi-Fi after accessing the facility's Facebook page.
 - Provides insight into a facility's customer base through demographic reports.



Note Cisco CMX supports Facebook Connect through access points in local mode or FlexConnect mode.

- Custom Portal:
 - Enables the administrator of a facility to create and host a guest splash page with customized branding and advertisements.
 - Provides social network authentication with Facebook, Instagram, and Foursquare using OAuth 2.0.
 - Collects OAuth 2.0 user social information

For a complete list of new features in the Cisco CMX Connect service, see the What's New in This Release section of the *Release Notes for Cisco CMX* at:

<https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-release-notes-list.html>



Note You cannot install both the Location service and the Presence Analytics service on the same Cisco CMX instance in this release. Therefore, you can have either of the following:

- Connect with Location
- Connect with Presence Analytics

For the Connect Service to operate as intended, ensure to add Presence sites.

Restrictions

- The Facebook Wi-Fi authentication feature for Cisco CMX Connect is not supported in Cisco IOS XE 3.3.x SE, Cisco IOS XE 3.6.x E, Cisco IOS XE 3.7.x E.
- After you upgrade from Cisco CMX 10.1 to 10.2, you need to clear your browser's cache, and then launch the Cisco CMX Connect UI. If you do not perform this operation, the portal will not be upgraded, and all CMX Connect features will not work properly.

Comparison of Facebook Wi-Fi and Custom Portal

Table 2: Comparison of Facebook Wi-Fi and Custom Portal

	Facebook Wi-Fi	Custom Portal
Landing page	Hosted on Facebook (Facebook page)	Hosted on Cisco Connected Mobile Experiences (Cisco CMX)
Social authentication	Facebook only	Facebook, Instagram, and Foursquare (Using OAuth 2.0)
Facebook app permission pop-up	No	Yes
Post on timeline	Check-in is visible on users' timeline (Dependent on privacy setting)	Check-in is unavailable
Demographic data	Stored on Facebook at an aggregate level (Requires more than 30 check-ins to be enabled)	Stored on Cisco CMX (at an individual level)
Export of demographic data	No	Yes

	Facebook Wi-Fi	Custom Portal
Customer profile	<ul style="list-style-type: none"> Marketing teams with Facebook advertising budget or social media teams or both Service providers managing multiple small stores 	Marketing teams and IT teams that prefer to keep data in-house
Support for Post Auth URL	No	Yes

Preparatory Tasks

You must have a Facebook account for a business page. For more information, see the [Creating a Facebook Page for Your Organization, on page 79](#).

Adding a Connect or ConnectExperience User

Procedure

-
- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Choose **MANAGE > Users**.
- Step 3** Click **New User**.
- Step 4** In the Add New User dialog box, enter the first name, last name, username, and password of a user.
- Step 5** From the **Roles** drop-down list, select **Connect** or **ConnectExperience**.
- Note** For information about access rights for the Cisco CMX services available to the Connect and ConnectExperience user roles, see [User Role Summary, on page 73](#).
- Step 6** Click **Submit**.
-

User Role Summary

The following table lists the user roles that have access to the Connect & Engage service.

Table 3: User Role Summary

Role	Connect & Engage Service				Other Services
	Dashboard	Experiences	Policy	Settings	
Admin	Read	Read/Write	Read/Write	Read/Write	Read/Write
Connect	Read	Read/Write	Read/Write	Read/Write	No
ConnectExperience	No	Read/Write	Read	Read*	No

* Write permission for SMS, Number of Devices, and Time to Expire.

The Connect Dashboard

To view the Connect Dashboard, log in to Cisco CMX and choose **CONNECT> Dashboard**.

The Connect Dashboard window displays the summary report and two historical reports.

Use the navigation bar at the top of the page to set the location and interval of reports.

Location consists of the following levels:

- **Global**
- **Campuses**
- **Buildings**
- **Floors**
- **Zones**
- **Sites**

From the **Interval** drop-down list in the Connect & Engage Dashboard window, you can select the time frame for generating historical reports:

- **Last 7 Days** (default)
- **Last 28 Days**
- **Last 365 Days**

Summary Information

The summary information presents users' usage information for the present day. Note that the time used is server time, and not web browser time.

Historical Information

The Connect & Engage Dashboard displays historical information:

- **New and Repeat Visitors**—New Visitors are the people seen for the first time. Repeat Visitors are those recognized from an earlier visit.
- **Network Usage**—Network Usage is the total amount of data uploaded and downloaded by all visitors.
- **Pages Served vs Submitted**—Pages Served is the number of times a portal page was displayed to the visitors' devices. Pages Submitted is the number of times a portal page was submitted by the visitors.
- **SMS Sent vs Authenticated**—SMS Sent is the total number of texts sent. SMS Authenticated is the number of texts that were used to successfully authenticate visitors.
- **Languages Used**—Languages used is the count of visitors authenticated using each language.

In historical reports, you can choose the type of chart you want to be displayed in the reports:

- Area Chart

- Line Chart
- Column Chart

Visitor Search

The Connect & Engage Dashboard provides a search option, where the following types of searches can be performed:

- Advanced Search
- Export All Visitors

To search for a visitor, enter a search term, for example, name or email address, in the **Visitor Search** field.

Additional Information

- The Search table provides a preview of up to 100 clients per page.
- The entire search result can be exported to a .CSV file.
- The search time range is based on the Cisco CMX system time, and not on the web browser time.
- Partial search is supported; however, wildcards (*) are not supported.
- Advanced search can be performed based on the following parameters:
 - All
 - MAC
 - Facebook Name
 - Facebook Gender
 - Facebook Locale
 - Facebook Timezone
 - Facebook Friends
 - Foursquare Name
 - Foursquare Email
 - Instagram Name
 - Instagram Email
 - Registration Form Email
 - Registration Form Gender
 - Registration Form Name
 - Registration Form Phone Number

Connect Experiences

Overview

Using Connect Experiences, you can choose between two types of guest on-boarding experiences:

Facebook Wi-Fi

The Facebook Wi-Fi feature provides organizations with a simple and fast guest access solution. With Cisco CMX for Facebook Wi-Fi, organizations can:

- Save time and effort on designing their own captive portal by directing guests to a facility's Facebook page.
- View aggregate social data gathered from visitors connected to Wi-Fi with their Facebook logins for tailoring social media marketing strategy.

Facebook Wi-Fi is based on WLAN web passthrough authentication on Cisco Wireless Controllers (Cisco WLCs). Cisco WLC intercepts HTTP traffic and redirects the client browser to Cisco CMX. Cisco CMX finds the client location and redirects the client browser location to the configured location-specific Facebook page. After a successful Facebook sign-in and check-in, Cisco CMX redirects the client browser to the specific Facebook page. For Facebook Wi-Fi feature, both the client and Cisco CMX uses HTTPS traffic to communicate with Facebook.



Note Only http traffic will be redirected to Facebook. Facebook Wi-Fi/OAuth login is not useful for any https traffic.

For information about setting up Facebook Wi-Fi, see the [Setting Up a Facebook Wi-Fi Portal, on page 76](#).

Custom Portal

Custom Portal enables you to perform the following tasks:

- Create location-specific splash pages
- Enable branding consistency using splash pages
- Own registration information from customer sign-in page, which turns the captive portal into a data source for targeted marketing later via email marketing

For information about setting up a custom portal, see [Setting Up a Custom Portal, on page 80](#).

Setting Up a Facebook Wi-Fi Portal

Setting up a Facebook Wi-Fi portal involves the following tasks:

Configuring Access Control Lists on Cisco Wireless Controller

Procedure

- Step 1** Log in to the web UI of a Cisco Wireless Controller (Cisco WLC) that is associated with Cisco CMX.
- Step 2** Choose **SECURITY > Access Control Lists > Access Control Lists**.
- Step 3** On the **Access Control Lists** window, click **New** to add an access control list (ACL).
- Step 4** On the **Access Control Lists > Edit** window, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.
- Step 5** Choose the ACL type as either **IPv4** or **IPv6**.
- Step 6** Click **Apply**.
- Step 7** On the **Access Control Lists** window, click the name of the new ACL.
- Step 8** On the **Access Control Lists > Edit** window, click **Add New Rule**.

The **Access Control Lists > Rules > New** window is displayed.

Step 9 Configure the following ACLs, as listed in the table below:

Note The following ACL table lists the rules for social login. If you use HTTPS as the authentication method, use the rules one and two to access Facebook.com.

Table 4: ACLs for Facebook Wi-Fi Portal

Seq.	Action	Source IP/ Mask	Destination IP/ Mask	Protocol	Source Port	Destination Port	DSCP	Direction
1	Permit	0.0.0.0/0.0.0.0	0.0.0.0/ 0.0.0.0	TCP	HTTPS	Any	Any	Any
2	Permit	0.0.0.0/0.0.0.0	0.0.0.0/ 0.0.0.0	TCP	Any	HTTPS	Any	Any
3	Permit	MSE_IP/ 255.255.255.255	0.0.0.0/ 0.0.0.0	TCP	HTTP	Any	Any	Any
4	Permit	0.0.0.0/0.0.0.0	MSE_IP/ 255.255.255.255	TCP	Any	HTTP	Any	Any

Table 5: ACLs for Facebook Authentication using Cisco CMX

Seq.	Action	Source IP/ Mask	Destination IP/ Mask	Protocol	Source Port	Destination Port	DSCP	Direction
1	Permit	CMX_IP/ 255.255.255.255	0.0.0.0/0.0.0.0	TCP	HTTPS	Any	Any	Any
2	Permit	0.0.0.0/0.0.0.0	CMX_IP/ 255.255.255.255	TCP	Any	HTTPS	Any	Any

Note For Facebook to work in the DNS ACL, configure the below URLs:

- facebook.com
- m.facebook.com
- fbcdn.net

To create DNS-ACL, you must create an ACL and add DNS entries to the selected ACL. For more information, see the "[Configuring and Applying Access Control Lists](#)" in the Cisco Wireless Controller Configuration Guide, Release 7.6.

Configuring WLAN for Web Passthrough Authentication



Note After upgrading to Cisco CMX 10.2, or after newly installing Cisco CMX 10.2, the sslmode is enabled by default. Therefore if you want to have the HTTP redirect, you need to disable sslmode. Otherwise, you need to configure https://<CMX>/... in WLC SSID config. And modify ACL rules to reach MSE_IP using HTTP.

To provide network access to users, you must configure a wireless LAN (WLAN) on the Cisco WLC, for which you must set up the web passthrough on Layer 3 security of WLAN for Connect & Engage.

Procedure

- Step 1** From the web UI of Cisco WLC, click **WLANs**.
- Step 2** On the **WLANs** window, click the corresponding WLAN ID.
- Step 3** On the **WLANs > Edit** window, choose **Security > Layer 2**.
- Step 4** From the **Layer 2 Security** drop-down list, choose **None**.
- Step 5** Click **Apply**.
- Step 6** Under the **Layer 3** tab, from the **Layer 3 Security** drop-down list, choose **Web Policy**.
- Step 7** For web passthrough, choose **Passthrough**.
- Step 8** Choose the **Preauthentication ACL** defined using the procedure described in the [Configuring Access Control Lists on Cisco Wireless Controller, on page 76](#).
- Step 9** To override the global authentication and web authentication pages, check the **Over-ride Global Config** check box.
- Step 10** To define the web authentication pages for wireless guest users, from the **Web Auth Type** drop-down list, choose **External (Re-direct to external server)**.
This redirects clients to an external server for authentication.
- Step 11** In the **URL** field, enter the Facebook Wi-Fi page URL. The external redirection URL should point to the corresponding portal on Cisco CMX for Facebook Wi-Fi, for example:
Example:

```
https://<CMX>/fbwifi/forward
```
- Step 12** Enable this Service Set Identifier (SSID).
- Step 13** Click **Apply**.
- Step 14** Click **Save Configuration**.

Note Connect & Engage redirection requires special configuration on Cisco WLC for Apple iOS devices. Run the following command using the Cisco WLC CLI:

config network web-auth captive-bypass enable.

For more information, see the *Cisco Wireless LAN Controller Command Reference, Release 8.0*, at:

http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/command-reference/b_cr80/b_cr80_chapter_0

Creating a Facebook Page for Your Organization

Follow the instructions provided in Facebook to create a Facebook page for your organization. To create a Facebook page, go to <https://www.facebook.com/pages/create.php>.



Note Currently, Facebook Wi-Fi does not support age and country restricted Facebook Pages. We recommend to remove any age and country restrictions from the Facebook Page in order to successfully pair Facebook Wi-Fi with Cisco CMX.

Assigning a System Default Facebook Page

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Choose **CONNECT > Connect Experiences** .
- Step 3** In the **Facebook Wi-Fi** column, click **Assign Default**.
The Facebook Wi-Fi Configuration option opens in a new browser tab.
- Step 4** Perform the following tasks:
- Select the page.
 - Select the **Bypass Mode**.
 - Select the **Session Length**.
 - Click the optional Terms of Service if additional Terms of Service are required.
 - Click **Save Settings**.
- Step 5** After assigning Facebook Wifi Configuration, navigate to **Connect Experience** tab and click **Click Here When Finished**.


Note When on boarding guest Wi-Fi using Facebook Wi-Fi, some guest client browsers displays "Network Not Found" error message. However, if you are using default Facebook WiFi settings for all the locations, you will not encounter this issue. This issue occurs only if you have setup your Facebook WiFi configuration in a Parent-Child location hierarchy, for example, **Campus > Building > Floor > Zone**.

You can pair different facebook pages with different child nodes in the hierarchy, like Campus is paired with Facebook page 1 and Building with Facebook page 2. In this scenario, you can get the network not found error message while using Facebook Wi-Fi. To resolve this issue, remove the Facebook pairing with all the child nodes to inherit the pairing from the parent.

Assigning a Location-Specific Facebook Page

After the system default page has been set, you can assign a location-specific Facebook page:

Procedure

-
- Step 1** Select a specific campus, building, floor, or zone and click or hover over the Gear  icon.
- Step 2** Click **Assign New**.
-

Setting Up a Custom Portal

You can create a custom portal page using the following four types of templates:

- **Registration Form**—This template contains the following elements:
 - Logo or image
 - Registration form to specify name, email address, and phone number of a visitor
 - Terms and conditions
 - The **Submit** button



Note When you specify a phone number, select the **SMS Auth** check box to get notification through SMS. For more information, see [Enabling Multi-language Support in Custom Portals, on page 82](#).

- **Social Login**—This template contains the following elements:
 - Logo or image
 - Social login element that includes three options: Facebook, Instagram, and Foursquare.

The Social login element enables on-boarding of visitors using social OAuth 2.0.



Note If you have the **Terms and Conditions** checkbox element in the live portal, all the social login elements are enabled only when you select the **Terms and Conditions** checkbox.

- **Social or Registration Login**—This template contains both the Social Login element and the Registration Form element.
- **SMS Form**—This template enables you to create a portal for SMS authentication. Verify your portal has a Registration Form element, or add one if required. All that this element requires is a phone number field, but you may include others if required. The Registration form allows you to receive the auth code on a SMS capable device and still enter it on a non-SMS capable device.
- **Custom**—This template is empty and allows you to create your template from scratch. The template choice does not limit the type of elements you can add. For example, if a Social Login template is selected, you can always modify it to use the Registration Form elements instead.

The following options are available to design a custom portal:

- The left side of the window shows a preview of the custom portal and the right side of the window shows the options to edit the portal and its elements.
- The **CONTENT** tab allows you to add or edit the portal elements. Click an element to preview an area of the portal and edit the element's settings. For more information, see [Using Content Elements for Creating Portals, on page 94](#).
- The **BACKGROUND** tab allows you to:
 - Upload an image from the image library
 - Specify the background color and opacity for the portal.
- The **THEMES** tab allows you to specify a theme for the portal.
- The **LANGUAGES** tab allows you to choose the language of your choice. To add a language, choose your desired language from the **Select language** drop-down list, and then click **Add to list**.



Note

- You can get a preview of the custom portal for a mobile, PC, or tablet.
- For **Registration Form** element, you can add three input fields: **Text**, **Drop-down**, and **Checkbox/Radio**. If you choose to add a check box or a radio button, you must specify at least one field value. An error message is displayed when you try to save a portal with no input field values and **Submit** button added to the **Registration Form** element.

- **Engage**—This template enables you to create a portal for engage services.

Creating a Default Custom Portal Page

Procedure

- Step 1** Log in to Cisco CMX as an admin user.
 - Step 2** Choose **CONNECT > Connect Experiences**.
 - Step 3** Under **Custom Cisco CMXs**, click **Create Default**.
 - Step 4** In the **Portal Title** field, enter the name of your custom portal.
 - Step 5** Click the template that you want to use and click **Next**.
 - Step 6** Design the template according to your requirements.
 - Step 7** Click **Save**.
-

Assigning Location-Specific Custom Portal Page

After the system default portal has been set, you can assign a location-specific custom portal page.

Procedure

- Step 1** Select a specific campus, building, floor, or zone from the corresponding custom portal drop-down list.
 - Step 2** Click **Create New** to create a new portal and assign it to that location. Alternatively, assign an existing portal to that location.
-

Enabling Multi-language Support in Custom Portals

Cisco CMX does not contain any language translation engine. Administrator must edit each language page individually and manually translate all text entries.



Note The portal page translations are not supported for right-to-left languages such as Hebrew and Arabic.

To support multiple pages by a portal page, each page must have the desired languages added to the page before it can be enabled. Multi-language support can be added when the portal is created. The non-English languages can be disabled or re-enabled one at a time when translations are completed.

To enable multi-language support, the admin user should perform the following tasks:

- Create a portal.
- Add the languages that have to be supported.
 - To add a language, click the **Languages** tab inside the portal editor. Select the language from the drop-down, and click **Add Language**. Only the Enabled languages(languages that are selected) are used.
- Provide translations for each language that is enabled.

- Change which portal translation is currently being viewed by selecting different language from the drop-down list above the preview area in the portal editor.
 - Most elements' translations are portal specific, which means, translating a text element in one portal does not effect a text element in another portal.
 - However, the registration fields' translations are shared across all portals. When a field is changed in one portal, the field is changed in every other portal.
- Confirm that translations are correct by using the Live View, switching between each language and verifying translation, and then saving the portal.

When the splash page is displayed to an end user, Cisco CMX uses the browser's settings to determine the end user's most preferred languages. It then selects the preferred language that is available and displays that version of the portal. An end user can manually select a different language by using the drop-down list on the top-right corner of the splash page.

End-user devices will have a predefined language. This list of preferred languages is passed as part of the HTTP header. Cisco CMX analyzes the HTTP header and displays the closest available translation of a portal.

For example, if a user prefers languages such as English, Spanish, and French (in this order) and the portal only has languages such as Russian, Spanish, Italian, German, then Spanish is displayed because it is the most preferred language from among the available languages.

To view a portal in a different language, a portal user can use the Language drop-down list to select from the list of available translations.

Configuring Connect Portal Pages for Sites

After you create a portal, you can assign it to a site by performing the following steps:

Procedure

- Step 1** Choose **Connect > Connect Experiences**.
- Step 2** In the **Custom Portal** column, click **Create Default** for the site that you want to assign as default.
- Note** If portals are already existing, select the desired portal from the available list.
- Step 3** In the **Post Auth URL** column, click **Assign Default** for the site that you want to assign to the portal.
- Step 4** In the **Post Auth URL for <site name>** dialog box, enter the post Auth URL, then click **Set**.
- Note** After a successful authentication, the clients will be redirected to the URL entered as the post Auth URL.
-

Viewing Connect Clients with Sites

To view the Connect clients with sites, perform the following steps:

Procedure

-
- Step 1** Choose **Connect & Engage > Dashboard**.
 - Step 2** From the **Location** drop-down list, choose **Sites**.
 - Step 3** From the **Select a Location** drop-down list, select a site.
 - Step 4** From the **Interval** drop-down list select the interval.
-

Device-Browser Matrix

Device-Browser Matrix for Connect and Engage

The following table lists the tested devices and browsers for Connect & Engage in the context of custom portals.

Table 6: Device-Browser Matrix for Connect and Engage for Custom Portals

Device and Name	OS Version	Default Browser and Version	Remarks
Google Nexus 7	4.3	Google Chrome 32.0.1700.99	—
Amazon Kindle	13.3.2.2	Silk 1.0.454.220	—
Apple iPad	7.0	Safari 7.0	—
Apple iPhone	6.1.3	Safari 6.0	—
Apple Macbook Pro	10.8.4	Safari 6.0	—
Samsung (Snow OS)	33.0.1750.152	Google Chrome 33.0.1750.152	—
Apple iPad Mini	7.0	Safari 7.0	—
Microsoft Windows tablet	Windows RT 8.1	Internet Explorer 11	Issues with social connector
Samsung	4.2.2	Default browser	—

Device-Browser Matrix for Facebook Wi-Fi



Note The portal pages with Social OAuth do not work properly on Mozilla Firefox browser.

The following table lists the tested devices and browsers for Facebook Wi-Fi.

Table 7: Device-Browser Matrix for Facebook Wi-Fi

Device and Name	OS Version	Default Browser and Version	Other Browser and Version
Google Nexus 7	4.3	Google Chrome 32.0.1700.99	—
Amazon Kindle	13.3.2.2	Silk 1.0.454.220	—

Device and Name	OS Version	Default Browser and Version	Other Browser and Version
Apple iPad	7.0	Safari 7.0	—
Apple iPhone	6.1.3	Safari 6.0	—
Apple Macbook Pro	10.8.4	Safari 6.0	—
Samsung (Snow OS)	33.0.1750.152	Google Chrome 33.0.1750.152	—
Apple iPad Mini	7.0	Safari 7.0	Google Chrome 34.0.1874.114
Microsoft Windows tablet	4.2.2	Internet Explorer 11	—
Samsung	4.2.2	Default browser	—
One+ phone	5.0.1	Google Chrome	—
Amazon Reader	5.6.2.1	Default browser	—

Offering Opt-Out and Opt-In Options for Cisco CMX Services

Overview of the Opt-Out Option

Your login portal can include the **Opt-Out** option, which allows a client to opt out of having their mobile device location history maintained and used by Cisco CMX.

When a client opts out, Cisco CMX stops detecting the client's device MAC address and thus stops storing analytics data for that device. Either the client no longer appears on maps or appears not to be moving (that is XY location data remains the same).

The default is **Opt-In**.

The **Opt-Out** option is applicable when location tracking is enabled by default. With Cisco CMX Release 10.4 or earlier, the **Opt-Out** configuration was applicable for the complete Cisco CMX system. In Cisco CMX Release 10.5, the **Connect** service offers the **Opt-In** configuration that allows administrators or partners to collect consent from end users to being tracked using Cisco CMX.

Configuring the Opt-Out Option

In Cisco CMX release 10.4 or earlier, location tracking is enabled by default. In this scenario, Cisco CMX Connect service offers clients an option to **Opt-out** from being tracked. The portal login page can include the **Opt-out** option that clients can select to opt-out from being tracked by Cisco CMX.

Procedure

-
- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
 - Step 2** Choose **Connect > Library > Templates**.
 - Step 3** Click a portal template, such as the **Registration Form** template.
You can add the opt-out element to any template.
 - Step 4** Enter the name of the portal that you want to create, and then click **OK**.
 - Step 5** Click the **Content** tab.

- Step 6** Click the **Opt-out** element.
 Edit the text for your opt-out message.
 If you do not want your portal to display the opt-out option, click **Remove element**.
- Step 7** Click **Save**.
-

Changing the Opt-Out Period

The default opt-out period is 180 days. When the opt-out period ends, the opt-out option reappears when the client displays your login portal.

You can:

- Modify the opt-out period to be longer or shorter.
- Add the opt-out element to any template.
- Remove the opt-out element so that it does not appear on your portal.

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Choose **Connect > Library > General** to display the **Connect Settings** window.
- Step 3** From the **Connect Settings** window, change the value in the **User Retention Period** field.
 The range is 1 to 1000 days. The default is 180 days.
- Step 4** Click **Save**.
-

Configuring Elements for Custom Portal Navigation

Configuring URLs for Custom Portal Navigation

After you create a custom portal, use the **Content** tab in the **Portal** window to design and customize the portal. You can select the elements (such as, Social Auth, Image & Text, Image Slider, External Content) in the right side of the window to edit the portal and the elements. You can configure website URLs for URL enabled elements such as images and logo. The URL enabled elements are **Image**, **Menu**, and **Image Slider**.



- Note** If you configure a URL enabled element in the login page, configure DNS-ACL to white list URL domain on WLC which requires 8.3 version. If you configure a URL enabled element in the success page, you need not perform any more configuration on WLC, because the client already has Wi-Fi access.
-

To configure a URL, perform the following steps:

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX) as an admin user.
- Step 2** Choose **CONNECT > Library**.
- Step 3** Create a portal. For more information about setting up a custom portal, see [Creating a Default Custom Portal Page, on page 82](#).
- Step 4** From the **Content** tab, click any of the following elements:
- **Image Element**
 - **Menu**
 - **Image Slider**
- Step 5** In the **Link** field or **Image URL** field, enter the URL.
- In the live view, you can click the image or logo to view the Website.
- Check the **Enable back button** check box to display the **Back to Portal** option in the live view of the portal page. Click **Back to Portal** to navigate back to the portal view. Not all the URLs are displayed within the frame view. Use the **Live View** option in the window to verify if the URL provided is displayed in the frame view. If the URL you configured is not compatible to be displayed within the same frame, the website is displayed as a separate web page in the browser window.
- If the **Enable back button** option is selected, links with HTTP response header “X-Frame-Options” will not be rendered on the portal.
 - If the **Enable back button** option is selected and SSL is enabled on CMX, use HTTPS links for the login portal. However, if SSL is not enabled on CMX, use either HTTP or HTTPS links for login portals.

