



Cisco CMX Dashboard Configuration Guide

Release 7.6
December, 2013

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

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

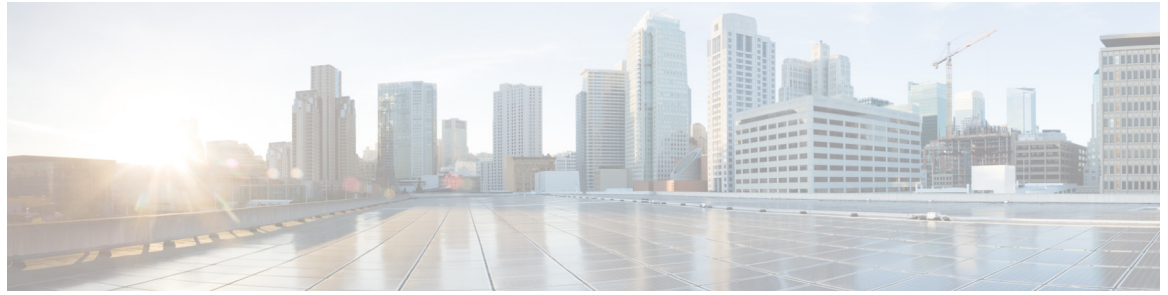
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

Cisco CMX Dashboard Configuration Guide

© 2013 Cisco Systems, Inc. All rights reserved.



Preface

This section discusses the objectives, audience, conventions, and organization of the *Cisco CMX Dashboard Configuration Guide* and provides general information about CMX Browser Engage service.

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more up to date than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription.

Objectives

This guide describes the workflow and components of CMX Dashboard and contains corresponding information of the CMX Browser Engage service.

Audience

This publication is intended primarily for users who implement the mobility services using Cisco Unified Wireless Network. The publication is intended for the Marketing and IT staff who use the Cisco CMX Dashboard.

Organization

This chapter describes the contents of each chapter in this document.

Table 1 **Organization**

Chapter	Title	Description
Chapter 1	Introduction	Introduction of CMX Dashboard
Chapter 2	Prerequisites	Prerequisites of the Configuration guide
Chapter 3	Getting Started	Initial steps for configuration
Chapter 4	Account Management	CMX Dashboard Accounts
Chapter 5	Points of Interest Management	Specific location in CMX Dashboard Configuration
Chapter 6	Navigation Management	Navigation at a venue
Chapter 7	Banner Management	Types of messages
Chapter 8	Campaign Management	CMX Dashboard Banners
Chapter 9	Service Management	Types of services and messages
Chapter 10	Browser Display & End User Experience	The runtime behavior and the appearance of the CMX Dashboard
Chapter 11	CMX Dashboard Reports	Analysis of the use of services
Chapter 12	CMX Dashboard Visitor Connect	Access to network for the customers
Appendix A	HTTP and TCP Proxy	HTTP traffic
Appendix B	CMX Cloud Connector	Cloud connector in decentralized CMX Dashboard set up

**Note**

Please provide your feedback by clicking on “Make a wish” menu in CMX Dashboard, which is available on the top right corner of the page. To disable the feature, remove the “Visitor Connect” operation from the Super Admin role.

Command Syntax Conventions

Table 2 describes the syntax used with the commands in this document.

Table 2 **Command Syntax Guide**

Convention	Description
boldface	Commands and keywords.
<i>italic</i>	Command input that is supplied by you.
[]	Keywords or arguments that appear within square brackets are optional.
{ x x x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. You must select one.
^ or Ctrl	Represent the key labeled <i>Control</i> . For example, when you read ^D or <i>Ctrl-D</i> , you should hold down the Control key while you press the D key.

Table 2 **Command Syntax Guide**

Convention	Description
screen font	Examples of information displayed on the screen.
boldface screen font	Examples of information that you must enter.
< >	Nonprinting characters, such as passwords, appear in angled brackets.
[]	Default responses to system prompts appear in square brackets.



CHAPTER 1**Introduction 1-1**

- Connected Mobile Experiences 1-1
- CMX Engage 1-2
- CMX Browser Engage and CMX Dashboard 1-2
- Cisco Wireless Components 1-3
 - PI - MSE - CMX Dashboard Connection 1-4
- CMX Dashboard Workflow 1-5
- CMX Dashboard Components 1-5
 - Accounts & Roles 1-5
 - Campaigns 1-6
 - Banners 1-6
 - POI management 1-7
 - Appearance 1-7
- Services 1-7
 - Hyper-local search 1-8
 - Find Me 1-8
 - Deals 1-8
- Reports 1-9

CHAPTER 2**Getting Started 2-1**

- Adding a Mobility Services Engine to the Prime Infrastructure 2-1
- Enabling CMX Dashboard Service on the Mobility Services Engine 2-3
- Enabling Proxy Server on the Mobility Services Engine 2-3
- Logging into CMX Dashboard User Interface 2-3

CHAPTER 3**Account Management 3-1**

- Creating an Account 3-1
- Deleting an Account 3-2
- Making an Account active 3-2
- Making an Account inactive 3-2
- Roles, Domain and Server Settings 3-2
 - Roles 3-3
 - Domain 3-3

Server Settings 3-4

CHAPTER 4

Points of Interest Management 4-1

Adding Point of Interest 4-1

Updating Floor Maps 4-3

Deleting Floor Maps 4-3

CHAPTER 5

Navigation Management 5-1

Creating Navigation Points 5-1

CHAPTER 6

Banner Management 6-1

Welcome 6-1

Offer or Deal 6-3

Sponsorship 6-4

Advertisement 6-4

Difference between the types of messages 6-5

CHAPTER 7

Campaign Management 7-1

Web Banner 7-1

Creating a Campaign 7-1

Assigning Banner to a Campaign 7-2

Editing the Existing Banner 7-3

Deleting a Banner 7-3

Previewing the Existing Banner 7-4

Searching a banner 7-4

CHAPTER 8

Service Management 8-1

Hyper-local search 8-1

Editing Hyper-local Search Appearance 8-2

Map 8-2

Editing appearance of map 8-2

Deals 8-3

Editing Deals Appearance 8-3

CHAPTER 9

Browser Display & End User Experience 9-1

Browser Display 9-1

Icons or Images 9-2

UI templates	9-4
Animation	9-5
Setting the Services appearance	9-5
Setting the animation appearance	9-7
End User Experience	9-7
Make a Wish	9-8
Browser and Operating System support	9-8

CHAPTER 10**CMX Dashboard Reports 10-1**

Reports	10-1
Summary	10-7

CHAPTER 11**CMX Dashboard Visitor Connect 11-1**

Visitor Connect as Captive Portal	11-1
Workflow to Set up the CMX Visitor Connect	11-2
11-2	
Prerequisites for CMX Visitor Connect	11-2
Template Fields	11-8
Creating a splash Template Field	11-9
Editing the Splash Template Field	11-9
Deleting the splash Template Fields	11-9
Social Connectors	11-9
Configuring the Social Connector	11-10
Editing Social Connector	11-10
Deleting Social Connector	11-10
Splash Templates	11-11
Creating a Splash Template	11-11
Assigning a Splash Page Template to a Points of Interest or Floor	11-12
Visitor Connect Report	11-12
Monitor the Visitor Details	11-12
HTTP Flow	A-1
HTTP Proxy Service	A-1
Deployment Types	A-2
Configuration on the MSE	A-2
Enabling DNS and Default Domain Name via MSE Console	A-3
Prerequisites for the CMX Dashboard Connector	B-1
CMX Dashboard Connector	B-2
Initial Setup	B-2

- Web based Management UI **B-3**
- CMX Dashboard Connector Configuration **B-3**
 - Connectors **B-4**
 - HTTP Proxy **B-6**
 - System Information **B-7**



Introduction

This chapter introduces the concepts of Cisco Connected Mobile Experiences (CMX) and CMX Dashboard that is used to manage and configure CMX services.

Connected Mobile Experiences

The Cisco Connected Mobile Experiences (CMX) enable organizations to detect, connect, and engage with end users or the customers while inside their venue:

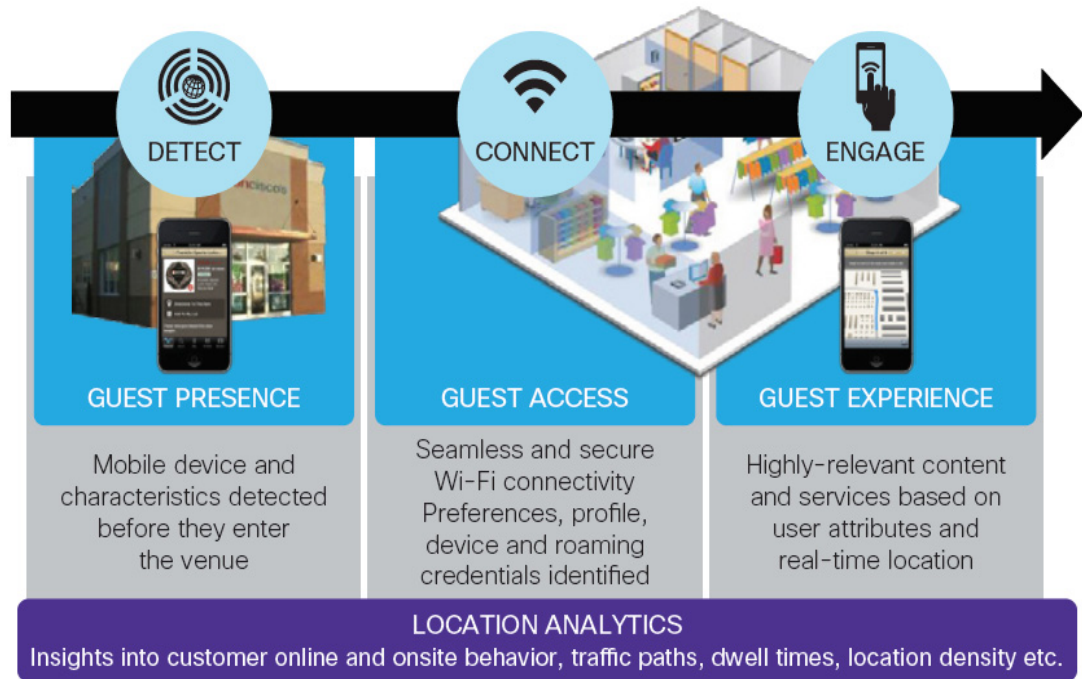
- **Detect:** The wireless signal from the customer's mobile device, and the device's characteristics, are detected as the customer approaches your location.
- **Connect:** After the customer receives notification of available Wi-Fi access and services, that customer can securely connect.
- **Engage:** Once customers have access, you can engage them with personalized content. Through this two-way communication, you can build a real-time, value-added relationship with your customers.

Following are the benefits of the CMX solution:

- Transition Wi-Fi from an IT cost center to a platform for end-user services.
- Increase customer intimacy by offering personalized, relevant content.
- Generate new revenue through third-party targeted mobile advertising.
- Increase venue effectiveness by using traffic flows to better position products or services, adjust floor layouts to better serve customers, and staff service locations according to traffic and time of day.

The following figure summarizes this process.

Figure 1-1 Detect, Connect, and Engage



CMX Engage

Engage allows organizations to communicate with users via different media on the mobile device, including:

- **Application Engage:** Location-enabled applications can include features such as indoor maps and navigation and personalized, location-specific notifications. It also includes the Mobility Services API, which enables our ecosystem partners to develop location-based applications.
- **Browser Engage:** Location and context-enabled browser banner notifications, menu items, and search capabilities.
- **Device Engage:** Location-enabled service discovery on the device, enabling organizations to communicate with users regardless of application or web capabilities. This capability is available on devices with the Qualcomm Snapdragon chipset.

CMX Browser Engage and CMX Dashboard

Cisco CMX Browser Engage is a new way to transform the in-venue experience through browser engagement. This enables organizations to communicate with opt-in mobile users - shoppers, guests, visitors - through their mobile browser.

CMX Dashboard is the back-end tool designed for administrative users to manage the CMX Browser engage experience. It allows the admin users to configure venue-specific menus, banners, and icons as well as content-aware search.

This guide will describe the use of the CMX Dashboard to configure and manage CMX Browser Engage services.

