Cisco Connected Mobile Experiences Configuration Guide, Release 10.2

First Published: 2015-09-23

Last Modified: 2016-05-31

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

CONTENTS

Preface

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.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	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.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.

Convention	Indication
<>	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	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 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-h

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

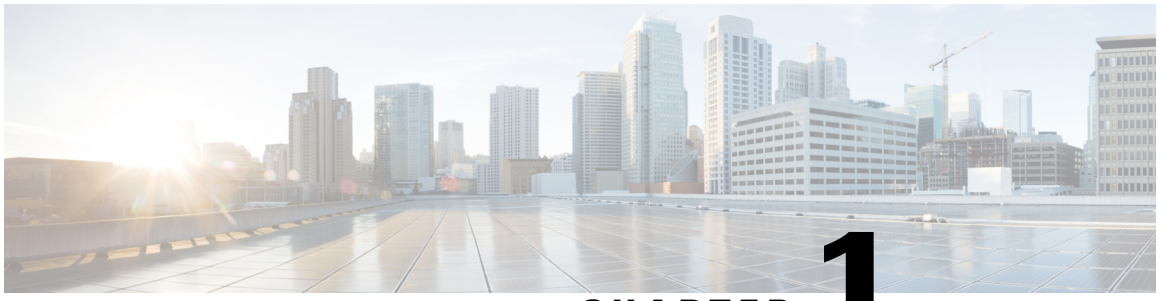
For more information about Cisco CMX Cloud, see:

https://support.cmxcisco.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 What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.



CHAPTER 1

Getting Started

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, see the *Release Notes for Cisco CMX, Release 10.2*, at:

http://www.cisco.com/c/en/us/td/docs/wireless/mse/release/notes/cmx_10_2_rn.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)
  - BLE Beacons (Bluetooth Icon)
  - Active Wifi RFID Tags (Tag icon)

  The background map can display:
  - Inclusion and Exclusion Zones imported from Cisco Prime Infrastructure
  - Analytics Zones created in Cisco CMX

  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 & ENGAGE—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 Connect and Engage Service, on page 41.
- **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 23.

- **CONNECT & ENGAGE—**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 Connect and Engage Service, on page 41.
- **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 devise 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 78.
  If you choose Presence during installation, you will see the following services in the Cisco CMX GUI.
  - PRESENCE ANALYTICS
  - CONNECT & ENGAGE
  - 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 91.
- **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 111.

For a complete list of new features supported by Cisco CMX 10.2, see the *Release Notes for Cisco CMX 10.2* at:

http://www-author.cisco.com/c/en/us/td/docs/wireless/mse/release/notes/cmx_10_2_rn.html

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

Prerequisites for Configuring Cisco CMX 10.2

The following components are mandatory for you to configure Cisco CMX 10.2:

- Exported maps (in the form of files) from Cisco Prime Infrastructure 1.3, 1.4, 2.2, 3.0, or 3.1

  Note Import maps from Cisco Prime Infrastructure only if you are using the Cisco CMX Location service. You do not have to import them if you are using the Presence Analytics service because this service does not require maps; all configurations are accomplished using the Presence Analytics Dashboard.

- Cisco Wireless Controller (Cisco WLC) 7.6, 8.0, 8.1, 8.2, or 8.3
- Cisco CMX 10.2 License (Cisco CMX 10.2 ships with a fully functional 120-day evaluation license that is activated after Cisco CMX is installed and started for the first time. For information about adding permanent licenses, see Adding a License, on page 92.)

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 CLI, perform one of the following tasks:

- Import the exported maps into Cisco CMX using 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, Release 10.2*, at:

  http://www.cisco.com/c/en/us/td/docs/wireless/mse/10-2/cmx_command/guide/cmxcli10.html.

Note When importing the maps from Prime Infrastructure using CLI, you also can import the zones. To import zone, set the import zone option as **Yes** and import the maps.

To import maps using the GUI, perform the following tasks:

1. Log in to Cisco Mobile Connected Experiences (Cisco CMX).
2. Click **SYSTEM > Dashboard**.
3. Click the **Gear** icon at the top-right corner of the window.
4. Click **Controllers and Maps Setup > Import**.

Note Cisco CMX 10.2 provides an **Delete & Replace Maps** option (**SYSTEM** > **SETTINGS**). By default, this option is enabled. When you enable this option, the Cisco CMX maps will be replaced with the maps defined in the file that you import.

If you want to delete the imported maps, you must provide the correct map hierarchy for CMX to locate the maps you intend to delete.

Adding Cisco WLCs

You can add Cisco WLCs using CLI or the CMX user interface. If you add Cisco WLCs using Prime Infrastructure, then the controller configuration will not work unless the NMSP connection is correct. However, the controller may be added successfully, but the connection may not work.

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, Release 10.2*, at:

http://www.cisco.com/c/en/us/td/docs/wireless/mse/10-2/cmx_command/guide/cmxcli10.html

Note After adding Cisco WLCs, you must verfiy 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 92.

Note The license file has an .lic extension. Make sure it is the .lic file that you install on Cisco CMX.

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 | qlesspyworker | 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 | qlesspyworker | 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, Release 10.2*, at:

http://www.cisco.com/c/en/us/td/docs/wireless/mse/10-2/cmx_command/guide/cmxcli10.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. 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-----
```

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 Log in to Cisco Connected Mobile Experiences (Cisco CMX) as cmxadmin user.
The PEM certificate must be in the home directory of the cmxadmin user.

Step 3 Ensure that the certificate file has minimum global read permissions (0644).

Step 4 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 5 To install the new certificate in CMX, run the following command:
cmxctl node sslmode enable --pem /home/cmxadmin/cert.pem

Step 6 Run the following commands to restart the agent and haproxy services:
cmxctl restart agent

cmxctl restart haproxy

Step 7 Navigate to the Cisco CMX URL in your web browser and then use the browser tools to confirm the new certificate.

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 93.

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.

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.

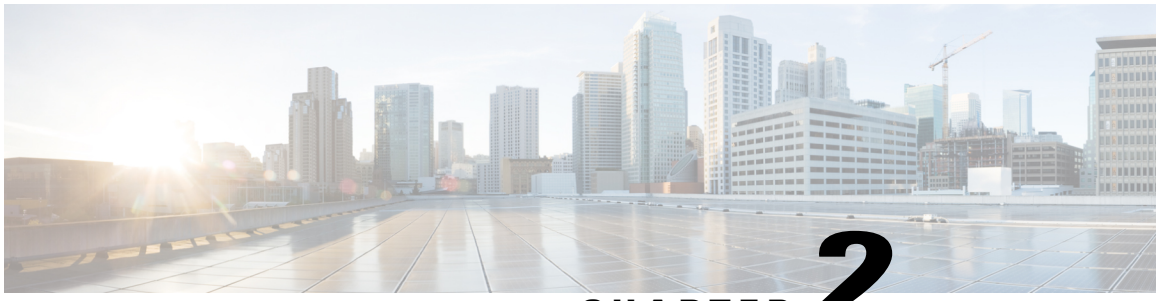
Step 3 In the /opt/cmx/bin/tzselect path, run the time zone script.

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

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) beacons.

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).

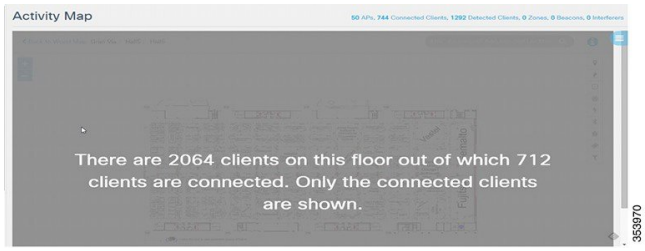
Step 2 Click **DETECT & LOCATE**.

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.

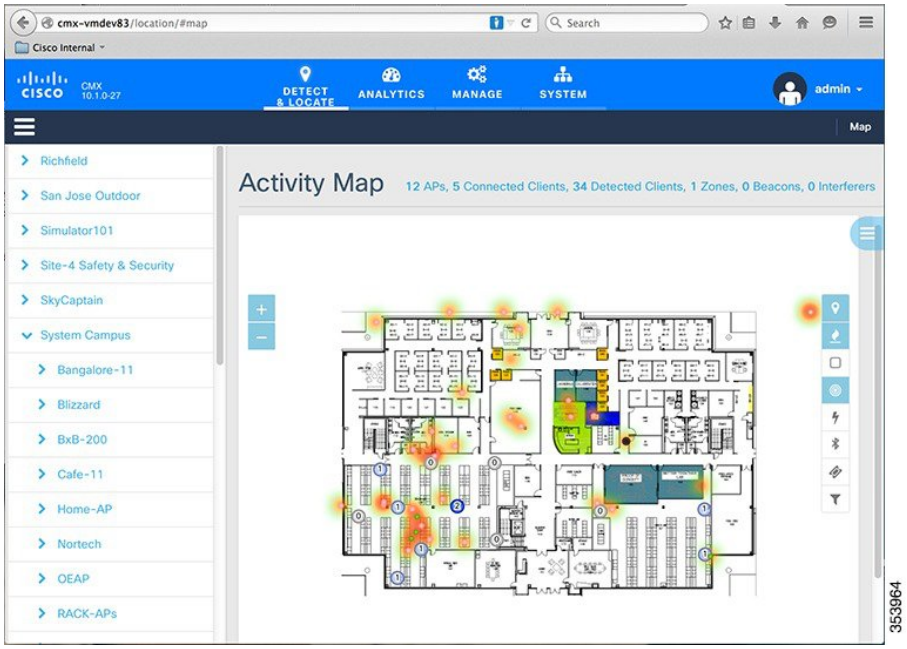
Step 4 Choose any combination of the following icons to customize your view of the devices:

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.

  Note
  - 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.
- **Beacons**—Click the **Beacons** icon to show or hide BLE-transmitting devices that have been detected by the wireless network. For more information about BLE beacons, see Managing BLE Beacons, on page 100.

  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 12.
- **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.

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.

Measuring Client Location Accuracy Using the Location Accuracy Test

In 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 mesaure 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 client.

Step 5 Click the corresponding client.
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**.
You can run the test for any required amount of time. The elapsed time of the test is displayed.

Step 10 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).

Step 11 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 12 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 or download the latest log or all logs.

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.

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 16.

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.

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.
- The Hyperlocation feature is enabled in Cisco CMX by default.
- 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** check box.

Step 6 Add Cisco WLC to Cisco CMX.

Step 7 If Cisco WLC was added before the Hyperlocation option was enabled, restart the NMSPLB service to start Hyperlocation, by entering the **cmxctl restart nmsplb** command.

Note To stop Cisco CMX from processing Hyperlocation, disable the Hyperlocation option (by unchecking the **Enable Hyperlocation** check box) in the **Location Parameters** window and restart the NMSPLB service.

For more information about the Cisco Hyperlocation solution, see the following documentation:

- *Release Notes for Cisco Connected Mobile Experiences (CMX)*, Release 10.2.0 and Later
- *Release Notes for Cisco Wireless Controllers and Lightweight Access Points for Cisco Wireless Release 8.1.123.0*
- "Configuring Cisco Hyperlocation in Cisco WLC" section in the *Cisco WLC Configuration Guide*
- *Cisco Aironet Hyperlocation Antenna (AIR-ANT-LOC-01=) Installation Guide*
- *Installing and Removing Cisco Aironet Access Point Modules*

Troubleshooting Hyperlocation

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.

Step 3 Choose the required building from the **Select Building** drop-down list.

Step 4 Choose the required floor from the **Select Floor** drop-down list.

Step 5 Click **Run Diagnostics** to start hyperlocation troubleshooting.

Note The Hyperlocation Diagnostics tests are documented in the *Hyperlocation Troubleshooting Guide*. To view this guide, click the **Troubleshooting Guide** in the **Hyperlocation Diagnostics** window.

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 sent 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.

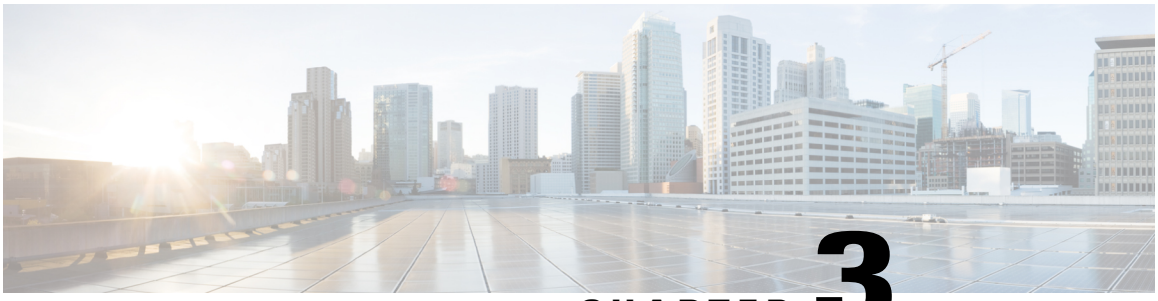
Step 5 Navigate to /opt/cmx/etc/ and open the node.conf file.

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**.



CHAPTER 3

The Cisco CMX Analytics Service

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.

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 In 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.
- **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.

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.

Note 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:

- Creating a Custom Report, on page 27
- Creating Scheduled Custom Reports, on page 29
- Deleting a Customized Report, on page 30

Creating 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** page is displayed.

Step 4 Click one of these options from the **Report Type** row in the right pane.

- Auto-Generate
- Customized

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 the + 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.
- **Associated Status—**Shows the number of visitors associated to and probing on the 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

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**.
Based on the Focus Area and Date filters that you speocified, the report name is geneated. The new report name is listed in the left pane under **Reports**.

Note

The following is a list of tasks that can be performed after a Custom report is created:

- **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** or **PDF**.
5. Click **Next**.

- 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**.
- 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 specify any comments, enter your comments in the **Add your comments here** text box.
  - In the **Footer** text box, 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**.

- 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. In the **SELECT REPORT OPTION** dialog box, choose **HTML** or **PDF**.
  5. 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 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.

- **Type—**Shows the report type, that is, HTML or PDF.
- **History—**Click**View** to display the history of the scheduled report.
- **Actions—**Click **Modify** or **Delete** to modify or delete the scheduled report.

Creating Scheduled Custom Reports

Besides creating customized reports and add a logo, text, header, and footer to a report to align it to 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 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**.

Downloading 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 **Seelct 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.

Step 5 Click **Next**.
The customized reports are downloaded in the selected format.

Deleting 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.

Viewing Global Alerts for Critical Services

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 services. For more information about alerts, see Viewing Live System Alerts, on page 128.

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

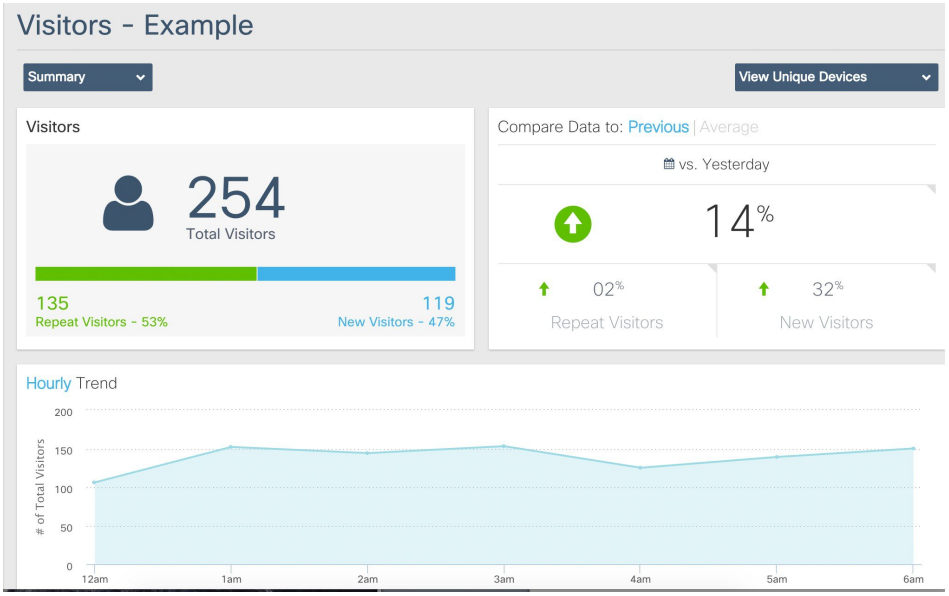
- **Values—**Ascending, Descending, Alphabetical

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 Average Dwell Time Widget

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

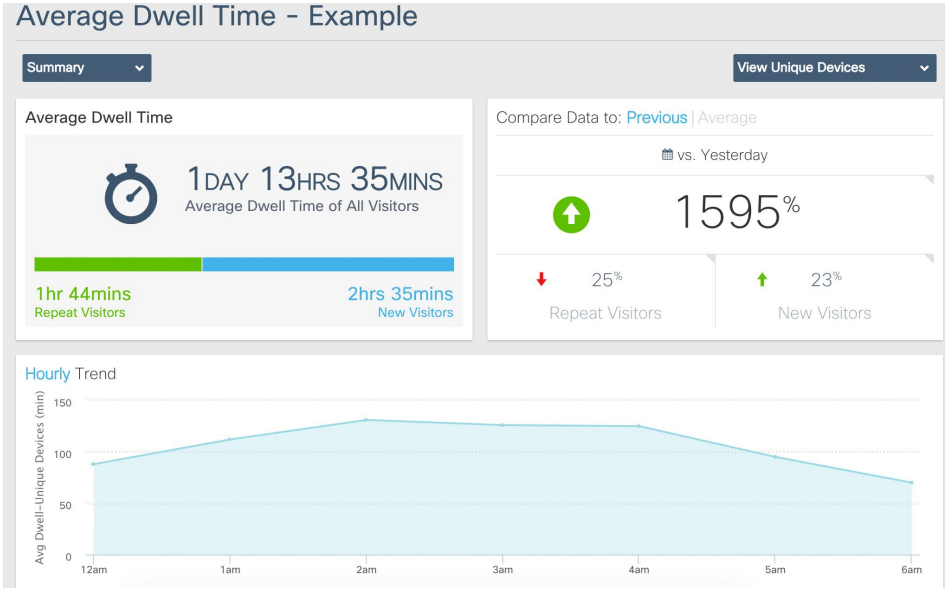
Average dwell time can be viewed in the following formats:

- **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 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.

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. 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 Associated Status Widget

The Associated Status widget displays a detailed summary of the number of clients that are associated with a network, and the clients that are probing the network:

- **Detected—**Refers to the client devices that are detected by APs in the network when they are probing the network.
- **Connected—**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

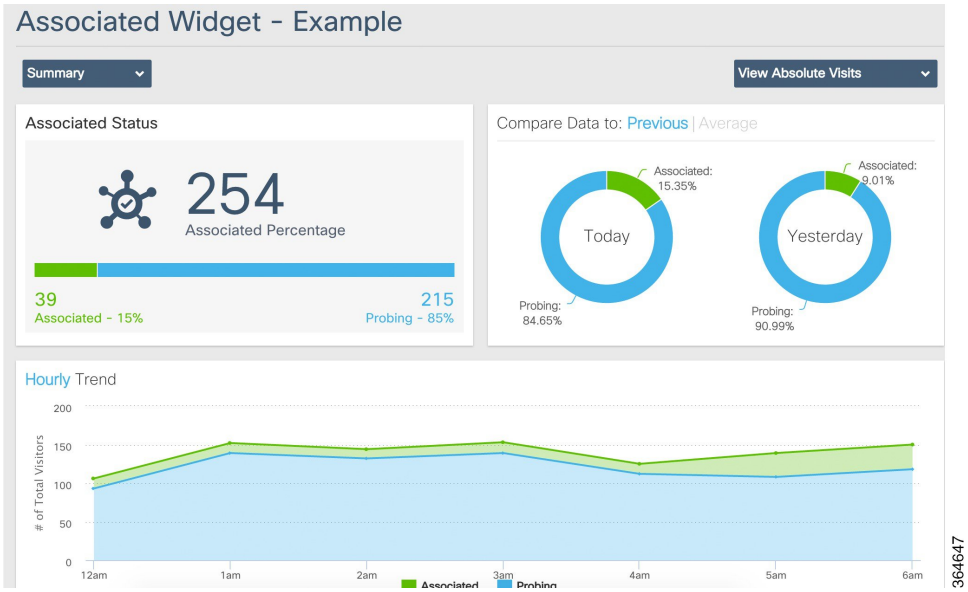
- Locations--Campus, Building, Floor, Zone, By Hour
- Values--Ascending, Descending, Alphabetical

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



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**.

Social Media Analytics

CMX 10.2 adds the ability to use data collected from social media to provide analytics used to enhance decision-making capabilities. Businesses can analyze their online reputation and view trends of the positive and negative comments about their events or services.

For example, managers of a restaurants can analyze their online reputation and view trends relating to positive and negative comments about their services. They can also configure the data for viewing information over a period of time, at a particular location, and during a specific time of the day. This information will enable them to make informed decisions about the services they offer.

Currently Social Media Analytics (SMA) supports posts coming from Twitter.

Note Currently, only English language posts are supported.

Also, Cisco CMX must be able to make API calls to Twitter servers.