FlexConnect AP Support on Cisco CMX

FlexConnect AP communicates through Cisco WLC for Authentication. FlexConnect AP is responsible for Policy Plan enforcement such as ACL, Rate-limiting and session timeout. Enforcement message comes from AAA to Cisco WLC, which the Cisco WLC pushes according to the per-user network policy to FlexConnect AP. FlexConnect Access Point cannot function when communication with Cisco WLC is down. CMX Connect relies on Web Authentication which is handled by Cisco WLC. The supported FlexConnect modes are Local Switching and Central Switching.

The following Cisco CMX features are supported on a FlexConnect Access Point:

- Location
- Analytics
- Connect



Note Cisco CMX supports FlexConnect mode for both Facebook OAuth and Facebook Wi-Fi.

Configuring FlexConnect ACLs

You need to configure FlexConnect Access Control Lists (ACLs) only for Flex mode deployments. To configure FlexConnect ACLs, follow these steps:

Procedure

-
- Step 1** Choose **Security > Access Control Lists > FlexConnect ACLs** from the Controller UI.
- The FlexConnect ACL page is displayed. This page lists all the FlexConnect ACLs configured on the controller. This page also shows the FlexConnect ACLs created on the corresponding controller. To remove an ACL, hover your mouse over the blue drop-down arrow adjacent to the corresponding ACL name and choose Remove.
- Step 2** Add a new ACL by clicking New.
- The **Access Control Lists > New** page is displayed.
- Step 3** In the **Access Control List Name** text box, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.
- Step 4** Click **Apply**.
- Step 5** When the Access Control Lists page reappears, click the name of the new ACL.
- Step 6** When the **Access Control Lists > Edit** page appears, click **Add New Rule**.
- The **Access Control Lists > Rules > New** page is displayed.
- Step 7** Configure a rule for this ACL as follows:
- Note** The controller supports up to 64 rules for each ACL. These rules are listed in order from 1 to 64. In the Sequence text box, enter a value (between 1 and 64) to determine the order of this rule in relation to any other rules defined for this ACL.

If rules 1 through 4 are already defined and you add rule 29, it is added as rule 5. If you add or change a sequence number of a rule, the sequence numbers of the other rules are automatically adjusted to maintain a continuous sequence. For instance, if you change a rule's sequence number from 7 to 5, the rules with sequence numbers 5 and 6 are automatically reassigned as 6 and 7, respectively.

- a) From the **Source** drop-down list, choose one of these options to specify the source of the packets to which this ACL is applicable:
 - Any—Any source (This is the default value.)
 - IP Address—A specific source. If you choose this option, enter the IP address and netmask of the source in the corresponding text boxes.
- b) From the **Destination** drop-down list, choose one of these options to specify the destination of the packets to which this ACL applies:
 - Any—Any destination (This is the default value.)
 - IP Address—A specific destination. If you choose this option, enter the IP address and netmask of the destination in the text boxes.

- c) From the **Protocol** drop-down list, choose the protocol ID of the IP packets to be used for this ACL. The protocol options that you can use are the following:
- Any—Any protocol (This is the default value.)
 - TCP
 - UDP
 - ICMP—Internet Control Message Protocol
 - ESP—IP Encapsulating Security Payload
 - AH—Authentication Header
 - GRE—Generic Routing Encapsulation
 - IP in IP—Permits or denies IP-in-IP packets
 - Eth Over IP—Ethernet-over-Internet Protocol
 - OSPF—Open Shortest Path First
 - Other—Any other Internet-Assigned Numbers Authority (IANA) protocol

Note If you choose **Other**, enter the number of the desired protocol in the Protocol text box. You can find the list of available protocols in the INAI website.

The controller can permit or deny only the IP packets in an ACL. Other types of packets (such as Address Resolution Protocol (ARP) packets) cannot be specified. If you chose TCP or UDP, two additional parameters, Source Port and Destination Port, are displayed. These parameters enable you to choose a specific source port and destination port or port range. The port options are used by applications that send and receive data to and from the networking stack. Some ports are designated for certain applications, such as Telnet, SSH, HTTP, and so on.

- d) From the **DSCP** drop-down list, choose one of these options to specify the differentiated services code point (DSCP) value of this ACL. DSCP is an IP header text box that can be used to define the quality of service across the Internet.
- Any—Any DSCP (This is the default value.)
 - Specific—A specific DSCP from 0 to 63, which you enter in the DSCP text box
- e) From the **Action** drop-down list, choose **Deny** to cause this ACL to block packets, or **Permit** to cause this ACL to allow packets. The default value is Deny.
- f) Click **Apply**.
- The **Access Control Lists > Edit** page is displayed on which the rules for this ACL are shown.
- g) Repeat this procedure to add additional rules, if any, for this ACL.

Step 8 Click **Save Configuration**.

What to do next

For setting up WLC with FlexConnect ACL, see [Setting Up a Controller with FlexConnect ACLs, on page 90](#).

Setting Up a Controller with FlexConnect ACLs

After configuring the FlexConnect ACLs, you must apply the FlexConnect ACLs to the SSID.

Procedure

-
- Step 1** From the web UI of Cisco WLC, click **WLANs**.
The **WLANs** window is displayed.
 - Step 2** Click the corresponding WLAN ID.
The **WLANs > Edit** window is displayed.
 - Step 3** Click **Advanced** tab.
 - Step 4** To configure the WLAN for FlexConnect Local Switching, select the **FlexConnect local Switching** check box in the **FlexConnect** section.
 - Step 5** Click **Security > Layer 3**.
 - Step 6** From the **Layer 3 Security** drop-down list, select **Web Policy** to configure the security policy for the WLAN.
To enable External Web Authentication, you must configure **Web Policy** as the security policy for the WLAN.
 - Step 7** From the **Preauthentication ACL IPv4** and **IPv6** drop-down list, select **None**.
 - Step 8** To apply FlexConnect ACLs to the SSID, select **FlexConnect ACL on SSID** from the **WebAuth FlexAcl** drop-down list.
-

Offering Portal Pages on HTTP from Cisco CMX Connect

Disabling HTTPS

Procedure

-
- Step 1** In the Cisco MSE CLI, disable SSL mode by entering the **cmxctl node sslmode disable** command.
 - Step 2** In Cisco WLC (**WLANs > Security > Layer 3**), use HTTP instead of HTTPS for URL. For example, enter **http://<IP address>/visitor/login** instead of **https://<IP address>/visitor/login**.
 - Step 3** In Cisco WLC (**Management > HTTP-HTTPS**), set the **WebAuth SecureWeb** and **HTTPS Redirection** options to **Disable**.
- Note** If the **WebAuth SecureWeb** option is enabled, you need to upload a proper certification to WLC to avoid certificate warning. We recommend to disable this option to avoid certificate warning on client.
-

Adjusting ACLs on Cisco WLC

Procedure

- Step 1** Adjust the ACLs on the Cisco WLC to match HTTP.
 - Step 2** In Cisco WLC, (**WLANs > Security > Access Controller**), use HTTPS instead of HTTP.
-

SMS Authentication

To provide a proof of the identity of the connected individual, Cisco CMX 10.2 offers the ability to add SMS based authentication to a custom portal. Currently this feature only integrates with Twilio accounts for SMS authentication. You must establish your own Twilio account (see <https://www.twilio.com/user/account/settings>). Also, this feature requires you to have an SMS capable device to gain access to the network.

Without an appropriately configured preauth ACL the wireless client will not be able use the link provided in the SMS message to return the auth code to Cisco CMX and will remain in the WebAuth required state.

To use this feature, either edit an existing portal or use a template to create a new portal to use SMS Auth. You can only have one Twilio account, but that account can have many phone numbers associated with it so you can use the same account with multiple portals, but each portal can only have a single number associated with it. The Reset button is used to remove the association between the portal and the configured Twilio account.

The From Number that you configure in the Twilio Configuration area should be purchased from Twilio. You cannot use an existing number.

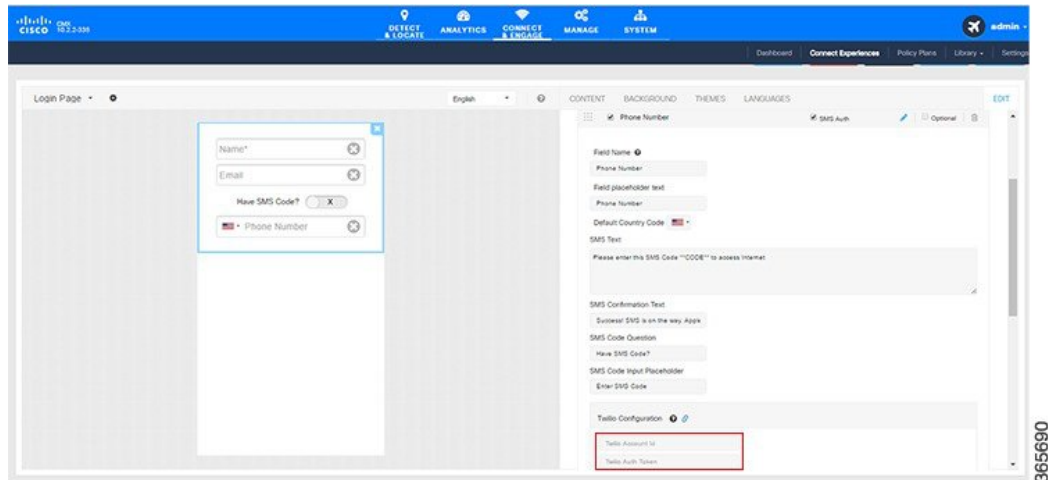
Procedure

- Step 1** Ensure that your portal has a Registration Form element, or add one if required
- Step 2** Ensure that you specify a phone number field, but you may include other fields if desired.
- Step 3** In the **Registration Form** area, check the **SMS Auth** check box.

The Registration form allows you to receive the auth code on a SMS capable device and still enter it on a non-SMS capable device.

- Step 4** Select the **Edit** icon (next to the SMS Auth check box) to enter the Twilio account information.
- Step 5** In the **Twilio Configuration** area (see the figure below), enter the following parameters:

Figure 6: Twilio Account Configuration



You can click the **Edit** button next to the Twilio Configuration field to access your Twilio account information.

- Enter your **Twilio Account ID**. This is a 34 character string that uniquely identifies the Twilio account.
- Enter the **Twilio Auth Token**.
- Enter the **From Number**. This number is purchased from Twilio. You cannot use an existing phone number.
- Click **Create**.

You can click the **Reset** button to remove the association between the portal and the configured Twilio account (that is, removing the connector).

Step 6 Click **Save**.

Customizing a Policy Plan

The Cisco CMX Policy Plans feature gives you the option to provide your client with the highest available bandwidth as the client moves from one location to the next. Use the CMX Policy Plans window to configure this feature. Use this feature to offer specific Wi-Fi policies for each site or location and thereby enhance the guest Wi-Fi experience.

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 (**Cisco CMX > Connect > Policy Plans**) is selected, the client retains the higher bandwidth when returning to the lobby.



Note The CMX Policy Plans feature is not supported when you add a PMS server.

Before creating the policy plans, ensure that you have the configured FreeRADIUS and Wireless Controllers. For more information, see [Configuring the FreeRADIUS on Cisco CMX, on page 102](#) and [Cisco WLC Configurations, on page 104](#).

Procedure

-
- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Choose **Connect > Policy Plans**.
- Step 3** Click **New Policy Plan**.
The **CREATE POLICY PLAN** window is displayed.
- Step 4** Enter a name for the new policy plan.

Ensure to specify the name without spaces and special characters. For example, **PolicyOne**. The maximum characters allowed for a policy name is 20.
- Step 5** Enter the bandwidth, in kbps.

The maximum bandwidth allowed is a 10 digit value.
- Step 6** Click **Create**.
- Note** The new policy plan is displayed in the **Policy** drop-down list in the **Connect Experiences (Connect > Connect Experiences)** tab.
-

Using the Connect Library

To view the Connect Library, log in to Cisco CMX and choose **CONNECT > Library**. The following options are available:

- **Portal Library**—Lists the portals that you have created, both drafts and completed ones. Click **Create Portal** to create a new portal using the available template.



Note Select the **Disable Portal Cache** check box to disable HTTP cache for all portals.

In the Portal Library, you can:

- **Edit**—Edit a portal that is in progress.
 - **Copy**—Allows you to copy or duplicate a portal.
 - **View**—Allows you to view a portal.
 - **Delete**—Allows you to delete a portal.
- **Templates Library**—Provides pre-defined templates that you can use to create your own portal. The following templates are available:
 - **Registration Form**

- Social Login
 - Social or Registration Login
 - SMS Form
 - Custom
 - Engage
 - PMS Auth Form—Available in the template library if a PMS server is configured.
- Image Library—The image library allows an imported image to be used for multiple portals. There is no size limit on uploaded images as they are scaled during the upload. Once uploaded, the images can be rotated, cropped, or have their aspect ratio changed using the built-in image editor. In the Image Library, you can:
 - Add—Allows you to add new images. Images are scaled down so that you get a thumbnail view of the image.
 - View—Allows you to preview an image. When you preview an image, you can crop, resize or set its aspect ratio. After making changes in the image editor, click **Save** and **Close** to copy the image into the Image Library or overwrite the existing image.
 - Delete—Allows you to delete images from the Image Library.

Using Content Elements for Creating Portals

If you want to create a new Portal, use any of the existing templates available under **Connect > Library > Templates**.

The **Content** tab includes **Common** and **Advertisement** elements that can be used to create a login page or a success page. To add an element, drag and drop the element from the Content tab to the canvas or just click the required element.

The following table list some of the common elements available:

Table 8: Common Elements

Elements	Description
Image	To add a logo or image
Text	To add a text field
Registration Form	To add registration form fields such as name and email address.
Social Auth	To add preferred social login credentials
Terms & Conditions	To add terms and conditions for accessing Wi-Fi
Image and Text	To add image with text content
Submit Button	To add Submit button

Elements	Description
Contact us	To add contact information
Spacer	To add space element
PMS	To add PMS details
Menu	To add menu items
Opt-out	To add opt-out check box For more information, see Configuring the Opt-Out Option, on page 85 .

Authentication with Social Network Accounts

To configure OAuth for each social network platform (Facebook, Instagram or Foursquare), you need to first register your app/client with the Cisco CMX Connect service. If you want to remove a particular social network connection, uncheck the check box to the left of the social network name.

Configuring OAuth with Facebook



Note If Facebook is configured with OAuth, the client uses HTTPS to communicate with Facebook. The portal pages with Social OAuth do not work properly on Mozilla Firefox browser.

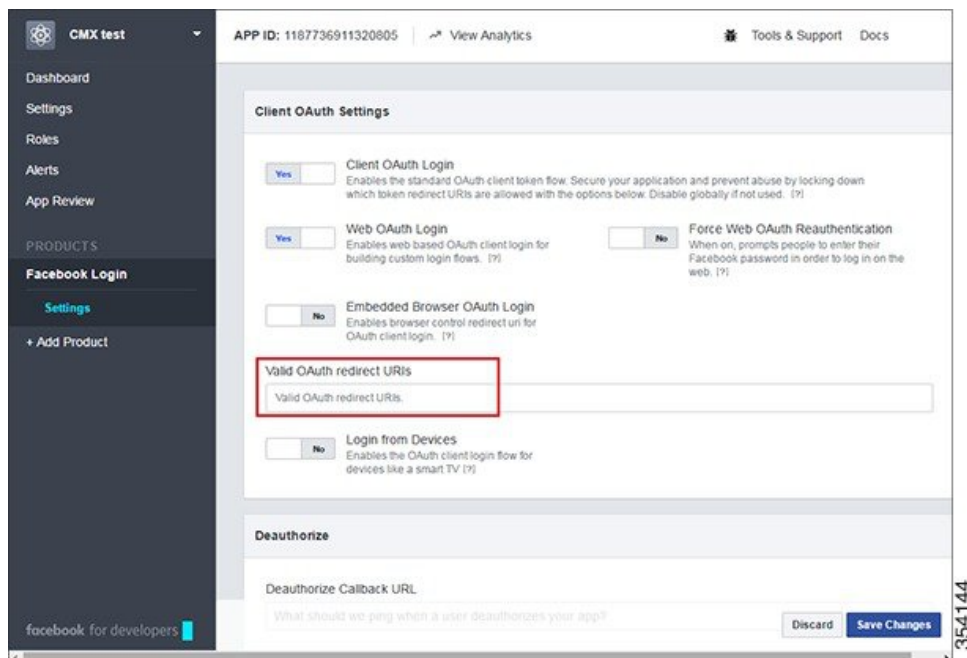
Procedure

- Step 1** In the Social Login element of the custom portal, click on the link (🔗) icon to the right of Facebook to go to the associated developer website.
- Step 2** Log in to Facebook with your username and password.
- Step 3** Click the **+Add a New App** button.
- Step 4** Click the **Website** button.
- Step 5** Enter a name for the application, and then click the **Create New Facebook App ID** button.
- Step 6** From the **Choose a Category** drop-down list, choose a category for the new application, and then click the **Create App ID** button.
- Step 7** Scroll down to the **Tell us about your website** area and enter the same URL as the Wireless LAN Controller (WLC) redirect URL (`http://<CMX>/visitor/login`) in the **Site URL** field, and then click the **Next** button.

Note This configuration will fail if Cisco CMX has an IP address in the 172.x.x.x range as it will be seen as a Facebook URL.
- Step 8** Click the **Skip to Developer Dashboard** link.
- Step 9** Select and copy the App ID for a later step.

- Step 10** To add Facebook Login as a new product, under **Product Setup**, click **Get Started** next to the Facebook Login option.
- Facebook Login** is added as a new product and is displayed under **PRODUCTS** in the left navigation pane.
- Step 11** Click **Settings** under **Facebook Login** product, and enter the client OAuth settings.
- Step 12** To configure a private IP address for the Facebook OAuth configuration, enter **http://cmxIP/visitor/login** in the **Valid OAuth redirect URIs** field. By default, the **Valid OAuth redirect URIs** field is empty.

Figure 7: Client OAuth Settings



- Step 13** Click **Save Changes** to save the client authentication settings.
- Step 14** (Optional) To view basic and advanced settings, click **Settings** in the left navigation pane, update the settings, and click **Save Changes**.

Figure 8: Basic Settings

The screenshot shows the Facebook Developer console for an app named "CMX test" with APP ID: 1187736911320805. The left navigation pane includes Dashboard, Settings (Basic and Advanced), Roles, Alerts, App Review, and PRODUCTS (Facebook Login, + Add Product). The main content area displays the following settings:

- App ID:** 1187736911320805
- App Secret:** [Redacted] (Show button)
- Display Name:** CMX test
- Namespace:** [Empty]
- App Domains:** [Empty]
- Contact Email:** ashalathatom@gmail.com
- Privacy Policy URL:** Privacy policy for Login dialog and App Details
- Terms of Service URL:** Terms of Service for Login dialog and App Details
- App Icon:** [Placeholder image, 1024 x 1024]
- Category:** Health & Fitness

At the bottom, there is a "+ Add Platform" button and "Discard" and "Save Changes" buttons. A vertical ID "354143" is visible on the right side.

Figure 9: Advanced Settings

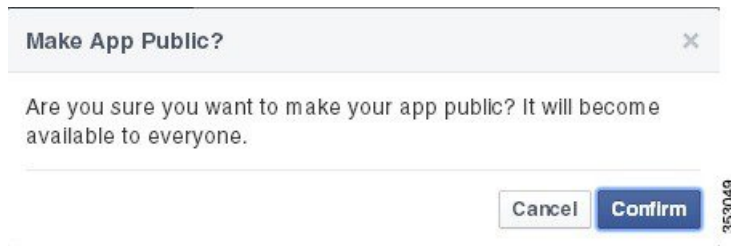
The screenshot shows the Facebook Developer console for the same app, displaying the Advanced Settings. The left navigation pane is the same as in Figure 8. The main content area displays the following settings:

- Native or desktop app?** No. Enable if your app is a native or desktop app.
- App Restrictions:**
 - References Alcohol:** No. Restricts age in some locations (?).
 - Age Restriction:** Anyone (13+)
 - Social Discovery:** Yes. App usage stories can appear in Ticker or News Feed.
 - Country Restricted:** No. Restrict app to users in selected countries.
- Security:**
 - Server IP Whitelist:** [Empty text box]. App requests using the app secret must originate from these IP addresses.
 - Update Settings IP Whitelist:** [Empty text box]. App Settings can only be updated from these IP addresses.

At the bottom, there is a "Delete App" button, a "Notification Email" field, and "Discard" and "Save Changes" buttons. A vertical ID "353060" is visible on the right side.

Step 15 Click **App Review** in the left navigation pane, and click **Yes** in the slider to make the app available to the general public.

Step 16 Click **Confirm**.



- Step 17** If you want to collect information such as first name, last name, friend list, submit those items for approval by Facebook.
- Step 18** Go to the custom portal and click **Create New**, add the App name, paste the App ID information that you generated using the preceding steps.
- Step 19** From the **Scope** drop-down list, choose the scope to collect Social Network data, and then check the **Facebook** checkbox.

Facebook Data Collection

Cisco CMX collects information about Facebook Friends, but the Facebook API only returns the information about friends who also using the same app.


Configuring OAuth with Instagram

Procedure

- Step 1** In the Social Login element of the custom portal, click on the link (🔗) icon to the right of Instagram to go to the associated developer website.
- Step 2** To log in to Instagram, click **Log In** on the top right hand side, then enter username and password and click **Log in**.
- Step 3** In the **Manage Clients** tab, click **Register a New Client**.
- Step 4** Enter the application name and the description.
- Step 5** Enter the same URL as the Wireless LAN Controller (WLC) redirect URL (`http://<CMX>/visitor/login`) in the website field and in the **OAuth redirect_url** field. Check the **Disable Implicit OAuth** check box.
- Step 6** Enter the **Captcha** and click the **Register** button.
- Step 7** Select and copy the Client ID for the next step.
- Step 8** Go to the custom portal and click **Create New**, add the App name, paste the Client ID that you generated using the preceding step.

Configuring OAuth with Foursquare

Procedure

- Step 1** In the Social Login element of the custom portal, click on the link () icon to the right of Foursquare to go to the associated developer website.
- Step 2** Log in to Foursquare by clicking on the My Apps tab at the top right hand side.
- Step 3** Enter your email address and password and click the **LOG IN** button.
- Step 4** Click the **CREATE A NEW APP** button.
- Step 5** Enter the same URL as the Wireless LAN Controller (WLC) redirect URL (`http://<CMX>/visitor/login`) in **Download/welcome page url** field, in the **Your privacy policy url** field, and in the **Redirect URI(s)** field.
- Step 6** Click **SAVE CHANGES**.
- Step 7** Select and copy the Client ID for the next step.
- Step 8** Go to the custom portal and click **Create New**, add the App name, paste the Client ID that you copied using the preceding step.
- Step 9** From the **Scope** drop-down list, choose the scope to collect Social Network data, and then check the checkbox.
-

Connect Settings

To view the **Connect Settings** window, log in to Cisco CMX as an admin user and choose **CONNECT > Settings**.

Connect Settings

The following data retention settings are available:

- **User Retention Period**—This value indicates how long a user entry is retained in data store if the user does not reconnect. The default user retention value is 180 days. The oldest entries are removed if the system has reached the capacity even if the value specified in the User Retention Period is not reached. This is to ensure that the system continues to serve new users.
- **Statistics Retention Period**—Statistics are calculated once every day for each location. The statistics entries, which were calculated before the value that you configured in this text box will be purged. The range is 7 to 1000 days. The default retention value is 365 days.
- **SMS: Number of Devices**—This is the total number of devices that can use a single SMS code. The range is 1 to 10 devices. The default value is three devices.
- **SMS: Time to expire (in min)**—This value indicates how long you want to keep the SMS code active. The range is 3 to 1440 minutes. The default retention value is 15 minutes.

Connect prunes users based on the user retention period. This task is run once every day at three AM server time. If the maximum user capacity is exceeded, older users within the retention period are pruned to make room for new users. To avoid losing any user data, we recommend that you perform the following tasks:

- Periodically export data from Cisco CMX.

- Adjust the retention period based on projected days for full capacity, which is calculated based on usage patterns. The usage patterns are established after the system has been operational for a while.

Changing the 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.

Procedure

-
- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
 - Step 2** Choose **Connect > 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**.
-

Using the CMX Connect Debugging Tools

The CMX Connect debugging tool allows you to delete a client record based on its MAC address.



Note The debugging tools are meant for debugging purpose only.

Procedure

-
- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
 - Step 2** Choose **CONNECT > Settings**.
 - Step 3** Click the **Debugging Tools** tab.
 - Step 4** Under the **Delete User Tool** area, enter the user's MAC address to delete its record based on the MAC address
 - Step 5** Click **Delete User**.
-

Configuring the Property Management System

Use the Connect service in Cisco CMX 10.2.2, to integrate a Property Management System (PMS) solution (for example, a PMS solution used by a hospitality industry).



Note Currently, Cisco CMX Connect integrates only with Unlink Rest Management accounts. Unlink Rest Management is a paid service that customers subscribe to for getting access to the PMS console.

The PMS solution provides customers with the following capabilities:

- Provides guest Wi-Fi portal at a hotel.
- Provides the flexibility to assign different Wi-Fi plans to different portals at different locations.

For example, a hotel can offer a click-through guest portal in common areas such as the lobby and recreational spaces. However, in guest rooms, the portal may require guests to enter their Room Number and Last Name, while the convention area may require guests to enter the Guest Code on the portal to access Wi-Fi. Besides these, guest rooms can also be charged for Wi-Fi usage.