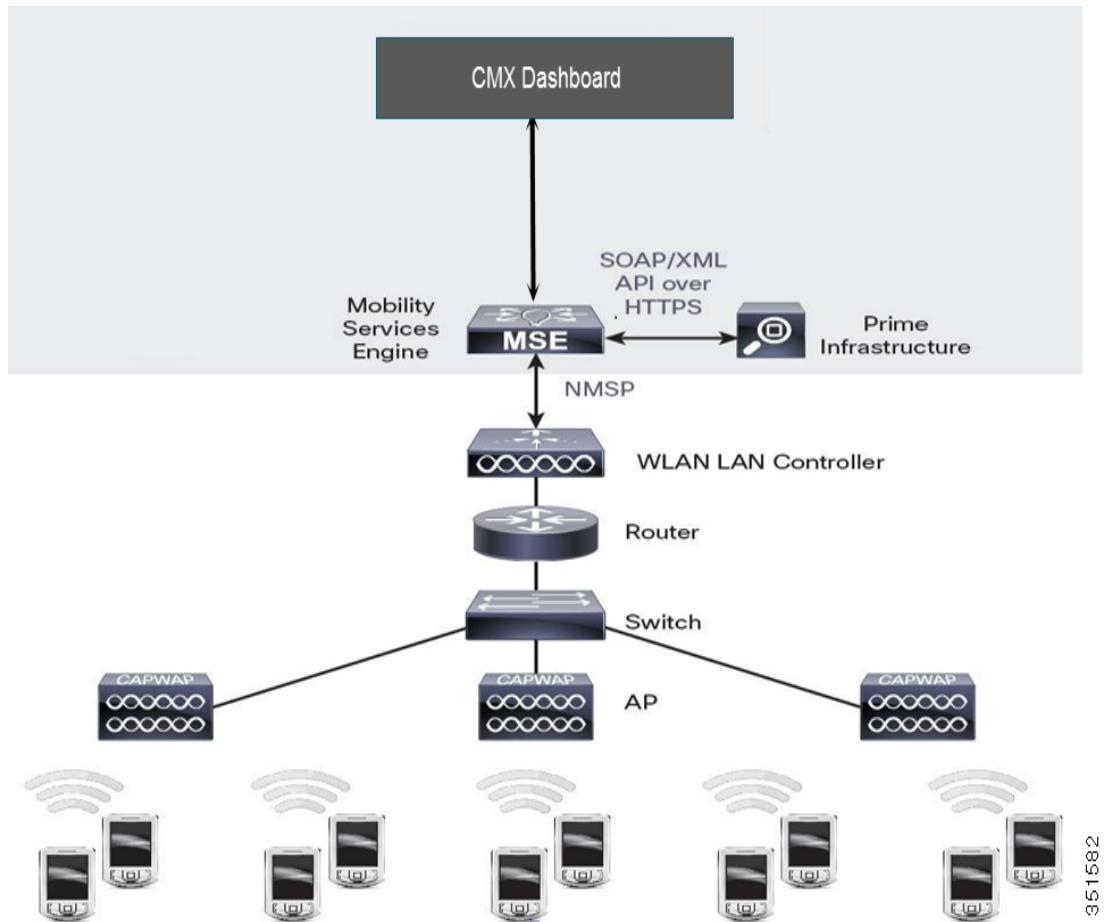
Cisco Wireless Components

The Cisco Wireless is designed as a wireless solution that increases employee productivity, enhances collaboration, and improves responsiveness to customers. The Cisco Wireless is an unified network. It addresses the security, deployment, management, and control issues facing large-scale enterprises and commercial wireless LAN users.

Following are the components of the unified network:

- Cisco Prime Infrastructure (PI) — combines the wireless functionality of Cisco Prime Network Control System (NCS) and the wired functionality of Cisco Prime LAN Management Solution (LMS).
- Cisco Wireless LAN Controller — enables network administrators to have the visibility and control necessary to effectively and securely manage business-class WLANs and work with the Mobility Services Engine.
- Access Points (AP) — connect wireless devices to wired networks providing ubiquitous network access.
- Mobility Services Engine (MSE) — a set of value-added network services that consolidate intelligence from various points in the network to enable and optimize the delivery of business mobility applications.

Figure 1-2 Overview of PI- MSE - CMX Dashboard



PI - MSE - CMX Dashboard Connection

The admin user has to enable the CMX Browser Engage and Proxy Services on the MSE using PI 1.4.



Note

The domain name and at least one DNS IP address must already be configured on the MSE to enable the service. To have the CMX Dashboard operational, the PI needs to be deployed.

The admin user provides the CMX Browser Engage server information to the Proxy service. The admin user gives the Location MSE information to CMX Browser Engage server.

The admin user clicks Save. All the campus, building, and floor information managed by the Location PI/MSE is sent to CMX Browser Engage server along with the floor images and dimensions.

To access the back-end tool - the CMX Dashboard, use the following details.

The URL is `http://<MSE_IP_address>:8081/Mario`. The default username and password are admin and admin.

CMX Dashboard Workflow

This section lists out the high level configuration steps for the CMX Dashboard in brief and the flow of this document as well.

Following is the workflow for the CMX Dashboard:

**Note**

The following flow of the actions is based on a condition that Admin users have configured the PI and then MSE's have been added and the maps have been synced.

-
- Step 1** Log in to the CMX Dashboard and verify that maps are updated in the points of interests menu. This step is covered in detail in the chapters *Points of Interest Management & Account Management*.
 - Step 2** Then create the display banners. The banner can be one of the types: a welcome message, an offer or deal, sponsorship, advertisement. Upload the images to display and add the keywords for the product/service at the venue and activate the banners. This step is covered in detail in the chapter *Banner Management*.
 - Step 3** Create a new campaign and add the description and keywords for easy search. This step is covered in detail in the chapter *Campaign Management*.
 - Step 4** After the creation of the banners and campaigns, as admin user you can customize the appearance of the services tool bar by choosing logos and animation. CMX Dashboard enables to preview the tool bar on mobile devices of different screen size. The steps are covered in detail in the chapters *Service Management* and *Browser Display & End User Experience*.

CMX Dashboard Components

The following are the components of the CMX Browser Engage:

Accounts & Roles

Accounts tab allows the admin user to define a set of accounts and users for each account.

For example, in case of a Mall, admin user can go to **Account > Create New Account** to make separate accounts for each store.

There are keywords associated with each account which will help locate the stores when the end user searches with these keywords.

The Account information is useful for the easy navigation at the venue.

CMX Dashboard also allows creating and assigning roles such as Account Admin, Marketing Admin, and Super Admin. The admin user can allocate tasks to each role.

For example, admin user can go to **Settings > Roles** to assign the tasks such as Campaign Approver, Banner Approver, and Reports amongst others.

Campaigns

Admin user can create campaigns for specific location, and assign the campaigns to offers, deals, sponsorships, advertisements, and welcome messages.

Campaigns Management allows you to choose the banners that are available and ascribe some rules with each banner type.

For example you can go to **Campaigns > Create New Campaign** and specify the account, active period and other rules.

Campaigns Management allows manage, edit and delete a specific campaign.

Banners

Banners are the messages that can be displayed on browser of the customer's mobile device.

The messages can be welcome message, offer, deal, sponsorship and advertisement. As an admin user you can set the type of rules and display for a specific banner.

For example, you can go to **Banners > Create New Banner** and set up a banner with details such as the text, image, type, and target URL.

You can choose whether the welcome message is displayed all the time user clicks on CMX Browser Engage icon or only the first time we detect that user.

Banners management allows making the banners as active or inactive.

Advantage of the Banners management is that you can choose to provide any offer or deal based on loyalty. If the customer spends more time at a specific Point of Interest, you can device a special offer.

POI management

In Point of Interest (POI) Management, you can see all the campus, building, floor/zone information that is taken from the Location MSE.

If there is any change in the Floor dimensions or map image on PI, you need to manually update that information using '**Update Floor Maps**' feature in POI sub menu.

You can add any additional POI on the floors using the tools available on the floor map.

For example, you can go to **Points of Interest > System Campus > Floor > Add Point of Interest** and set up a POI with specific information such as service categories, keywords, and image.

Appearance

You can set up appearance of banners on customer's mobile device.

To customize the look click **Appearance**.

You can define how you want to display the toolbar and the CMX Browser Engage icon. You can also define the default icon that shows up on the end device.

Following are the important parameters:

- **Display** - defines whether the CMX Browser Engage toolbar is expanded always or only when the user clicks on the icon.
- **Position** - defines whether the icon or toolbar should be displayed on the top or bottom.
- **Exceptions** - display the icon or toolbar on top or bottom as defined in the position, except for the URLs specified here.
- **Banner display time** - the after which a banner is be refreshed.
- **Default Logo** - the default logo or icon that is shown on the customer's mobile device
- **Animations tab** - the way and effect logo is displayed with.

As you set up the basic parameters as mentioned above, you are ready to offer the services.

Services

There are two methods of interaction with the customers at the venue. You can have messages as mentioned the above section.

Other significant way is to offer services - these are the value-added offerings that attract the customers to the venue. CMX Browser Engage as the name suggests takes part in enriching shopping experience and has potential to build the customer satisfaction and loyalty.

CMX Browser Engage offers effective services such as hyper-local search, 'Find me', and deals.

Hyper-local search

This service is helpful to the customers at a venue. There is a search icon pre-loaded on the CMX Browser Engage toolbar that appears on the customer's mobile device.

As Admin user, you can save the database of the stores and deals.

For example, a customer can find stores, sales deals, products and discount coupons using hyper-local search. Customer needs to enter the keyword in the search field and the result will show the location of the Point of Interest available nearby.

Find Me

It is helpful service to get different directions at a venue.

When the customer clicks on the Map icon that is displayed on the CMX Browser Engage toolbar, it shows the floor map along with a blue dot showing the customer's current location.

The customer can search for a specific item all stores and shows them on the map in form of dots.

Then the customer can click on a specific store and look for directions. In order to provide this information, admin needs to setup the floor navigation and plot the stores on the map using the icons.

For example, to search food items, the customer needs to enter food as keyword, and a food outlet is shown.

If some zone is closed for cleaning, refurbishing or other maintenance works and is not available for the customer, you can upload such information for the customers.

Deals

The venue owner or the stores can decide the various deals of different products and send these to the customers.

The admin user needs to update the data on deals. You can have the deals that are specific time bound promotions and sales offers.

The icons that appear above the CMX Browser Engage toolbar denote the deals service. It has the data on all the deals in the venue at the time. If the customer clicks on the icon all the details of that particular deal is displayed.

For example a store wants to offer a discount on the retail price of footwear, they can prepare such deal and corresponding icon appears above the CMX Browser Engage toolbar.

Reports

After setting up the CMX Browser Engage and offering services, as an admin user, you would require the information on the performance of services and messages.

The CMX Dashboard enables you to extract various reports for analysis. With the reports you can study the actual use of services and the customer behavior.

The additional advantage is the possibility to sell the customer data to advertising agencies and consumer goods companies.

For instance, you can click **Reports**, to view the performance of the services and messages for a specific time interval such as hour, day, week or month.

You can study the visitor trends using the CMX Visitor Connect.



Getting Started

This chapter describes information on system requirements and starting the Cisco Mobility Services Engine (MSE) on Prime Infrastructure and CMX Dashboard.



Note

For information on set up see *Cisco Prime Infrastructure Quick Start Guide*.

Adding a Mobility Services Engine to the Prime Infrastructure

You can add MSE using the Add Mobility Services Engine dialog box in the Mobility Service page. In this dialog box, you can add licensing files, tracking parameters, and assign maps to MSE. If you launch the wizard with an existing MSE for configuration, the Add MSE option appears as Edit MSE Details.



Tip

To learn more about Cisco Adaptive wIPS features and functionality, go to Cisco.com to watch a multimedia presentation.



Note

The Prime Infrastructure Release 1.4 recognizes and supports MSE 3355 appropriately.

To add a mobility services engine to the Prime Infrastructure, log in to the Prime Infrastructure and complete these steps:



Note

The Services > Mobility Services Engine page is available only in the virtual domain in Release 7.3.101.0

If you have not specified the username and password during the setup process, use the defaults.

The default username and password are both *admin*.

- Step 1** Verify that you can ping the mobility services engine.
- Step 2** Choose **Services > Mobility Services** to display the Mobility Services page.
- Step 3** From the Select a command drop-down list, choose Add **Mobility Services Engine** and click **Go**.

- Step 4** In the Device Name text box, enter a name for the mobility services engine.
- Step 5** In the IP Address text box, enter the IP address of the mobility services engine.
- Step 6** (Optional) In the Contact Name text box, enter the name of the mobility services engine administrator.
- Step 7** In the User Name and Password text boxes, enter the username and password for the mobility services engine. This refers to the Prime Infrastructure communication username and password created during the setup process.

**Note**

If you changed the username and password during the automatic installation script, enter those values here. If you did not change the default passwords, we recommend that you rerun the automatic installation script and change the username and password.