User can configure the hashtags using the SMA configuration page and SMA will fetch the tweets for those hashtags and run them thorough the social media analysis engine pipeline. The SMA Dashboard shows the detailed social media analysis and trend.

Configuring Social Media Analytics

Setting Up Twitter Handle

Procedure

Step 1 Create a Twitter user account

a) Log in to http://twitter.com in browser.
b) Enter Full Name, Email, and Password in the Sign Up page.
c) Complete the sign-up procedure.

Step 2 Create a twitter app using the credentials of your user account.

a) Log in to https://apps.twitter.com/.
b) Click the **Create New App** button to create a new application.
c) Provide necessary information about your organization.
d) Agree to developer agreement and create application.

Step 3 Get consumer key and consumer secret key for the application from the Keys and Access tokens tab after creating the applications.

Initial Provisioning of Cisco CMX SMA

- Enable CMX SMA in 10.2.2, by entering the following commands:
  a) **cmxctl config featureflags analytics.sma true**
  b) **cmxctl analytics restart**
  c) **cmxctl qlesspyworker restart**
- Enter the **cmxctl config sma twitter** command to provision SMA with your Twitter credentials. For more information about the Cisco CMX commands, see the Cisco Connected Mobile Experiences (CMX) Command Reference Guide, Release 10.2.

Configuring Proxy Setting

- If your system is behind a proxy, enter the **cmxctl config sma proxy** command to set up SMA to use it.

Configuring Hashtags

SMA gets tweets from Twitter based on the hashtags. It could be name of the product or location or related context. For example, restaurants hashtag could be restaurant name such as '#olivegarden', '#applebee'.

Procedure

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

Step 2 Choose **Analytics > Social**.

Step 3 In the Social analytics page, click the Gear icon to configure Social Media Analytics. You can choose **All** from the Location drop-down list to load hashtags for all buildings.

The **Configure Hash tag** window is displayed.

Step 4 Enter location-specific hash tags that are relevant to your business and click the **Add** button.

Step 5 Click the **Social** tab to go back to the **Social Analytics** window.

After hashtags are configured, Cisco CMX may take one to two hours to fetch the tweets and show the result on the dashboard.

Viewing Social Media Analytics

The SMA dashboard provides detailed social media analysis for the configured hashtags. You can filter the results based on location and date/time range. You can also look at the statistics for various business hours.

Procedure

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

Step 2 Choose **Analytics > Social**.

Step 3 Filter the data to view. The following options are available:

- **Location**-Select the locations you would want the social media data from. You can select multiple locations.
- **Date**-Select the duration for which you want the social analytics data.
  - **Today**-From this drop-down list, select the required duration: **Today**, **Yesterday**, **Last Week**, **Last 2 Weeks**, **This Month**, **Last Month**, **Last 3 Months**, **This Year**, **Last Year**.
  - **All Day**-From this drop-down list, select the window within which you want the social media data. The options are:**All Day**, **Morning (5am-9am)**, **Business Hours (9am - 5pm)**, **Evening (5pm - 9pm)**, and **Custom Time**.

The SMA dashbaord displays the following information:

- **Hashtags—**This section shows which hashtags the statistics refer to.
- **Statistics—**Statistical data includes the following information about the location: **total posts**, **photos**, **reposts**, **likes**, **dislikes**, **neutral**. The graphical representation includes a line chart showing the trend based on the selected criteria.
- **Details—**Detailed data includes the following information: photos reposts, **likes**, **dislikes**, and **neutral**. A stacked chart is displayed showing the details in numbers.

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.

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.
- **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.
- **Actions—**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 106.

CHAPTER 4

The Connect and Engage Service

Overview of the Connect and Engage Service

CONNECT & ENGAGE 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.
- 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 10.2* at the following URL:

http://www.cisco.com/c/en/us/td/docs/wireless/mse/release/notes/cmx_10_2_rn.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 and Engage with Location
- Connect and Engage with Presence Analytics

  For the Connect and Engage Service to operate as intended, ensure to add Presense 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 on the Cisco 5760 Wireless LAN Controllers and Cisco Catalyst 3850 Series Switches.
- 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

	Facebook Wi-Fi	Custom Portal
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
Customer profile	• 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 48.

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 43.

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.

Connect and Engage Settings

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

Connect Settings

The following data retention settings 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 caluclated 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 & Engage 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.

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 & ENGAGE** > **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**.

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 46.

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 the .

Setting Up a Facebook Wi-Fi Portal

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

1. Configuring Access Control Lists on Cisco Wireless Controller, on page 46
2. Configuring WLAN for Web Passthrough Authentication, on page 47
3. Creating a Facebook Page for Your Organization, on page 48
4. Assigning a System Default Facebook Page, on page 49
5. Assigning a Location-Specific Facebook Page, on page 49

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:

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	HTTPS	Any	Any	Any
4	Permit	0.0.0.0/ 0.0.0.0	MSE_IP/ 255.255.255.255	TCP	Any	HTTPS	Any	Any

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 conigure 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 46.

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. Enter the following command using the Cisco WLC CLI:**config network web-auth captive-bypass enable.** For more information, see: http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/command-reference/b_cr80/b_cr80_chapter_010.html#wp2423541535.

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 & ENGAGE > 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:

a) Select the page.
b) Select the **Bypass Mode**.
c) Select the **Session Length**.
d) Click the optional Terms of Service if additional Terms of Service are required.
e) 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 Fabcebook 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 occuers only if you have setup your Facebook WiFi configuration in a Parent-Child location hierarcy, for example, **Campus >Bulding>Floor>Zone**.

You can pair different facebook pages with different child nodes in the hieraracy, like Campus is paired with Facebook page 1 and Building with Facebook page 2. In this scenarion, 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
  When you specify a phone number, select the **SMS Auth** check box to get notification through SMS. For more information, see the Enabling Multi-language Support in Custom Portals, on page 53.

- **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.

- **Social & 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.

Note You can get a preview of the custom portal for a mobile, PC, or tablet.

- 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.
- 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**.

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).
The Access Control Lists > New window is displayed.

Step 4 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**.
The Access Control Lists page is displayed.

Step 7 Click the name of the new ACL.

Step 8 Cick **Add New Rule**.
The **Access Control Lists > Rules > New** window is displayed.

Step 9 Configure the ACLs, as listed in either tables below:

Table 5: Configuring ACLs With Only Registration Fields (No Social Network Login)

Seq.	Action	Source IP/ Mask	Destination IP/ Mask	Protocol	Source Port	Destination Port	DSCP	Direction
1	Permit	MSE_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	MSE_IP/ 255.255.255.255	TCP	Any	HTTPS	Any	Any

OR

Table 6: Configuring ACLs With Social Network Login

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

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

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 conigure 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 web passthrough on Layer 3 security of WLAN for the Connect & Engage service.

Procedure

Step 1 From the web UI of Cisco WLC, choose **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, click the **Passthrough radio button**.

Step 8 Choose the **Preauthentication ACL** defined using the procedure described in the Configuring Access Control Lists on Cisco Wireless Controller, on page 46.

Step 9 To override the global authentication configuration 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 custom portal URL. The external redirection URL should point to the corresponding portal on Cisco CMX for custom portal, for example:

Example:

```
https://<CMX>/visitor/login
```

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. Perform this by entering the following command in the Cisco WLC CLI:**config network web-auth captive-bypass enable** For more information, see http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/command-reference/b_cr80/b_cr80_chapter_010.html#wp2423541535.

Creating a Default Custom Portal Page

Procedure

Step 1 Log in to Cisco CMX as an admin user.

Step 2 Choose **CONNECT & ENGAGE > 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 & Engage** > **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.

Offering an Opt-Out of Cisco CMX Services

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

The default is opt-in.

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

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.

Configuring the Opt-Out Option

Procedure

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

Step 2 Choose **Connect & Engage > 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

Procedure

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

Step 2 Choose **Connect & Engage > 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 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 58.

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 Twillio accounts for SMS authentication. You must establish your own Twillio 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 Twillio 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 Twillio account.

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

Procedure

Step 1 Ensure that your portal has a Registration Form element, or add one if required

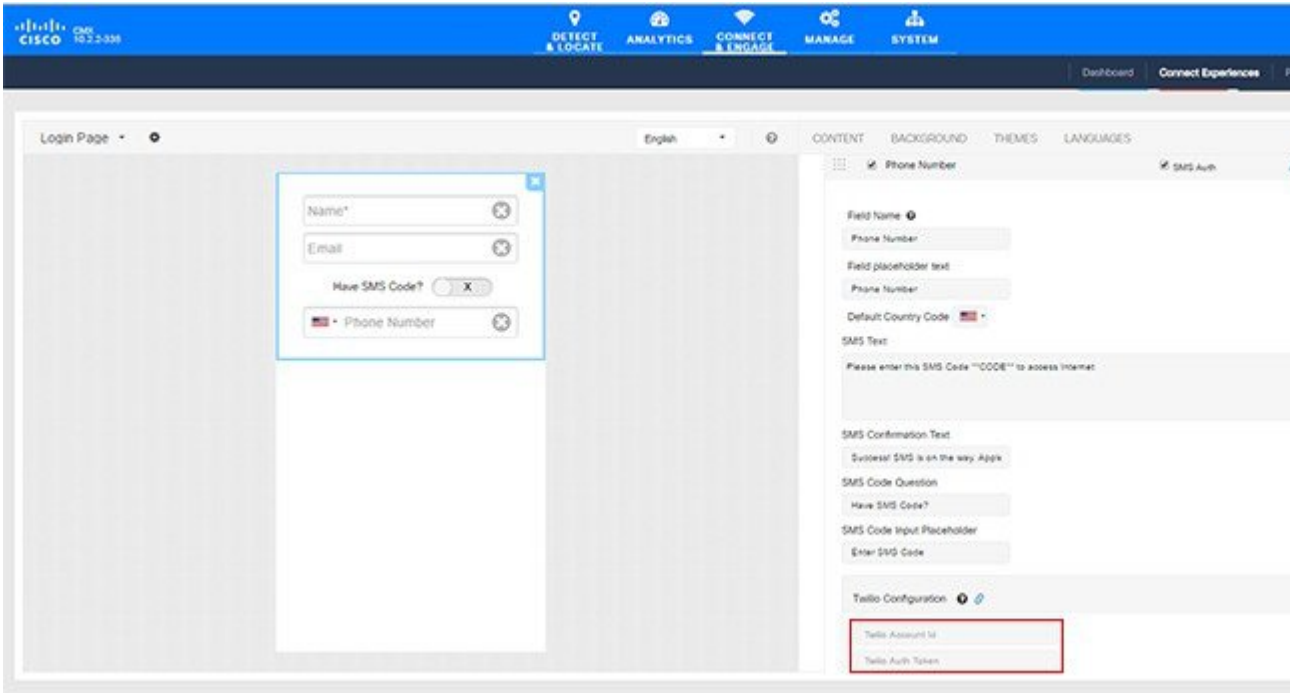
Step 2 Ensure that you specify a phone number field, but you may include other fields if desired.

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 1: Twilio Account Configuration



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

a) Enter your **Twilio Account ID**. This is a 34 character string that uniquely identifies the Twilio account.
b) Enter the **Twillio Auth Token**.
c) Enter the **From Number**. This number is purchased from Twillio. You cannot use an existing phone number.
d) Click **Create**.
You can click the **Reset** button to remove the association between the portal and the configured Twillio account (that is, removing the connector).

Step 6 Click **Save**.

The Connect and Engage Dashboard

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

The Connect & Engage 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

Using the Connect and Engage Library

To view the Connect & Engage Library, log in to Cisco CMX and choose **CONNECT & ENGAGE** > **Library**.

- Portal Library—Lists the portals that you have created, both drafts and completed ones. 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.

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 7: 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 8: 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	—
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	—

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. Unilink 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 67.

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.

Option	Description
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 **Acess 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:

a) To configure Layer 2 settings, check the **Mac Filtering** check box.

b) 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.

c) 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.

a) 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 & Engage > 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 & Engage > 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 & ENGAGE > 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 & Engage > 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 & Engage > 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

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 & Engage > 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 67 and Cisco WLC Configurations, on page 69.

Procedure

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

Step 2 Choose **Connect & Engage > 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. For example, PolicyOne.

Step 5 Enter the bandwidth, in kbps.

Step 6 Click **Create**.

Note The new policy plan is displayed in the **Policy** drop-down list in the **Connect Experiences** (**Connect & Engage > Connect Experiences**) tab.

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 enables 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 & ENGAGE > Library**.

Step 3 Create a portal. For more information about setting up a custom portal, see Creating a Default Custom Portal Page, on page 53.

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.

CHAPTER 5

The Cisco CMX Presence Analytics Service

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 Cisco CMX Release 10.2*. 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 80.
- Add sites in bulk. For more information, see Adding Sites in Bulk, on page 81.
- 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 83.

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 butons 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).

- Clients with RSSI below the low threshold (-95 dBm default) are discarded.
- Clients with RSSI above the low threshold are classified as “passer-by”.
- 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.

Step 9 Click **Save**.

Adding Sites in Bulk

Procedure

Step 1 Log in to 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*For example, *Test Site,123 Main Street City CA US,-65,-95,5*

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 83.
- 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 84.

Adding an AP to a Site

Note If you do not see the AP list, youshould 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 visitors / (visitors + passersby) x 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.

- 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.

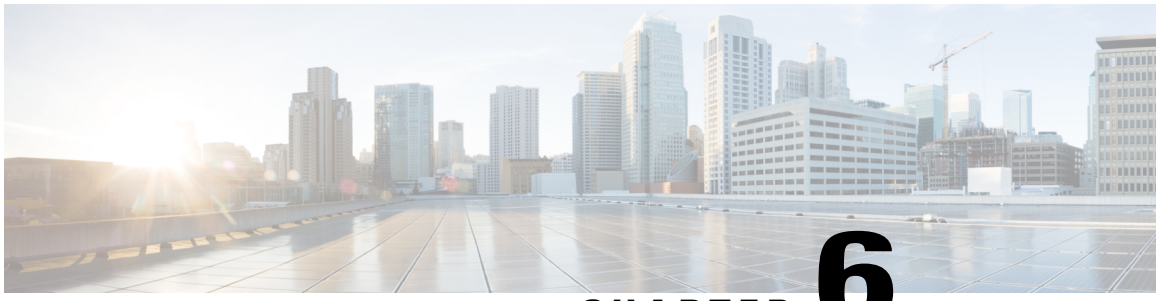
Procedure

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

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.
- **Licenses—**Enables you to manage and add licenses.
- **BLE Beacons—**Enables you to manage and add Bluetooth low energy (BLE) beacons.
- **Notifications—**Enables you to manage and add email and HTTP notifications.
- **Users—**Enables you to manage and add users.
- **Verticalization—**Enables you to generate vertical specific reports.

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 93.

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.

For information about the licenses required to operate Cisco CMX, see the Cisco CMX 10.2 Ordering and Licensing Guide.

Note Cisco CMX Release 10.2 comes with a 120-day full-functionality evaluation license. All the access points (APs) connected to Cisco CMX must be licensed.

Adding 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 Click **Add License**.
The **UPLOAD LICENSE** dialog box is displayed.

Step 5 Click **Browse** to select the corresponding license file, and then click **Upload**.

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 the "User Roles".