The following are the components of the PMS:



- Client—Client devices (connected and detected) that are being tracked by your Cisco CMX. The clients can be classified as new clients and repeat clients.
 - New Clients—Clients seen by Cisco CMX Connect for the first time.
 - Repeat Clients—Clients that have been tracked by Cisco CMX Connect previously.
- Cisco WLC—Cisco Wireless Controller (Cisco WLC) is responsible for imposing policies.
- Cisco CMX—Cisco CMX helps you create personalized mobile experiences for end users and gain operational efficiency with location-based services. For example, by linking a hotel's property management service with Cisco CMX, the hotel can seamlessly guide guests through the check-in and Wi-Fi login process.
- Cisco CMX AAA Lite—Cisco CMX uses a customized AAA server (named AAA Lite), which enables you to control session duration and bandwidth throttling. CMX AAA Lite is based on the free, open-source FreeRADIUS. Cisco Connect uses FreeRADIUS to support PMS configuration. For example, a hotel may provide different Wi-Fi plans to its customers. Based on the time that a customer is buying the Wi-Fi plan, the AAA server controls the session duration and manages the upload or download speed.
- Nevotek—Cisco CMX uses the Nevotek gateway that helps hotels connect with guests. By linking the hotel's property management service with Cisco CMX, the hotel can seamlessly guide guests through the check-in and Wi-Fi login process. Guests are seamlessly authenticated and provided the correct level of access based on their reservation, preferences, and/or past loyalty history. Using the Nevotek gateway, Cisco CMX can even support different Wi-Fi access levels based on the location within the corresponding hotel, including guest rooms, conference rooms, and public spaces. Resulting charges, if any, are automatically posted to the guests' accounts.

Prerequisites for the Property Management System

Before you begin

- Configure a fully-functional Cisco CMX solution
- Configure fully-functional Cisco WLCs
- Ensure that you have an account with Nevotek and the setup is fully-functional.
- Configure and run FreeRADIUS
- Ensure that you have configured FreeRADIUS on Cisco CMX before configuring PMS.

PMS Policy Enforcement

When you add a PMS server into CMX, the policies defined in the PMS system are imported into CMX.

Location Based and Site Based PMS Policy Enforcement

Based on a user's location or site, Cisco CMX can enforce a policy using AAA. For example, if a user enters a hotel and goes to the lobby area, specific policy can be enforced (the user might receive a certain amount of bandwidth). Similarly, if the user goes to a room, the user might get a different bandwidth because of a different policy that is enforced.

The policy enforcement features perform the following tasks:

- Managing session timeout—If a user has been connected for more than the specific duration within the same day, the user will be disconnected. The session duration is within a day.
- Managing bandwidth—Cisco CMX Controller enforces the bandwidth limit sent from FreeRADIUS server.
- Managing the number of clients—Limit the number of devices connected per account (room number, and last name or passcode).

Configuring the FreeRADIUS on Cisco CMX

Procedure

- Step 1** Use Secure Shell (SSH) to connect to Cisco CMX.
You must have root access credentials to configure the FreeRADIUS in Cisco CMX.
- Step 2** Run the `su -l` command and provide the root password.
- Step 3** Run the `freeradius-conf` command to execute the script to configure the FreeRADIUS in Cisco CMX.
Note that you can run this command from any directory in Cisco CMX. For more information about the FreeRADIUS configuration script, see [Customizing the FreeRADIUS Server, on page 103](#).
- Step 4** Press 1 to configure the FreeRADIUS.
- Step 5** Enter the Cisco CMX UI admin user name and password.
- Step 6** Enter the IP address of the Cisco WLC.

- Step 7** Enter the secret key.
- Step 8** Confirm the entered values.

Customizing the FreeRADIUS Server

To support the AAA functionality, the Cisco CMX Connect service uses a customized version of the FreeRADIUS server. This acts as an agent between Cisco CMX and Cisco WLC by providing policy enforcement. The Cisco CMX Connect service uses the FreeRADIUS server to provide the following functionalities:

- **Session Duration Policy**—A PMS policy with a 60 minute session duration can be enforced using the FreeRADIUS server. The server will disable the connection at the end of 60 minutes.
- **Bandwidth Policy**—A PMS policy with limited upload and download speed can be controlled by the FreeRADIUS server. The bandwidth can be throttled.

You can run the executable shell script to setup the FreeRADIUS.

Using the FreeRADIUS Configuration Script

To configure the FreeRADIUS server to work in your environment, use the executable script. This script allows you to configure the FreeRADIUS server to be used with the Cisco CMX Connect service. You must set up a fully functional Cisco CMX server along with a configured Cisco WLC before running the script.

The following example shows the output of the FreeRADIUS configuration script:

```
[root@cmx-server]# freeradius-conf

*****
** This script will help you configure **
**   FreeRADIUS for CMX Connect   **
*****

1) Configure FreeRADIUS
2) Show FreeRADIUS Config
3) Add CMX Information
4) Add WLC(s)
5) Remove WLC
6) Check FreeRADIUS Status
7) Start FreeRADIUS
8) Stop FreeRADIUS
9) Restart FreeRADIUS
10) Start FreeRADIUS Debug
11) Tail FreeRADIUS Log (Control \) to Exit
12) Quit Config Script

Please choose an option or ENTER for menu :
.
.
.
```

The following table lists the key fields in the FreeRADIUS script output.

Table 9: FreeRADIUS Script Key Fields

Option	Description
Configure FreeRADIUS	Initial configuration option to run the FreeRADIUS. Sets up the environment by adding a Cisco CMX client, and one or more Cisco WLCs and to start the RADIUS server. This option is mandatory for a new installation.
Show FreeRADIUS Config	Displays the FreeRADIUS server's configuration changes.
Add CMX Information	Updates the Cisco CMX configuration information by overwriting the existing configuration.
Add WLC(s)	Sets up additional Cisco WLCs.
Remove WLC	Removes an existing Cisco WLC from the configuration. You must restart the FreeRADIUS server for the changes to take effect.
Check FreeRADIUS Status	Checks the running status of the FreeRADIUS server.
Start FreeRADIUS	Starts the FreeRADIUS server.
Stop FreeRADIUS	Stops the FreeRADIUS server.
Restart FreeRADIUS	Restarts the FreeRADIUS server.
Start FreeRADIUS Debug	Starts the FreeRADIUS server in debugging mode.
Tail FreeRADIUS Log (Control \) to Exit	Displays the running server log to inspect logged issues, if any.
Quit Config Script	Quits the configuration script.

Cisco WLC Configurations

Creating an Access Control List

Procedure

-
- Step 1** Log in to the web UI of a Cisco Wireless Controller (Cisco WLC) that is associated with Cisco CMX.
 - Step 2** Choose **SECURITY > Access Control List > Access Control Lists**.
 - Step 3** In the **Access Control Lists** window, click **New** to add an access control list (ACL).
 - Step 4** In the **Access Access Control Lists > Edit** window, enter a name for the new ACL.
You can enter up to 32 alphanumeric characters.
 - Step 5** Choose the ACL type as either **IPv4** or **IPv6**.
 - Step 6** Click **Apply**.
 - Step 7** In the **Access Control Lists** window, click the name of the new ACL.

- Step 8** In the **Access Control Lists > Edit** window, click **Add New Rule**.
-

Configuring Authentication Server

Procedure

- Step 1** Log in to the web UI of a Cisco Wireless Controller (Cisco WLC) that is associated with Cisco CMX.
- Step 2** Choose **SECURITY > AAA > RADIUS > Authentication**.
- Step 3** Click **New**.
- Step 4** Enter the RADIUS server's IP address, shared secret key.
- To view the added server, choose **WLANS > <WLAN ID> > Security > AAA Servers**. In the AAA Servers window, the newly added server name is displayed in the **Authentication Server** drop-down list.
- Step 5** Click **Apply**.
-

Configuring WLAN

Procedure

- Step 1** Log in to the web UI of a Cisco Wireless Controller (Cisco WLC) that is associated with Cisco CMX.
- Step 2** Click **WLANS** and then choose **Create New** from the drop-down list.
- Step 3** Click **Go** .
The **WLAN > New** window is displayed.
- Step 4** Add profile name and SSID information.
- Step 5** Click **Apply**.
- Step 6** In the **WLANS > Edit** window, click the **Security** tab.
- Step 7** To configure the security settings:
- To configure Layer 2 settings, check the **Mac Filtering** check box.
 - To configure Layer 3 settings, click the **On MAC Filter Failure** radio button so that if Layer 2 fails, a redirection will be made to the server that you specified in the URL field and also specify the IP address of Cisco CMX in the **URL** field.
 - To configure AAA servers settings, specify the IP address and port number of the AAA server that you want to use for authentication.
- Step 8** Choose the **Advanced** tab.
- Select the **Allow AAA Override** check box to enable AAA override.
- Step 9** Click **Apply**.
- Step 10** Click **Save Configuration**.
-

Configuring a PMS User's Account and Wi-Fi Plan

Before you begin

You must have a user account (with a username and password) with Unilink Rest Management to access the PMS console.

Procedure

- Step 1** Log in to the PMS console (that is, the Unilink Rest Management console).
- Step 2** Choose **Configuration > Parameter Maintenance**.
- Step 3** Configure the required parameters.
- Step 4** Choose **Price > Price Plan**.
- Step 5** Click **Add new record**.
- Step 6** Enter the required parameters for the price plan.

The **Free** field should not be left empty. Even if the price plan is free, price value should be entered as 0.00 in the **Free** field.

Note Default price plans should be created according to **Connection Types** using the same page. When Cisco CMX synchronizes with PMS, all price plans created on the PMS are populated on the portal. When configuring the PMS element, the price plans associated with the property are displayed and you can select as per the customer requirement.

Configuring Connect Settings for PMS

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
 - Step 2** Choose **Connect > Settings**.
 - Step 3** Click **PMS**.
 - Step 4** Click the **PMS Account** tab.
 - Step 5** In the **PMS Connect Account** area, enter the following information pertaining to the REST credentials in Nevotek:
 - **Server IP**—Username that is used to access the PMS server.
 - **Username**—Username that is used to access the PMS server.
 - **Password**—Password that is used to access the PMS server.
 - Step 6** Click **Create**.
- Click **Refresh** to enable the Wi-Fi plans that you configured in the PMS to be listed in the **Plans** area of the **Settings** window.

Click **Delete** to delete the pairing between your PMS Connect account and Cisco CMX Connect. If you delete the PMS server information from CMX, the PMS configurations in all the portals will be deleted.

Editing the PMS Connect Settings

You can edit the pairing between your PMS Connect account and Cisco CMX Connect.

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Choose **Connect > Settings**.
- Step 3** Click **PMS**.
- Step 4** Click the **PMS Account** tab.
- Step 5** Click **Edit**.
A dialog box is displayed asking you to confirm the modifications.

Caution Portals will be modified automatically if they offer the plans that are affected by this edit.

Setting Up a Custom Portal for PMS

You can use a PMS template to create a custom portal page for PMS.

Procedure

- Step 1** Log in to Cisco CMX.
- Step 2** Choose **CONNECT > Library**.
- Step 3** Click **Templates**.
- Step 4** Click the **PMS Auth Form** template.

Note All available templates will have the **PMS** element in active state. You can either select the **PMS Auth Form** template or the **PMS** element in any other template to configure PMS.

all templates that are available will have the PMS element in active state

- Step 5** Enter a name for the PMS portal.
 - Step 6** Ensure that your portal has a **Registration Form** element, or add one from the **Content** elements.
 - Step 7** Choose the required PMS Property from the **Select a Property** drop-down list.
The PMS plan types for the selected property is displayed in the **PMS Properties** section.
 - Step 8** Select the required **PMS Plan Types** by checking the appropriate check boxes under **PMS Properties**.
 - Step 9** Click **Save**.
-

Assigning a PMS Portal to Sites or Locations

After you create a PMS portal, you can assign it to a site or location by performing the following steps:

Procedure

- Step 1** Choose **Connect > Connect Experiences**.
- Step 2** In the **Custom Portal** column, from the **Click to assign portal** drop-down list, choose the custom portal that you want to assign to the site.
- Step 3** In the **PMS Property** column, from the **Click to assign property** drop-down list, choose the property to be assigned to the site.
-

Using the Visitors Search to Find PMS Information

You can view PMS-related information pertaining to a client when you perform a Visitors Search in the Cisco CMX Connect Service.

Procedure

- Step 1** Choose **Connect > Dashboard**.
- Step 2** In the **Visitors Search** area, click the **Search** icon.
The following information is displayed in the **Visitors Search** window:
- MAC Address—MAC address of the client device
 - State—Client state, that is Active or Inactive
 - First Login Time—Date and time when the client logged in to Cisco CMX for the first time.
 - Last Login Time— Date and time when the client logged in to Cisco CMX for the last time.
 - Last Accept Time
 - Location/Site
 - Portal
 - Type—Type of the portal
 - Auth Type—Type of the authentication
 - Device
 - Operating System
 - Bytes Received
 - Bytes Sent
 - Social Facebook Name
 - Social Facebook Gender

- Social Facebook Locale
 - Social Facebook Timezone
 - Social Facebook Friends
 - Social Facebook Email
 - Social Foursquare Name
 - Social Foursquare Email
 - Social Instagram Name
 - Social Instagram Email
 - Email
 - Phone Number
 - Gender
 - Username
 - Profile Downloaded
 - Profile Downloaded on
 - Secure Login On
 - PMS Property Name of the Hotel
 - PMS Plan Type
 - PMS Plan
 - PMS Title
 - PMS First Name
 - PMS Last Name
 - PMS Room Number
 - PMS Guest Code
 - PMS User Name
 - PMS Check In Date
 - PMS Check Out Date
-

Configuring Connect Services in Cisco CMX High Availability

Procedure

- Step 1** To create a WLAN for the connect portals, use a Virtual IP address (VIP), for example, `https://<VIP>/visitor/login` Or `http://<VIP>/visitor/login`.
- Step 2** Allow HTTP and HTTPS traffic on the ACL for the VIP.
- Step 3** To configure the Facebook Wi-Fi WLAN, use the VIP, for example, `https://<VIP>/fbwifi/forward`.
- Step 4** To work with policy plan or Property Management System (PMS), create an authentication server for the VIP in Cisco WLC. The "Configuring Authentication Server" section explains how to create authentication server for an IP address (Cisco CMX Primary IP or Virtual IP). For more information, see [Cisco WLC Configurations, on page 104](#).

- Note**
- During a failover or failback event, if new clients or existing clients in an unauthorized state on Cisco WLC tries to connect to WLAN, they will not be redirected to the portal and will not have access to the internet.
 - If the VIP is down, all Virtual IP address will be replaced with the Cisco CMX IP address that is in active state for all the redirect URLs in WLANs, and the authentication server must be changed. The following error message is displayed on the clients if the IP address of Cisco CMX that is not in an active state is given in the redirect URLs of the WLANs:

503 Service Unavailable

No server is available to handle this request
-



CHAPTER 5

The Cisco CMX Presence Analytics Service

- [Overview of the Presence Analytics Service, on page 111](#)
- [Installing the Presence Analytics Service, on page 112](#)
- [Benefits of the Presence Analytics Service, on page 112](#)
- [Initial Configurations, on page 112](#)
- [Presence Analytics Dashboard, on page 113](#)
- [Adding Sites, on page 114](#)
- [Viewing Available Sites, on page 116](#)
- [Editing an Existing Site, on page 116](#)
- [Deleting an Existing Site, on page 116](#)
- [Searching for a Site, on page 117](#)
- [Adding APs, on page 117](#)
- [Deleting an AP, on page 119](#)
- [Viewing Site Details for a Specified Period, on page 119](#)
- [Viewing Device Proximity, Count, and Distribution for a Specific Site, on page 120](#)
- [Emailing a Report, on page 121](#)
- [Printing a Report, on page 121](#)
- [Generating a PDF Report, on page 121](#)
- [Managing Reports, on page 122](#)
- [Specifying Filter Parameters , on page 123](#)
- [Enabling a Global Site, on page 123](#)
- [Creating a Site Group, on page 123](#)
- [Changing the Presence Analytics Theme, on page 124](#)

Overview of the Presence Analytics Service

The Cisco Connected Mobile Experiences (Cisco CMX) Presence Analytics service enables organizations with small deployments, even those with only one or two access points (APs), to use the wireless technology to study customer behavior.

The Cisco CMX Presence Analytics service is a comprehensive analytics and engagement platform that uses APs to detect visitor presence based on their mobile devices' Received Signal Strength Indication (RSSI). The AP detects these client mobile devices irrespective of the latter's wireless association state as long as they are within the specified signal range, and the wireless option is enabled on the mobile device (ability to detect devices wirelessly even if they are not connected to the network).

You can use the **PRESENCE ANALYTICS Dashboard** to view the following key performance indicators (KPIs) of the various client mobile devices at a specific site:

- Visitors
- Average Dwell Time
- Peak Hour
- Passerby-to-visitor conversion rate
- Manufacturers of popular client mobile devices detected by AP

These KPIs can be viewed for any duration (day, week, month, or custom) not exceeding 180 days from the current date. You can also customize the display to show data for a specific day, weekend, or even trends over a month.

Installing the Presence Analytics Service

You cannot run the Presence Analytics and the Location services on the same box. Therefore, you should choose either the Location service or the Presence Analytics service during the initial installation.

Benefits of the Presence Analytics Service

- Enables organizations with small deployments, even those with just one or two APs, to understand customer behavior.
- Enhances on-site customer experience through insights into their mobile behavior across locations.
- Measures customer engagement and loyalty across sites through location statistics.
- Compares visitor trends between sites to gauge the effect of marketing actions.

Initial Configurations

In order to use the Cisco CMX Presence Analytics service, choose the **Presence** option when you install Cisco MSE Virtual Appliance. For more information, see the “Installing a Cisco MSE Virtual Appliance” section in the *Cisco MSE Virtual Appliance Installation Guide* for this release at: <http://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/products-installation-and-configuration-guides-list.html>. After installation, perform the following operations:

- Add Controllers.
- Add sites.
- Add APs.

Presence Analytics Dashboard

The Presence Analytics Dashboard contains the following charts:

Table 10: Presence Analytics Charts

Chart	Description
Insights	Shows key insights for a week and month, including busiest days, busiest hours, peak days, and peak counts. Note Insight data allows comparison of current site metrics in comparison to the previous week and month. It is computed daily for all sites during aggregation.
Proximity	Shows information such as those pertaining to passersby, visitors, and connected devices, by hour (if it is a single day or last 3 days), or by day, for the given site.
Proximity Distribution	Shows information such as those pertaining to passers-by or visitors, and connected percentages for a given site for a given duration.
Dwell Time	Shows the visitor dwell levels by hour or by day. You can see the following dwell levels: 5-30 mins—Visitors who spent 5-30 mins in the site. 30-60 mins—Visitors who spent 30-60 mins in the site. 1-5 hours—Visitors who spent 1-5 hours in the site. 5-8 hours—Visitors who spent 5-8 hours in the site. 8+ hours—Visitors who spent more than 8 hours in the site.
Dwell Time Distribution	Shows visitor dwell-level percentages for a given site for a given duration.

Chart	Description
Repeat Visitors	Shows repeat visitors by hour or by day. You can see the following repeat visitor categories: Daily—Visitors who visited the selected site at least 5 days in the last 7 days. Weekly—Visitors who visited the selected site at least on 2 different weeks over the last 4 weeks. First Time—Visitors who visited the selected site for the first time. Occasional—Visitors who are not daily, weekly, or first-time visitors. Yesterday—Visitors who visited the site the previous day.
Repeat Visitors Distribution	Shows the repeat visitor distribution percentage.

Adding Sites

You can add new sites individually, or upload a .CSV list of sites to add sites in bulk.

You can add new sites using one of the following methods:

- Add sites individually. For more information, see [Adding Sites Individually, on page 114](#).
- Add sites in bulk. For more information, see [Adding Sites in Bulk, on page 115](#).
- Create sites from APs. This allows administrator to create sites by filtering APs by name and adding them directly to a new site. For more information, see [Adding an AP to a Site, on page 117](#).

Adding Sites Individually

To add a site individually, perform the following task:

Procedure

-
- Step 1** Log in to Cisco CMX.
 - Step 2** Choose **PRESENCE ANALYTICS > Manage**.
 - Step 3** Click the **Sites** tab.
 - Step 4** Click **Add Site**.
 - Step 5** In the **Name** field, enter the name of the site.
 - Step 6** In the **Address** field, enter the address of the site.
 - Step 7** Configure the **Signal Strength Threshold** to determine whether a client device is in the site or is just a passer-by. You can move the circular blue buttons to specify the Visitor Signal Threshold and Ignore Signal

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

Note The lower RSSI threshold is bounded to -95 dBm to -45 dBm and the higher threshold is bounded to -90dBm to -40 dBm.

The difference between the two threshold must not be less than 5.

The minimum dwell time is bound to 0 to 20

- Clients with RSSI below the low threshold (-95 dBm default) are discarded.
- Clients with RSSI above the low threshold are classified as “passer-by”. The RSSI threshold range for passer-by clients is between -95dBm and -75 dBm.
- Clients with RSSI above high threshold over x minutes (default 5) in past 20 minutes are classified as visitors.
- Clients associated with AP in a site are classified as connected clients at the site.

Step 8 In the **Configure the Minimum Dwell Time For Visitor (minutes)** field, specify the minimum dwell time for visitors. The minimum dwell time for visitors is 20 minutes.

Step 9 Click **Save**.

Adding Sites in Bulk

Procedure

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

Step 2 Choose **PRESENCE ANALYTICS > Manage**.

Step 3 Click **Import**.

Step 4 Under **Sites**, click **Browse**.

The **File Upload** dialog box is displayed.

Note The file that you upload for importing site information must be in .csv format.

Step 5 Navigate to the location of the CSV file that contains the list of sites you wish to upload, select the CSV file, and click **Open**. To import the site details correctly, store them in the following order and format: *Site Name, Address, RSSI High Threshold, RSSI Low Threshold, Dwell Time in Minutes, Timezone*. For example, *Test Site, 123 Main Street City CA US, -65, -95, 5 US/Pacific*.

Step 6 Click **Import**.

A set of new sites is created and added to the table of sites under **PRESENCE ANALYTICS > Manage**.

Viewing Available Sites

Procedure

- Step 1** Log in to Cisco CMX.
 - Step 2** Choose **PRESENCE ANALYTICS > Manage**.
 - Step 3** Under the **Sites** tab, you can view a list of available sites in a tabular format, sorted alphabetically by site name. You can customize your view of the Sites table by sorting according to **Location**, **Timezone**, or **AP count**.
-

Editing an Existing Site

Procedure

- Step 1** Log in to Cisco CMX.
 - Step 2** Choose **PRESENCE ANALYTICS > Manage**.
 - Step 3** Under **Sites**, click the name of the corresponding site listed in the table of available sites.
The dialog box is displayed.
 - Step 4** Edit the site **Name**, site **Address**, **Signal Strength Threshold** limits, or the **Minimum Dwell Time for Visitor**.
 - Step 5** Click **Save**.
-

Deleting an Existing Site

Procedure

- Step 1** Log in to Cisco CMX.
- Step 2** Choose **PRESENCE ANALYTICS > Manage**.
- Step 3** Under **Sites**, check the check box of the site that you want to delete.
- Step 4** Click **Delete**.
You will receive a confirmation dialog box when you try to delete a site. Click **OK** to confirm the delete action.

Note If you want to delete all available sites simultaneously, select the check box in the header row, and then click **Delete**.

Searching for a Site

Procedure

- Step 1** Log in to Cisco CMX.
- Step 2** Choose **PRESENCE ANALYTICS > Manage > Sites**.
- Step 3** In the **Search** field on the top right-corner of the window, enter the site's name, and press the **Return** key. If the specified site has already been added to **PRESENCE ANALYTICS**, it is displayed in the search results.
-

Adding APs

You can add new APs individually or by uploading a .CSV list of APs to add them in bulk.

You can add new APs, with or without maps, using one of the following methods:

- Add APs individually—Add individual APs to specific sites. For more information, see [Adding an AP to a Site, on page 117](#).
- Add APs in bulk—Add multiple APs at one go by importing a list of APs in .CSV format. For more information, see [Adding APs in Bulk, on page 118](#).

Adding an AP to a Site



Note If you do not see the AP list, you should update the community string of the WLC using the **System > Settings** window. The AP information is retrieved from the WLC using SNMP.

Procedure

- Step 1** Log in to Cisco CMX.
- Step 2** To add an AP to a site individually:
- a) Choose **PRESENCE ANALYTICS > Manage > Sites**.
 - b) In the table of available sites, click the name of the site to which you want to associate the new AP.
 - c) Click the **Details** icon next to **AP count**.
- A list of available APs is displayed in a tabular format.

- d) Enter the MAC address of the AP you want to add and associate to the specified site.
- e) Click **Add**.

The specified AP is added and associated to the specified site.

Step 3 To add one or more APs to a site:

- a) Choose **PRESENCE ANALYTICS > Manage > Access Points**.
- b) From the **APs by Controller** drop-down list, select the APs that you want to add to a site.

You can use the **Ctrl+a** or **Command+a** keys to select all sites from drop-down list.

- c) After selecting the APs, click **Close**.

The count of the APs you selected from the available APs is shown in the drop-down list, for example, 8 of 160 selected.

- d) Click **Add to Site**.
- e) Select the site to which you want to add the selected APs.
- f) Click **Add**.

The selected APs are added and associated to the specified site.

To create a site from this page, click **Create Site**.

Step 4 Under **Controller AP list**, click **Download CSV** to download the .CSV file, add the missing site names for APs, and import the file again from the Import tab.

CSV Format: Radio MAC Address,Ethernet MAC Address,Name,Site Name,Site Address

Example: aa:bb:cc:dd:ee:ff,bb:cc:dd:ee:ff:11,AP-1,Site-1,123 Main St City CA US

Adding APs in Bulk

To add APs to a site in bulk:

Procedure

Step 1 Log in to Cisco CMX.