- Step 8** Select the **HTTP** check box to allow communication between the mobility services engine and third-party applications. By default, the Prime Infrastructure uses HTTPs to communicate with the MSE.
- Step 9** Select the **Delete synchronized service assignments** check box if you want to permanently remove all service assignments from the MSE. This option is applicable for network designs, wired switches, controllers and event definitions. The existing location history data is retained, however, you must use manual service assignments to perform any future location calculations.
- Step 10** Click **Next**. The Prime Infrastructure automatically synchronizes the selected elements with the MSE.
- Step 11** After the synchronization, the MSE License Summary page appears. You can use the MSE License Summary page to install a license, add a license, remove a license, install an activation license, and install service license. The Select Mobility Service page appears.
- Step 12** To enable a service on the MSE, select the check box next to the service. Services include Context-Aware Service and wIPS.
 Select the CMX Dashboard Service and HTTP Proxy Service to enable the services.
 You can choose CAS to track clients, rogues, interferers, wired clients, and tags.
 Choose Partner Tag Engine to track tags.

- Step 13** Click **Save**.
 After adding a new mobility services engine, you can synchronize network designs (campus, building, and outdoor maps), controllers, switches (Catalyst Series 3000 only), and event groups on the local mobility services engine using the Prime Infrastructure. You can perform this synchronization immediately after adding a new mobility services engine or at a later time. To synchronize the local and the Prime Infrastructure databases, see Synchronizing Mobility Services Engines.

Enabling CMX Dashboard Service on the Mobility Services Engine

To enable CMX Browser Engage and Dashboard, complete these steps:

-
- Step 1** Choose **Services > Mobility Services Engine**. The Mobility Services Engines page appears.
 - Step 2** In the Mobility Services page, click the **Device Name** to configure its properties.
 - Step 3** Select the check box next to the CMX Dashboard service.
 - Step 4** Click **Save**.
 - Step 5** Click **Done** to save the settings.

Enabling Proxy Server on the Mobility Services Engine

To enable proxy server, complete these steps:

-
- Step 1** Choose **Services > Mobility Services Engine**. The Mobility Services Engines page appears.
 - Step 2** In the Mobility Services page, click the **Device Name** to configure its properties.
 - Step 3** Select the check box next to the Proxy Service.
 - Step 4** Click **Save**.
 - Step 5** Click **Done** to save this settings.

Logging into CMX Dashboard User Interface

To configure the CMX Dashboard and Proxy services, do the following in the Prime Infrastructure:

-
- Step 1** Choose **Mobile Concierge Service > CMX Dashboard Configuration**. Choose the Location MSE that the CMX Dashboard MSE gets the maps and location data from. It can be the same MSE or a different MSE.
 - Step 2** Choose **Mobile Concierge Service > Proxy Configuration**. Choose the CMX Dashboard MSE that provides the information of the banners to the end device. The CMX Dashboard MSE is served from this Proxy MSE.

To log into CMX Dashboard user interface through a web browser, complete these steps:

-
- Step 1** Type `https://mseip/dashboard/` in the web browser.
 - Step 2** Enter the default username as admin.

Step 3 Enter the default password as admin.



Note

To change the default password click **My Account** on the top right corner. Enter and re-enter the new password of choice, and click **Submit**.



Account Management

The CMX Dashboard enables you to create and assign accounts depending on the product or service.

An Account is an entity that owns the content that is published through the CMX Dashboard. The account contains information of all the events including view, number of clicks of the specific messages, and services.

Account Management allows you to define and set up different set of accounts and users. An Account user is entitled to a role with specific functionality permissions for that role.

The CMX Dashboard Administrator can create an account for a store. Customers can locate stores using the keywords associated with each account. Account information is used while plotting the store in the Floor Navigation.

Creating an Account

To create a new account, complete the following steps:

- Step 1** Choose **Accounts** from the left side bar menu.
- Step 2** Click **Create New Account**. The Add/Edit Account and Address group boxes appear.
- Step 3** In the Add/Edit Account group box, do the following:
 - Enter the name of the account in Account Name:* text box.
 - To upload a logo of the account, click **Click to upload a Logo**. Locate the image file from File Upload dialog box and click **Open**.
 - In the Account Description* text box, enter the description of the account.
 - Enter the keywords about the account you want to create in the Keyword* text box. These keywords help locate the store easily when a customer searches on the mobile device browser.
- Step 4** In the Address group box, do the following:
 - Enter the email address of the account in the Email* text box.
 - Enter the URL of the account in the Website URL* text box.
 - In the Phone* text box, enter the phone number of the account.
 - In the text boxes Street Line 1* and Street Line 2* enter the address of the account.
 - In the City* text box, enter the name of the city.
 - In the State* text box, enter the name of the state.

- Enter the area zip code in the Zip Code* text box.
- Step 5** Click **Submit**.

Deleting an Account

To delete a new account, follow these steps:

-
- Step 1** Choose Accounts from the left side bar menu. Click **All** to view all the accounts in the CMX Dashboard database. All Accounts group box appears.
- Step 2** In the Active Accounts group box, select the account you want to delete.
- Step 3** Click **Delete**.

Making an Account active

To make an active account active, follow these steps:

-
- Step 1** Choose Accounts from the left side bar menu. Click **Inactive** to view all the accounts in the CMX Dashboard database. Inactive Accounts group box appears.
- Step 2** In the Inactive Accounts group box, select the account you want to reactivate.
- Step 3** Click **Make Active**.

Making an Account inactive

To make an active account inactive, follow these steps:

-
- Step 1** Choose Accounts from the left side bar menu. Click **Active** to view all the accounts in the CMX Dashboard database. Active Accounts group box appears.
- Step 2** In the Active Accounts group box, select the account you want to delete.
Click **Make Inactive**.

Roles, Domain and Server Settings

The CMX Dashboard UI provides the feature to organize roles, domain setup and the server settings.

Roles

To set the roles follow these steps:

-
- Step 1** From the left side bar menu, select Settings. Click **Roles**.
 - Step 2** Click **Create New Role**. Select Operations box appears.
 - Step 3** Enter the name of the role category in Name: textbox.
 - Step 4** Enter the name that you want on display in Display Name:
 - Step 5** Choose and change the roles from Available Operations and Existing Operations.
 - Step 6** Click **OK**.
 - Step 7** To edit a role, click the role in the list that appears when you select Settings and click **Roles**.
 - Step 8** Click **Edit**. Change the operations and click **OK**.
 - Step 9** To delete a role, click the role in the list that appears when you select Settings and click **Roles**.
 - Step 10** Click **Delete**.
 - Step 11** Click **OK** in the Delete Confirmation dialog box.

Domain

To set the domains follow these steps:

-
- Step 1** From the left side bar menu, select Settings. Click **Domain Setup**.
 - Step 2** Click **Create New Domain**. Add/Edit Domain group box appears.
 - Step 3** In Domain Name: enter name of the domain.



Note You have to set up key-value mapping for the webpage or domain, before adding it to a Point of Interest.

- Step 4** In Domain URL: enter the URL of the domain.



Note Please don't use http://

- Step 5** In Key Handlers: enter the keywords.



Note If more than one key handler, please enter them separated by comma.

- Step 6** Click **Submit**.

- Step 7** To edit or delete a domain, click the domain in the list that appears in Domain Setups group box when you select Settings and click **Domain Setup**.

Step 8 Click **OK**.

Server Settings

To set up the server parameters follow these steps:

-
- Step 1** From the left side bar menu, select Settings. Click **Server Settings**.
 - Step 2** Choose the default or MSE in Location Resolver:
 - Step 3** Enter the time in seconds in Location Resolver Stale Time:
 - Step 4** In Campaign Cache Refresh Frequency: enter the time in hours.
 - Step 5** In Campaign Cache DB sync time: enter the time in seconds.
 - Step 6** In Index refresh time: enter the time in seconds.
 - Step 7** In Reports data retention time: enter the number of days you want to retain the data.
 - Step 8** In Default location ID: enter the ID of the location.
 - Step 9** In Banner welcome delay: enter the time period in seconds.
 - Step 10** Choose the collectors of data in BBX Statistic collectors.



Note Default logo is that of Cisco.

Step 11 Click **Save**.



Points of Interest Management

A Point of Interest (POI) is a specific location within the venue where a product or a service is available. With the CMX Dashboard user interface you can create various POIs highlighting specific zones.

The maps and location data for the campus, building, or floor are uploaded to the Prime Infrastructure and synchronized with the Location MSE. The CMX Dashboard displays these maps.

You can update the map in the CMX Dashboard by clicking **Update Floor Maps** in **Points of Interest** menu.

As an administrator, you can create zones inside a venue to use location specific messages, offers, and deals.

You can mark the specific area on the map that you want to make a point of interest in the CMX Dashboard UI.

Adding Point of Interest

To add or update a Point of Interest, complete the following steps:

-
- Step 1** From the left sidebar menu, select **Points of Interest**.
 - Step 2** Click the white triangular icon in the right pane located at the left side of PointOfInterests.
 - Step 3** Click the white triangular icon in the right pane located at the left side of System Campus.
 - Step 4** Click the white triangular icon in the right pane located at the left side of name of the venue.
 - Step 5** In the right pane Add/ Update Point of Interest group box appears.

Figure 4-1 Add/Edit POI

Add/Update Point of Interest

Name: *

Description:

Service Categories:

Domain Mapping:

Splash Template:

Tags / Keywords:

Choose Image: **Click to upload a Logo**

**Click or drag and drop on existing image to upload a new Image, Recommended logo size is 45px by 45px. Bigger files will be automatically resized.

! Any changes to POI dimensions might be overridden when updating floor maps.

351705

- Step 6** Enter the name of the POI in the Name:* text box.
- Step 7** Enter the description of the POI in the Description: text box.
- Step 8** Select the appropriate service (Map, Deals, or Search) that you want to provide from the Service Categories drop-down list.
- Step 9** From the Domain Mapping drop-down list, choose the domain mapping.



Note The banners related to a domain are associated to a campaign and assigned to a Point of Interest.

- Step 10** Choose the type of splash template from the Splash Template drop-down list.
- Step 11** Enter the keywords in the Tags/Keywords: text box.
- Step 12** To upload a logo, click **Click to upload a Logo** and browse to choose an image and click Open.

Step 13 Click **Submit**.



Note Any changes to POI dimensions may be changed when floor maps are updated.

Step 14 To define a zone go to **PointsOfInterests > System Campus > Venue** and then to the floor. You can draw & set up a zone on the map of that floor with **Draw Polygon** setting. Double-click on the zone after you finish drawing to close & save it. You can also use the settings like **Drag, Edit, & Delete Selected** polygon once you select it.

Updating Floor Maps

To update floor maps, complete these steps:

-
- Step 1** Create floors and POIs on Mobile Services Engine.
 - Step 2** Log in to the CMX Dashboard User Interface.
 - Step 3** Choose Points of Interest from the left side bar menu.
 - Step 4** Click **Update Floor Maps** in the right pane.
 - Step 5** The Update Confirmation dialog box appears.
 - Step 6** Click **OK**. To cancel, click **Close**.



Note If you modify the campus, building, or floor on PI, you have to update them in the CMX Dashboard UI by clicking **Update Floor Maps** to get the modified information.

Deleting Floor Maps

If you remove any data for floors, building, or campus from the PI, is not deleted from the CMX Dashboard. You have to delete the information from the CMX Dashboard UI.

To delete a floor map, complete these steps:

-
- Step 1** Choose Points of Interest from the left side bar menu.
 - Step 2** Go to **System Campus > Venue > Floor**.
 - Step 3** Click **Delete Floor**.



Navigation Management

CMX Dashboard enables you to organize the navigation of the zones of venue per your need. You must configure all the Points of interest, maps, and directions in the CMX Dashboard database. The floor map is based on the data from the Mobility Services Engine. CMX Dashboard also enables you to assign a campaign to a specific zone on a floor.

When customers click on the map logo on his mobile device browser, they view their location and a map of the zone he is situated in. The light blue icon denotes the actual location of the customer. If the customer searches for an item, navigation helps to identify the location of that product or service. When the customer clicks on the logo, the store information, the directions, the buttons to email or call the store appear. Along with that, map guides you to those locations of availability via the shortest route. The CMX Dashboard supports this navigation management.

Creating Navigation Points

To create a navigation point on a floor, complete the following steps:

- Step 1** Choose **Floor Navigation** from the left side bar menu.
- Step 2** Click the white triangular icon in the right pane located at the left side of PointOfInterests.
- Step 3** Click the white triangular icon in the right pane located at the left side of System Campus.
- Step 4** Click the white triangular icon in the right pane located at the left side of name of the venue.
- Step 5** Click the name or the number of the floor. A map of that floor appears in the right pane.
- Step 6** Click **Start Over**. A dialog box to confirm that you want to start floor navigation design appears. Click **Yes**.
- Step 7** To place the stores in the floor map, click the **Plot Store** icon at the top panel.