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 & ENGAGE** 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 SYSTEM service

Role	Allows
Manage	Read/Write access to the MANAGE service
Location	Read/Write access to the DETECT & LOCATE service
Analytics	Read/Write access to the ANALYTICS service
Connect	Read/Write access to the CONNECT & ENGAGE service
Connect Experiences	• 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 93.

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 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:

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.

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.

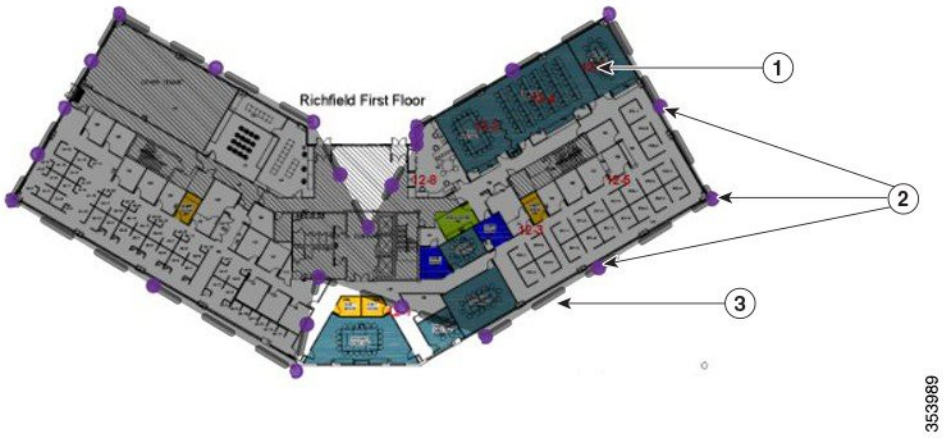
Step 5
In the **Zone Editor** window, click the **CREATE A PERIMETER**  icon.
The cursor changes to a drawing tool.

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 2: A Perimeter and its Vertices



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 3: A Zone and its Vertices

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 BLE Beacons

Bluetooth low energy (BLE) beacons, are used to engage with Bluetooth-enabled mobile devices at close proximity.

Note Cisco CMX has the capability to view the current location of beacons using access points (APs). No more than 25 BLE-Beacons can be detected by an AP. Cisco CMX can determine if a beacon is missing or has been misplaced.

To use the BLE beacons feature, choose **MANAGE** > **BLE Beacons**. This opens the **Beacons Activity Map** window, where you can:

- View the number of beacons, and the status and location of each beacon. The status of a beacon is indicated by the color of its icon, which is described in the table below.
- Keep track of the positions of all the BLE beacons on a particular floor.
- Position the BLE beacons on a floor map.

Table 12: Beacon Status

Beacon Status Icon	Meaning	Description
	Unplaced	A newly created beacon that is yet to be placed. Positioned at the top-left corner of a map.
Icon in green	Known	A beacon that has been defined and placed, or converted from Rogue status.
Icon in red	Missing	A beacon that is marked as Missing because the network status of the beacon is inactive.
Icon In blue	Misplaced	A beacon that has been moved beyond its accuracy range. For example, if the accuracy range is 5 feet, and the currently detected location is beyond a radius of 5 feet of the configured location.
Icon in yellow	Rogue	A newly discovered beacon that has not been defined or changed to Known status.

Adding a Beacon to a Map

Procedure

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

Step 2 Choose **MANAGE** > **BLE Beacons**.

Step 3 In the left pane, drill down to the floor level and click the floor in which you want to add a beacon.

Step 4 In the **Beacons Activity Map** window that is displayed, click **New Beacon**.

Step 5 In the **CREATE A NEW BEACON** dialog box that is displayed, enter the beacon details and click **Add**. The new beacon will be positioned on the top-left side of the map, ready to be placed.

Step 6 Drag the new beacon to the desired location on the map.

Deleting a Beacon

Procedure

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

Step 2 Choose **MANAGE** > **BLE Beacons**.

Step 3 In the left pane, drill down to the floor level and click the floor in which you want to add a beacon.

Step 4 In the **Beacons Activity Map** window that is displayed, click the beacon you want to delete.
A slide-out pane containing the details of that beacon is displayed.

Step 5 Click the **Trash** icon in the slide-out pane to delete the beacon.

Changing a Beacon Name

Procedure

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

Step 2 Choose **MANAGE** > **BLE Beacons**.

Step 3 In the left pane, drill down to the floor level and click the floor in which you want to rename a beacon.

Step 4 In the **Beacons Activity Map** window that is displayed, click the beacon you want to rename.
A slide-out pane containing the details of that beacon is displayed.

Step 5 Click the **Edit** icon adjacent the current name, and change the name.

Converting a Rogue Beacon to a Known Beacon

Note All newly discovered beacons will be marked as Rogue.

Procedure

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

Step 2 Choose **MANAGE** > **BLE Beacons**.

Step 3 In the left pane, drill down to the floor level and click the floor in which you want to add a beacon.

Step 4 In the **Beacons Activity Map** window that is displayed, click the rogue beacon that you want to convert. A slide-out pane containing the details of that beacon is displayed.

Step 5 Click **Convert to Known**.

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:

Creating 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.

Step 4 Enter a name for the notification and other the details.
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 13: Notification Types

Notification Type	Used for
Association	Generating a notification when a client is associated or unassociated.
Beacon Movement	Generating a notification when a BLE beacon has moved more than a specified distance.
Absence	Generating a notification when a client is undetected for more than 15 minutes.
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.
Beacon Absence	Generating a notification when a BLE beacon has been undetected for more than 5 minutes.
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.

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.

- 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.

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 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
    - Visitor Count
    - Connected Clients
    - Average Dwell Time
    - Location Correlation
    - Most Popular Zones
    - Path Analysis
- 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

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.
- **Inventory—**Enables you to view the inventoty details such as disk types, disk capacity, SSD details, memory usage, and so on.

Viewing the Overall System Health

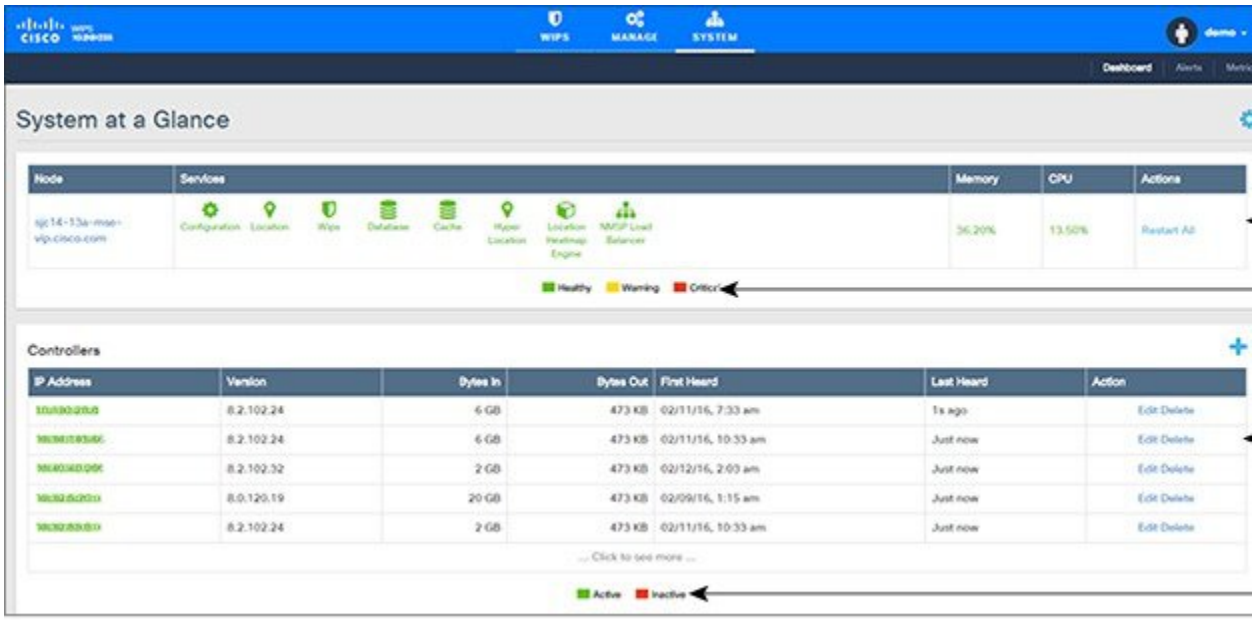
Procedure

Log in to Cisco Mobile Connected Experiences (Cisco CMX).
The **System at a Glance** window, which contains the following sections, is displayed:

- System at a Glance. For details, see Using the System at a Glance Table, on page 113.
- Controllers Table. For details, see Understanding the Controllers Table, on page 114.

The Cluster table and the Controllers table are shown in the following figure:

Figure 4: System at a Glance



The following list shows the parts of the **System at a Glance** window:

- 1—Gear icon for setting cluster services and metrics
- 2—System at a Glance table
- 3—Legend of status indicators for the cluster table service
- 4—Controllers table
- 5—Legend of status indicators for the Cisco Wireless Controllers (Cisco WLC) in the Controllers table. The IP addresses of active controllers are shown in green. The IP addresses of inactive controllers are shown in red.

Using the System at a Glance Table

The **System at a Glance** window contains the following information:

- **Node—**Lists all the associated Cisco CMX nodes.
  - Click a node name to view its metrics. See Viewing CMX Node Metrics, on page 122.
- **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 128.
- **CPU—**Shows the load on the CPU, in percentage.