Step 2 Choose **PRESENCE ANALYTICS > Manage > Import**.

Step 3 Under **APs**, click **Browse**.

The **File Upload** dialog box is displayed.

Step 4 Navigate to the location of the .CSV file that contains the list of APs you want to upload, select the .CSV file, and click **Open**.

To import the AP details correctly, store them in the following order and format: *Radio MAC Address, Ethernet MAC Address, Name, Site Name, Site Address*, for example, *aa:bb:cc:dd:ee:ff,bb:cc:dd:ee:ff:11,AP-1,Site-1,123 Main St City CA US*

Step 5 Click **Import**.

A set of new APs is created and added.

Deleting an AP

Procedure

- Step 1** Log in to Cisco CMX.
- Step 2** Choose **PRESENCE ANALYTICS > Manage > Sites**.
- Step 3** In the table of available sites, click the name of the site from which you want to delete and unassociate the corresponding AP.
- The dialog box is displayed.
- Step 4** Click the **Details** icon next to **AP count**.
- A list of available APs is displayed in a tabular format.
- Step 5** Click the **Delete** icon next to the AP that you wish to delete.
-

Viewing Site Details for a Specified Period

Procedure

- Step 1** Log in to Cisco CMX.
- Step 2** Click **PRESENCE ANALYTICS**.
- Step 3** Select a site from the **SITE** drop-down list.
- Step 4** Select a duration from the **DATE** drop-down list. You can choose from the following options:
- **Today**
 - **Yesterday**
 - **Last 3 Days**
 - **Last 7 Days**
 - **Last 30 Days**
 - **This Month**
 - **Last Month**
 - **Custom**—Specify a date range and click **Change**. You can either manually enter the dates in the **FROM** and **TO** fields in yyyy-mm-dd format, or select the dates from the respective calendars. These calendars

are displayed when you select **Custom** or click the **FROM** or **TO** fields. The window is refreshed to show the site KPIs based on your selection.

Note You can choose a single day by selecting the same date in both the **FROM** and the **TO** fields.

Viewing KPI Summary

You can click any of the following KPI buttons that appear at the top of the window to view further details about a visitor's behavior at the site:

- **Visitors**—Clients associated with AP in a site are classified as visitors at the site.
- **Average Dwell Time**—Average dwell time or a wait time of all the visitors in a location.
- **Peak Hour**—The hour at which maximum number visitors are found in a location.
- **Conversion Rate**—Conversion rate is a percentage of passersby who are converted to visitors and is computed as $\text{visitors} / (\text{visitors} + \text{passersby}) \times 100$.
- **Top Device Maker**—Manufacturer of popular client mobile devices detected by AP

Viewing Device Proximity, Count, and Distribution for a Specific Site

Procedure

Step 1 Log in to Cisco CMX.

Step 2 Click **PRESENCE ANALYTICS**.

Step 3 Select a site from the **SITE** drop-down list.

Step 4 Select or specify a duration from the **DATE** drop-down list.

The window is refreshed to show the site details based on your selection.

Step 5 Click the corresponding elements within the **Proximity** or **Proximity Duration** chart to view hourly breakdown of passersby, visitors, and connected devices for the selected site during the specified duration.

Note If the duration selected in **Step 4** exceeds one day, clicking the elements in the **Proximity** chart will display the details for the selected site for the specific date.

Emailing a Report

Procedure

- Step 1** Log in to Cisco CMX.
- Step 2** Click **PRESENCE ANALYTICS**.
- Step 3** Click the **Email** icon.
- Step 4** Enter the email address of a recipient.
- Step 5** Enter notes, if any.
- Step 6** Click **Send**.

If you want to send this email later, check the **Schedule** check box and enter Schedule parameters such as **Start From** (date and time) and **Frequency** (**Daily** or **Weekly**), and then click **Schedule**.

Printing a Report

Procedure

- Step 1** Log in to Cisco CMX.
 - Step 2** Click **PRESENCE ANALYTICS**.
 - Step 3** Click the **Printer** icon.
 - Step 4** Specify the printer settings.
 - Step 5** Click **OK**.
-

Generating a PDF Report



Note You can customize the logo on the PDF reports. To view an archived report, choose **PRESENCE ANALYTICS** > **Manage** > **Reports**.

Procedure

- Step 1** Log in to Cisco CMX.
- Step 2** Click **PRESENCE ANALYTICS**.

- Step 3** Click the **PDF Report** icon.
- Step 4** Enter notes for the PDF report, if any.
- Step 5** Enter the email address (optional) of the recipient. If there are multiple recipients for the report, separate the email addresses using a comma.
- Step 6** Click **Submit**.

If you want to schedule the PDF report to a future date, check the **Schedule** check box and enter the Schedule parameters such as **Start From** (date and time) and **Frequency (Daily or Weekly)**, and then click **Schedule**.

Managing Reports

The **Presence Analytics** service enables you to manage the scheduled and generated reports. In addition, you can customize the logo that appears on the generated PDF reports.

The **Reports** window contains the following areas:

- **Report Logo**—Enables you to upload an image file that you can use as a logo for your PDF report.
- **Scheduled Reports**—Enables you to modify or delete a report that is already scheduled (email or PDF).
- **Generated PDF Reports**—Enables you to download or delete a generated PDF report.

Procedure

- To upload a logo for your report, perform the following steps:
 - a) Log in to Cisco CMX.
 - b) Click **PRESENCE ANALYTICS > Manage**.
 - c) Click **Reports**.
 - d) In the **Report Logo** area, click **Browse** and then choose the image file that you want upload as the report logo.
 - e) Click **Upload**.
- To edit or delete a scheduled report, perform the following steps:
 - a) Log in to Cisco CMX.
 - b) Click **PRESENCE ANALYTICS > Manage**.
 - c) Click **Reports**.
 - d) In the **Scheduled Reports** area, under the **Link** column, click either **Edit** or **Delete**.

If you choose to edit a scheduled report, the existing schedule details are displayed in the **EDIT SCHEDULED REPORT** window, where you can make the necessary changes.

- To download or delete a generated PDF report, perform the following steps:
 - a) Log in to Cisco CMX.
 - b) Click **PRESENCE ANALYTICS > Manage**.
 - c) Click **Reports**.
 - d) In the **Generated Reports** area, under the **Link** column, click either **Download** or **Delete**.

Specifying Filter Parameters

The **Filter Parameters** tab allows you to exclude data from a specific SSID, MAC address, or defined duration.

Procedure

- Step 1** Log in to Cisco CMX.
 - Step 2** Choose **PRESENCE ANALYTICS > Manage > Filters**.
 - Step 3** Check the **Enable Exclusion Filters** check box to exclude data.
 - Step 4** Click **Save**.
-

Enabling a Global Site

Enabling a Global site combines all the existing data from all the individual sites into a single large site so that you can view the data for all the sites at once. You must provide a time zone for the global site, which will override all individual site time zones. All the analysis will be in context of the time zone defined for the global site.

Procedure

- Step 1** Log in to Cisco CMX.
 - Step 2** Choose **PRESENCE ANALYTICS > Manage > Global Sites**.
 - Step 3** Check the **Enable Global Site** check box.
 - Step 4** Specify **Site Name, Address, and Time Zone**.
 - Step 5** Click **Save**.
-

Creating a Site Group

Site groups allow you to combine information from multiple sites for analysis, for example, all the sites in the same time zone.

Procedure

- Step 1** Log in to Cisco CMX.
- Step 2** Choose **PRESENCE ANALYTICS > Manage > Site Groups**.
- Step 3** Click **Create Group**.
- Step 4** Specify **Group Name, Address, Timezone, and Sites**.

Step 5 Click **Save**.

Changing the Presence Analytics Theme

Procedure

- Step 1** Log in to Cisco CMX.
 - Step 2** Click **PRESENCE ANALYTICS**.
 - Step 3** Click the **Themes** icon.
 - Step 4** Choose your desired theme.
-



CHAPTER 6

Managing Cisco CMX Configuration

- [Overview of the Manage Service, on page 125](#)
- [Managing Perimeters and Zones on Location Maps, on page 126](#)
- [Managing Licenses, on page 131](#)
- [Managing Users, on page 134](#)
- [Managing Notifications from Applications, on page 136](#)
- [Managing Cisco CMX Cloud Apps, on page 145](#)
- [Setting Up Outbound Proxy, on page 148](#)
- [Managing Verticalization, on page 149](#)

Overview of the Manage Service

The Cisco Connected Mobile Experiences (Cisco CMX) **MANAGE** service comprises the following tabs, which help you perform a variety of tasks to effectively manage the Cisco CMX configuration, including, but not restricted to those listed here:

- **Locations**—Enables you to manage and add location zones and tags. For more information, see [Managing Perimeters and Zones on Location Maps, on page 126](#).
- **Licenses**—Enables you to manage and add licenses. For more information, see [Managing Licenses, on page 131](#).
- **Users**—Enables you to manage and add users. For more information, see [Managing Users, on page 134](#).
- **Notifications**—Enables you to manage and add email and HTTP notifications. For more information, see [Managing Notifications from Applications, on page 136](#).
- **Cloud Apps**—Enables you to manage Cisco CMX Cloud service. For more information, see [Managing Cisco CMX Cloud Apps, on page 145](#).
- **Verticalization**—Enables you to generate vertical specific reports. For more information, see [Managing Verticalization, on page 149](#).



Note All the Manage service tasks can be performed only by users with corresponding user roles. For information on user roles, see [User Roles, on page 134](#).

Managing Perimeters and Zones on Location Maps

A perimeter is an all-inclusive zone where clients are always inside of this. The individual zones are inside the perimeter.



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

Viewing Campus, Building, Floor, and Zone Details

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **MANAGE > Locations**.
- Step 3** In the left pane of the window that is displayed, click **Campus, Building, Floor, or Zone** depending on the area you want to view.
Items corresponding to the area selected are displayed as boxes.
- Step 4** Click the curved arrow at the top-right corner of each item box to view details pertaining to that item.
This opens the **Zone Editor** map view, displaying a floor map.

Note The curved arrow at the top-right corner of a floor box is called the **Go to map view** arrow. This arrow is available on the box of items at any level. For example, for a building, this opens the first floor. For a campus, this opens the first floor of the first building. You can then switch to other buildings and floors in that campus.

Managing Tags

You can add tags to a campus, building, floor, or zone.

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **MANAGE > Locations**.
- Step 3** From the right panel, choose the item for which you want to add the tag.
- Step 4** Click the **Tag** icon at the top-right corner of the window.
The **Location Tag Manager** window is displayed with available tags.
- Step 5** In the **Create New Tag** field, enter a new name for the tag and press **Enter**.

- Step 6** (Optionally) Click on any existing tag to see all the geo items that are tagged against it.
-

Creating an Inclusion or 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.

Procedure

- 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. If you already have an inclusion region, creating a new inclusion region will overwrite the existing region.
 - 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.
-

Creating a Perimeter

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **MANAGE > Locations**.
- Step 3** In the left pane of the window that is displayed, click **Zone**.
- The zone is used for the analytics purpose.
- The **Zone Item** boxes are displayed.


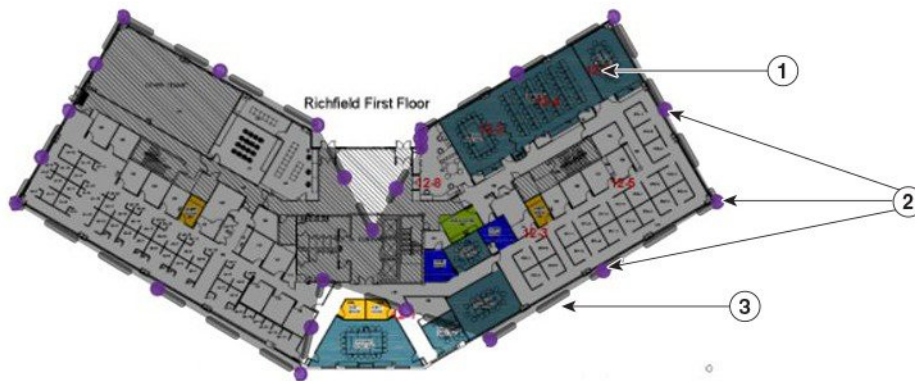
- Step 4** Click the Subzone in the corresponding zone.
- Step 5** In the **Zone Editor** window, click the **CREATE A PERIMETER**  icon. The cursor changes to a drawing tool.
- Step 6** Click each point that you want to designate as a vertex of the perimeter. Double-click the last vertex point to complete marking the vertices of the perimeter and closing the perimeter. When you double-click the last vertex point, the **CREATE A PERIMETER** dialog box opens.
- Step 7** Click **Add** to add this perimeter to the floor.

Figure 10: A Perimeter and its Vertices




353989


1	Dark gray area indicating an area encircled by the perimeter.	3	Dark gray bar indicating the perimeter.
2	Purple indicating vertices of the perimeter.		

Deleting a Perimeter

Procedure


- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **MANAGE > Locations**.
- Step 3** In the left pane of the window that is displayed, click **Zone**. The **Zone Item** boxes are displayed.
- Step 4** Click the Subzone in the corresponding zone.
- Step 5** In the **Zone Editor** window, click the **Edit Perimeter**  icon.
- Step 6** Click inside the perimeter to be deleted.

The perimeter will be highlighted in gray.

- Step 7** Click the **Trash**  icon.
- Step 8** In the **DELETE PERIMETER** confirmation dialog box, click **Confirm** to delete the perimeter.
-


Editing a Perimeter

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **MANAGE > Locations**.
- Step 3** In the left pane of the window that is displayed, click **Zone**.
The **Zone Item** boxes are displayed.
- Step 4** Click the Subzone in the corresponding zone.
- Step 5** In the **Zone Editor** window, click the **Edit Perimeter**  icon.
- Step 6** Click inside the perimeter that is to be edited.
The perimeter will be highlighted in gray and the vertices in purple.
- Step 7** Drag the purple vertices to modify the shape of the perimeter.
- Step 8** After you have the required shape, click outside the perimeter. This saves the new shape.
-

Creating a Zone

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **MANAGE > Locations**.
- Step 3** In the left pane of the window that is displayed, click **Zone**.
The **Zone Item** boxes are displayed.
- Step 4** Click the Subzone in the corresponding zone.
- Step 5** In the **Zone Editor** window, click the **Draw Polygon Zone**  icon.
The cursor will change to a drawing tool.
- Step 6** Click each point that you want to designate as a vertex of the perimeter. Double-click the last vertex point to complete marking the vertices of the perimeter and for closing the perimeter see the figure below.
When you double-click the last vertex point, the **CREATE A NEW ZONE** dialog box is displayed.
- Step 7** Click **Add** to add this zone to the corresponding floor.
An Item pane pertaining to this zone is displayed on the right side of the window. You can add existing tags from the drop-down list, or add a new tag.

Note Zones cannot be outside the floor map and they cannot overlap. Overlapping zones can be created using Cisco Prime Infrastructure.

Figure 11: A Zone and its Vertices




353988

1	A zone named Lab.	3	Purple indicating vertices of the zone.
2	Gray bar indicating the perimeter.	4	Other zones on the map.




Deleting a Zone

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **MANAGE > Locations**.
- Step 3** In the left pane of the window that is displayed, navigate to the zone that you want to delete.
- Step 4** Click the **Trash**  icon.
The **DELETE ZONE** confirmation dialog box is displayed.
- Step 5** Click **Confirm**.

Editing a Zone

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **MANAGE > Locations**.
- Step 3** In the left pane of the window that is displayed, click **Zone**. The **Zone Item** boxes are displayed.
- Step 4** Click the Subzone in the corresponding zone.
- Step 5** In the **Zone Editor** window, click the **Gear**  icon to view the zone editing options.
- Step 6** To change the shape of the zone, use the **Pencil**  icon to reshape the zone by moving the vertices. The **DELETE ZONE** confirmation dialog box is displayed.
- Step 7** To move the zone, use the drag tool, denoted by the **Hand**  icon, to drag the zone around. Click the **Hand** icon, move the cursor to the center of the zone, where it will change to an **Arrow** icon. You can then drag the zone.
- Step 8** Click outside the zone to save your changes.

Note Zones cannot be outside the floor map and they cannot overlap. Overlapping zones can be created using Cisco Prime Infrastructure.

Managing Licenses

To view the list of licenses that your Cisco Connected Mobile Experiences (Cisco CMX) system has, log in to Cisco CMX and choose **MANAGE > Licenses**. The list of licenses is displayed in the **Licenses** window.

Figure 12: Licenses Window

The screenshot shows the Cisco CMX Licenses window. At the top, there is a navigation bar with icons for DETECT & LOCATE, ANALYTICS, CONNECT & ENGAGE, MANAGE, and SYSTEM. Below this is a sub-navigation bar with 'Licenses' selected. The main content area is titled 'Licenses' and contains two tables.

License Type	License Class	Total AP Licenses	Total APs Installed	Compliance
CMX Base	Evaluation	200	1079	45 days remaining
CMX Advanced	Evaluation	200	1079	45 days remaining

Below the first table is a 'Hide Installed Licenses -' button. The second table is titled 'License Files' and has the following data:

License Name	CMX Base (APs)	CMX Advanced (APs)	Install Date	Expiry Date
MSE201611211436043950.lic	100	100	November 30, 2016	
internal-base-eval	100	0	July 29, 2016	
internal-cmx-eval	0	100	July 29, 2016	

At the bottom of the 'License Files' table, there are checkboxes for 'Evaluation' and 'Permanent'.

Cisco CMX has the three license models:

- **CMX Default**—Includes access to **Cloud Apps** (for enabling connection to Cloud applications) and **License** (for Base or Advanced License installation) features, **MANAGE** and **SYSTEM** services, and sending Northbound notifications.
- **CMX Base License**—Includes RSSI Location Calculation, GUI access to **DETECT**, **MANAGE**, **SYSTEM** services.
- **CMX Advanced**—Includes CMX Base features and Angle of arrival, **CONNECT**, **PRESENCE ANALYTICS**, and **LOCATION ANALYTICS** services, access to partner stream, and access to Cisco CMX complete user interface.



Note The Cisco CMX Base License no longer provides access to Cisco CMX Hyperlocation or Partner Stream. The Cisco CMX Advanced License is required to access these services. Cisco CMX Hyperlocation, Cisco CMX Connect, Cisco CMX Advance Location services migrated from CMX Base License to CMX Advance license will continue to work after upgrade from CMX 10.3.x release. However, an alert is generated every 24 hours for license upgrade. Any new Cisco CMX installation will require a CMX Advance license.

For information about the licenses required to operate Cisco CMX, see the [Cisco CMX 10 Ordering and Licensing Guide](#).



Note Cisco CMX comes with a 120-day full-functionality evaluation license. All the access points (APs) connected to Cisco CMX must be licensed.

Cisco CMX Release 10.3 supports High Availability. For more information, see [Enabling High Availability for Cisco CMX, on page 166](#).

CMX Evaluation licenses are not synchronized between Cisco CMX High Availability (HA) pairs. Once the evaluation license expires on the primary server, Cisco CMX HA will not invoke failover to the secondary server. You must add a permanent license to make the HA setup functional.

Cisco CMX permanent licenses will be synchronized between the primary and secondary servers in the CMX HA pair. You need not upload the permanent licenses on the secondary server.

Add a License

Procedure

-
- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **MANAGE > Licenses**.
- Step 3** Click **Add License**.
The **TERMS AND CONDITIONS** dialog box is displayed.
- Step 4** To accept the terms and conditions, enter your name, and then click **Accept & Continue**.
When you accept and proceed to install a certificate, a dialog box is displayed with the message indicating that you can use only the Analytics or Location features.
The **UPLOAD LICENSE** dialog box is displayed.
- Step 5** Click **Browse** to select the corresponding license file, and then click **Upload**. Ensure to select a license file with the .LIC extension.
- Note** Cisco CMX uses a license file with .LIC extension. This file is obtained when an order is placed for any of the Cisco CMX per Access Point SKUs, for example, L-AD-LS-1AP-N - CMX Advanced license for one access point.
The file is available as part of your licensing PAK and will be attached to an email from licensing. Extract the .LIC file to your system and upload to Cisco CMX when adding a new license.
- Step 6** In the **Licenses** window, click **See Installed Licenses** to view the list of installed licenses. You can view the **License Name**, **CMX Base (APs)**, **CMX Advanced (APs)**, **Install Date**, and **Expiry Date** for the installed licenses.
-

Deleting a License

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **MANAGE > Licenses**.
- Step 3** In the **Licenses** window, click **See Installed Licenses** to view the list of installed licenses.
- Step 4** In the **Action** column adjacent the license you want to delete, click **Delete**. The **DELETE LICENSE** dialog box is displayed.
- Step 5** Click **Delete License** to proceed with the deletion.
-

Managing Users

Cisco Connected Mobile Experiences (Cisco CMX) is shipped with a default admin user account and password. An admin user can add, edit, and delete other users.

Adding a User

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **MANAGE > Users**.
The **Users** window, where all the current users are listed, is displayed.
- Step 3** Click **+ New User** at the bottom of the table.
The **ADD NEW USER** dialog box is displayed.
- Step 4** Enter the details and select one or more roles for the user from the **Roles** drop-down list.
For information about the roles available for selection, see [User Roles, on page 134](#).
- Note** The password for the new user must be minimum of eight characters.
- Step 5** Click **Submit**.
-

User Roles

Your Cisco Connected Mobile Experiences (Cisco CMX) system comes with the following services, depending on whether or not you have the license for that service:

- **SYSTEM** service (included with Cisco CMX base license)
- **MANAGE** service (included with Cisco CMX base license)

- **DETECT & LOCATE** service (included with Cisco CMX base license)
- **CONNECT** service (included with Cisco CMX base license)
- **ANALYTICS** service (provided only with Cisco CMX advanced license; not included with Cisco CMX base license)

When setting up users in Cisco CMX, you can select one or more roles for each user. Each role provides access privileges to one or more services, provided your license includes those services.

See the table below for a description of the access privileges associated with each role.

Table 11: User Roles and Associated Access Privileges

Role	Allows
Admin	Read/Write access to all the services
System	Read/Write access to the service
Manage	Read/Write access to the service
Location	Read/Write access to the service
Analytics	Read/Write access to the service
Connect	Read/Write access to the service
Connect Experiences	<ul style="list-style-type: none"> • Read/Write access to Connect Experiences in the CONNECT & ENGAGE service • Read-only access to all the settings in the CONNECT & ENGAGE service • No access to the Dashboard in the CONNECT & ENGAGE service
Read Only	Read-only access to all the services



Note

- A user can be allocated the System, Manage, Location, Analytics, and Connect roles. This allows the user to function like an admin user. Such nonadmin users can be deleted by admin users, but not vice-versa.
- Only an admin user can delete another admin user.
- An admin or Connect user has both read/write access to the Policy Plans. However, Connect Experience users only have Read access to the Policy plans page.

Changing the Default Admin Password

Procedure

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

- Step 2** Choose **MANAGE > Users**.
The **Users** window, where new users can be added and the roles of existing users modified, is displayed.
- Step 3** Click **Edit** in the **Actions** column adjacent the admin user.
This opens the **EDIT USER** dialog box for that admin user.
- Step 4** Change the default factory-shipped admin password.
- Step 5** Click **Submit**.
-

Editing User Information

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **MANAGE > Users**.
The **Users** window, where all the current users are listed, is displayed.
- Step 3** Click **Edit** in the **Actions** column adjacent the user whose details you want to edit.
The **EDIT USER** dialog box is displayed.
- Step 4** Edit the details of the user. Note that the username cannot be edited.
For information about user roles, see [User Roles, on page 134](#).
- Step 5** Click **Submit**.
-

Deleting a User

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **MANAGE > Users**.
- Step 3** Click **Delete** in the **Actions** column adjacent the user whose details you want to delete.
The **DELETE USER** confirmation dialog box is displayed.
- Step 4** Click **Delete User** to proceed with the deletion.
-

Managing Notifications from Applications

You can set up notifications for your own applications and for third-party applications. The Notifications feature supports the following:

- HTTP receiver
- MAC address scrambling, which is enabled by default

- Two message formats, JSON and XML
- Alerts
- Network configuration change notification
- REST notification over HTTPS

The following sections describe the notifications-related tasks that you can perform:

Create a New Notification

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **MANAGE > Notifications**.
The **Notifications** window is displayed.
- Step 3** Click **New Notification**.
The **CREATE NEW NOTIFICATION** dialog box is displayed.

Figure 13: Create New Notification

CREATE NEW NOTIFICATION

Name

Type Chokepoint ▾

Conditions ChokepointMac

MacAddress

Receiver http ▾

: /

HTTP Headers Key : Value +

MAC Hashing ON **Message Format** JSON ▾

Hash Key

Cancel
Create

355286

Step 4 Enter the following parameters to configure the new notification:

- **Name**—Enter a name for the new notification name.
- **Type**—From the **Type** drop-down list, choose the notification type.

For a description of the available notification types, see the table below. When specifying the details, note that:

- If a location hierarchy is selected, the hierarchy will be the specific area filter for that notification.
- If a MAC address is entered, the MAC address will be a filter for that notification.

Table 12: Notification Types

Notification Type	Used for
Association	Generating a notification when a client is associated or unassociated.
Absence	Generating a notification when a client is undetected for more than 15 minutes.

Notification Type	Used for
Location Update	Generating a notification when a device's location is being recalculated. The Location Update notification is based on the RSSI from the different APs that detect the device.
In/Out	Generating a notification when a device is detected as moving into or moving out of a specific area in the location hierarchy.
Movement	Generating a notification when a device moves more than a specified distance.
Area Change	Generating a notification when a device changes its location between campuses, buildings, or floors.
Network Configuration Change	Generating a notification when maps are changed.
REST Notification over HTTPS	Enabling REST notification over HTTPS.
Passerby Detected	Generating a notification when a client is detected as a passer-by client.
Passerby Became Visitor	Generating a notification when a client becomes a visitor.
Visitor Went Away	Generating a notification when a client is no longer a visitor for the current site.
Site Entry Changed	Generating a notification when a client has moved out of the current site.