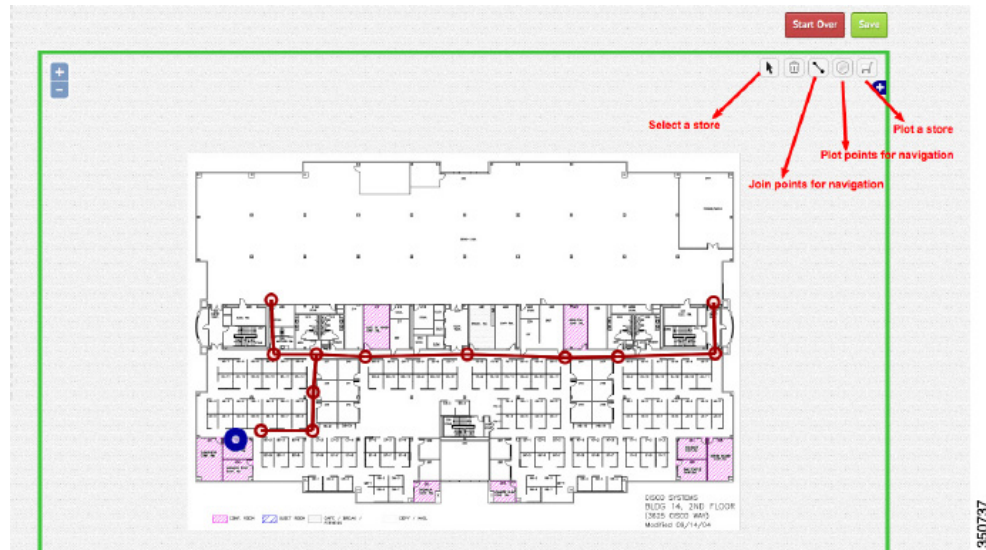


Note The Account information is used while plotting the store.

- Step 8** To place the paths, click **Draw Points** icon.
- Step 9** To connect various locations and the paths on the floor, click **Draw Line** icon.
- Step 10** To add additional information about a specific location, click **More Info** icon.
- Step 11** After finishing the allocation of all the locations, paths, and stores on the floor map, Click **Save**.

The following figure shows the creation of navigation points.

Figure 5-1 Creation of navigation points



Note

From the CMX Dashboard user interface (UI), you can access the CMX Analytics UI. With CMX Analytics you can collate and analyze the information based on location and customer behavior. For more information, see *CMX Analytics Configuration Guide, Release 7.5*.



Note

For the CMX Dashboard navigation, POI specific campaigns to work, the prerequisites are to create floor maps in PI, position access points in PI, and to synchronize maps to a Location MSE. For more information, see *Cisco Connected Mobile Experiences Configuration Guide, Release 7.5*.



Banner Management

Banner Management allows you to create different types of messages to interact with the customers at the stores or venues. You can set the message specific rules and validity rules.

An Admin user or account user with credentials creates messages, previews them and publishes for approval.

You may compose a message in either text with image or as an image. The message dissemination depends on various factors such as the day, date, time, type of user, preferences, and location.

These are the four types of messages or banners.

1. Welcome
2. Offer or Deal
3. Sponsorship
4. Advertisement

Welcome

Welcome message is the first message that appears when a guest or customer walks into the venue of an enterprise. The welcome message also appears if the customer moves from one Point of Interest to another.

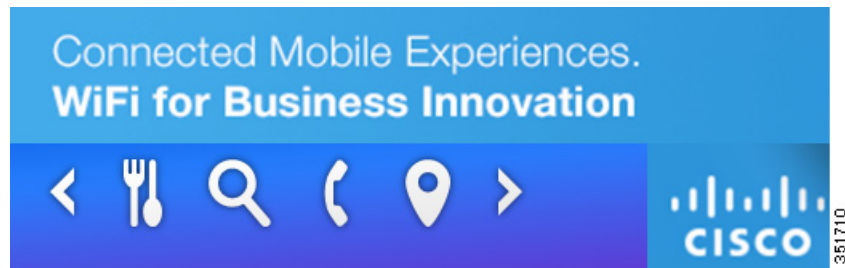
Point of interest is a specific location of sale of a product or service within the venue of an enterprise.

For instance when guest walks in ABC Mall, the welcome message is “Welcome to ABC Mall”.

Similarly, when a guest walks into the food court, the message is “Welcome to the International Food Court.”

Following figures show the example of a welcome message:

Figure 6-1 Welcome message



You can change the welcome messages depending on the location and the Point of Interest.

The Welcome Message can be customized depending on a visitor walks into the venue for the first time or the second.

For instance, for a new visitor to the XYZ Mall, the welcome message would be “Welcome to XYZ”.

For returning customers, the message would be “Welcome Back to XYZ Mall”.

Following figure shows the creation of welcome message.

Figure 6-2 Create welcome message

To create a welcome message, complete the following steps:

-
- Step 1** Go to **Banners** and click **Create New Banner**.
 - Step 2** Enter the message name.
 - Step 3** Choose **Welcome** from the **Type of Message** menu.

**Note**

The CMX Dashboard shows the welcome message only once in the campaign; the other type of messages can be repeated.

Step 4 Choose the type of account that owns the message from the account list.

Step 5 Chose either of the following options of the message display:

- Text with Logo

For this option, enter the text for the message using a text formatting tool similar to MS Word, where you can select font, size, color, and style.

- Image

Step 6 To upload a picture or image, click **Upload**.

**Note**

If you want guests to click on the welcome message and get directed to an URL, you need to enter the URL.

Step 7 Enter the keywords for hyper-local search.

Step 8 Click **Submit**.

Offer or Deal

An offer message is an advertisement for the guests and customers. For instance a store inside a mall can inform about new fall season collections.

A Deal messages is a special type of the offer message. Deal message relate to a specific time bound sales promotion. Using deal as the keyword, a customer can use the hyper-local search to view the deals available.

To create an Offer or Deal message, complete the following steps:

Step 1 Go to **Banners** and click **Create New Banner**.

Step 2 Enter the message name.

Step 3 Choose **Offer** or **Deal** from the **Type of Message** menu.

Step 4 Choose the type of account that owns the message from the account list.

Step 5 Chose either of the following types of message display:

- Text with Logo

For this option, enter the text for the message using a text formatting tool similar to MS Word, where you can select font, size, color, and style.

- Image

Step 6 To upload a picture or image, click **Upload**.

**Note**

If you want guests to click on the Offer and get directed to an URL, you need to enter the URL.

Step 7 Enter the keywords for hyper-local search.

Step 8 Click **Submit**.

Sponsorship

Sponsorship Messages are advertisements of an external party in a particular section of the venue. The external entity buys a part of the advertisement inventory in the CMX Dashboard and highlights its brands, products, and services through messages.

For example XYZ Corp advertises its product A.

To create a Sponsorship message, complete the following steps:

Step 1 Go to **Banners** and click **Create New Banner**.

Step 2 Enter the message name.

Step 3 Choose **Sponsorship** from the **Type of Message** menu.

Step 4 Choose the type of account that owns the message from the account list.

Step 5 Choose either of the following types of message display:

- Text with Logo

For this option, enter the text for the message using a text formatting tool similar to MS Word, where you can select font, size, color, and style.

- Image

Step 6 To upload a picture or image, click **Upload**.

**Note**

CMX Dashboard If you want guests to click on the Sponsorship banner and get directed to an URL, you need to enter the URL.


Step 7 Enter the keywords for hyper-local search.

Step 8 Click **Submit**.

Advertisement

Advertisements are messages from an external party promoting its brands.

To create an Advertisement, complete the following steps:

-
- Step 1** Go to **Banner** and click **Create New Banner**.
- Step 2** Enter the message name.
- Step 3** Choose **Advertisement** from the **Type of Message** menu.
- Step 4** Choose the type of account that owns the message from the account list.
- Step 5** Chose either of the following types of message display:
- Square picture with text
For this option, enter the text for the message using a text formatting tool similar to MS Word, where you can select font, size, color, and style.
 - Rectangular Image
- Step 6** To upload a picture or image, click **Upload**.
-  **Note** If you want guests to click on the Advertisement and get directed to an URL, you need to enter the URL.
-
- Step 7** Enter the keywords for hyper-local search.
- Step 8** Click **Submit**.

Difference between the types of messages

The types of messages are - Welcome, Offer, Sponsorship, Advertisement, and Deal. The difference between these messages is based on the rules that the admin user sets up.

Welcome message appears when a guest or customer walks the first time, into the venue. It also appears if the customer moves from one zone to another. It is not repeated.

Deals are the bargains that are given to customers on per-day basis.

Offers are provided on the basis of the frequency of the customer's visit to the venue.

Sponsorship is the message used depending on the venue, for example Google could sponsor free Wi-Fi to all users in a convention center or at educational conference.

Advertisement is more relevant in case of the retail stores. For example a company may advertise a launch of a product at a mall.



Campaign Management

Campaign Management enables enterprises to create and implement various campaigns.

You can create campaigns for specific points of interests, and assign the campaigns to messages such as offers, deals, sponsorships, advertisements, and welcome messages.

You can set triggering rules to specific messages and validity rules for the campaigns.

To create a campaign, you must have an account and a banner.

Web Banner

The web banner is a type of advertising on the CMX Dashboard. When a guest or a customer walks in a store or venue and connects to the wireless network, you can place a web banner in form of a logo or image on the customer's mobile device.

Creating a Campaign

Before creating campaign, you must have an account and banner.

To create a campaign, complete these steps:

-
- Step 1** From the left side bar menu, select Campaigns.
 - Step 2** Click **Create New Campaign**, in the right pane.
 - Step 3** In the Campaign Name:* text box, enter the campaign name.
 - Step 4** Select the account from the Account: drop-down list. It is the account that you want to assign this campaign to.



Note You must create a point of interest to populate in the Points of Interests: list box.

- Step 5** Select the point of interest from the Points of Interests: list box. It is the zone where you want to display the campaign.

- Step 6** Click **Active Period**:* to open a calendar and choose a start date and time along with end date and time. The campaign is on within these time slots.
- Step 7** To apply any additional rules and policies, click **Add** in the Campaign Rules group box. The Add/Edit Policy Rules window appears.
- Step 8** Complete the following steps, in the Add/Edit Policy Rules window:
- Click the **Dates** to open the calendar and choose the start time and end time.
 - Select the day of the week from the Days list. The possible options are: Mon, Tue, Wed, Thu, Fri, Sat, Sun. This is the day of the week when you want to publish this campaign.
 - Click the **Time** to open the calendar and choose Time, Hour, and Minute.
 - Click **Save**.
- Step 9** To assign a welcome message to the campaign, click **Next**. The Welcome Setup tab appears.
- Step 10** From the Active Welcomes list box, choose the welcome banner.
- Step 11** To assign any offer banner that you have already created to the campaign, click **Next**.
- Step 12** Select the active offers from the Active Offers list box.
- Step 13** Click **Next** to assign any offers to this campaign.
- Step 14** Select the active sponsorship from the Active Sponsorships list box.
- Step 15** To assign any advertisements that you have created with this campaign, click **Next**.
- Step 16** Choose the advertisement from the Active Advertisements list box.
- Step 17** Click **Next** to assign deals to this campaign.
- Step 18** Select deals from Active Deals list box.
- Step 19** Click **Submit**.
- Step 20** To publish an active campaign, click **Publish Active Campaigns**, in the right pane.

**Note**

By default the newly created campaigns are inactive. You have to make them active before publishing. After activation the banner appears in the Active Banners group box. You must associate a newly created banner to a campaign.

Assigning Banner to a Campaign

To assign various banners like welcome message, offer, sponsorships, advertisements, and deals to a campaign, complete the following steps:

- Step 1** Select Campaigns from the left side bar menu.
- Step 2** Click to highlight the campaign in the Active Campaigns group box. You can assign various banners to the selected campaign.
- Step 3** Click **Edit**. The Add/Edit Campaign group box appears.

- Step 4** To assign a welcome message, go to Welcome Setup tab and select the welcome message from the Active Welcomes drop-down list and click **Next**.
- Step 5** The Offers Setup tab opens. Select banner of the offer from the Active Offer drop-down list and click **Next**.
- Step 6** The Sponsorship Setup tab opens. Select the sponsorship from the Active Sponsorship drop-down list and click **Next**.
- Step 7** The Advertisement Setup tab opens. Select the advertisements offer banner from the Active Advertisements drop-down list and click **Next**.
- Step 8** The Deals Setup tab opens. Select the deals from the Active Deals drop-down list.
- Step 9** Click **Submit**.