  - Click it to view the **Live Alerts** window. See Viewing Live System Alerts, on page 128.
- **Actions—**Allows you to restart all the services for a node.

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.

Viewing the Cisco CMX General Settings

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 the Gear icon at the top-right corner of the window.
The **Settings** window is displayed with the **General** tab already selected. The following details of the node are displayed:

- **Name—**Cisco CMX node name.
- **Associated Nodes—**Cisco CMX nodes that are associated with this node.

Viewing Cisco CMX Node Details

Procedure

Step 1 Log in to Cisco CMX.

Step 2 Choose **System > Dashboard**.
The **System at a Glance** window is displayed.

Step 3 Click the Gear icon at the top right corner of the page.
The **Settings** window is displayed.

Step 4 Click the **Node Details** tab.

Step 5 Click a node name to view its details, including **Node ID, Name, Hostname** and **Type**.

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 the Gear icon at the top-right corner of the window.
The **Default Cluster Settings** dialog box is displayed.

Step 4 Click the **Tracking** tab.
The **Tracking Parameters** table is displayed.

Step 5 In the **Elements** column, check the check box of each device that you want to select for tracking.
Only the elements selected here will be tracked by the network location service and will appear on the **Activity Map** window.

Note To track Bluetooth low energy (BLE) beacon tags, check **Interferers**. For BLE beacon-enabled devices to be tracked, you require a Cisco WLC with software Release 8.0.115.0 or later.

Step 6 Click **Save**.

Setting Filter 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 the Gear icon 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—**This is a percentage value. Interferers with a Duty Cycle that is less than the specified cutoff will not be tracked.
- **RSSI Cutoff—**This is the radio signal strength cutoff for filtering. The default is -85 dBm.
- **Exclude probing clients—**Check this check box to filter out clients that are only probing. This enables the system to track only connected clients.
- **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.

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 the Gear icon 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.
- **User 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—**Check this check box to enable hyperlocation in Cisco CMX. This parameter is disabled by default.
  Note For Cisco CMX 10.2.2 release, the **Enable Hyperlocation** option is enabled by default.
- **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—**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—**Enter the time, in minutes, 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.
- **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 compariosn 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 Parameter:

- **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 the Gear icon at the top-right corner of the window.
The **Deault luster 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 address to which the notifications should be sent.
- **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 **Test Settings**, and then click **Send e-mail**.

Step 6 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:

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 the Gear icon at the top-right corner of the window.

Step 4 Choose the **Controllers and Maps Setup** > **Import** tab, and enter the following parameters:

a) **Username—**Username of the Cisco Prime Infrastructure server.

b) **Password—**Password of the Cisco Prime Infrastructure server.

c) **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 **Override Maps** check box.

By default, the override check box is checked, which is same as synchronization. Cisco CMX will remove the existing maps and they are replaced by the ones in the file that you import. Existing zones are also removed when you override the maps. We recommend to redraw the zones if you plan to update the maps using Cisco Prime Infrastructure.

If this check box is unchecked, Cisco CMX will add the maps in the file.

Step 5 To test your settings, click **Test Settings**, and then click **Send e-mail**.

Step 6 Click **Save** to save your settings if the test is successful.

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 the Gear icon at the top-right corner of the window.

Step 4 Choose the **Conrollers and Maps Setup** > **Advanced** tab.

Step 5 To manually import a map, perform the following:

a) Under the **Maps** area, click **Browse** .
The File Upload dialog box is displayed.

Note If you check the **Delete & replace existing maps** 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.

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 **NGWC**.
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**.

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 the Gear icon 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

Viewing System Summary Metrics

The **System Summary Metrics** window displays the following information:

- **Number of Active Clients—**The metrics for the active clients in last 15 minutes.
- **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 uesage 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**
- **Number of open connections**
- **Number of queries**

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**.

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**
- **Connected clients**
- **Used memory**
- **Evicted keys**

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**
- **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 Rates—**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 Dashbaord

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**.

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.
- **Incoming Rate—**Displays the number of Network Mobility Services Protocol (NMSP) messages received from the NMSP load balancer.
- **iOS8 Devices—**Displays the total number of iOS devices.
- **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.
- **Dropped Notifications—**Displays the notifications sent to the Analytics service by Cisco CMX, but were dropped because of some reason, for example, because the Analytics queue is full.
- **NMSP LB Read Operations—**Displays the number of bytes received from socket.
- **Redis Connections Received—**Displays the total number of connections received by the cache service.

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.

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.

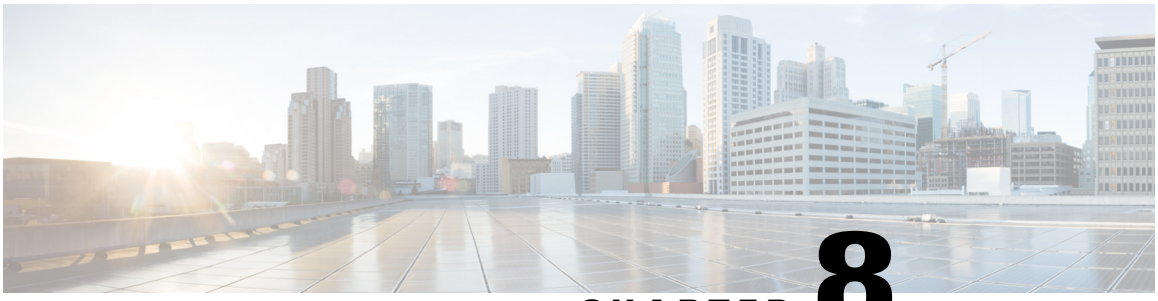
Viewing Live System Alerts

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.



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

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 133.

- 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.

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.

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. The following components are included in the backup:

- Database
- Cache
- Cassandra
- Influxdb
- Consul
- Floormaps
- Licenses
- Setup
- Conf

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 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 ~]$
```