- **Conditions**—Depending on the notification type selected, the **Conditions** parameters are displayed. Enter the required conditions for the new notification.

- Note**
- For some notification types such as **Association**, **Absence**, and so on, you must provide **Device Type** as a condition parameter. The **Device Type** field on the **Create New Notification** window provides these options: **All**, **RFID Tag**, **Client**, **BLE Tag**, and **Interferer**. For notification types **Area Change**, **In/Out**, **Location Update**, and **Movement**, the **Device Type** condition has the following additional options: **Rogue Client** and **Rogue AP**.
 - For the **In/Out** notification type, 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*.
 - For the **Location Update**, **In/Out**, and **Movement** notification type, choose the device status from the **Status** drop-down list. The association status for the client device are **All**, **Probing Only**, and **Associated**. This condition helps to filter the clients by their association status and sends notifications only for the filtered subset of client devices.
 - For the **Location Update** notification, Cisco CMX provides a new **Status** option for the **Client** device type. Use this option to filter notifications to either associated or probing devices. If the **Status** option is not selected, the default option (**All**) is considered, and then notifications are sent for both associated and probing clients.
 - To view In/Out notification details for all locations, we recommend that you configure separate In/Out notifications for each hierarchy created in the **Activity Map** window.
- **MacAddress**—Enter the MAC address. The default is **all**.
 - **Receiver**—From the **Receiver** drop-down list, choose the receiver type as **HTTP**, **HTTPS**, or **Email**. For HTTP and HTTPS receiver, you must provide the host address, port number, and url.
 - **HTTP Headers**—Enter the HTTP header inputs for **Key** and **Value**. Click the plus icon to add more custom HTTP headers to the notification. You can add a maximum of three custom HTTP headers.
- Note** HTTP headers are mandatory for northbound notifications to connect to third party services.
- **MAC Hashing**—Click to disable the MAC hashing. By default, MAC hashing is enabled.
 - **Message Format**—From the **Message Format** drop-down list, choose the format as **JASON** or **XML**.
 - **Salt**—Enter a secret hash key.

Step 5 Click **Create**. The new notification is created and displayed in the Notifications window.

Making Changes to Notifications



Note If you are a non-admin user, you can make changes to only those notifications that were created by you. A non-admin user cannot make changes to notifications created by other users.

The following are the changes that you can make to notifications:

Enabling and Disabling a Notification

When a notification is created, it is enabled by default.

Procedure

- To disable a notification, in the **NOTIFICATIONS** window, under the **Status** column adjacent the notification, click **Enabled**.
The label changes to **Disabled** and the notification is disabled.
- To enable a notification, in the **NOTIFICATIONS** window, under the **Status** column adjacent the notification, click **Disabled**.
The label changes to **Enabled** and the notification is enabled.

Editing a Notification

Procedure

-
- Step 1** To edit a notification, in the **NOTIFICATIONS** window, under the **Actions** column adjacent the notification, click **Edit**.
The **EDIT NOTIFICATION** dialog box is displayed.
- Step 2** Edit the details of the notification, as required.
- Note** You cannot edit the name of the notification.
-

Viewing Northbound Notifications

You can now view northbound notifications from the Cisco CMX UI and CLI. To view Northbound Notifications:

Procedure

-
- 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.

Viewing Northbound Notification Attributes

The following table lists the Northbound Notification attributes:

Table 13: Northbound Notification

Type	Description
Notification Type	What type of notification this output describes (For example, locationupdate)
Subscription Name	The name of the notification created in CMX (user provided)
Event ID	Unique for notification identification per event
Location Map Hierarchy	The Hierarchy string that shows campus, building, floor, and zone (if applicable)
Location Coordinate	XY location for the device
Geo Coordinate	GPS location for device, if GPS markers are set
Confidence Factor	Represents a square box of where the client should be, lower means better location accuracy
AP Mac Address	The AP that the client is connected to
Associated	is this device Associated or not
Username	The username of this Associated client if using 802.11x
IP address	If this client is associated, what IP address(es) are assigned to it, can include IPv4 and IPv6 addresses
SSID	The SSID of the client is Associated
Band	802.11 band the device is it connected to
Floor Id	Long value representing hieracrchy, would not use
Floor Ref Id	New to 10.3.1, represents a long for what hierarchy it is on (Floor Id might be rounded if the number is large enough due to a conversion from long to double), only is filled in for location update, recommended for use
Entity	What type of device is it, Client (normal devices), RFID Tag (these are devices that send a chirp on an interval), Interferers (Devices that are connected to APs or are APs that aren't on the network controlled by a controller on this CMX)
Device Id	MAC address of device
Last Seen	Timestamp of packet last received from controller for this device

Type	Description
Raw Location	-
Area Global Id List	-
Tag Vendor Data	For RFID tags, information that was encoded in packets we received like battery life or something like that.
Manufacturer	Based on the first half of the MAC address of this device
Timestamp	When the notification generated
status	Refers to what the status of the device is - IDLE(0), AAA_PENDING(1), AUTHENTICATED(2), ASSOCIATED(3), POWERSAVE(4), DISASSOCIATED(5), TO_BE_DELETED(6), PROBING(7), BLACK_LISTED(8), WAIT_AUTHENTICATED(256), WAIT_ASSOCIATED(257);

Managing Proxy Settings for Notifications

In Cisco CMX, configure proxy settings for notifications that need to pass through specific proxy when sending notification to client devices. If proxy is set in Cisco CMX, you need to set the **no_proxy** variable for all notification addresses that need not go through the proxy.

Procedure

- Step 1** To verify the current proxy settings, run the **cmxos sysproxy show** command. The following is a sample output:

```
[cmxadmin@cmx-nortech ~]$ cmxos sysproxy show
USE_PROXY=1
HTTP_PROXY_URL=""
HTTPS_PROXY_URL=http://proxy.esl.cisco.com:80
FTP_PROXY_URL=""
NO_PROXY_LIST=192.0.2.1
```

Note The proxy variable required for CMX notifications is the **HTTPS_PROXY_URL**. If this variable is set and you are not getting the notification, follow the below steps to configure the **no_proxy** variable.

- Step 2** To set the **no_proxy** variable, run the **sysproxy no_proxy host name: port** command, wherein the host name is domain associated with your host machine IP address, for example, **cmxos sysproxy no_proxy 192.0.2.1:8000**

To find out the domain name, run the **host ip addresss** command and identify the domain name pointer value.

If you have multiple domain values, enter all of them as comma separated **no_proxy** values in the command, for example, **cmxos sysproxy no_proxy no_proxy_value1, no_proxy_value2: port number**.

For example, **cmxos sysproxy no_proxy 192.0.2.1,example.com:8000**

Step 3 Run the following commands to restart the agent and location services. **cmxctl agent restart** **cmxctl location restart**.

The notifications will be send to your client devices as per the notification type configuration. If the notification listener is outside the Cisco firewall, set proxy using the **cmxos sysproxy http_proxy** command. If the notification listener is within Cisco firewall, use the **cmxos sysproxy no_proxy** command to add all IP addresses that do not require a proxy setting.

The following table lists the commands used for setting proxy:

Table 14: Cisco CMX Proxy Setting Commands

Scenario	Cisco CMX Proxy Command	Cisco WSA Proxy Version	Squid Version - By default, uses web socket connection method.	McAfee Web Gateway Version
Northbound notifications with listener inside Cisco Firewall	cmxos sysproxy no_proxy 192.0.2.1	Proxy is not used	Proxy is not used	Proxy is not used
Northbound notifications with external listener in AWS cloud (outside of Cisco firewall) To send to the cloud use the following: http://ip address:9094/api/v1/notify To check the cloud instance use the following REST API: http://ip address:9094/api/v1/notifications	cmxos sysproxy http_proxy <hostname>:<port number> For example, cmxos sysproxy http_proxy example.com:80/ cmxctl agent restart cmxctl location restart	Yes	Yes	Yes
BLE (HTTPS, web socket: defaults, supports HTTP as well)	cmxos sysproxy http_proxy <hostname>:<port number> For example, cmxos sysproxy http_proxy example.com:80/ cmxctl agent restart cmxctl location restart	Yes	Yes	Yes

Scenario	Cisco CMX Proxy Command	Cisco WSA Proxy Version	Squid Version - By default, uses web socket connection method.	McAfee Web Gateway Version
Connect (SMS & FB) (HTTP & HTTPS)	cmxos sysproxy https://<url><port> For example, cmxos sysproxy http_proxy example.com:80/ cmxctl agent restart cmxctl location restart	Yes	Yes	Yes

Deleting a Notification



Caution

A notification delete action takes effect immediately without a delete confirmation dialog box being displayed.

Procedure

To delete a notification, in the **NOTIFICATIONS** window, in the **Actions** column adjacent the notification, click **Delete**. The notification is immediately deleted.

Managing Cisco CMX Cloud Apps

Cisco CMX helps to calculate location of any connected devices. These location information can be shared with various other CMX apps available as cloud services. Most of these cloud services are configured using a set of northbound notifications from Cisco CMX to the CMX application hosted on the cloud.



Note

An outbound proxy is required for connecting to the Cisco CMX applications. For more information, see [Cisco CMX Cloud Proxy Configuration Guide](#). To setup outbound proxy, see [Setting Up Outbound Proxy](#), on page 148.

Before you begin

To get a Cisco CMX Beacon Management Cloud account and for all support regarding the Cisco CMX Cloud Beacon Management Service, contact beaconmanager-support@external.cisco.com.

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Choose **MANAGE > Cloud Apps**. The Cloud Application window displays cloud application name, description, documentation links, web interface login links, and enable/disable options Cloud Apps.

Figure 14: Cloud Apps

The screenshot shows the Cisco CMX Cloud Applications management interface. The top navigation bar includes 'DETECT & LOCATE', 'ANALYTICS', 'CONNECT', 'MANAGE', and 'SYSTEM'. The 'MANAGE' tab is active, and the 'Cloud Applications' section is displayed. The 'Description' section explains that CMX provides calculated device locations for various applications, which are configured using northbound notifications. A link to 'Instructions' is provided for outbound proxy requirements. Below this is a table listing the available cloud applications.

Name	Description
Cisco Workplace Analytics	Cisco Workplace Analytics uses the technology you already have in place—your Cisco Wi-Fi network and third-party access security systems. Cisco Connected Mobile Experiences, or CMX, uses your Cisco Aironet® wireless network to detect the Wi-Fi signals of employee laptops, tablets, and smartphones. CMX places those devices on a map of your workplace, building an analytical profile of the number of employees, their dwell times, and locations to support floor usage studies.
CMX Engage	The Cisco CMX Engage is a location intelligence, digital customer acquisition and multi-channel engagement platform that enables companies to connect, know, and engage with visitors at their physical business locations. This innovative cloud-based software platform delivers rich customer experiences and provides actionable location insights by unifying location engagement across all location technologies with unmatched reliability, while leveraging your existing infrastructure investments in the best possible way.
Cisco Operational Insights	Cisco Operational Insights is a cloud based solution to manage assets within a location. Using various input signals, this solution allows you to operationalize and benefit from better understanding of assets within an environment.
Cisco Beacon Management	Cisco Beacon Management is a comprehensive resource for detecting and monitoring Bluetooth Low Energy (BLE) Beacons, as well as managing CCX BLE Devices within your network.

- Step 3** Manage Cloud Apps using the available options. The Cloud Apps available are:
- **Cisco Workplace Analytics**—Uses the technology you already have in place—your Cisco Wi-Fi network and third-party access security systems.

- **CMX Engage**—A location intelligence, digital customer acquisition and multi-channel engagement platform that enables companies to connect, know, and engage with visitors at their physical business locations.
- **Cisco Operational Insights**—A cloud based solution to manage assets within a location. This solution helps to operationalize and benefit from better understanding of assets within an environment.
- **Cisco Beacon Management**—A comprehensive resource for detecting and monitoring BLE beacons/tags as well as managing CCX BLE devices within your network.

Step 4 Use the options available in the **Links** and **Actions** column to access documentation and connect with required Cloud App:

- **Documentation**—Click to access the documentation for the corresponding Cloud App.
- **Login**—Click to log in to the required Cloud App.
- **Enable**— To enable the cloud app, click the **Enable** option in the **Actions** column for the required cloud app.

After you enable the Cloud App, you will be able to view the options to **Update** or **Disable** the same.

Note If you enabled Cloud App through **Manage > Cloud Apps**, Cisco CMX continues to send notifications to Cloud App even though the Cisco CMX license has expired. However, if you enabled Cloud App from **Manage > Notification**, Cisco CMX stops sending notifications to the Cloud App if Cisco CMX license is expired.

For example, for enabling Cisco Beacon Management, follow the below steps:

a) In the **Actions** field, click **Enable**.

Note To enable **Cisco Beacon Management** service, you must have a Cisco CMX Cloud Beacon Center account. **Cisco CMX Cloud Beacon Center** is a subscription software delivered via the cloud. For more information about Cisco Beacon Center, see [Cisco Beacon Center](#).

b) In the pop-up window that is displayed, enter the token to enable **Cisco Beacon Management**.

The token to enable Cisco Beacon Management can be obtained from **Cisco Beacon Center** service available in the Cisco CMX Cloud. In the **Cisco CMX Cloud Beacon Center**, the token information is displayed in the **Setup** tab under **Beacons**.

c) Click **Save & Enable**.

We recommend that you verify the outbound proxy configuration, Cisco WLC 8.7, and Cisco 4800 APs setup to successfully complete the cloud app enabling process.

For more information about enabling **Cisco Operational Insights**, see [Operational Insight Configuration Guide](#). To get an Operational Insights cloud account and for all support regarding the Cisco Operational Insights service, contact opinsights-support@external.cisco.com.

Step 5 Use the **Notifications** section to view notification name, receiver details, total number of notifications sent, acknowledged notification count, unacknowledged notification count, success percent, failure percent, and latency.

Figure 15: Cloud Apps Notification

Name	Notification Receiver	Total Sent	Acknowledged Count	Unacknowledged Count	Success Percent
gateway-BeaconManagement-Test-mapChange-479	https://beaconcenter-test.cmxdemo.com:443/api/ble/v1/beacon/xy?jwttoken=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJyb2xiOiJQRWtaW4iLCJ0ZW5hbnRJCi6NDc5LCJleHAiOiE1MjY2ODAxMDF9.Fi7L-kTj-rX6zFwTQHzRhLLZ1Lh4q4NTPfprjWqk	3	0	3	0.00%
gateway-blemgmtadmin-mapChange-479	https://abp5mk0kz9.execute-api.us-west-2.amazonaws.com:443/test/listener/782826a7-04fd-473a-9f30-e7c4dc8fd740?cmxididentifier=a1991c30-8cfd-11e7-b51c-bb23d688f84b	3	0	3	0.00%
gateway-BeaconManagement-Test-bleinfo-479	https://beaconcenter-test.cmxdemo.com:443/api/ble/v1/beacon/xy?jwttoken=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJyb2xiOiJQRWtaW4iLCJ0ZW5hbnRJCi6NDc5LCJleHAiOiE1MjY2ODAxMDF9.Fi7L-kTj-rX6zFwTQHzRhLLZ1Lh4q4NTPfprjWqk	34693	0	34693	0.00%
OperationalInsight-tag	https://opinsights.cisco.com:443/api/am/v1/events	173815	173498	317	99.82%
gateway-blemgmtadmin-bleinfo-479	https://abp5mk0kz9.execute-api.us-west-2.amazonaws.com:443/test/listener/782826a7-04fd-473a-9f30-e7c4dc8fd740?cmxididentifier=a1991c30-8cfd-11e7-b51c-bb23d688f84b	34693	34538	155	99.55%
operational-insights-tag	https://opinsights.cisco.com:443/api/am/v1/events	217128	216702	426	99.80%
gateway-BeaconManagement-Test-feedback-479	https://beaconcenter-test.cmxdemo.com:443/api/ble/v1/beacon/xy?jwttoken=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJyb2xiOiJQRWtaW4iLCJ0ZW5hbnRJCi6NDc5LCJleHAiOiE1MjY2ODAxMDF9.Fi7L-kTj-rX6zFwTQHzRhLLZ1Lh4q4NTPfprjWqk	0	0	0	0%
operational-insights-client	https://opinsights.cisco.com:443/api/am/v1/events	0	0	0	0%
gateway-blemgmtadmin-feedback-479	https://abp5mk0kz9.execute-api.us-west-2.amazonaws.com:443/test/listener/782826a7-04fd-473a-9f30-e7c4dc8fd740?cmxididentifier=a1991c30-8cfd-11e7-b51c-bb23d688f84b	0	0	0	0%

Note To reset a notification, click the **Reset** option in the **Actions** column against each notification.

Setting Up Outbound Proxy

If your Cisco CMX on-premise setup requires a forward proxy for internet access, you must configure the proxy and restart your Cisco CMX services. Proxy setting is mandatory for Cisco CMX wants to communicate with Cloud.

For example, Cisco Beacon Management requires HTTP_PROXY and HTTPS_PROXY environment variables set as proxy and the NO_PROXY environment variable set to localhost.

Procedure

- Step 1** Connect to CMX via SSH.
- Step 2** To setup proxy, run the following commands:
- ```
cmxos sysproxy proxyhttp://<proxy><Port #>
cmxos sysproxy proxyhttps://<proxy><Port #>
cmxos sysproxy no_proxy localhost,company.com
```
- Step 3** To stop and restart agent and Cisco CMX services, run the following commands:
- ```
cmxos stop -a
cmxctl agent start
cmxctl start
```
-

Managing Verticalization

Cisco CMX Analytics comes packaged with a report generator that can automatically generate reports with the most important metrics for specific businesses. By selecting a vertical, you can take advantage of predefined reports that can help you make informed decisions based on the vertical your network is set up for. This feature is called verticalization.

Customizing your vertical enables you to quickly generate valuable reports specific to the requirements of that vertical. The customized verticals can also be configured with the correct tags suitable to your vertical. CMX Analytics' verticalization feature enables you to customize the names of your entities such that they are specific to a vertical. Depending on the vertical you choose, the CMX Analytics verticalization feature can generate customized reports.

The following are some of the verticals supported by Cisco CMX, along with the reports they contain:

- Default—By default, Cisco CMX is packaged with **Default** vertical. If you want to configure another vertical, you must choose a vertical.
- Retail
 - Store Type Popularity
 - Average Shopping Time
 - Most Popular Entrance
 - Most Popular Department
 - Department Transition
 - Footfall
- Mall
 - Store Type Popularity

- Average Shopping Time
- Most Popular Entrance
- Most Popular Restaurant
- Department Transition
- Footfall
- Hospitality
 - Most Popular Restaurant
 - Connected Clients
 - Most Used Amenity
 - Local Correlation
 - Longest Used Amenity
 - Path Analysis
- Education
 - Corridors vs Classroom
 - Connected Clients
 - Diners per Hall
 - Local Correlation
 - Library Time
 - Path Analysis
- Healthcare
 - Visitor Count
 - Connected Clients
 - Busiest Department
 - Wait Times
 - Diners per Cafeteria
 - Path Analysis
- Airport
 - Visitor Count
 - Average Waiting Time
 - Busiest Flights
 - Wait Times

- Longest Used Amenity
- Path Analysis

Queue Analytics

The Queue Analytics feature provides a breakdown of the average time spent in a queue. This feature allows you to select a queue start area and one or more queue end areas, enabling the computation of the average time taken (15 minutes, hour, day, week, month, or year) for devices to move from the start area to an end area.



Note Currently, the Queue Analytics feature is supported only for the Airport vertical.

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
 - Step 2** Choose **MANAGE > Verticalization**.
The **Verticalization** window displays with a list of the supported verticals.
 - Step 3** Select **Airport** vertical.
Depending on the selection, the **Verticalization** window is displayed with additional vertical information.
 - Step 4** Click **Run Setup Wizard** to start the verticalization process.
 - Step 5** In the **Location Tags** window, select **Security** as queue time tag and click **Continue**.
 - Step 6** In the **Review Your Tag Selection** window, verify the tag, and widgets, and click **Save & Continue**.
 - Step 7** Tag **Security** queue time tag to a desired zone, and click **Review**.
 - Step 8** Click **Create a Report** to create a report with the tag **Security**.
The Queue Time information is displayed in the report instead of Dwell Time.
-

Customizing Verticals

Customizing a vertical means changing the names of the entities in your vertical based on your business. You can optimize your vertical by customizing it to meet your specific needs. Customizing includes naming the hierarchy of your vertical, association of icons, building a tag library, and specifying tag locations.

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **MANAGE > Verticalization**.
The Verticalization window is displayed with a list of the supported verticals.
- Step 3** Choose a vertical by clicking the icon corresponding to that vertical.
The customized widgets available for the chosen vertical are displayed.

- Step 4** Click **Run Setup Wizard**.
The setup wizard displays the steps required to optimize the vertical and complete the customization.
- Step 5** Click **Get Started**.
The Hierarchy Configuration window is displayed.
- Step 6** Configure the hierarchy levels of your vertical. Follow the instructions on the Hierarachy Configuration window to configure hierarchy levels for Campus, Building, Floor, and Zone and select an icon. If you approve of the default hierarchy name and the associated icon, click **Skip Step**.
- Step 7** Click **Continue**.
- Step 8** Tags are used to categorize locations and devices. Click **Continue** to configure tagging.
- Step 9** Depending on the vertical you select, the tags specific to that vertical are listed. Select the tags you want to create by clicking the button corresponding to that tag. The setup wizard creates the tags. Click **Continue**.
- Step 10** Location tags can be applied to specific locations based on your hierarchy. The setup wizard iterates through the hierarchies in your vertical. Select the hierarchies that you want to tag by clicking the corresponding name. The right pane lists the Zone item name and a list of tags to choose from. Select the tags that are applicable to the Zone. Click **Continue**.
- Step 11** Click **Create a Report**.
The **Analytics Reports** window is displayed with the list of customized wizards for your vertical.
-

Configuring Basic CMX Settings

The GUI allows you to set up maps, Cisco WLC, and mail server.

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Click **SYSTEM**.
The **SETUP ASSISTANT** window is displayed.
- Step 3** Click **Next** to set up the **New UI Password**.
The **Maps and Controllers** window is displayed.
- Step 4** Choose either **Default** or the **Advanced** option.
- In the **Default** window, provide Cisco Prime Infrastructure credentials such as **Username**, **Password**, and **IP Address**, and click **Import Controllers and Maps**. This imports the Controllers and maps from Cisco Prime Infrastructure.
 - In the **Advanced** window, provide the map and Cisco WLC information, and click **Next**.
- Note** If the **Override** checkbox is checked, the import will override the existing entries.
- Step 5** In the **Mail Server** window that is displayed, enter the corresponding details.
- Step 6** Click **Next** to complete the configuration.
-

Root User Changes

In releases prior to Cisco CMX 10.2, all the processes used the root user role. This has been changed in Cisco CMX 10.2 by introducing two new user roles: `cmx` and `cmxadmin`. The `cmx` user is a no-login user who owns all the processes, except `postgres`. The `cmxadmin` is the primary user who performs all the administrative tasks.

The root user is not disabled; this user can still be used for installation and debugging. You cannot directly log in to root through SSH or console. First you have log in as `cmxadmin` and then issue the `su` command to go to the root user level.



Caution

Do not use the root user account; unless explicitly directed to do so by the Cisco Technical Assistance Center team.



CHAPTER 7

Managing Cisco CMX System Settings

- [Overview of the System Service, on page 155](#)
- [Viewing the Overall System Health, on page 155](#)
- [Understanding the Node Table, on page 156](#)
- [Understanding the Coverage Details Table, on page 157](#)
- [Understanding the Controllers Table, on page 158](#)
- [Managing Dashboard Settings, on page 158](#)
- [Viewing Live System Alerts, on page 169](#)
- [Viewing Patterns, on page 169](#)
- [Understanding the Metrics Tab, on page 170](#)

Overview of the System Service

The Cisco CMX **System** service comprises the following tabs, which help you perform a variety of system-related tasks, including, but not restricted to, those listed here:

- **Dashboard**—Enables you to have an overall view of the system.
- **Alerts**—Enables you to view live alerts.
- **Patterns**—Enables you to detect patterns of various criteria, such as Client Count, CPU Usage, Memory Usage, and so on.
- **Metrics**—Enables you to view system metrics.

Viewing the Overall System Health

Procedure

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

Step 2 Choose **System > Dashboard**.

The **System at a Glance** window (see the image below) is displayed.

The screenshot displays the 'System at a Glance' dashboard. The top navigation bar includes 'DETECT & LOCATE', 'ANALYTICS', 'CONNECT', 'MANAGE', and 'SYSTEM'. The main content area is divided into three sections:

- Node Table:** A table with columns for Node, IP Address, Node Type, Services, Memory, and CPU. The 'Node' column contains 'cmx-mon1ch'. The 'IP Address' is '10.22.243.125'. The 'Node Type' is 'High-End'. The 'Services' column shows icons for Configuration, Location, Analytics, Connect, Database, Cache, Hyper Location, Location Heatmap Engine, and MSST Load Balancer. The 'Memory' is 30.60% and 'CPU' is 4.38%.
- Coverage Details:** A table with columns for Access Points, Map Elements, Active Devices, and System Time. The 'Access Points' section includes Placed AP (14), Missing AP (0), Active AP (6), and Inactive AP (8). The 'Map Elements' section includes Campus (1), Building (1), Floor (1), and Zone (5). The 'Active Devices' section includes Associated Client (6), Probing Client (104), RFID Tag (23), Interferer (38), Rogue AP (159), and Rogue Client (12). The 'System Time' is 'Fri Nov 24 03:18:58 PST 2017'.
- Controllers:** A table with columns for IP Address, Version, Bytes In, Bytes Out, First Heard, Last Heard, and Action. It lists two controllers: one with IP 10.22.243.156 (Version 8.3.112.0, Bytes In 830 MB, Bytes Out 536 KB, First Heard 11/22/17, 1:54 am, Last Heard 1s ago) and another with IP 10.22.243.211 (Version 8.6.1.140, Bytes In 0, Bytes Out 0, First Heard Never, Last Heard 3h 18m 56s ago).