Editing the Existing Banner

To edit the existing banner, complete the following steps:

- Step 1** Choose Banners from the left side bar menu.
- Step 2** Click **All** in the right pane to view both the active and inactive banners.
- Step 3** In the All Banners group box click to highlight the banner that you want to edit.
- Step 4** Click **Edit**.
- Step 5** Make the necessary changes in the Add/Edit Banner group box and Setup Content group box.
- Step 6** Click **Submit** to apply your changes.



Note To cancel the changes, click **Cancel**.

Deleting a Banner

To delete a banner, follow these steps:

- Step 1** Choose Banners from the left side bar menu.
- Step 2** In the right pane click **ALL** to view both the active and inactive banners.
- Step 3** Select the banner that you want to delete in the All Banners group box.
- Step 4** Click **Delete**.
- Step 5** Confirmation dialog box appears. Click **OK** to delete the banner.



Note If you don't want to delete the banner, click Close.

Previewing the Existing Banner

To view the existing active or inactive banner, follow these steps:

- Step 1** Choose Banners from the left side bar menu.
- Step 2** Click **ALL** in the right pane, to view both the active and inactive banners.
- Step 3** Select the banner in the All Banners group box and click **Preview**.
- Step 4** It shows the banner's display when available to the customers on mobile device.

Searching a banner

To search a banner, follow these steps:

- Step 1** Choose Banners from the left side bar menu.
- Step 2** Click **Active** in the right pane to view and search all the active banners.
- Step 3** Click **Inactive** in the right pane to view and search all the inactive banners.
- Step 4** Click **All** to search all the active and inactive banners.



Service Management

The CMX Dashboard interacts with the customers at the venue in two ways - services and messages. Services are the value-added offerings that attract the customers to the CMX Dashboard. Services are helpful to engage customers when they enter a venue. Messages help the enterprise in revenue generation. Messages are the ads, offers, and sponsorships.

The first step to create a service for an enterprise is to identify the appropriate service that the CMX Dashboard can offer to the customers.

Currently the CMX Dashboard offers the effective services such as hyper-local search, map, and deals.

The Admin user can configure the hyper-local search and map services in the CMX Dashboard. Admin user can also create additional services specific to a venue.

CMX Dashboard renders an engagement method as an icon on the CMX Dashboard tool bar on the browser on the customer's mobile device.

Hyper-local search

Hyper-local Search is in-built in the CMX Dashboard. The search icon is pre-loaded into the CMX Dashboard and cannot be changed by the user. The customer can enter keywords and the CMX Dashboard provides results that are specific to the venue.

Hyper-local Search service has been pre-configured to appear everywhere in the venue, and is not location-based.

The CMX Dashboard administrator generates the hyper-local search function using the data the users have uploaded in the system. When the admin user creates messages, advertisement, and accounts, the user can search for these services using keywords.

The customer can click one of the results and get the directions to a Point of Interest nearby. The customer can also click the URL link specific to a store for more information.



Note

If the customer clicks close without saving the information, the search results are lost.

Editing Hyper-local Search Appearance

To change the appearance of search icon, follow these steps:

-
- Step 1** From the left hand bar menu, select Menu. In the right pane, Menu Categories group box appears.
- Step 2** Select Search. Click **Edit**. Add/ Edit Service group box appears.
In the Service Name:* text box, 'Search' exists by default.
- Step 3** If you want to change the appearance of search icon on the mobile device browser, choose the display style as either Grid or List.
The status of the search is Active, by default.
- Step 4** If you want to change the logo, click the icon in Choose Logo:*
- Step 5** Locate the image file from File Upload dialog box and click **Open**.
- Step 6** Click **Submit**.

Map

The maps are in-built in the CMX Dashboard.

The customer can use the maps to

- Find Me/ Locate self
- Locate a store

The CMX Dashboard guides the customer to find a way at the venue and prompts the directions to the point of interest.

The CMX Dashboard administration user must upload the map of the entire venue into CMX Dashboard database.

Editing appearance of map

To change the appearance of map, follow these steps:

-
- Step 1** From the left hand menu, select Menu. In the right pane, Menu Categories group box appears.
- Step 2** Select Map. Click **Edit**. Add/ Edit Service group box appears.
In the Service Name:* text box, 'Map' is there by default.
- Step 3** If you want to change the appearance of map icon on the mobile device browser, choose the display style as either Grid or List.
The status of the map is Active, by default.
- Step 4** If you want to change the logo, click the icon in Choose Logo:*
- Step 5** Locate the image file from File Upload dialog box and click **Open**.

Step 6 Click **Submit**.

Deals

It is created by system on the basis of the deals that admin user has entered into the system. The deals appear on the CMX Dashboard indicating all the deals in the venue at the time.

Deals icon appears on the mobile device browser of the customer only if there are any deals active at any specific point of interest.

Editing Deals Appearance

To change the appearance of deals, follow these steps:

-
- Step 1** From the left hand menu, select Menu. In the right pane, Menu Categories group box appears.
- Step 2** Select Deals. Click **Edit**. Add/ Edit Service group box appears.
In the Service Name:* text box, 'Deals' is there by default.
- Step 3** If you want to change the appearance of deals icon on the mobile device browser, choose the display style as either Grid or List.
The status of the deals is Active, by default.
- Step 4** If you want to change the logo, click the icon in Choose Logo:*
- Step 5** Locate the image file from File Upload dialog box and click **Open**.
- Step 6** Click **Submit**.



Browser Display & End User Experience

CMX Dashboard Administration tool enables the admin user to manage the runtime behavior and the appearance of the CMX Dashboard.

There are configuration specifications that drive the CMX Dashboard behavior and the User Interface.

Browser Display

Browser Display enables the admin user to see and manage the appearance of the CMX Dashboard services on mobile devices of the customers at the venue.

The simulator is provided as part of the CMX Dashboard Administration tool to replicate the representation specific to the end-user devices.

Currently, the CMX Dashboard supports the most of the Android & iOS devices including iPhone 4S, Samsung Galaxy S, Samsung Galaxy Tab, iPad 2.

The following is the schematic representation of the mobile browser.

Figure 9-1 **Mobile browser**



The administrator user can select a device type and simulate the following:

- Runtime behavior
- Appearances of the various settings
- Banner appearance with different colors and logos
- Banner animation

Icons or Images

Following are the various icons for which logos or banners can be used.

- Search
- Deals
- HTML5 Maps

Following are the details of the logo and banner.

- Main logo:

In this 7.5 release, CMX Dashboard Admin tool supports uploading the main logo as a square of any size, but is limited to 45x45 pixel to support the display aspects of various mobile devices.

- Banner:

Banner should go across the end-user device in conjunction with the main logo icon. CMX Dashboard Admin tool provides color palette to pick the following

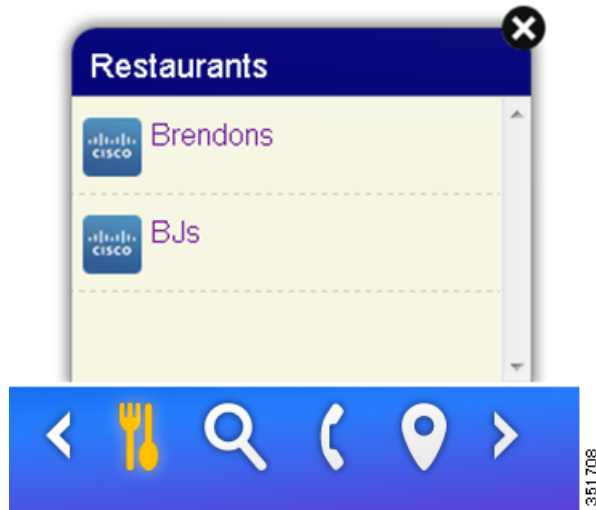
- Background Color start
- Background Color end (can be the same as start if no fading required)
- Service icons are the ones that show up on the banner across and are location aware. Service icon specification are:
 - 45x45 pixel for Mobile
 - 64x64 pixel for Tablet/Desktop

Figure 9-2 **Icon example**



The service icons can be uploaded while creating/editing individual Services via Administration tool and can be previewed through the simulator tool.

- Service Item icons are the ones that pop-up when user clicks on a Service. Service items includes deal items, offer items, map icons, store icons, messages. These icons have with the following specifications.
 - 60x40 pixel
 - 75x50 pixel
- Rolling Messages (Advertisements) - Same as Service Item icons.

Figure 9-3 Service icons example

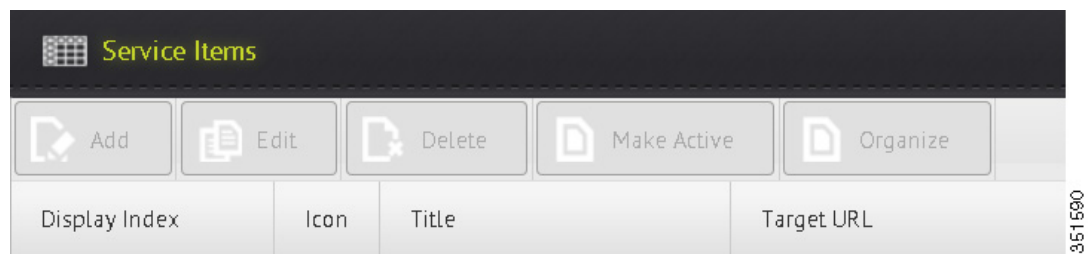
UI templates

The UI template is a page layout that is designed for the CMX Dashboard UI.

Runtime presentation of Service Items for a specific service should be driven through UI templates and should be configurable via Administration tool.

Currently, the following templates are supported:

- Table (Item Icon, Item name + description) - Entire row can be clicked if a URL is provided. For instance, the Maps Service has various items that can be shown as a table.

Figure 9-4 Table example

- Grid - It is with icon and name to display. For example, a point of interest has various items (Casino, Restaurants, and Coffee) as a 2 x 3 grid.

Figure 9-5 Grid example

Name: *

Description:

Service Categories:

351585

Animation

Animation focuses on gaining and retaining the user attention while browsing live at the venue. It enables the admin user to define the way logo displays on the mobile device browser.

Setting the Services appearance

To set the appearance of the services, complete the following steps:

From the left side bar menu, select Appearance. Service Bar and Animation tabs appear. Figure 12-2 depicts the settings.

On the Service Bar tab, do the following.

-
- Step 1** Choose the type of display of the services as on-demand or always from Display.
 - Step 2** Choose the position of the service bar from Position. You can choose the position at the top of the mobile device browser or at the bottom.
 - Step 3** Enter the URLs of the websites where you do not want the services bar to appear, in the Exceptions: text box.
 - Step 4** Choose the background color from Background Color Start and Background Color End.
 - Step 5** Enter the time in (number of seconds) for which the services bar appears on the mobile device browser, in the Banner Display Time text box.



Note Minimum display time is ten seconds.

The Cisco logo is loaded as the default logo.

Step 6 To view the changes in the real time, click **Auto-Preview**. The right pane displays the preview.

Step 7 To save and apply the settings, click **Save Settings**.

Figure 9-6 Services appearance

The screenshot shows the configuration interface for the Services Bar Animation. The interface is divided into two tabs: 'Services Bar' and 'Animation'. The 'Animation' tab is active, showing the following settings:

- Display:** Radio buttons for 'Always' (selected) and 'On-demand'.
- Position:** Radio buttons for 'Top' and 'Bottom' (selected).
- Exceptions:** A text input field containing 'cisco.com, yahoo.com'.
- Background Color Start:** A color picker showing the hex code '3da610'.
- Background Color End:** A color picker showing the hex code 'c96e24'.
- Banner Display Time (Min 10 sec):** A text input field containing the value '10'.
- Default Logo (48px X 48px):** A preview of the Cisco logo.

At the bottom of the configuration pane, there is a checkbox labeled 'Preview changes in realtime' which is checked. To the right of this checkbox are two buttons: a red 'Auto-Preview' button and a green 'Save Settings' button.