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.

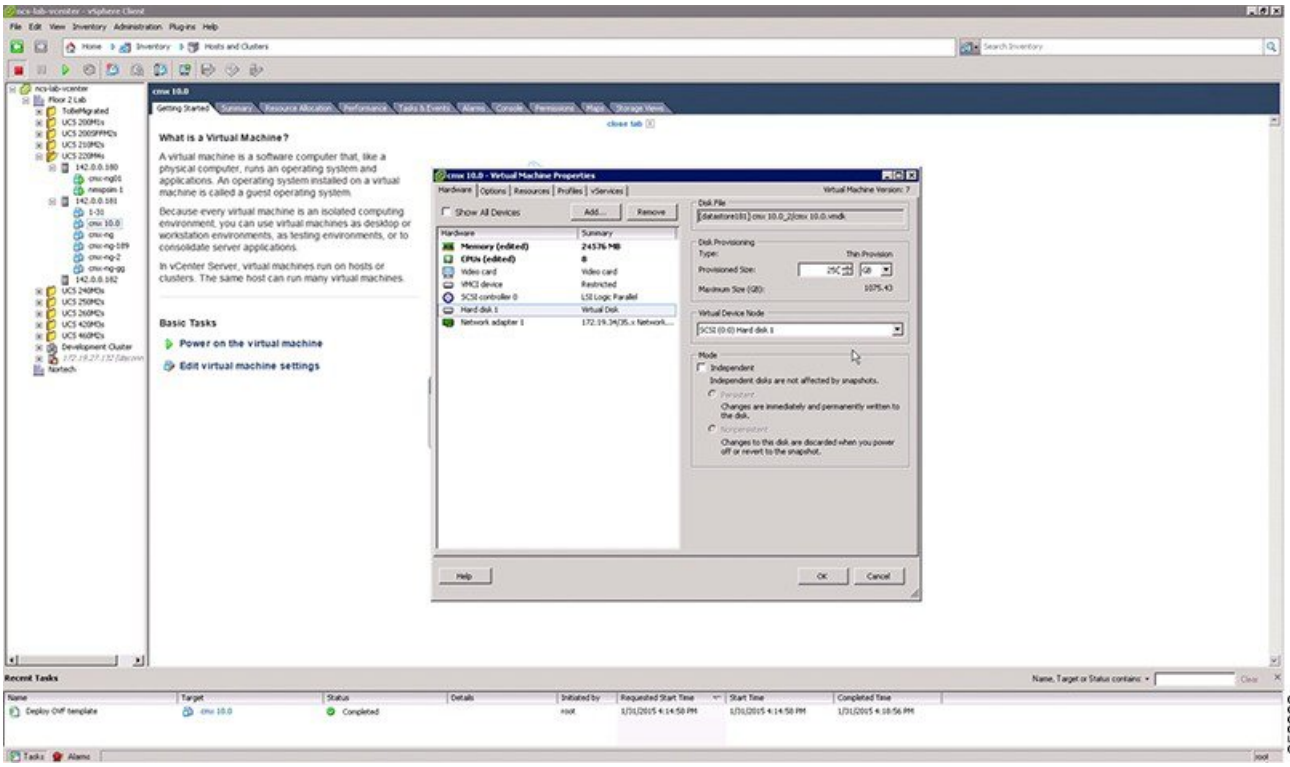
Procedure

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.



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.

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.