Step 3 View the following sections:

- **Node Table.** For details, see [Understanding the Node Table, on page 156](#).
- **Coverage Details Table.** For details, see [Understanding the Coverage Details Table, on page 157](#).
- **Controllers Table.** For details, see [Understanding the Controllers Table, on page 158](#).

Understanding the Node Table

The **Node** table in the **System at a Glance** window displays the following Cisco CMX node information:

- **Node**—Lists all the associated Cisco CMX nodes.
 - Click a node name to view its metrics. See [Viewing CMX Node Metrics, on page 171](#).
- **IP Address**—Shows the IP address of the Cisco CMX node.
- **Node Type**—Shows the type of the Cisco CMX node.
- **Services**—Lists all the services for each Cisco CMX node.
 - The colors of the icons pertaining to these services indicate the status of these services. Ensure that the services are in green color; this indicate a healthy status.
 - Click a service icon to view the corresponding service or system metrics.
- **Memory**—Shows the load on the memory, in percentage.
 - Click it to view the **Live Alerts** window. See [Viewing Live System Alerts, on page 169](#).
- **CPU**—Shows the load on the CPU, in percentage.

- Click it to view the **Live Alerts** window. See [Viewing Live System Alerts, on page 169](#).

Understanding the Coverage Details Table

The **Coverage Details** table in the **System at a Glance** window displays the following information:

- **Access Points**—Shows the number of access points placed on Cisco CMX map.
 - **Placed AP**—Shows the total count of access points placed on Cisco CMX map.
 - **Missing AP**—Shows the number of access point which has sent location details but not found on the map. This could impact the accuracy of the location.
 - **Active AP**—Shows the number of access point active for the last 24 hours. This helps to troubleshoot and determine if there are access points that are not placed on Cisco CMX map.
 - **Inactive AP**—Shows the number of inactive access points for the last 24 hours.
- **Map Elements**—Shows the number of elements available on Cisco CMX map.
 - **Campus**—Shows the number of campuses in Cisco CMX.
 - **Building**—Shows the total number of buildings in Cisco CMX.
 - **Floor**—Shows the total number of floors in Cisco CMX.
 - **Zone**—Shows the total number of zones in Cisco CMX.
 - **Total**—Shows the summation of all the previous elements. This is the total elements in Cisco CMX .
- **Active Devices**—Shows the number of active devices available on Cisco CMX map.
 - **Associated Client**—Shows the number of associated clients.
 - **Probing Client**—Shows the number of probing clients.
 - **RFID Tag**—Shows the number of active RFID tags.
 - **Interferer**—Shows the number of interferers.
 - **Rogue AP**—Shows the number of rogue access points.
 - **Rogue Client**—Shows the number of rogue clients.
 - **BLE Tags**—Shows the number of bluetooth devices.
 - **Total**—Shows the summation of all the previous devices.
- **System Time**—Shows the current system time with the time zone set as on Cisco CMX system .

Understanding the Controllers Table

The **Controllers** table in the **System at a Glance** window lists the Cisco WLCs that are sending Network Mobility Services Protocol (NMSP) data to Cisco CMX. The table displays the following details for each Cisco WLC:

- **IP Address**—The color of the table border to the left of each IP address indicates whether the Cisco WLC is active or not.
- **Version**—Cisco WLC software version.
- **Bytes In and Bytes Out**—Number of bytes received from and sent to the Cisco WLC.
- **First Heard**—Number of seconds since the first communication received from the Cisco WLC.
- **Last Heard**—Number of seconds since a communication was received from the Cisco WLC.
- **Action**—Allows you to modify the details of an existing controller or delete an existing controller. Click **Edit** to edit the controller details in the **Edit Controller** window. Click the plus icon to view the **Controllers and Map Setup** tab details in the **Settings** window.



Note The IP addresses of active controllers are shown in green. The IP addresses of inactive controllers are shown in red.

Managing Dashboard Settings

The **Settings** option in the **System at a Glance** window enables you to manage the configurations and other settings related to **Cisco CMX System** service.

Setting Device Tracking Parameters

Procedure

- Step 1** Log in to Cisco Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **System > Dashboard**.
The **System at a Glance** window is displayed.
- Step 3** Click **Settings** at the top-right corner of the window. The **SETTINGS** window is displayed.
By default, the **Tracking Parameters** tab is displayed.
- Step 4** In the **Elements** column, check the check box of each device that you want to select for tracking.

Figure 16: Tracking Parameters

SETTINGS

Tracking Parameters

Network Location Service

Elements	Active Value	Not Tracked
<input checked="" type="checkbox"/> Wireless Clients	0	0
<input checked="" type="checkbox"/> Rogue Access Points	91	0
<input checked="" type="checkbox"/> Rogue Clients	8	0
<input checked="" type="checkbox"/> Interferers	0	0
<input checked="" type="checkbox"/> RFID Tags	0	0
<input checked="" type="checkbox"/> BLE Tags	0	0

Close Save

Only the elements selected here will be tracked by the network location service and will appear on the **Activity Map** window.

The following elements are available for tracking:

- Wireless Clients
- Rogue Access Points
- Rogue Clients
- Interferers
- RFID Tags
- BLE Tags

Note BLE capable APs are discovered by Cisco Prime Infrastructure. Use Cisco Prime Infrastructure to place the APs on the maps and export the maps. Cisco CMX will utilize the map file exported from Cisco Prime Infrastructure.

Bluetooth low energy (BLE) beacons are detected in two ways:

- **Clean air over NMSP**—To enable this tracking method, check **Interferers** option. You require a Cisco WLC with software Release 8.0.115.0 or later for this method.
- **Fast path over UDP**—To enable this tracking method, check **BLE Beacons** option. You require a Cisco WLC with software Release 8.6.1.146 or later for this method.

Step 5 Click **Save**.

Setting Filtering Parameters

Procedure

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

Step 2 Choose **System > Dashboard**.
The **System at a Glance** window is displayed.

Step 3 Click **Settings** at the top-right corner of the window.

Step 4 Click the **Filtering** tab.

Here, you can configure the following filtering parameters:

- **Duty Cycle Cutoff (Interferer)**—This is a percentage value. Interferers with a Duty Cycle that is less than the specified cutoff will not be tracked.
- **RSSI Cutoff (Probing Only Clients)**—This is the radio signal strength cutoff for filtering. The default is -85 dBm.
- **Exclude Probing Only Clients**—Check this check box to filter out clients that are only probing. This is the best effort to stop detecting probing clients. However, a small percentage of probing clients may appear for short duration. So this should not be considered as complete probing client removal from the system. If you check this option, the **Probing Client Filtering** service is enabled on Cisco WLC and Cisco CMX will not receive any probing client information.
- **Enable Locally Administered MAC filtering**—Check this check box to filter out self-assigned MAC addresses. This parameter is checked by default. This discards Apple iOS8 random MAC addresses.
- **Enable Location MAC Filtering**—Check this check box to filter out specific MAC addresses. For example, you can use this to filter out MAC addresses of employees' devices. After checking this, you can either specify a MAC address that you want to allow or disallow, or choose to allow, disallow, or delete previously entered MAC addresses.
- **Enable Location SSID Filtering**—Check this check box so that the Location service excludes all visitor devices associated to a particular SSID.
 1. Click **Enable SSID Filtering**.
 2. 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.
 3. Click **Filter SSID** to add the selected SSID to the filter list.

Step 5 Click **Save**.

Setting Location Calculation Parameters

Procedure

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

Step 2 Choose **System > Dashboard**.

The **System at a Glance** window is displayed.

Step 3 Click **Settings** at the top-right corner of the window.

The **SETTINGS** dialog box is displayed.

Step 4 Click the **Location Setup** tab.

Here, you can configure the following **Location Calculation Parameters**:

- **Enable OW Location**—Check this check box to enable the use of Outer Walls (obstacles) for location calculation. The Calibration model includes information regarding the Walls. This setting controls whether the CMX should honor the walls while calculating the heatmaps or not.
- **Enable Location Filtering**—Check this check box if you want the system to use previous location estimates for estimating the current location. This parameter will be applied only for client location calculation. Enabling this parameter reduces location jitter for stationary clients and improves location tracking for mobile clients. This parameter is enabled by default.
- **Use Default Heatmaps for Non Cisco Antennas**—Check this check box to enable the usage of default heat maps for non-Cisco antennae during location calculation.
- **Chokepoint Usage**—Check this check box to enable the usage of chokepoint proximity to determine the location of a device. This applies only to Cisco-compatible tags that are capable of reporting chokepoint proximity. This parameter is enabled by default.
- **Enable Hyperlocation/FastLocate/BLE Management**—Check this check box to enable hyperlocation, fastlocate, and BLE management in Cisco CMX. This parameter is disabled by default.

Note This option will not be displayed if the system is not a large OVA installation. Hyperlocation requires a high end system to run and if run on lower system the option is hidden. For high end system (20 vCPU) and Bare metal (3365), Hyperlocation option is enabled by default and displayed in the GUI. For standard (16 vCPU) and low end system (8 vCPU), Hyperlocation option is hidden.

- **Optimize Latency**—Check this check box to enable latency optimization. If you enable this option, Cisco CMX enables faster location computation over less data affecting accuracy due to not using the fully available data for computation. By default, this option is not enabled. If not enabled, Cisco CMX will provide location updates at default intervals computed over full available data. If you check this option, the **Relative discard RSSI time** and **Relative discard AoA time** values will be changed to 30. You will not be able to edit these values. We recommend you to enable this option only if recommended by Cisco.
- **Use Chokepoints for Interfloor conflicts**—Use this drop-down list to specify the frequency to determine the correct floor during interfloor conflicts.

- **Chokepoint Out of Range Timeout (secs)**—After a Cisco-compatible tag leaves a chokepoint proximity range, RSSI information will be used again to determine the location only after this timeout value is exceeded. Specify a timeout value, in seconds, accordingly.
- **Relative discard RSSI time (secs)**—Enter the time, in seconds, after which the RSSI measurement should be considered obsolete and discarded from use in location calculations. This time is from the most recent RSSI sample, and not an absolute time. For example, if this value is set to 3 minutes, and two samples are received at 10 minutes and 12 minutes, both the samples will be retained. However, an additional sample received at 15 minutes will be discarded. We recommend that you do not modify this parameter without the guidance of Cisco Technical Support.
- **Relative discard AoA time**—Enter the time, in seconds, after which the AoA measurement should be considered as obsolete and discarded from use in location calculations. We recommend that you do not modify this parameter without the guidance of Cisco Technical Support.
- **Absolute discard RSSI time**—Enter the time, in minutes, after which the RSSI measurement should be considered obsolete and discarded from use in location calculations regardless of the most recent sample. We recommend that you do not modify this parameter without the guidance of Cisco Technical Support.
- **RSSI cutoff**—Enter the RSSI cutoff value, in dBm, at which you want the server to discard AP measurements. We recommend that you do not modify this parameter without the guidance of Cisco Technical Support.

You can also set the following **Movement Detection Parameters**:

- **Individual RSSI change threshold**—Enter a threshold, in dBm, beyond which you want individual RSSI movement recalculation to be triggered. We recommend that you do not modify this parameter without the guidance of Cisco Technical Support.
- **Aggregated RSSI change threshold**—Specify the Aggregated RSSI movement recalculation trigger threshold. We recommend that you do not modify this parameter without the guidance of Cisco Technical Support.
- **Many new RSSI change percentage threshold**—Specify the trigger threshold recalculation (as a percentage) for many new RSSI changes. We recommend that you do not modify this parameter without the guidance of Cisco Technical Support. This parameter indicates the threshold for comparing against the aggregated APs value. This comparison will help you to decide whether the location computation is required.
- **Many missing RSSI percentage threshold**—Specify the trigger threshold recalculation (as a percentage) for many missing RSSI changes. We recommend that you do not modify this parameter without the guidance of Cisco Technical Support.

You can set the following **History Storage Parameters**:

- **History Pruning Interval**—Specify the number of days of client location history to be stored for the location maps.

Step 5 Click **Save**.

Configuring the Mail Server for Notifications

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **System > Dashboard**.
The **System at a Glance** window is displayed.
- Step 3** Click **Settings** at the top-right corner of the window.
The **Settings** dialog box is displayed.
- Step 4** Click the **Mail Server** tab.
Here, you can configure the following:
- **From Email Address**—Email address of the mail server host.
 - **To Email Address Address**—Enter the email addresses to which the notifications should be sent. You can add multiple email addresses separated using the delimiters comma, semi-colon, and space.
 - **Server**—Mail server URL.
 - **Port**—Port number for the mails. The default is port 25.
 - **Authentication**—Option to enable or disable email authentication.
 - **SSL**—Option to enable or disable email security with Secure Sockets Layer (SSL) to prevent third parties from potentially viewing your email messages.
 - **TLS**—Option to enable or disable email secured with Transport Layer Security (TLS).
- Step 5** To test your settings, click **Save and Test Settings**.
- Step 6** Enter the email address and then click **Send e-mail**.
- Step 7** Click **Save** to save your settings if the test is successful.
-

Importing Maps and Controllers into Cisco CMX

To import maps and controllers directly from Cisco Prime Infrastructure, do the following:

Before you begin

Ensure that while exporting maps from Prime, check the **Include Calibration Information** option. Cisco CMX will not be able to compute the location for network elements (Clients/ Interferers / Tags) for maps having no calibration information.

Import operation for map archive files will fail if **Include Calibration Information** option is not selected in the Prime Infrastructure while importing maps. While importing maps, the upload utility validates if the calibration model is available for each floor in the given maps archive file. If not available, map import will fail with an error message: 'Calibration model is missing in the uploaded map archive. Please select the option 'Include Calibration Information' on Prime Infrastructure GUI while exporting maps archive.

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **System > Dashboard**.
The **System at a Glance** window is displayed.
- Step 3** Click **Settings** at the top-right corner of the window.
- Step 4** Choose the **Controllers and Maps Setup > Import** tab, and enter the following parameters:
- Username**—Username of the Cisco Prime Infrastructure server.
 - Password**—Password of the Cisco Prime Infrastructure server.
 - IP Address**—IP address of the Cisco Prime Infrastructure server. Ensure that the SNMP community string is properly configured in Cisco Prime Infrastructure.
 - To save the Cisco Prime Infrastructure credentials, check the **Save Cisco Prime Credentials** check box.
 - To override the existing maps that currently exist in Cisco CMX while importing, check the **Delete & replace existing maps & analytics data** check box.
 - To override the existing zones that currently exist in Cisco CMX while importing, check the **Delete & replace existing zones** check box.
- Note** We recommend exporting updated maps only from Cisco Prime Infrastructure. In addition, when importing updated maps to Cisco CMX, make sure the **Delete & replace existing maps & analytics data** check box and the **Delete & replace existing zones** check box are unchecked.
- Step 5** Click **Import Controllers and Maps**.
- Step 6** Click **Save**.
-

Importing Maps and Adding Controllers

You can manually import maps and add Cisco WLCs into Cisco CMX using the web interface.

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **System > Dashboard**.
The **System at a Glance** window is displayed.
- Step 3** Click **Settings** at the top-right corner of the window.
- Step 4** Choose the **Controllers and Maps Setup > Advanced** tab.
- Step 5** To manually import a map, perform the following:
- Under the **Maps** area, click **Browse**.
The File Upload dialog box is displayed.

Note If you check the **Delete & replace existing maps & analytics data** check box, the maps existing in Cisco CMX will be replaced by the maps that you import from Cisco Prime Infrastructure. Existing zones are also removed when you override the maps.

If you check the **Delete & replace existing zones** check box, the existing zones in Cisco CMX will be replaced by zones that you import from Cisco Prime Infrastructure.

Ensure that while exporting maps from Prime, check the **Include Calibration Information** option. Cisco CMX will not be able to compute the location for network elements (Clients/ Interferers / Tags) for maps having no calibration information.

- b) Navigate to the location of the map file, select the map file, and then click **Open**.
- c) Click **Upload**.
- d) Click **Save**.

Step 6 To import a Cisco WLC, configure the following parameters under the **Controllers** area:

- a) **Controller type**—Choose from **Cisco WLC** or **Unified WLC**.
- b) **IP address / Hostname**—IP address or hostname of the Cisco WLC.
- c) **Controller Version**—(Optional) Software version of the Cisco WLC.
- d) **Applicable Services**—Check the CAS check box if Context Aware Service (CAS) is applicable.
- e) **Controller SNMP version**—Choose from **v1**, **v2c**, or **v3**.
- f) **Controller SNMP Write Community**—Enter the controller SNMP write Community string. The default is *private*.
- g) Click **Add Controller**.

Note If you are adding Unified WLC, ensure that SSH is enabled on the controller before adding it to Cisco CMX.

Step 7 Click **Save**.

Upgrading Cisco CMX

After you install Cisco CMX 10.2, future upgrades can be performed via the Cisco CMX GUI or by using the **cmxos upgrade** CLI command and the .cmx file, for example, **cmxos upgrade <CISCO_CMX\$\$\$>.cmx**, while logged in as **cmxadmin**.

To upgrade Cisco CMX to a future release using the GUI, perform the following task:

Procedure

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

Step 2 Choose **System > Dashboard**.

The **System at a Glance** window is displayed.

Step 3 Click **Settings** at the top-right corner of the window.

Step 4 In the **SETTINGS** dialog box, click the **Upgrade** tab and then click **Upgrade**.

Step 5 Either choose a local .cmx file or point to the URL of the .cmx file

Before selecting the local file option, ensure that the .cmx file is available on the machine from which access to the web GUI is being made.

The upgrade process involves the following tasks:

1. The .cmx file is copied to /opt/image/newimage.
2. The **cmxos upgrade** command is executed in the background:
 - Services are stopped
 - New files are copied and configured
 - Services are restarted

What to do next

For more information about upgrading Cisco CMX using CLI, see [Upgrading Cisco CMX Using CLI](#).

Enabling High Availability for Cisco CMX

High Availability (HA) is a simple and reliable failover mechanism. It helps Cisco CMX host and support multiple mobility applications seamlessly without any interruption.

The definition of servers described in this section are as follows:

- **Active Server**—The Cisco CMX server that is actively serving traffic from the controllers. The virtual IP address (VIP) for the HA pair should point to the current active server. The VIP address is optional.
- **Primary Server**—The Cisco CMX server that will be initially active in the HA pair.
- **Secondary Server**—The CMX server that will be the backup or standby server in the HA pair.

Cisco CMX HA requires two servers. The primary server acts as the active Cisco CMX server. Cisco CMX server can use virtual IP addresses too. The primary Cisco CMX server is installed by selecting the Location or Presence node type. In an active HA deployment, data on the primary server will be continuously synchronized with the secondary server. If the primary server encounters any issues, the secondary server will take over the responsibility as the active server.

Install Cisco CMX Release 10.3.x on both the servers. From the web installer, choose either **Presence** or **Location** as the node type. Both the servers should have the same node type. After installation completes, each server is considered a standalone server and has the primary HA role. HA requires both primary and secondary servers, the role for one server needs to change. To change the HA role of a server from primary to secondary, use the **cmxha secondary convert** command in cmxadmin mode.

The Cisco CMX HA Admin interface is hosted on Cisco CMX port 4242 and can be accessed using `http://cmx_ip_address:4242/`. Log in to the web interface using `cmxadmin` as user ID and the password configured for cmxadmin during the primary and secondary server installation. This Cisco CMX HA Admin interface is different from the regular Cisco CMX interface that can be accessed at `http://cmx_ip_address`. Use the Cisco CMX HA Admin interface specifically monitoring and managing HA.

Every active Cisco CMX instance is backed by another (inactive) instance. The second CMX instance is not active until the failover procedure is initiated, either manually or automatically.

You can enable HA by using either Cisco CMX web UI or CLI.



Note We recommend that you use the Cisco CMX web UI for HA configuration.



Tip Cisco CMX High Availability documentation is embedded in the product. From the Cisco CMX user interface, choose **Documentation** from the drop-down list on the top-right corner.

Pre-requisites for HA

- Both the primary and the secondary server should be of the same size and the same type (VM or physical appliance).
- Both the primary and the secondary server should have the same Cisco CMX version.
- Both the primary and the secondary server should be connected on the same subnet.
- Both the primary and the secondary server should be connected on the same subnet if Layer 2 HA is required.
- Both the primary and the secondary server should be IP connected with delay of less than 250ms if Layer 3 HA is used.

Enabling High Availability for Cisco CMX Using the Web UI

Procedure

- Step 1** Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2** Choose **System > Dashboard**.
The **System at a Glance** window is displayed.
- Step 3** Click **Settings** at the top-right corner of the window.
The **Settings** dialog box is displayed.
- Step 4** Click the **High Availability** tab.
- Step 5** Configure the following parameters:
 - **Secondary IP Address**—Enter the IP address of the secondary server. The primary server will be continuously synchronized with the secondary server. If the primary server encounters any issues, the secondary server will take over the responsibility as the active server.
 - **Secondary Password**—Enter the password for the *cmxadmin* user on the secondary server.
 - **Use Virtual IP Address**— By default, this option is checked. (If you do not check this option, the **Virtual IP Address** field is dimmed, and this address will not be used for HA configuration.)
If you decide to retain the default, enter the corresponding virtual IP address.

- **Virtual IP Address**—(Optional) Enter the virtual IP address for the HA pair if the **Use Virtual IP Address** check box is checked. .
- **Failover Type**—From the **Failover Type** drop-down list, choose **Auto** or **Manual**.
 - Note** If you choose **Auto**, Cisco CMX automatically fail over to the secondary server when a serious issue is detected. If you choose **Manual**, manual intervention is required to initiate failover from the web interface or command line. The failure will be reported via a notification, but no action will be taken.
- **Notification Email Address**— Enter the email address to which HA notifications are to be sent. You can add multiple email addresses.

Step 6 To enable HA, click **Enable**.

Cisco CMX will verify the HA settings and start enabling HA between the primary and secondary servers.

Step 7 Click **Save**.

The initial synchronization of the primary and the secondary server takes time and the **System at a Glance** window displays the state as **Primary Syncing** while the synchronization is in progress. After the synchronization is complete, the primary server will be in the state **Primary Active** state. Also, after synchronization, an informational alert is generated in Cisco CMX and an email is sent to the addresses that have been provided, indicating that HA is enabled and synchronized successfully.

Tip Click the **Help** link in the top-right corner of the **Settings** dialog box to launch the HA online help. For more information about the HA installation process, see http://cmx_server/docs/ha/.

Enabling High Availability Using CLI

Procedure

Step 1 To enable HA using CLI, run the **cmxha config enable** command.

Step 2 Follow the command prompt and enter the HA parameters.

The HA options are similar to the ones available in Cisco CMX Web UI:

```
$ cmxha config enable
```

```
Are you sure you wish to enable high availability? [y/N]: y
Please enter secondary IP address: 192.0.2.250
Please enter the cmxadmin user password for secondary:
Do you wish to use a virtual IP address? [y/N]: y
Please enter the virtual IP address: 192.0.2.251
Please enter failover type [manual|automatic]: automatic
Please enter an email address(es) for notifications (Use space, comma or semicolon to
separate): email@cisco.com
Attempting to configure high availability with server: 192.0.2.250
Configuring primary server for HA
Configuring secondary server for HA
.....
Synchronizing Postgres data from primary to secondary
.....
Synchronizing Cassandra data from primary to secondary
```

```

.....
Syncing primary files to secondary
Successfully started high availability. Primary is syncing with secondary.

```

Viewing Live System Alerts

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **System > Alerts**.
- Step 3** In the **Live Alerts** window that is displayed, sort the alerts **By Severity**, **By Node**, or **By Service**, using the drop-down list at the top-right corner.
- To dismiss an alert, in the **Actions** column adjacent the corresponding node name, click the **Dismiss** icon.
-

Viewing Patterns

The **Patterns** window shows the pattern of a specific feature, such as client count, unique devices, and so on over the week for a selected time period. For example, if you select client count for the last 1 month, it shows which days or times of the week had the most client counts in the last 1 month. The larger dots indicates a larger count for the specific feature. You can hover cursor over the dots to interpret the pattern details.

- **Client Count**—Displays the total devices seen at a given time.
- **Location Calculation Time**—Displays the average amount of time, in milliseconds, taken by the Location algorithm, to calculate a client's location.
- **CPU Usage**—Displays the percentage of used CPU on a per-node basis.
- **Memory Usage**—Displays the percentage of used memory on a per-node basis.
- **Redis Connections Received**—Displays the total number of connections received by the cache service.
- **Locally Administered MAC count**—Displays the total number of iOS devices.



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**.
-

To view patterns:

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **SYSTEM > Patterns**.
The **Patterns** window is displayed.
- Step 3** From the **Select Criteria** drop-down list, choose the criteria for which you want to view pattern data.
- Step 4** From the **Select Date Range** drop-down list, choose the time frame for the criteria pattern.
- Note** By default, the pattern data is displayed for the last one week for all the nodes in the cluster. You can view the average for the days from Monday to Sunday at all times for the selected time frame.
- Step 5** Optionally, from the **Select Server** drop-down list, choose the Cisco CMX node for which you want pattern data to be displayed. By default, the pattern data for all the Cisco CMX nodes in a cluster is displayed.
-

Understanding the Metrics Tab

The **Metrics** tab in the Cisco CMX System service enables you to view system metrics, database metrics, cache metrics, location metrics, and analytics notification metrics. Metrics information related to the following criterias are displayed:

- System Summary
- Node Metrics
- Database Metrics
- Cache Metrics
- Location Metrics
- Analytics Notification Metrics

Viewing System Summary Metrics

The **System Summary Metrics** window displays the following information:

- **Number of Active Clients**
- **Number of NMSP messages processed by the system per second, in the last one minute**
- **Overall CPU usage metrics**
- **Overall memory usage metrics**
- **Overall disk usage metrics**

Procedure

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

Step 2 Choose **SYSTEM > Metrics**.