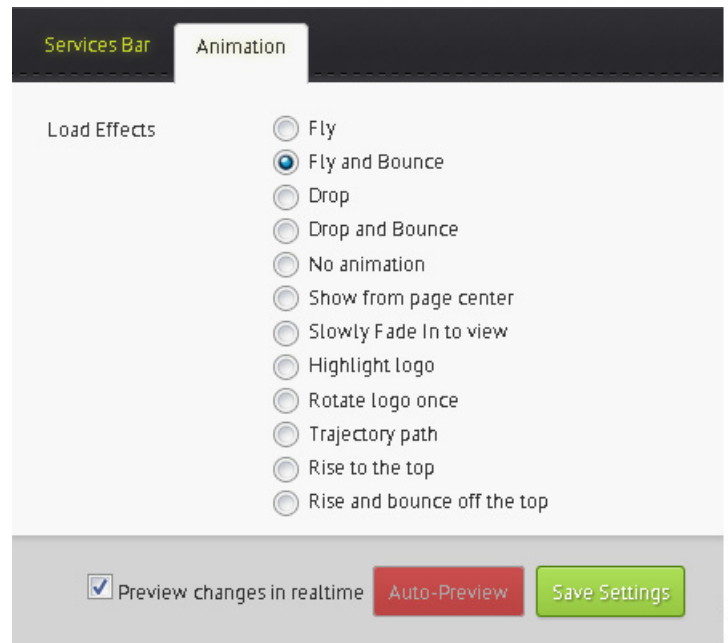
350749

Setting the animation appearance

You can set the way in which the service bar appears on the browser. The CMX Dashboard admin user can choose the type of animation for the service bar.

There are various options such as show from the page center, fly and bounce, rotate the logo once, rise to the top, or no animation amongst others. The following figure shows the different animation options available.

Figure 9-7 Animation options



To set the animation, do the following:

- Step 1** From the left side bar menu, select Appearance. Service Bar and Animation tabs appear.
- Step 2** On the animation tab, choose the animation effect for the service bar from Load Effects.
- Step 3** To preview the changes in the real time, click **Auto-Preview**. The right pane displays the preview.
- Step 4** To save and apply the load effect settings, click **Save Settings**.

End User Experience

The CMX Dashboard is simple and intuitive to use and provide value-added services to the customers, while the enterprise can explore revenue generation by mobile ads and analytics.

The guest or the customer at the venue is the end user of the CMX Dashboard. Following is the end user experience for instance, at a shopping center with a Wi-Fi network managed by XYZ.

- A customer walks into the enterprise that has a Wi-Fi network.
- The customer starts to avail the internet at the venue on the mobile device.

- On the web page, a XYZ logo appears on the browser at the bottom right corner. This is an indication CMX Dashboard service is available.

**Note**

The logo of the enterprise would appear on every web page that the customer browses.

- The customer clicks the XYZ logo and opens the CMX Dashboard service bar. There is a toolbar that shows the CMX Dashboard services available at the enterprise.
- The customers can click “hyper-local search” icon, enter a search keyword, and the CMX Dashboard shows the results on top of the CMX Dashboard banner. The guest can click the map logo, enter name of store or keyword, and the CMX Dashboard opens a map that displays the results.

If the enterprise wants to utilize the CMX Dashboard to generate revenue with mobile advertisement, the admin user can set the appearance of the ads.

For instance, the ad is from one of XYZ clients. They have business relationships with the ad agencies who buy ad inventory on XYZ cable television network. These ad agencies would buy the new ad inventory generated by the CMX Dashboard on XYZ Wi-Fi network. There can be a process of integration of the CMX Dashboard with XYZ's ad server.

Make a Wish

The Make a wish link on the top right corner enables you to send the feedback through email.

To access, click **Make a wish**. It directs you to the email id mse-wishlist-external@cisco.com on the MS Outlook.

You can send the response and comments on the CMX Dashboard to this email id.

Browser and Operating System support

The following are the web browsers and the operating systems that the CMX Dashboard supports currently.

Table 9-1 Browser & OS

Browser	Operating Systems
Safari	iOS
Android browser	Android
Chrome	Google Chrome OS
Mozilla Firefox	Windows, OS X, and Linux, with a mobile version for Android

**Note**

CMX Dashboard is not supported on Windows Internet Explorer on desktop devices and on Windows phones. CMX Dashboard is not supported on Blackberry.

**Note**

If you access the desktop version of the CMX Dashboard UI on a mobile device, it can be small and unusable.

**Note**

The CMX Dashboard supports approximately 95% of all websites.



CMX Dashboard Reports

The CMX Dashboard enables the administration user in an enterprise to analyze the use of services and the customer behavior.

The admin user can also study the pattern of sales across the domains in a venue.

For instance, the admin user can view services performance and can analyze the use of hyper-search, map, and deals services.

On the basis of these reports, the enterprise can explore the opportunities to propose more and more customer centric offers. This enables the enterprise to attract and engage more customers at a particular venue.

Reports

The CMX Dashboard supports taking out reports of services for a specific venue. The reports enable the admin user to analyze the performance for a certain period of time.

To access the reports in the CMX Dashboard, follow these steps:

-
- Step 1** From the left side bar menu, select Reports.
The Services, Message, Domain Metrics, and Visitor Connect tabs appear.
- Step 2** To view the Services Performance and Service Clicks for today, in the Services tab, click **Today** and then click **Apply**.



Note Service Performance is a custom service usage report.

- To view the daily Services Performance and service Clicks, click **Daily** and then click **Apply**.
- To view the monthly Services Performance and Service Clicks, click **Monthly** and then click **Apply**.

Following figures show the monthly performance and number of clicks.

Figure 10-1 Service performance

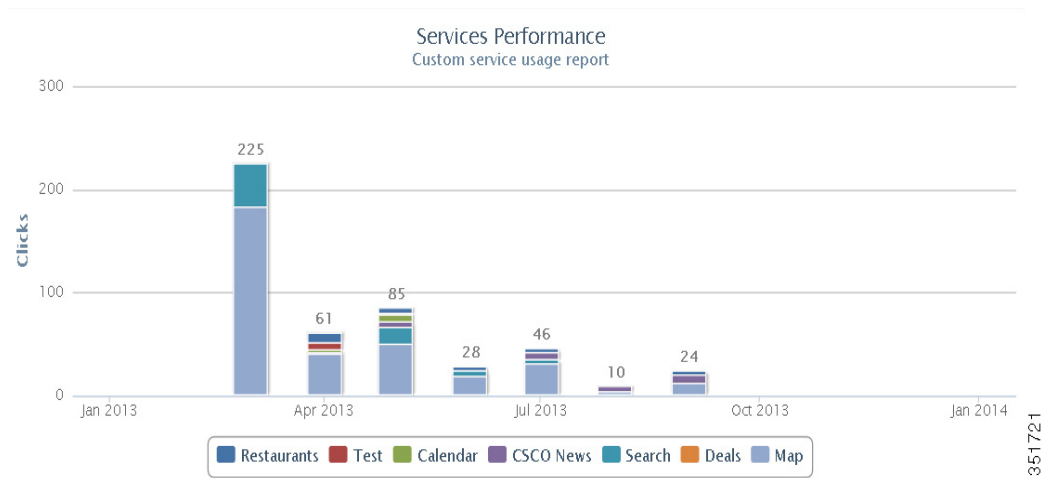
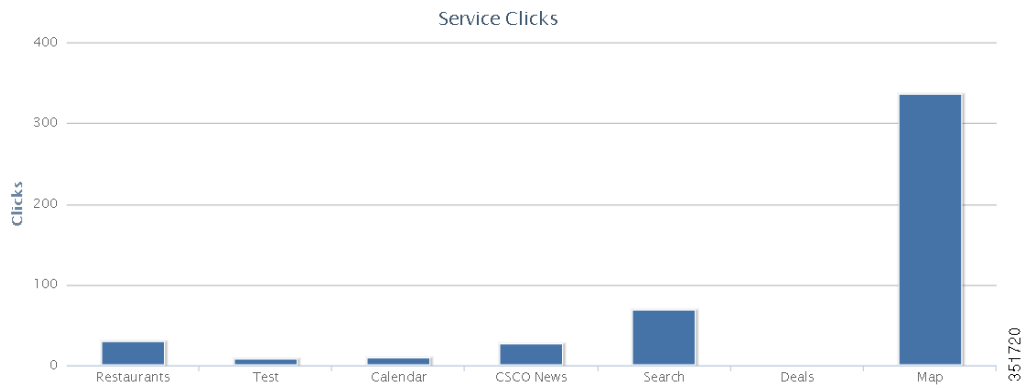


Figure 10-2 Number of service clicks

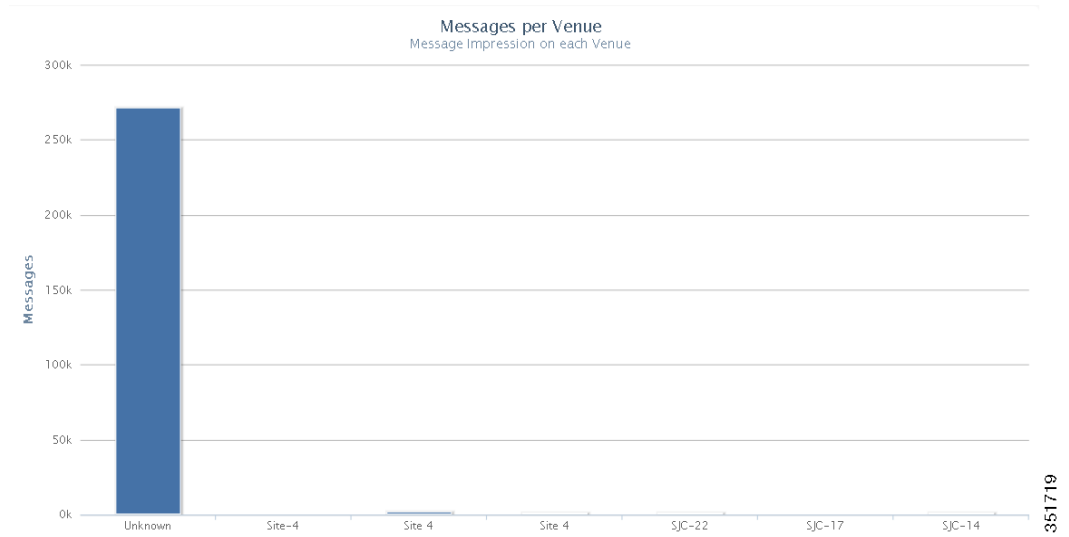


- To view the report for dates of your choice click Custom. Select those dates in the calendars in **From** and **To**. Click **Apply**.

Step 3 To view the number of messages for each venue, Click **Message**.

Following figure shows the number of messages for a venue.

Figure 10-3 Messages per venue



Step 4 To study the domain wise performance, click **Domain Metrics**.

Select the time frame from the **This Hour, Today, This Week, and This Month**.

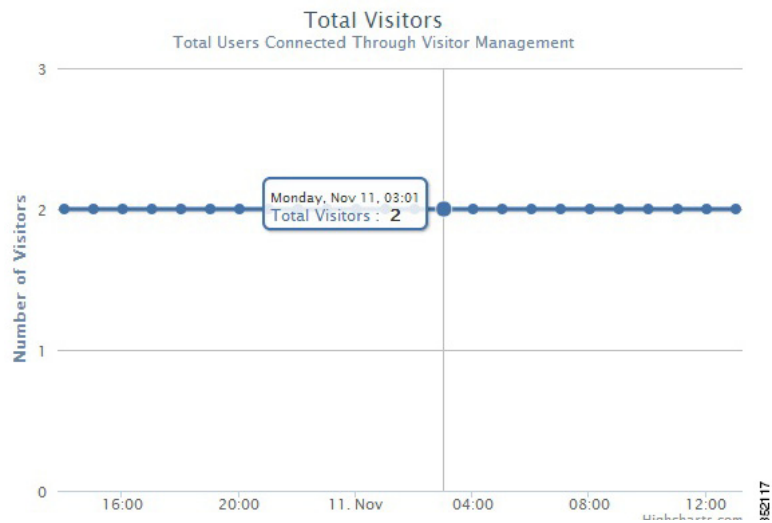
Step 5 To monitor the visitor details, click **Visitor Connect**.

- To view the hourly based trend for new visitors and total visitors connected through visitor connect, click **Hourly** and choose the start date and time and end date and time.

Figure 10-4 Hourly Trend for New Visitors



Figure 10-5 *Hourly Trend for Total Visitors*



- To view daily trend for new visitors and total visitors, click **Daily** and choose the start date and end date.