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
$
```

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 reset ui-password

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.

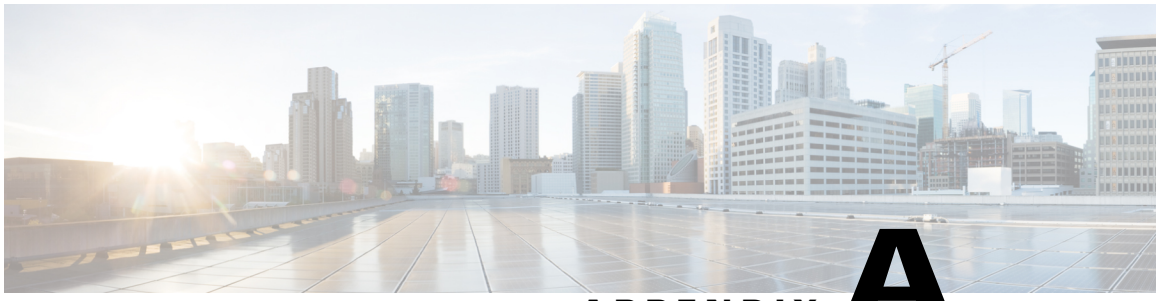
Step 6 After the system boots and you are at the # prompt:

a) Enter **passwd** <*username*> and press Enter.
b) When prompted, enter the new password for the user (root/cmxadmin) 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.

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. After you have sufficient space, restart your Cisco CMX server by running the **cmxctl start –a** command.



APPENDIX A

Authentication with Social Network Accounts

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 the 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.

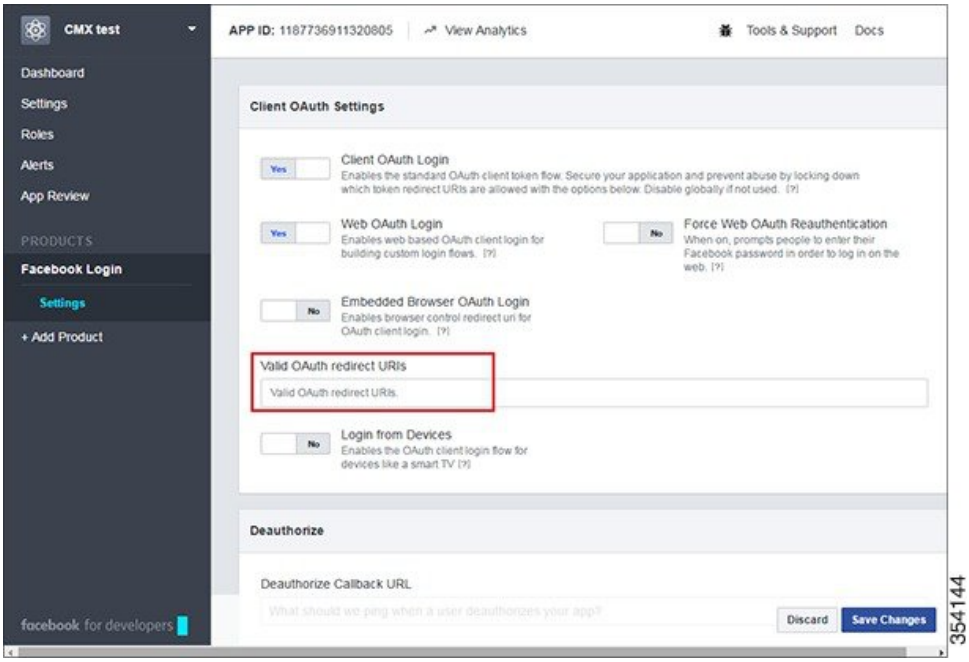
Step 9 Select and copy the App ID for a later step.

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 5: 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 6: Basic Settings

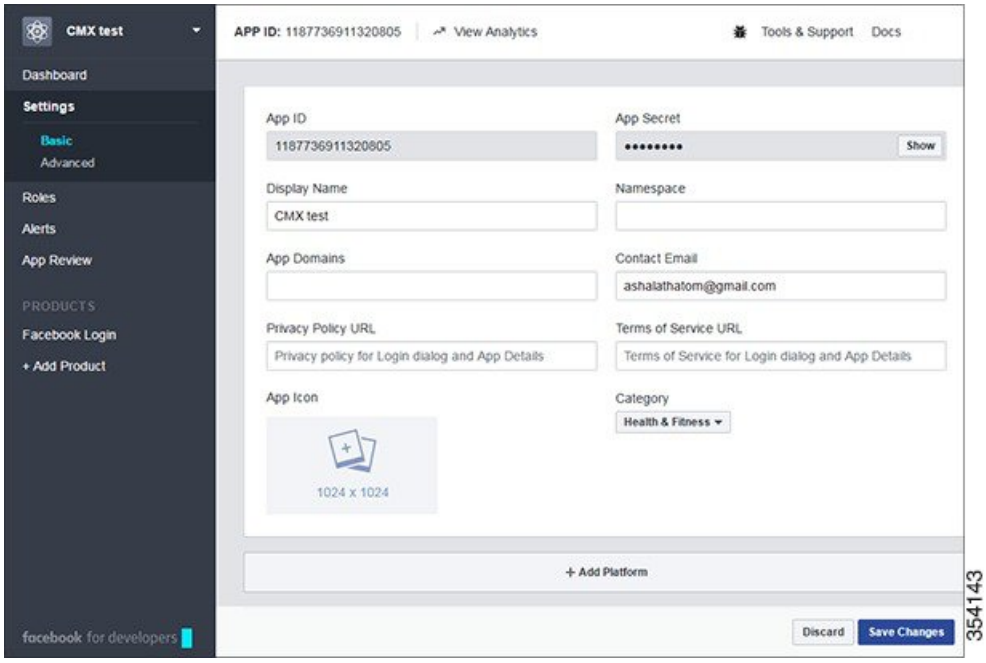
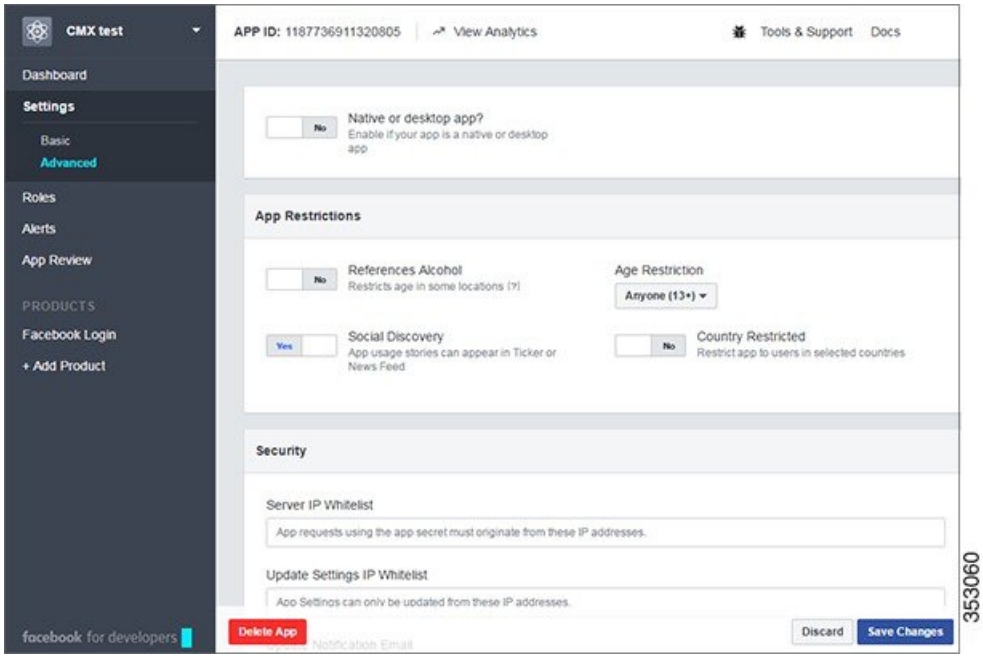
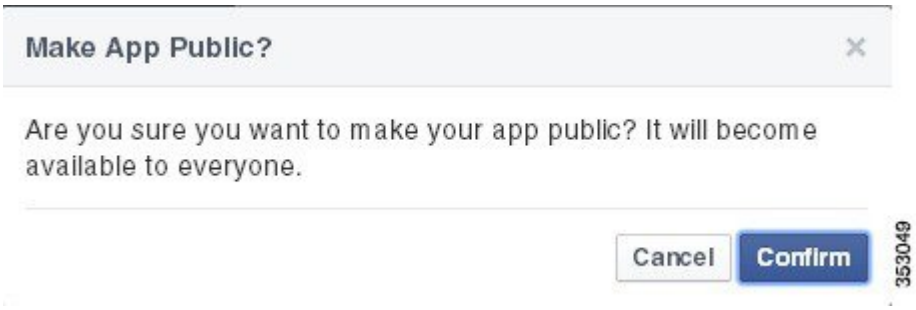


Figure 7: Advanced Settings



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.