The **System Summary** tab in the left pane is selected by default, and the corresponding details are displayed.

Viewing System Summary Metrics Using the Dashboard

Alternatively, to view the System Summary metrics from the Dashboard:

Procedure

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

Step 2 Choose **SYSTEM > Dashboard**.

The **System at a Glance** window is displayed.

Step 3 In the **Services** column, click the **Configuration**, **Location Heatmap Engine**, **NMSP Load Balancer**, or **Proxy** icon to view the corresponding **System Summary** metrics.

Note Hover your cursor over the metrics and graphs for descriptions and details.

Viewing CMX Node Metrics

The **CMX Node Metrics** window for a Cisco CMX node displays the following information:

- **Number of active clients**
- **Location latency time**
- **Number of incoming and outgoing NMSP messages**
- **Number of Controllers**
- **CPU usage metrics for each service**
- **Memory usage metrics for each service**
- **Disk IO metrics**
- **Disk usage metrics**
- **redis-iops**
- **jdbc-iops**
- **redis-errors**
- **jdbc-errors**

To view the Node metrics for a Cisco CMX node:

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
 - Step 2** Choose **SYSTEM > Metrics**.
 - Step 3** In the left pane, click a Cisco CMX node name to view the metrics for that node.
-

Viewing CMX Node Metrics Using the Dashboard

Alternatively, to view the node metrics from the Dashboard:

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
- Step 2** Choose **SYSTEM > Dashboard**.
The **System at a Glance** window is displayed.
- Step 3** In the **Node** column, click a Cisco CMX node name to view the metric details for that node.

Note Hover your cursor over the metrics and graphs for descriptions and details.

Viewing Database Metrics

The **Database Metrics** window displays the following metrics:

- **Database Size**—Shows the active memory used by the Cassandra and Postgres database.

To view the Database metrics:

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
 - Step 2** Choose **SYSTEM > Metrics**.
 - Step 3** In the left pane, click **Database Metrics**.
- Note** Hover your cursor over the Database metrics graph for descriptions and details regarding the database usage.
-

Viewing Database Metrics Using the Dashboard

Alternatively, to view the database metrics from the Dashboard:

Procedure

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

Step 2 Choose **SYSTEM > Dashboard**.

The **System at a Glance** window is displayed.

Step 3 In the **Services** column, click the **Database** icon.

Note Hover your cursor over the metrics and graphs for descriptions and details.

Viewing Cache Metrics

The **Cache Metrics** window displays the following metrics:

- **Blocked connections**—Shows the number of clients pending on a blocking call to finish.
- **Connected clients**—Shows the number of client connections in use.
- **Used memory**—Shows the total number of bytes allocated by Redis using its allocator .
- **Evicted keys**—Shows the number of evicted keys due to maxmemory limit.

To view the Cache metrics:

Procedure

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

Step 2 Choose **SYSTEM > Metrics**.

Step 3 In the left menu, click **Cache Metrics**.

Viewing Cache Metrics Using the Dashboard

Alternatively, to view the Cache metrics from the Dashboard:

Procedure

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

Step 2 Choose **SYSTEM > Dashboard**.

The **System at a Glance** window is displayed.

Step 3 In the **Services** column, click the **Cache** icon.

Note Hover your cursor over the metrics and graphs for descriptions and details.

Viewing Location Metrics

The **Location Metrics** window displays the following metrics for each Cisco CMX node:

- **Location Counts**—The total computations done per second.
- **Location Times**—The location calculation time includes the mathematical portion of the location computation, and in most cases, is about 10 to 20 milliseconds. The location latency is the total time of latency computation from when the message comes from NMSPLB, to location, aggregation, creating cache, and calculation.
- **Location and Nmsplb Location and Nmsplb**—The rate of Network Mobility Service Protocol (NMSP) messages coming in to the NMSPLB.
- **Hyperlocation Rates**—The rate of incoming hyperlocation messages.
- **Location Computation**—The chart for location computation.

To view the Location metrics:

Procedure

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

Step 2 Choose **SYSTEM > Metrics**.

Step 3 In the left pane, click **Location Metrics**.

Viewing Location Metrics Using the Dashboard

Alternatively, to view the Location metrics from the Dashboard:

Procedure

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

Step 2 Choose **SYSTEM > Dashboard**.

The **System at a Glance** window is displayed.

Step 3 In the **Services** column, click the **Location** icon.

Note Hover your cursor over the metrics and graphs for descriptions and details.

Viewing Analytics Notification Metrics

The **Analytics Notification Metrics** window shows the most important performance indicators relating to the Analytics service. A notification is sent from the Location service to the Analytics service when significant movement is detected from a device. Each notification contains an update on the location of a single device.

The Analytics Notification Metrics window displays the following metrics for each Cisco CMX node:

- **Notification processing time**—The average time taken to process an incoming notification. This time will depend on a number of factors, but most notably, the size of the network, that is, the number of buildings, floors, zones, tags, and so on. This metric is relatively stable although you can expect peaks when the system is starting up.
- **Notification queue size**—The size of the queue for incoming notifications, which are queued before being processed. Depending on the system load, the Location service will send the notifications in batches. Therefore, you can always expect a queue of size greater than 0. This mechanism may also result in a very irregular graph at some zoom levels, that is, one with many ups and downs. This is the expected behavior. The queue size is expected to rise when the incoming rate increases. If it continues to grow, you will begin to see dropped notifications in the Notification dropped rate metric
- **Notification dropped rate**—The size of the queue for incoming notifications is limited. Hence, if the queue gets too big, notifications will be rejected. The **Notification dropped rate** graph shows how many notifications are rejected per second. Ideally, you require this chart to show a flat line of 0. If it does not show 0, you should consider adding another server to the cluster for running the Analytics service. This will distribute the load over the two servers.
- **Notification incoming rate**—This is the number of notifications received by the Analytics service per second. This trend should roughly equal the client count, that is, the more clients are detected by the Location service, the more notifications are expected. However, the trend is also influenced by the clients' movement rates because notifications are only sent when the location of a device changes.

To view the Analytics Notification metrics:

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
 - Step 2** Choose **SYSTEM > Metrics**.
 - Step 3** In the left pane, click **Analytics Notification Metrics**.
-

Viewing Analytics Notification Metrics Using the Dashboard

Alternatively, to view the Analytics Notification metrics from the Dashboard:

Procedure

- Step 1** Log in to Cisco Mobile Connected Experiences (Cisco CMX).
 - Step 2** Choose **SYSTEM > Dashboard**.
- The **System at a Glance** window is displayed.

Step 3 In the **Services** column, click the **Analytics** icon.

Note Hover your cursor over the metrics and graphs for descriptions and details.

Viewing Presence Metrics

The **Presence Metrics** window displays the following metrics:

- **Presence Counts**
- **Presence Rates**

To view the Presence metrics:

Procedure

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

Step 2 Choose **SYSTEM > Metrics**.

Step 3 In the left pane, click **Presence Metrics**.



CHAPTER 8

Performing Administrative Tasks

This chapter describes how to perform administrative tasks using Cisco CMX. Users who are assigned administration privileges can perform administrative tasks.

- [Cisco CMX User Accounts, on page 177](#)
- [Unlocking Users, on page 178](#)
- [Recovering Password, on page 178](#)
- [Using FTP Commands for Cisco CMX, on page 179](#)
- [Backing Up Data, on page 179](#)
- [Restoring Data, on page 183](#)
- [Troubleshooting Cisco CMX Server Shutdown Problems, on page 184](#)

Cisco CMX User Accounts

Prior to Cisco CMX 10.2 all Cisco CMX processes ran under the Linux root user account. Cisco CMX 10.2 introduces two new user accounts (cmx and cmxadmin) to prevent any potential risks and secure the system.

- root—Root user account. Users should not use this account.



Note The password of the root account is now being set and maintained by the system owners, and no longer has a default password configured. This way, the account is still available for special-case installation and tackling debugging issues, and the root user will be owned by the end-user. Password recovery is accomplished through the use of the single user login process. For more information see [Recovering Password, on page 178](#).

- cmx—A no login account that now owns all the CMX processes with the exception of postgress.
- cmxadmin—Primary account used for the performance of all administrative tasks using CLI. User will *sudo* from this account to perform tasks requiring root-level access. This account is used to upgrade Cisco CMX 10.2 to a future release using GUI.
- admin—Admin user account for configuring maps, and Cisco WLCs, and restart services using Cisco CMX Web UI.
- normal user accounts—User-defined accounts.

Unlocking Users

You can unlock CMX access for a command line interface (CLI) or graphical user interface (GUI) user after they have been locked out, using the **cmxctl users unlock** command. For caveats and full details, refer to see the *Release Notes for Cisco CMX* at:

<https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-release-notes-list.html>

Before you begin

You must have root access credentials to modify these settings.

Procedure

- Step 1** Connect to CMX via SSH, or through the console if FIPS or UCAPL is enabled.
- Step 2** Enter one of the following commands to unlock a CMX user:
- **cmxctl users unlock cli** *username* to unlock a CLI user.
 - **cmxctl users unlock gui** *username* to unlock a GUI user.
-

The user can log in again from the user interface you unlocked.

Recovering Password

Cisco CMX Release 10.2 uses a single user mode to reset the root and cmxadmin user passwords.

To enter into the single user mode you require:

- A (non-SSH) console connection to the Cisco Mobility Services Engine (Cisco MSE).
- A power-cycle of the Cisco MSE appliance

The GUI admin user password can be reset to the default of admin from the Cisco MSE CLI using the following command:

cmxctl users passwd username

You should know the cmxadmin user password for CLI access.

To reset the root or cmxadmin password, perform the following tasks:

Procedure

- Step 1** Establish console access.
- Step 2** Power on the Cisco MSE.
- Step 3** Press the Up arrow key within 6 seconds of the first text appearing on screen.
- Step 4** When the GRUB menu is displayed:

- a) Verify if the first entry is highlighted.
 - b) Press the **e** key to edit.
- Step 5** Use the Down arrow key to highlight the entry that begins with the word *kernel*.
- a) Press the **e** key to edit the entry.
 - b) Press the space bar, type the word **single**, and then press Enter.
 - c) Press the **b** key to boot the selected entry.
- Step 6** After the system boots and you are at the # prompt:
- a) Enter **passwd** <username> and press Enter.
 - b) When prompted, enter the new password for the user (root/cmadmin) and press Enter.
 - c) Re-enter the password to verify.
- Step 7** Type **reload** and press Enter to reboot the system and load the Cisco CMX services.

Using FTP Commands for Cisco CMX

You can use File Transfer Protocol (FTP) commands for backing up and restoring data on Cisco CMX 10.x. We recommend you to follow the below best practice for data backup automation:

Procedure

- Step 1** Setup a NAS Storage and mount it to your Cisco CMX box, for example, mount the storage to a local directory such as */mnt/nas*.
- Step 2** Write a script to execute the CMX backup program.
- A sample backup script is as mentioned below:
- ```
#!/bin/sh
cd /mnt/nas/backups
ls -ltr cmx_backup* | head -n -3 | xargs -d '\n' rm -f --
cmxos backup --all --path /mnt/nas/backups --online
```
- Step 3** Place the script at */home/cmadmin/backup-cmx.sh*.
- Note** We recommend you to remove previous backups to prevent running out of disk space on the NAS storage.
- Step 4** Run the **cmxos backup --all --path /mnt/nas/backups --online** command.
- Step 5** Add a cron entry to the cmadmin user to execute the backup script, for example, *run everyday at 1:05am, 5*  
*1 \* \* \* \* /home/cmadmin/backup-cmx.sh.*

## Backing Up Data

After you install and run Cisco CMX successfully, you can take a backup to avoid losing any data.

You may lose data on your CMX server, if:

- The hard disk in your CMX server fails
- The data on your CMX server is corrupted while upgrading

Therefore, backing up your data enables you to restore it to the original state. You can back up data on either /tmp or /opt partition. The /tmp folder is allocated 25 GB storage.

If Cisco CMX contains huge amount of saved data, the backup operation will take up extra disk space. In that case, you can consider the following:

- Back up to an external drive if there is not enough space on the Cisco CMX server. You can perform this operation by plugging in a removable hard disk or a mounted hard disk.
- After the backup operation, move the backup file (using scp) to a different server and remove it from the Cisco CMX server.

You can backup data such as location history, current client location, floor maps, and licenses.


**Note**

We recommend that you backup database, floormaps, license and setup components to be compliant with General Data Protection Regulation (GDPR).

The following components are included in the backup:

- Database—Stores configuration data, such as, maps, controllers, location, and aggregated analytics data.
- Cache—Stores analytics repeat visits.
- Cassandra—Stores location history data and analytics raw visits.
- Influxdb—Stores metrics data for systems.
- Consul—Stores Consul configurations.
- Floormaps—Stores floor images for UI display.
- Licenses—Stores Cisco CMX license information.
- Setup—Stores CMX setup data.
- Conf—Stores node configurations.

**Procedure**

To perform a backup operation, run the **cmxos backup** command using the cmxadmin (non-root user) account.

You can include the **-i** (for example, `cmxos backup -i database`) parameter with the backup so that you can choose the components that you want to include in the backup.

The other backup options available are:

- **--all**—Include influxdb in the backup. The default is without influxdb and only includes postgres and Cassandra data.
- **--path**—Specify a location for the backup file. The default location is /tmp.



- **--online**—Perform the backup without stopping cmx services.
- **--offline**—Stop cmx services first and then perform the backup.

**Note**

- The destination directory for backup file requires rwx permission. When you specify a backup directory other than /tmp, ensure that the directory has "r/w/x" permission by user:cmx.
- If High Availability is enabled on Cisco CMX, online backup is supported only on primary and not secondary. If High Availability is disabled, online and offline backups are supported on both primary and secondary.

The following is a sample output from the **cmxos backup** command:

```
[cmxadmin@test ~]$ cmxos backup
Please enter the path for backup file [/tmp]: /tmp
[17:01:30] Preparing for backup...
Data size 287388806
Available disk space 139165282304
Pre-backup took: 0.0118758678436 seconds
['database', 'cache', 'cassandra', 'influxdb', 'consul', 'floormaps', 'licenses', 'setup',
'conf']
[17:01:30] Backup Database...
Backup database took: 1.15777993202 seconds
[17:01:32] Backup Cache...
Backup cache took: 0.383176088333 seconds
[17:01:32] Backup Cassandra...
Backup Cassandra DB took: 2.99715185165 seconds
[17:01:35] Backup InfluxDb...
Backup Influx DB took: 0.0846002101898 seconds
[17:01:35] Backup Consul...
Backup Consul took: 0.0185141563416 seconds
[17:01:35] Backup Floormaps...
Backup floor maps took: 0.000938892364502 seconds
[17:01:35] Backup licenses...
Backup licenses took: 0.000122785568237 seconds
[17:01:35] Backup setup...
Backup setup took: 0.000464200973511 seconds
[17:01:35] Backup node configuration...
Backup configuration took: 0.476609945297 seconds
[17:01:35] Creating tar file..
Post backup took: 16.3115179539 seconds
[17:01:52] Done Backup. Created backup file
/tmp/cmx_backup_test.cisco.com_2015_07_28_17_01.tar.gz
[cmxadmin@test ~]$
```

**What to do next**

You can automate the backing up process. For more information, see [Using FTP Commands for Cisco CMX, on page 179](#).

## Increasing the Hard Disk Space

You can increase the hard disk space if your Virtual Machine that runs Cisco CMX is run out of disk space for backup.

## Procedure

**Step 1** Stop all the Cisco CMX services by entering the following commands:

```
cmxctl stop
```

```
cmxctl stop -a
```

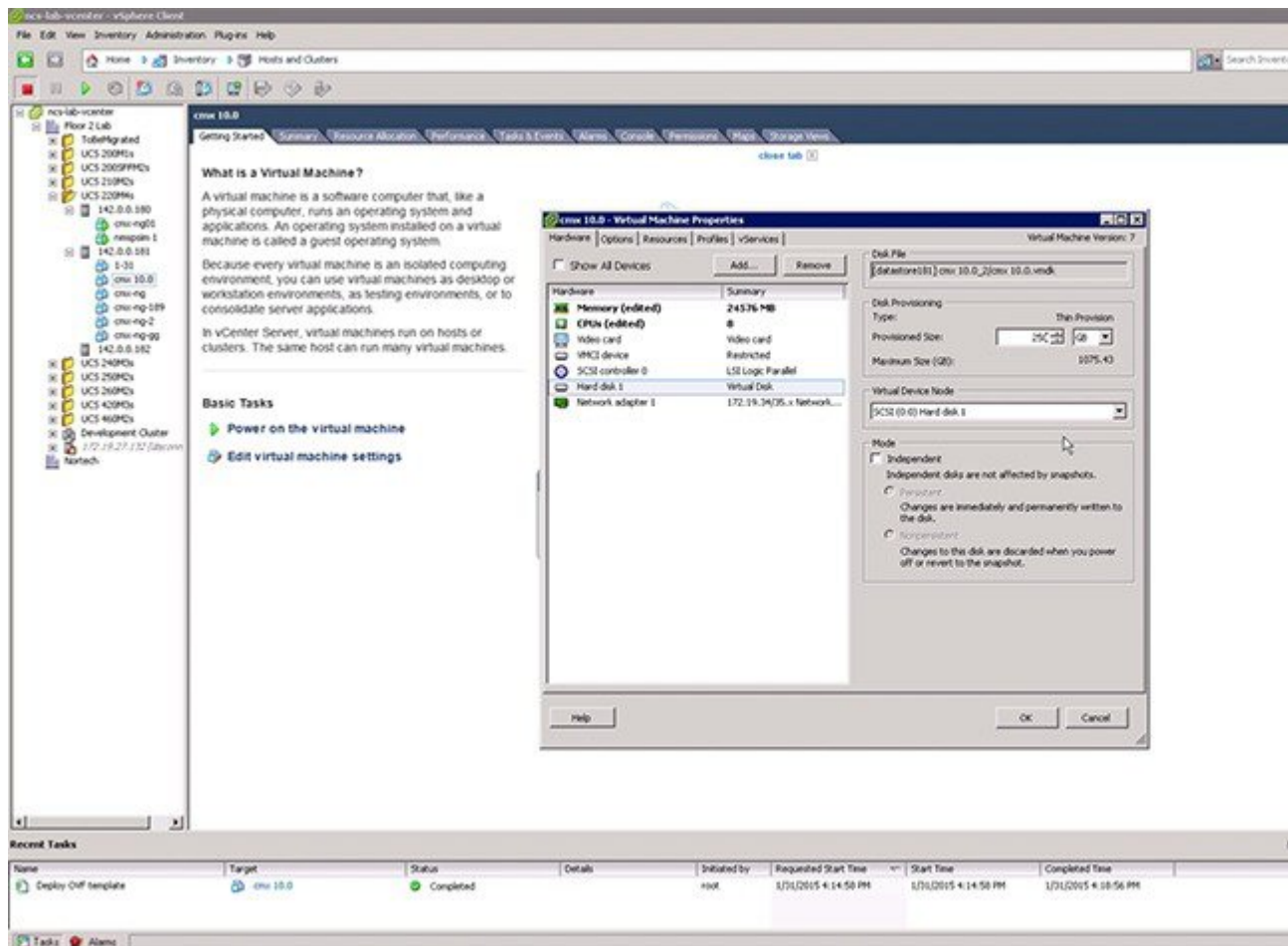
**Step 2** Shutdown the virtual machine by entering the following command:

```
Shutdown -h now
```

**Step 3** Edit the virtual machine settings and increase the hard disk space.

**Note** You cannot increase the hard disk space if the virtual machine was ever restored from snapshot.

**Figure 17: Virtual Machine Settings**



**Step 4** Reboot the virtual machine.

After performing these steps, you can back up Cisco CMX.

You can enter the **cmxctl status** command to verify the status of CMX services. If any of the services is not running, you may need to restart it by entering the **cmxctl restart** *<service name>* command.

## Restoring Data

After the backup, you can save the backup file in a safe location. If required, you can restore from this location.

To restore data, the Cisco CMX server must have free disk space which is 4 times the size of the backup file. If there is not enough disk space in the Cisco CMX server, you must increase the disk space. For more information, see [Increasing the Hard Disk Space](#).



### Note

When you restore data, if there is not enough disk space in the Cisco CMX server, try to untar the file from an external drive. The untarred files will be in binary format, which can be read by database servers. Restoring Cisco CMX data must be done on a device that has the same local time as the device from which the data is collected. Otherwise, you will not be able to correctly access the analytics data. In addition, the data will result in errors or zero values on reports.

### Procedure

To restore the data, enter the **cmxos restore** command using the **cmxadmin** (non-root user) account.

You can include the **-i** (for example, **cmxos restore -i database**) parameter with the **restore** command so that you can choose the components that you want to restore.

The following is a sample output from the **cmxos restore** command:

```
[cmxadmin@test~]$ cmxos restore
Please enter the backup file path: /tmp/cmx_backup_test.cisco.com_2015_07_28_17_01.tar.gz
Please enter the path for untar backup file [/tmp]: /tmp
[17:08:54] Preparing for restore...
Restore size 27866720
Available disk space in /tmp is 139137040384
Available disk space is 139424529077
[17:08:54] Untarring backup file...
[17:08:55] Stopping all services...
Pre restore took: 26.4669179916 seconds
[17:09:21] Restoring Database...
Created database mse
Running command /usr/bin/sudo -u postgres pg_restore -d mse -Fc
/tmp/cmx_backup_test.cisco.com_2015_07_28_17_01/postgres/mse.dump
Restored database mse
Restarting database...
Restore database took: 18.3071520329 seconds
[17:09:39] Restoring Cache...
Stopping cache_6383...
Restarting cache_6383...
Stopping cache_6380...
Restarting cache_6380...
.....
Stopping cache_6382...
Restarting cache_6382...
Stopping cache_6379...
```

```

Restarting cache_6379...
Stopping cache_6381...
Restarting cache_6381...
Stopping cache_6378...
Restarting cache_6378...
Restore Cache took: 46.7663149834 seconds
[17:10:26] Restoring Cassandra...
Stopping Cassandra...
Starting casandra
Creating cassandra scehma
.....
Restore Cassandra took: 29.5983269215 seconds
[17:10:56] Restoring Influxdb...
Stopping Influxdb...
Restarting Influxdb...
Restore Influx DB took: 13.9934449196 seconds
[17:11:10] Restoring consul...
Restore Consul took: 0.761927843094 seconds
[17:11:10] Restoring floormaps...
Restore floor maps took: 0.0269021987915 seconds
[17:11:10] Restoring licenses...
Restore licenses took: 0.00019907951355 seconds
[17:11:10] Restoring setup...
Restore setup took: 0.000532150268555 seconds
[17:11:10] Running Post Restore Tasks...
[17:11:10] Migrating Schemas...
[17:11:11] Migrating Cassandra schemas...
[17:11:12] Restarting all services...
stopping cassandra
Post restore took: 6.64956212044 seconds
[17:11:17] Starting all services...
.....
[17:12:45] Done
$

```

## Troubleshooting Cisco CMX Server Shutdown Problems

The Cisco CMX server shuts down all the services when disk space usage reaches 85 percent. If you encounter this issue, create additional disk space on your Cisco CMX server by deleting unnecessary files, if any, from the server. Run the `cmxos clean find/normal` command to find unnecessary files and delete it to free some disk space.

After you have sufficient space, you can choose to restart your Cisco CMX server by running the `cmxctl start -a` command, if required.



## APPENDIX A

# Guidelines for Managing Zones in Cisco CMX

---

For more information about managing zones, see [Managing Perimeters and Zones on Location Maps](#), on page 126.

Common issues related to map import:

### **Case 1: Clients not detected, Heatmap generation failed**

#### **Initial Observations**

A customer is using the 10.3.0-19 build and CMX is not detecting Clients / Tags. After debugging it was found that there are no heatmaps generated on CMX and the location computations are failing. Matlab-engine logs show a message 'No floors present in model info, heatmaps will not be computed'.

#### **What went wrong?**

While exporting maps from Prime Infrastructure, Calibration model information was not included in the exported map file.

#### **How to fix it?**

Calibration model information is a vital piece of data linked to a floor-map on CMX. Client detection, Location computation and heatmap generation depends on Calibration model information.

When we export Maps from Cisco Prime Infrastructure, there is an option **Include Calibration Information** which is selected by default. While exporting maps, We want to make sure that this option is checked all the time.



**Maps Tree View** ▾

- ▾ Root Area
  - ▶ System Campus
  - Unassigned
  - ▶ Nortech Campus
  - ▾ pwalawal-campus
    - ▾ pwalawal-building-1
      - pwalawal-floor-1
      - pwalawal-floor-2
    - ▾ pwalawal-zone-test-campus
      - ▾ pwalawal-zone-test-building
        - pwalawal-zone-test-floor-1
        - pwalawal-zone-test-floor-2

### Export Map

- Include Calibration Information
  - Calibration Information for Selected Maps
- Select All Maps
- Nortech Campus
- System Campus
- Unassigned
- pwalawal-campus
- pwalawal-zone-test-campus

Export Cancel

**Case 2: The 'Access point' shows up on two floor-maps.**

**Initial Observations**

The customer moved the Access points from Floor-X to Floor-Y on Prime Infrastructure and delete Floor-Y from Prime Infrastructure. Then they imported only 'Floor-X' on CMX. Now CMX shows same set of APs on both 'Floor-X' and 'Floor-Y'.