Figure 10-6 *Daily Trend for New Visitors*

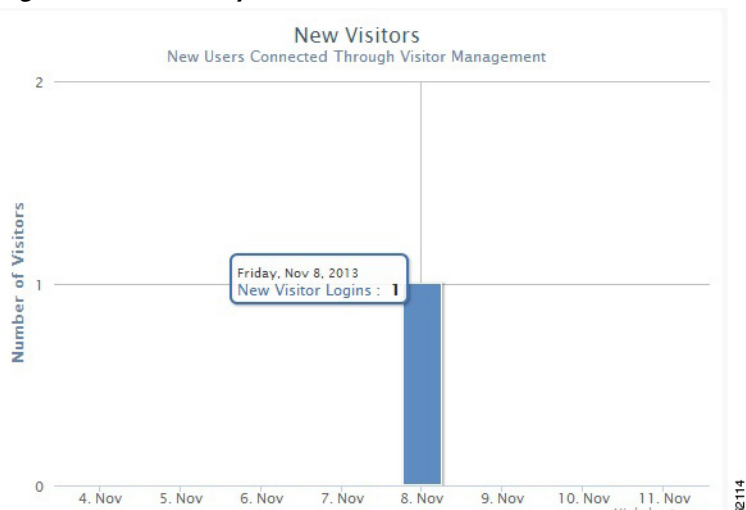


Figure 10-7 Daily Trend for Total Visitors



- To view weekly trend for new visitors and total visitors, click **Weekly** and choose the start date and end date.

Figure 10-8 Weekly Trend for New Visitors

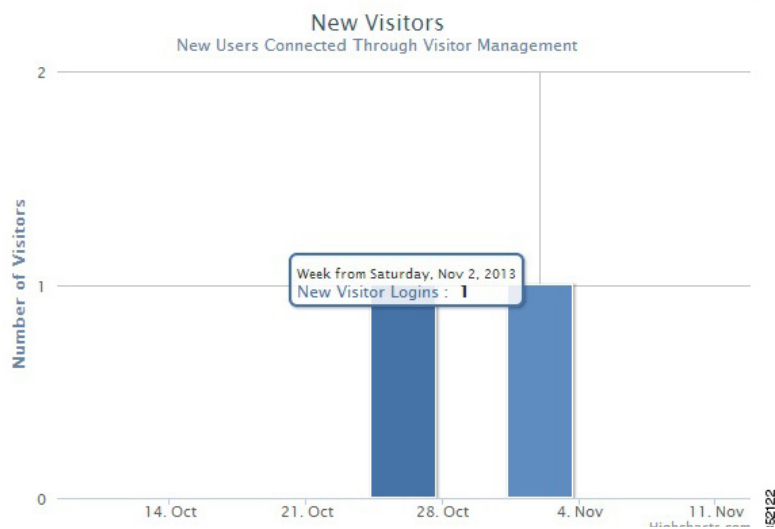


Figure 10-9 Weekly Trend for Total Visitors



- To view monthly trend for new visitors and total visitors, click **Monthly** and then choose the month.

Figure 10-10 Monthly Trend for New Visitors

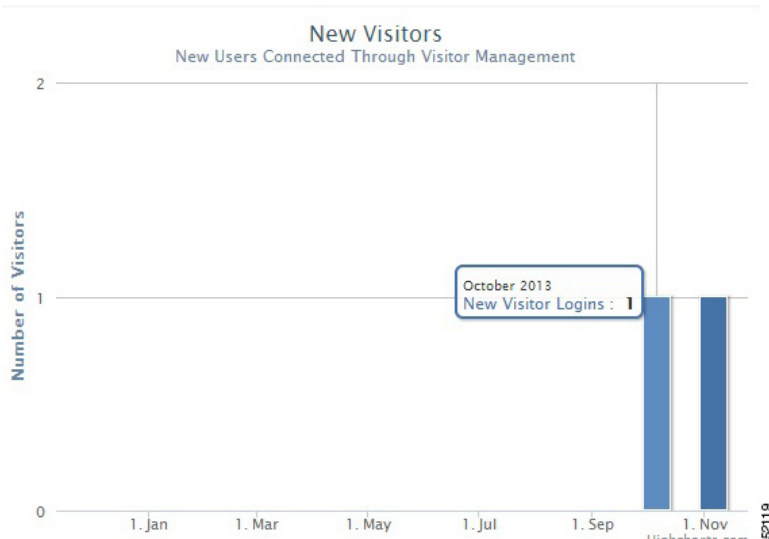
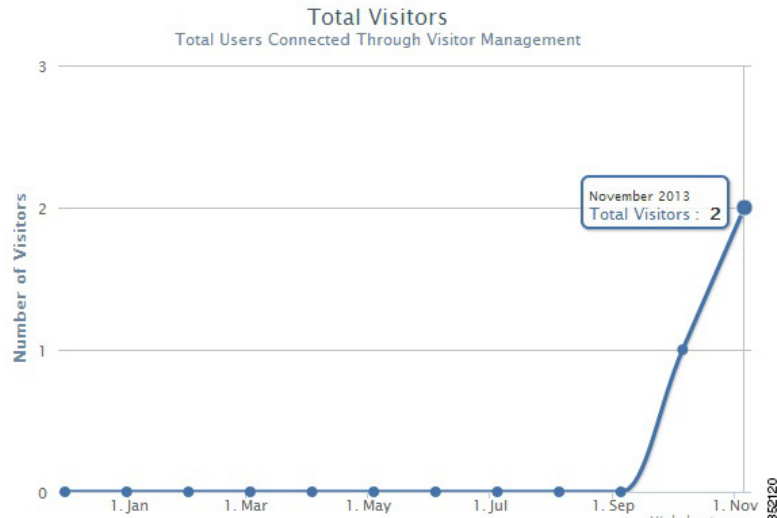


Figure 10-11 Monthly Trend for Total Visitors

- Step 6** Table at the bottom of the page lists the registration information about the active visitors based on the splash template configuration. This information in the table can be sorted and filtered.
- Step 7** Click **Export to CSV** to export the visitors details.

Summary

The CMX Dashboard has a dashboard that provides a schematic representation & summary of various factors important for analysis such as usage, point of interests, services, domains, device manufactures, and even the operating systems of the customer's mobile devices.

To access the dashboard summary, log in the CMX Dashboard user interface using the credentials.

From the left side bar menu, select Summary.

You can view the venues on the map in Venues. The venues are represented by big dots. You can view the active point of interest, current active campaigns, and total messages served.

To view the information charts for all the venues in the dashboard, click **Summary**. To view the information charts for a specific venue, click the green dot representing that venue on the map.

The usage of CMX Dashboard appears as a graph of impressions versus days. As you scroll down, you can view the top point of interests, top services, and top domains. To analyze the pattern of operating systems customer's mobile devices within a venue, you can view the top operating systems.

Following figures show the top POIs, services, top operating systems, and domains.