**What went wrong?**

When the APs were moved from Floor-X to Floor-Y and Floor-Y was deleted, A deleted operation for 'Floor-Y' was not executed on CMX. Unless user chooses the option 'Delete & replace existing maps & analytics data' while importing the maps, The entire map hierarchy will not be overwritten. If the option 'Delete & replace existing maps & analytics data' is not selected, CMX will only update the floors present in the uploaded map archive (i.e. Floor-X in this case).

**How to fix it?**

Before re-importing 'Floor-X', you want to make sure that 'Floor-Y' is deleted from CMX so that the APs linked to 'Floor-Y' are also deleted. This can be done via CMX CLI command as follows.

1. ssh to CMX as cmxadmin user.
2. List the floors and identify the floor from which the APs are moved.

```
[cmxadmin@cmx-prod opt]# cmxctl config maps floors
+-----+-----+-----+-----+
| Floor Name | Location Floor ID | Analytics Floor ID |
+-----+-----+-----+-----+
| Mall of America>Mall of America>Garage B2 | -60xxxxxxxxxxxxxxxxxxxx | 52 |
+-----+-----+-----+-----+
| Mall of America>Mall of America>Level 1 | -604xxxxxxxxxxxxxxxxxxxx | 53 |
+-----+-----+-----+-----+
```

3. Execute delete floormap command for the identified floor so that The APs linked to that floor are deleted form CMX.

```
[cmxadmin@cmx-prod opt]# cmxctl config maps delete
Please enter the hierarchy to be deleted
(campus-name>building-name>floor-name): Mall of America>Mall of America>Level 1
Confirm delete hierarchy:
Mall+of+America%3EMall+of+America%3ELevel+1 ? [y/N]: y
Hierarchy Mall+of+America%3EMall+of+America%3ELevel+1
deleted.
[cmxadmin@cmx-prod opt]#
```

4. Make sure that the floor is deleted by listing the floors.

```
[cmxadmin@cmx-prod opt]# cmxctl config maps floors
+-----+-----+-----+-----+
| Floor Name | Location Floor ID | Analytics Floor ID |
+-----+-----+-----+-----+
| Mall of America>Mall of America>Garage B2 | -60xxxxxxxxxxxxxxxxxxxx | 52 |
+-----+-----+-----+-----+
```

5. Export only 'Floor-X' from Prime Infrastructure and Import the maps file on CMX so that new APs are now added to 'Floor-X'.

6. Go to CMX GUI on 'Detect and Locate' page and observe the floor-maps. 'Floor-X' should have the new set of APs on it.





## APPENDIX B

### Cisco CMX Alerts

Cisco CMX alerts can be of different level of severity. For critical alerts, there is an immediate impact on Cisco CMX and as a customer you should take necessary steps to resolve. Else, you will be risking losing data, for example, if a controller is down, you will not be able to retrieve data for any floor/access point that the controller manages.

As a customer, you can only resolve the obvious alerts such as controller not working. Most of the other alerts either indicate an undersized Cisco CMX or a critical failure in Cisco CMX. Both these cases would require intervention from Cisco CMX technical experts. You can use some of the **cmxos** and **cmxctl** commands to fix these critical failures. We recommend that you seek Cisco CMX technical help for troubleshooting.

| Cisco CMX Alert          | Description                                              | Possible Solution                                                                                        |
|--------------------------|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| CPU_USAGE                | Displayed when your CPU exceeds 80% on a Cisco CMX box.  | Upgrade to a bigger Cisco CMX box.                                                                       |
| MEMORY_USAGE             | This alert is displayed when the memory usage is high.   | Reduce the load on the Cisco CMX. Probably need a bigger CMX. Support should be able to figure that out. |
| SERVICE_STATUS           | Displayed when a Cisco CMX service is crashed.           | We recommend that you call the support.                                                                  |
| DATA_PROCESSING_STATUS   | Displayed when the Analytics service is slowing down.    | Reduce load.                                                                                             |
| NMSP_CONNECTION_STATUS   | Displayed when the Controller goes down for some reason. | Troubleshoot for a probable networking issue.                                                            |
| OUT_OF_MEMORY            | Not used in Cisco CMX.                                   | NA.                                                                                                      |
| QUEUE_FULL               | Not used in Cisco CMX.                                   | NA                                                                                                       |
| ARRAY_INDEX_OUT_OF_BOUND | Not used in Cisco CMX                                    | NA                                                                                                       |

| Cisco CMX Alert                | Description                                                                                                | Possible Solution                                                                                                                           |
|--------------------------------|------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| BEACON_STATUS                  | Not supported                                                                                              | NA                                                                                                                                          |
| BEACON_MOVEMENT                | Not supported                                                                                              | NA                                                                                                                                          |
| DISK_USAGE                     | Displayed when the Hard drive is getting full.                                                             | Run the cmx cleanup tool or remove unnecessary load from the hard drive.                                                                    |
| AWIPS_LICENSE                  | Not used in Cisco CMX                                                                                      | NA                                                                                                                                          |
| NMSP_MSG_RATE_EXCEEDED         | Displayed when the system is getting too many NMSP messages for its box type.                              | We recommend that you either get a bigger box or clear unwanted clients by removing a controller or a map.                                  |
| LOCATION_OVERLOADED            | Critical alert that is not expected to happen.                                                             | NA                                                                                                                                          |
| EVAL_LICENSE_EXPIRY            | Displayed after the built in license expired after 120 days.                                               | We recommend that you buy and activate a new Cisco CMX license.                                                                             |
| AP_CONTROLLER_FETCH_STATUS     | Displayed if SNMP information from the controller cannot be fetched.                                       | Provide Cisco CMX with valid SNMP credentials.                                                                                              |
| SSID_CONTROLLER_FETCH_STATUS   | Same as AP Controller.                                                                                     | NA                                                                                                                                          |
| MAP_IMPORT_ERROR               | Displayed if maps are not imported successfully during the import process from Cisco Prime Infrastructure. | We recommend that you contact support to re-import maps from Cisco Prime Infrastructure.                                                    |
| ANALYTICS_MISMATCH             | Displayed if Analytics sanity test is failed.                                                              | We recommend that you call the Cisco support.                                                                                               |
| HETERARCHY_SIZE_LIMIT_EXCEEDED | Displayed if maps/aps/zones numbers exceed their limit for the corresponding Cisco CMX service type.       | This might affect Cisco CMX performance. We recommend that you either reduce the number of elements or move them to a larger Cisco CMX box. |

| Cisco CMX Alert | Description                                                                                                                    | Possible Solution                                       |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| mem_usage       | Displayed once the memory usage is above 80%. This is a critical error.                                                        | Consider upgrading hardware or VM specs.                |
| SERVER_STATUS   | Displayed after the High Availability is successfully disabled. The Primary server is no longer syncing with secondary server. | This is an informational alert, and no action required. |
| SERVER_STATUS   | Displayed when attempting to failback from secondary server to primary server: 192.168.99.110.                                 | This is an informational alert, and no action required. |

| Monit Email                  | Customer Action                                 |
|------------------------------|-------------------------------------------------|
| 1m Load avg. above 3         | No action required.                             |
| 1m Load avg. recovered       | No action required.                             |
| 5m Load avg. above 3         | No action required.                             |
| 5m Load avg. recovered       | No action required.                             |
| 15m Load avg. above 2        | No action required.                             |
| 15m Load avg. recovered      | No action required.                             |
| Adminui service is down      | Run the <b>cmxos adminui start</b> command.     |
| Agent service is down        | Run the <b>cmxctl agent start</b> command.      |
| Analytics service is down    | Run the <b>cmxctl analytics start</b> command.  |
| Analytics service recovered  | No action required.                             |
| cache_6378 service is down   | Run the <b>cmxctl cache_6378 start</b> command. |
| cache_6378 service recovered | No action required.                             |
| cache_6379 service is down   | Run the <b>cmxctl cache_6379 start</b> command. |
| cache_6379 service recovered | No action required.                             |
| cache_6380 service is down   | Run the <b>cmxctl cache_6380 start</b> command. |
| cache_6380 service recovered | No action required.                             |

| <b>Monit Email</b>                | <b>Customer Action</b>                             |
|-----------------------------------|----------------------------------------------------|
| cache_6381 service is down        | Run the <b>cmxctl cache_6381 start</b> command.    |
| cache_6381 service recovered      | No action required.                                |
| cache_6382 service is down        | Run the <b>cmxctl cache_6382 start</b> command.    |
| cache_6382 service recovered      | No action required.                                |
| cache_6383 service is down        | Run the <b>cmxctl cache_6383 start</b> command.    |
| cache_6383 service recovered      | No action required.                                |
| cache_6385 service is down        | Run the <b>cmxctl cache_6385 start</b> command.    |
| cache_6385 service recovered      | No action required.                                |
| cassandra service is down         | Run the <b>cmxctl cassandra start</b> command.     |
| cassandra service recovered       | No action required.                                |
| Collectd service is down          | No action required.                                |
| Collectd service is up            | No action required.                                |
| Confd service is down             | Run the <b>cmxctl confd start</b> command.         |
| Confd service is up               | No action required.                                |
| configuration service is down     | Run the <b>cmxctl configuration start</b> command. |
| configuration service recovered   | No action required.                                |
| Consul Service is down            | Run the <b>cmxctl consul start</b> command.        |
| Disk usage is above 80%           | Remove files. Add storage.                         |
| Disk usage recovered              | No action required.                                |
| DNSMasq service is down           | No action required.                                |
| File Descriptors are above bounds | No action required.                                |
| File Descriptors recovered        | No action required.                                |
| <b>File system</b>                |                                                    |
| HAProxy service is down           | Run the <b>cmxctl haproxy start</b> command.       |
| HAProxy service is up             | No action required.                                |
| hyperlocation service is down     | Run the <b>cmxctl hyperlocation start</b> command. |
| hyperlocation service recovered   | No action required.                                |
| Influxdb service is down          | Run the <b>cmxctl influxdb start</b> command.      |

| Monit Email                    | Customer Action                                                                                                                                                                                          |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Influxdb service is up         | No action required.                                                                                                                                                                                      |
| Inode usage is above 80%       | Remove files.                                                                                                                                                                                            |
| Inode usage recovered          | No action required.                                                                                                                                                                                      |
| Load                           | Suggested actions to lessen the load: <ul style="list-style-type: none"> <li>• Create fewer notifications</li> <li>• Run fewer reports</li> <li>• Remove some WLCs</li> <li>• Upgrade system.</li> </ul> |
| location service is down       | Run the <b>cmxctl location start</b> command.                                                                                                                                                            |
| location service recovered     | No action required.                                                                                                                                                                                      |
| matlabengine service is down   | Run the <b>cmxctl matlabengine start</b> command.                                                                                                                                                        |
| matlabengine service recovered | No action required.                                                                                                                                                                                      |
| Memory usage is above 80%      | Restart the system during a quiet period. Upgrade system.                                                                                                                                                |
| Memory usage recovered         | No action required.                                                                                                                                                                                      |
| Monit instance changed         | None. Informational.                                                                                                                                                                                     |
| nmsplb service is down         | Run the <b>cmxctl nmsplb start</b> command.                                                                                                                                                              |
| nmsplb service recovered       | No action required.                                                                                                                                                                                      |
| Port 5432 is not responding    | Run the <b>cmxctl database stop</b> and <b>cmxctl database start</b> command.                                                                                                                            |
| Port 5432 is responding        | No action required.                                                                                                                                                                                      |
| Port 6378 is not responding    | Run the <b>cmxctl cache_6378 stop</b> and <b>cmxctl cache_6378 start</b> command.                                                                                                                        |
| Port 6378 responding           | No action required.                                                                                                                                                                                      |
| Port 6379 is not responding    | Run the <b>cmxctl cache_6379 stop</b> and <b>cmxctl cache_6379 start</b> command.                                                                                                                        |
| Port 6379 responding           | No action required.                                                                                                                                                                                      |
| Port 6380 is not responding    | Run the <b>cmxctl cache_6380 stop</b> and <b>cmxctl cache_6380 start</b> command.                                                                                                                        |
| Port 6380 responding           | No action required.                                                                                                                                                                                      |

| Monit Email                 | Customer Action                                                                         |
|-----------------------------|-----------------------------------------------------------------------------------------|
| Port 6381 is not responding | Run the <b>cmxctl cache_6381 stop</b> and <b>cmxctl cache_6381 start</b> command.       |
| Port 6381 responding        | No action required.                                                                     |
| Port 6382 is not responding | Run the <b>cmxctl cache_6382 stop</b> and <b>cmxctl cache_6382 start</b> command.       |
| Port 6382 responding        | No action required.                                                                     |
| Port 6383 is not responding | Run the <b>cmxctl cache_6383 stop</b> and <b>cmxctl cache_6383 start</b> command.       |
| Port 6383 responding        | No action required.                                                                     |
| Port 6385 is not responding | Run the <b>cmxctl cache_6385 stop</b> and <b>cmxctl cache_6385 start</b> command.       |
| Port 6385 responding        | No action required.                                                                     |
| Port 6511 is not responding | Run the <b>cmxctl hyperlocation stop</b> and <b>cmxctl hyperlocation start</b> command. |
| Port 6512 responding        | No action required.                                                                     |
| Port 6531 is not responding | Run the <b>cmxctl location stop</b> and <b>cmxctl location start</b> command.           |
| Port 6531 responding        | No action required.                                                                     |
| Port 6532 is not responding | Run the <b>cmxctl location stop</b> and <b>cmxctl location start</b> command.           |
| Port 6532 responding        | No action required.                                                                     |
| Port 6541 is not responding | Run the <b>cmxctl analytics stop</b> and <b>cmxctl analytics start</b> command.         |
| Port 6541 responding        | No action required.                                                                     |
| Port 6542 is not responding | Run the <b>cmxctl analytics stop</b> and <b>cmxctl analytics start</b> command.         |
| Port 6542 responding        | No action required.                                                                     |
| Port 6551 is not responding | Run the <b>cmxctl configuration stop</b> and <b>cmxctl configuration start</b> command. |
| Port 6551 responding        | No action required.                                                                     |
| Port 6552 is not responding | Run the <b>cmxctl configuration stop</b> and <b>cmxctl configuration start</b> command. |

| Monit Email                                   | Customer Action                                                                       |
|-----------------------------------------------|---------------------------------------------------------------------------------------|
| Port 6552 responding                          | No action required.                                                                   |
| Port 6571 is not responding                   | Run the <b>cmxctl nmsplb stop</b> and <b>cmxctl nmsplb start</b> command.             |
| Port 6571 responding                          | No action required.                                                                   |
| Port 6572 is not responding                   | Run the <b>cmxctl nmsplb stop</b> and <b>cmxctl nmsplb start</b> command.             |
| Port 6572 responding                          | No action required.                                                                   |
| Port 6581 is not responding                   | Run the <b>cmxctl matlabengine stop</b> and <b>cmxctl matlabengine start</b> command. |
| Port 6581 is responding                       | No action required.                                                                   |
| Port 6582 is not responding                   | Run the <b>cmxctl matlabengine stop</b> and <b>cmxctl matlabengine start</b> command. |
| Port 6582 is responding                       | No action required.                                                                   |
| Port 9042 is not responding                   | Run the <b>cmxctl cassandra stop</b> and <b>cmxctl cassandra start</b> command.       |
| Port 9042 is responding                       | No action required.                                                                   |
| postgres service is down                      | Run the <b>cmxctl database start</b> command.                                         |
| postgres service is up                        | No action required.                                                                   |
| qllesspy service is down                      | Run the <b>cmxctl qllesspy start</b> command.                                         |
| qllesspy service recovered                    | No action required.                                                                   |
| Socket 5432 is not responding                 | Run the <b>cmxctl database stop</b> and <b>cmxctl database start</b> command.         |
| Socket 5432 is responding                     | No action required.                                                                   |
| Swap usage is above 80%                       | Increase swap space or reduce memory usage.                                           |
| Swap usage recovered                          | No action required.                                                                   |
| SYS CPU usage is above 60%                    | No action required.                                                                   |
| SYS CPU usage recovered                       | No action required.                                                                   |
| The analytics service is not reporting health | Run the <b>cmxctl analytics stop</b> and <b>cmxctl analytics start</b> command.       |
| The analytics service reporting health        | No action required.                                                                   |

| Monit Email                                       | Customer Action                                                                         |
|---------------------------------------------------|-----------------------------------------------------------------------------------------|
| The configuration service is not reporting health | Run the <b>cmxctl configuration stop</b> and <b>cmxctl configuration start</b> command. |
| The configuration service reporting health        | No action required.                                                                     |
| The hyperlocation service is not reporting health | Run the <b>cmxctl hyperlocation stop</b> and <b>cmxctl hyperlocation start</b> command. |
| The hyperlocation service reporting health        | No action required.                                                                     |
| The location service is not reporting health      | Run the <b>cmxctl location stop</b> and <b>cmxctl location start</b> command.           |
| The location service reporting health             | No action required.                                                                     |
| The matlabengine service is not reporting health  | Run the <b>cmxctl matlabengine stop</b> and <b>cmxctl matlabengine start</b> command.   |
| The matlabengine service reporting health         | No action required.                                                                     |
| The nmsplb service is not reporting health        | Run the <b>cmxctl nmsplb stop</b> and <b>cmxctl nmsplb start</b> command.               |
| The nmsplb service reporting health               | No action required.                                                                     |
| USR CPU usage is above 80%                        | No action required.                                                                     |
| USR CPU usage recovered                           | No action required.                                                                     |
| WAIT CPU usage is above 60%                       | No action required.                                                                     |
| WAIT CPU usage recovered                          | No action required.                                                                     |
| Memory usage is above 80%                         | Restart the system during a quiet period.<br>Upgrade system.                            |
| Memory usage recovered                            | No action required.                                                                     |
| Swap usage is above 80%                           | Increase swap space or reduce memory usage.                                             |
| File system                                       |                                                                                         |
| Disk usage is above 80%                           | Remove files.<br>Add storage.                                                           |
| Disk usage recovered                              | No action required.                                                                     |
| Inode usage is above 80%                          | Remove files.                                                                           |
| Inode usage recovered                             | No action required.                                                                     |
| File Descriptors are above bounds                 | Restart the system.                                                                     |



| <b>Monit Email</b>                               | <b>Customer Action</b>                                                                |
|--------------------------------------------------|---------------------------------------------------------------------------------------|
| File Descriptors recovered                       | No action required.                                                                   |
| ocation service is down                          | Run the <b>cmxctl location start</b> command.                                         |
| location service recovered                       | No action required.                                                                   |
| Port 6531 is not responding                      | Run the <b>cmxctl location stop</b> and <b>cmxctl location start</b> command.         |
| Port 6531 responding                             | No action required.                                                                   |
| Port 6532 is not responding                      | Run the <b>cmxctl location stop</b> and <b>cmxctl location start</b> command.         |
| Port 6532 responding                             | No action required.                                                                   |
| The location service is not reporting health     | Run the <b>cmxctl location stop</b> and <b>cmxctl location start</b> command.         |
| The location service reporting health            | No action required.                                                                   |
| matlabengine service is down                     | Run the <b>cmxctl matlabengine start</b> command.                                     |
| matlabengine service recovered                   | No action required.                                                                   |
| Port 6581 is not responding                      | Run the <b>cmxctl matlabengine stop</b> and <b>cmxctl matlabengine start</b> command. |
| Port 6581 responding                             | No action required.                                                                   |
| Port 6582 is not responding                      | Run the <b>cmxctl matlabengine stop</b> and <b>cmxctl matlabengine start</b> command. |
| Port 6582 responding                             | No action required.                                                                   |
| The matlabengine service is not reporting health | Run the <b>cmxctl matlabengine stop</b> and <b>cmxctl matlabengine start</b> command. |
| The matlabengine service reporting health        | No action required.                                                                   |
| nmsplb service is down                           | Run the <b>cmxctl nmsplb start</b> command.                                           |
| nmsplb service recovered                         | No action required.                                                                   |
| Port 6571 is not responding                      | Run the <b>cmxctl nmsplb stop</b> and <b>cmxctl nmsplb start</b> command.             |
| Port 6572 responding                             | No action required.                                                                   |
| The nmsplb service is not reporting health       | Run the <b>cmxctl nmsplb stop</b> and <b>cmxctl nmsplb start</b> command.             |
| The nmsplb service reporting health              | No action required.                                                                   |

| <b>Monit Email</b>            | <b>Customer Action</b>                                                            |
|-------------------------------|-----------------------------------------------------------------------------------|
| postgres service is down      | Run the <b>cmxctl database start</b> command.                                     |
| postgres service is up        | No action required.                                                               |
| Socket 5432 is not responding | Run the <b>cmxctl database stop</b> and <b>cmxctl database start</b> command.     |
| Socket 5432 is responding     | No action required.                                                               |
| Port 5432 is not responding   | Run the <b>cmxctl database stop</b> and <b>cmxctl database start</b> command.     |
| Port 5432 is responding       | No action required.                                                               |
| qlesspy service is down       | Run the <b>cmxctl qlesspy start</b> command.                                      |
| qlesspy service recovered     | No action required.                                                               |
| cache_6378 service is down    | Run the <b>cmxctl cache_6378 start</b> command.                                   |
| cache_6378 service recovered  | No action required.                                                               |
| Port 6378 is not responding   | Run the <b>cmxctl cache_6378 stop</b> and <b>cmxctl cache_6378 start</b> command. |
| Port 6378 responding          | No action required.                                                               |
| cache_6379 service is down    | Run the <b>cmxctl cache_6379 start</b> command.                                   |
| cache_6379 service recovered  | No action required.                                                               |
| Port 6379 is not responding   | Run the <b>cmxctl cache_6379 stop</b> and <b>cmxctl cache_6379 start</b> command. |
| Port 6379 responding          | No action required.                                                               |
| cache_6380 service is down    | Run the <b>cmxctl cache_6380 start</b> command.                                   |
| cache_6380 service recovered  | No action required.                                                               |
| Port 6380 is not responding   | Run the <b>cmxctl cache_6380 stop</b> and <b>cmxctl cache_6380 start</b> command. |
| Port 6380 responding          | No action required.                                                               |
| cache_6381 service is down    | Run the <b>cmxctl cache_6381 start</b> command.                                   |
| cache_6381 service recovered  | No action required.                                                               |
| Port 6381 is not responding   | Run the <b>cmxctl cache_6381 stop</b> and <b>cmxctl cache_6381 start</b> command. |
| Port 6381 responding          | No action required.                                                               |

| <b>Monit Email</b>           | <b>Customer Action</b>                                                            |
|------------------------------|-----------------------------------------------------------------------------------|
| cache_6382 service is down   | Run the <b>cmxctl cache_6382 start</b> command.                                   |
| cache_6382 service recovered | No action required.                                                               |
| Port 6382 is not responding  | Run the <b>cmxctl cache_6382 stop</b> and <b>cmxctl cache_6382 start</b> command. |
| Port 6382 responding         | No action required.                                                               |
| cache_6383 service is down   | Run the <b>cmxctl cache_6383 start</b> command.                                   |
| cache_6383 service recovered | No action required.                                                               |
| Port 6383 is not responding  | Run the <b>cmxctl cache_6383 stop</b> and <b>cmxctl cache_6383 start</b> command. |
| Port 6383 responding         | No action required.                                                               |
| cache_6385 service is down   | Run the <b>cmxctl cache_6385 start</b> command.                                   |
| cache_6385 service recovered | No action required.                                                               |
| Port 6385 is not responding  | Run the <b>cmxctl cache_6385 stop</b> and <b>cmxctl cache_6385 start</b> command. |
| Port 6385 responding         | No action required.                                                               |





# APPENDIX **C**

## Cisco CMX Network Protocols and Port Matrix

The following table lists the ports that Cisco CMX uses for communicating with wireless clients, controllers, Cisco Prime Infrastructure, and mail servers:

**Table 15: Cisco CMX Network Protocols and Port Matrix**

| Source Device         | Destination Device | Protocol | Destination Port | Description                                                  |
|-----------------------|--------------------|----------|------------------|--------------------------------------------------------------|
| Cisco CMX             | NMSP on WLC        | TCP      | 16113            | -                                                            |
| Cisco CMX             | SNMP on WLC        | UDP      | 161/162          | -                                                            |
| Cisco CMX             | NTP Server         | UDP      | 123              | -                                                            |
| Cisco CMX             | DNS Server         | -        | 53               | -                                                            |
| Cisco CMX             | Mail Server        | TCP      | 25               | -                                                            |
| Cisco CMX             | Internet           | -        | 80/443           | Used to pull down images of world map and validate addresses |
| Web                   | CMX HTTPS          | TCP      | 443              | Used to manage and administer Cisco CMX                      |
| Cisco CMX CLI via SSH | CMX Management     | -        | 22               | -                                                            |
| Web                   | CMX Management     | -        | 1948             | Used to upgrade Cisco CMX                                    |
| HTTPS                 | Clients            | TCP      | 443              | -                                                            |
| HTTP                  | Clients            | TCP      | 80               | -                                                            |

**Table 16: HA Port Information**

| HA Ports          | Description                                                                                            |
|-------------------|--------------------------------------------------------------------------------------------------------|
| 7000, 7001, 9042  | Cassandrs database                                                                                     |
| 6378 through 6385 | Redis                                                                                                  |
| 4242              | High availability REST and web service. An HTTPS protocol using REST to communicate between the CMX HA |
| 22                | SSH port and used to synchronize files between servers                                                 |

**Table 17: Cassandra Database**

| Cassandra Database | Protocol          |
|--------------------|-------------------|
| 7000               | TCP               |
| 7001               | TCP               |
| 9042               | SSL Communication |