Figure 10-12 Top POIs

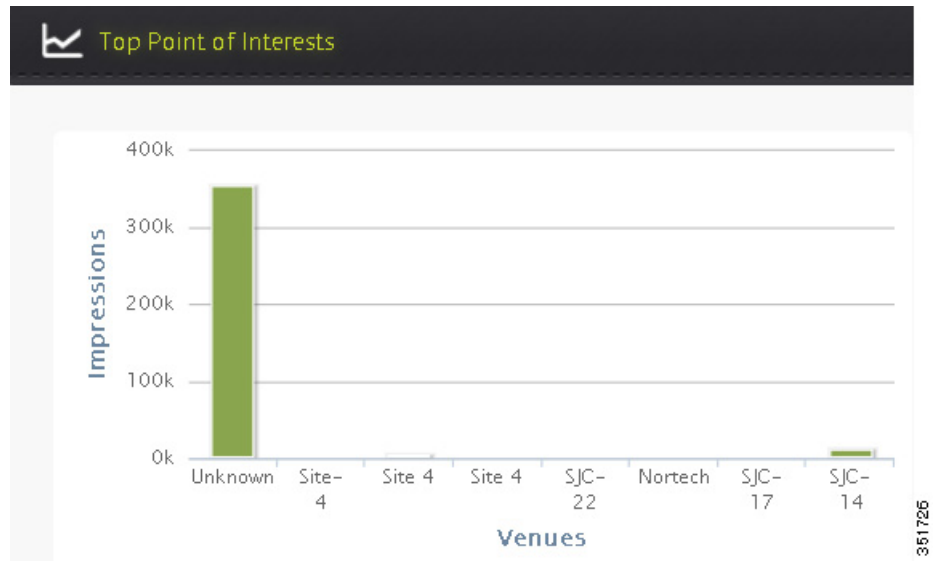


Figure 10-13 Top services

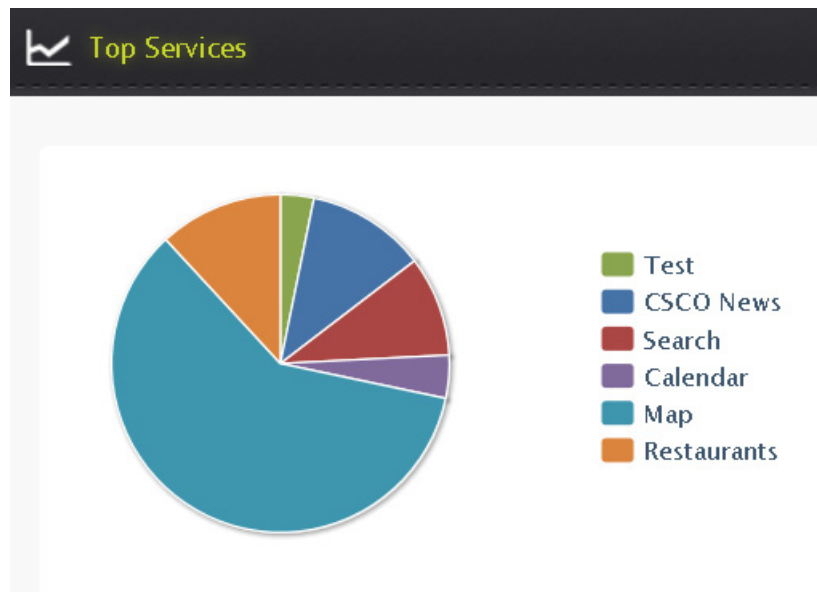


Figure 10-14 Top domains

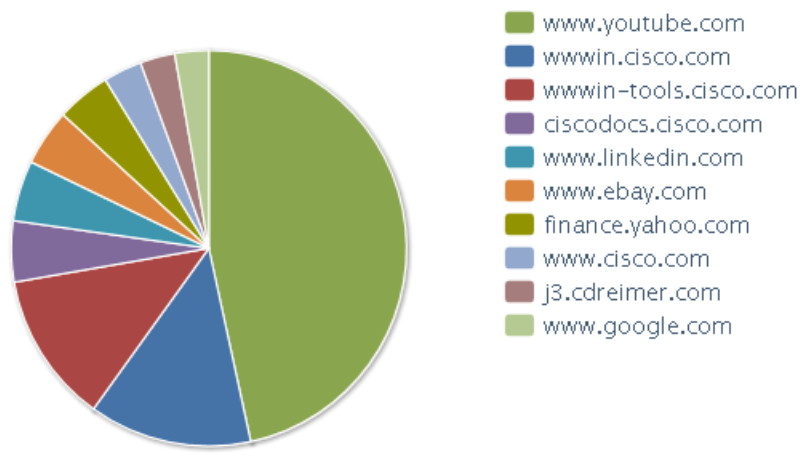
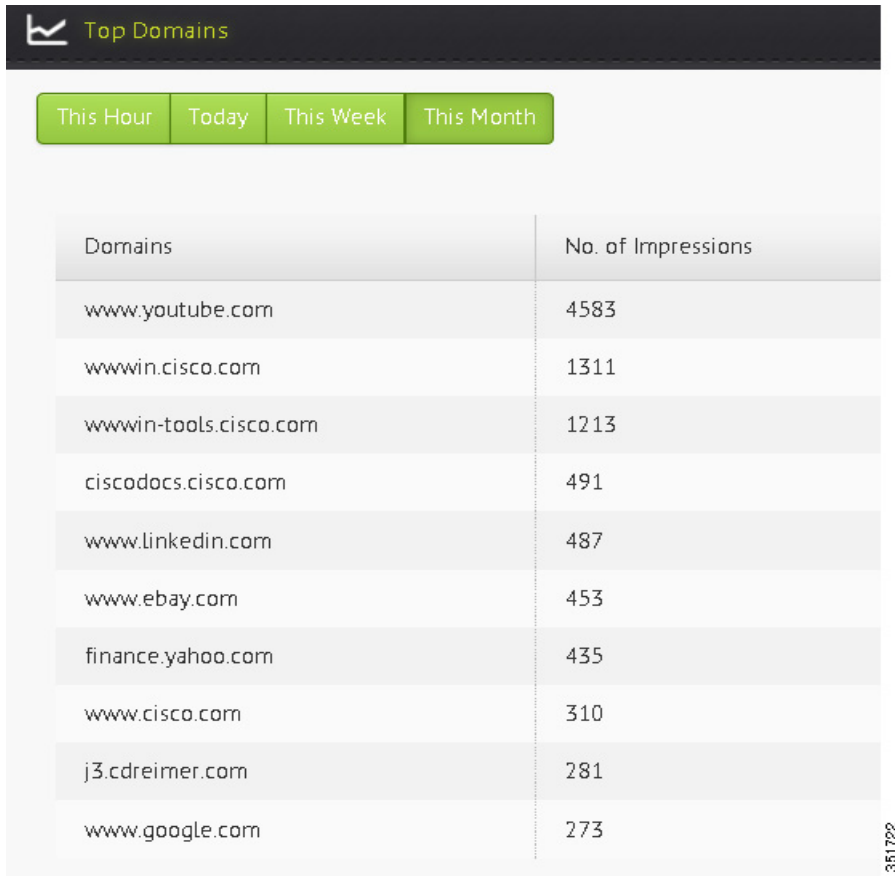
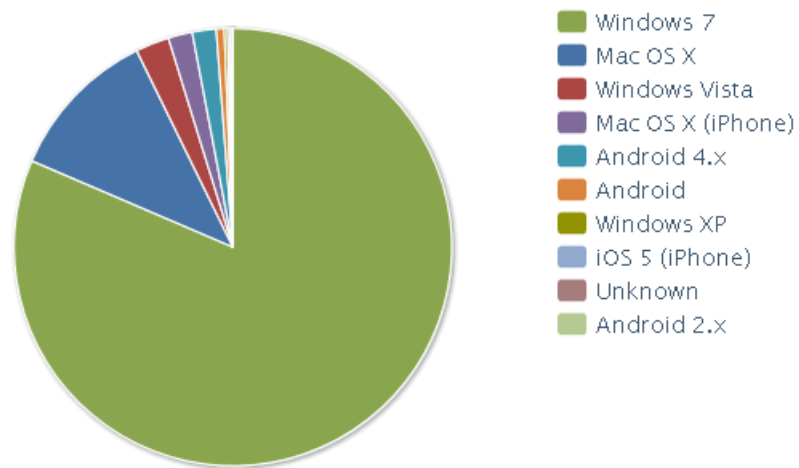
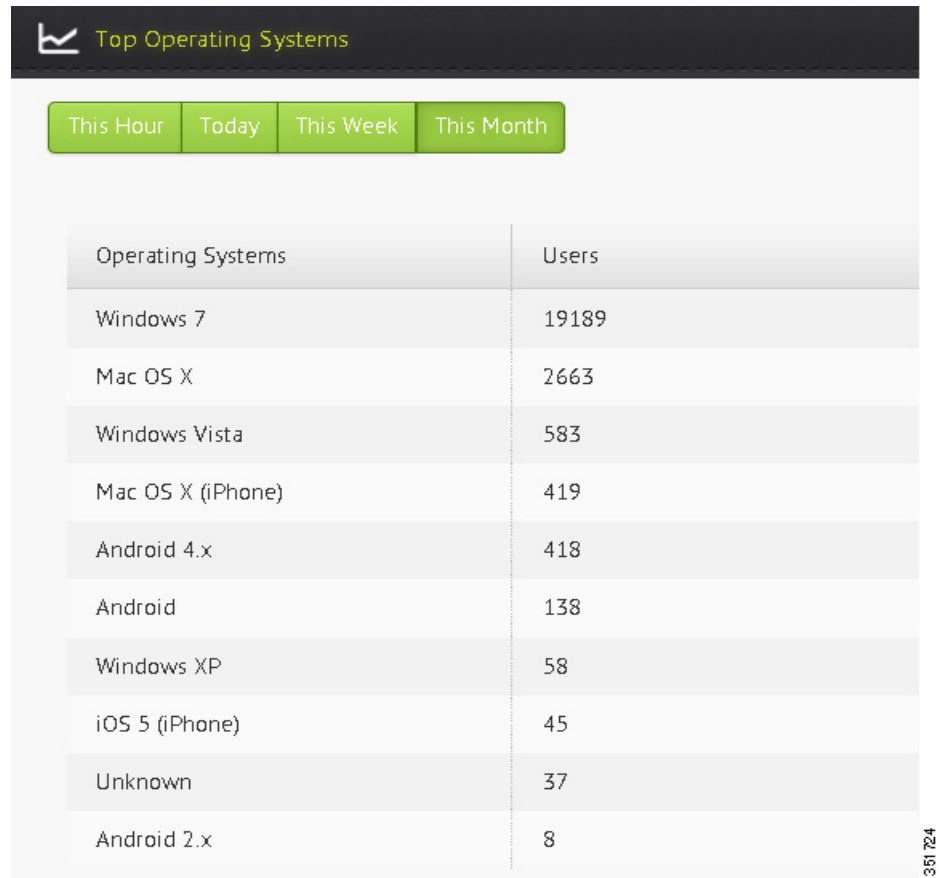


Figure 10-15 Top operating systems





CMX Dashboard Visitor Connect

Cisco CMX Visitor Connect is a guest access solution based on Mobility Services Engine (MSE), Cisco Wireless LAN Controller (WLC) and Lightweight Access points (AP). The CMX Visitor Connect is a location-enabled captive portal that enables you to create a custom onboarding experience for your visitors. This is designed to provide best experience for both mobile and laptop users.



Note

Please provide your feedback by clicking on “Make a wish” menu in CMX Dashboard, which is available on the top right corner of the page. To disable the feature, remove the “Visitor Connect” operation from the Super Administration role.

- [Visitor Connect as Captive Portal, page 11-1](#)
- [Template Fields, page 11-8](#)
- [Social Connectors, page 11-9](#)
- [Splash Templates, page 11-11](#)
- [Visitor Connect Report, page 11-12](#)

Visitor Connect as Captive Portal

CMX Visitor Connect is an intuitive simple guest captive portal that allows easy onboarding of the guests. The Visitor Connect is location aware and serve different splash templates to different locations or zones.

The venue owner has to enable the CMX Dashboard Service on the Prime Infrastructure UI for CMX Visitor Connect to function.

For the splash page, the Visitor Connect supports customization of:

- Page background
- Page header and footer with any HTML text
- Dynamic input fields
- Terms and Conditions
- Advertisement plug-in
- Social authentication plug-in like Facebook, LinkedIn, and Google+

The venue owner can:

- Customize location specific splash pages and advertisements for better visitor experience by creating multiple splash templates and assigning them to different Points of Interests (POI). For example, if the visitor is in the food court, the venue owner can advertise a food coupon, or the splash page could be in the local language based on the visitors location.

The visitor in the venue can gain access to the venue Wi-Fi by following these steps:

- Register to the venue owners Wi-Fi by providing required information like name, phone number, email, etc. This is a one time registration.



Note Visitor Connect differentiates a repeated user from the new user and skips the registration page for the repeated user.

- Accept terms and conditions.
- (Optional) Watch advertisements or announcements that is predetermined by the venue owner.
- (Optional) Log in to the social authentication page.

This section contains the following topic:

- [Prerequisites for CMX Visitor Connect, page 11-2.](#)

Workflow to Set up the CMX Visitor Connect

The following table describes the steps to be followed while setting up the CMX analytics system.

Table 11-1 *Process for Setting up the CMX Visitor Connect*

Process	Description
1. Configure FlexConnect ACLs	See the Configuring FlexConnect ACLs, page 11-3 for more information.
2. Configure WLAN for authentication	See the Configuring WLAN for Web Passthrough Authentication, page 11-4 for more information.
3. Social application authentication	See the Social Application Configuration, page 11-7 for more information.
4. Create splash template field	See the Creating a splash Template Field, page 11-9 for more information.
5. Create Splash page	See the Creating a Splash Template, page 11-11 for more information.
6. Assign Splash page to POI	See the Assigning a Splash Page Template to a Points of Interest or Floor, page 11-12 for more information.


Prerequisites for CMX Visitor Connect

- [Configuring FlexConnect ACLs, page 11-3](#)
- [Configuring WLAN for Web Passthrough Authentication, page 11-4](#)

- [Social Application Configuration, page 11-7](#)
- [Configuring CMX Visitor Connect, page 11-8](#)

Configuring FlexConnect ACLs

You must configure FlexConnect ACLs only for Flex mode deployments. To configure FlexConnect ACLs, follow these steps:

-
- Step 1** Choose **Security > Access Control Lists > FlexConnect Access Control Lists** 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.
- When the **Access Control Lists > Edit** page appears, click **Add New Rule**.
- The **Access Control Lists > Rules > New** page is displayed.
- Step 6** Configure a rule for this ACL as follows:
- 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.
-
-  **Note** 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.
-
- 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.
 - 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.
 - 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.

- e. 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
- f. 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**.
- g. Click **Apply**.
The **Access Control Lists > Edit** page is displayed on which the rules for this ACL are shown.
- h. Repeat this procedure to add additional rules, if any, for this ACL.

Step 7 Click **Save Configuration**.

Configuring WLAN for Web Passthrough Authentication

For providing network access to the customers, you need to configure WLAN on the Cisco Wireless LAN Controller (WLC). For this you need to set up the Web Passthrough on the layer three security of WLAN for CMX Visitor Connect.

To configure Web Passthrough configuration, follow these steps:

- Step 1** Define an ACL for pre-authentication from the Controller UI to allow the traffic to MSE IP address and to resolve DNS when in WEBAUTH_REQD state. All other traffic is blocked from clients connecting to SSID. For more information about configuring ACL, see the Cisco Wireless LAN Configuration Guide at:
http://www.cisco.com/en/US/products/ps12722/products_installation_and_configuration_guides_list.html.

Figure 11-1 Pre-Authentication ACL Configuration

Access Control Lists > Edit

General

Access List Name: pre-auth-acl

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.58.11.166 / 255.255.255.255	Any	Any	Any	Any	Any	0
2	Permit	10.58.11.166 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0

- Step 2** Choose **WLANs** to open the WLANs page from the Controller UI.
- Step 3** Click the ID number of the desired WLAN to open the WLANs > Edit page.
- Step 4** Choose **Security > Layer 2** tab.
- Step 5** From the Layer 2 Security drop-down list, choose **None**.
- Step 6** Click **Apply**.

Figure 11-2 Layer 2 Setting

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security

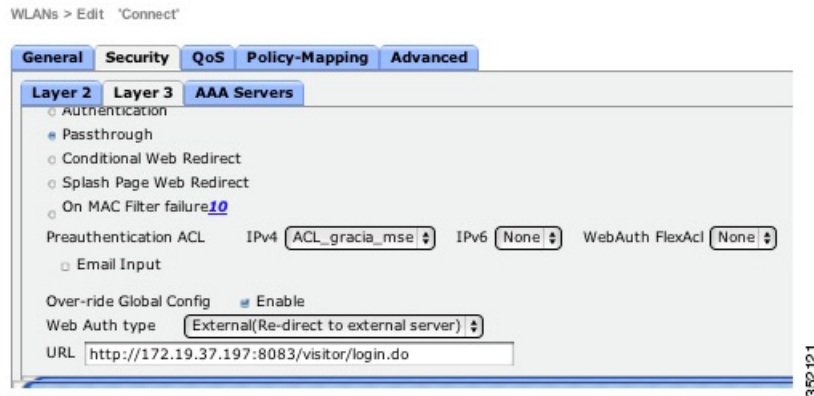
MAC Filtering

Fast Transition

Fast Transition

- Step 7** Choose the Security and Layer 3 tabs to open the WLANs > Edit (Security > Layer 3) page.

Figure 11-3 Web Passthrough Setting



- Step 8** Select the Web Policy check box.
- Step 9** Configure Preauthentication ACL to restrict the clients from accessing internet and rest of the network except MSE and DNS resolution. To redirect the user to a site external to the controller, choose the ACL that was configured from the Preauthentication ACL drop-down list.
- An Access Control List (ACL) is a set of rules used to limit access to a particular interface. You can create a preauthentication ACL for web authentication. Such an ACL could be used to allow certain types of traffic before authentication is complete. Both IPV4 and IPV6 are supported. IPV6 ACLs support the same options as IPV4 ACLs including source, destination, source and destination ports.
- Define an ACL for Pre-authentication to allow the traffic to MSE IP address and to resolve DNS when in WEBAUTH_REQD state. All other traffic will be blocked from clients connecting to SSID.
- The Pre-Authentication Flex Connect ACL is required for flex mode deployments. For more information, see the [Configuring FlexConnect ACLs, page 11-3](#).
- Step 10** To override global authentication configuration web authentication pages, select the **Over-ride Global Config** check box.
- Step 11** To define the web authentication pages for wireless guest users, choose **External** from the Web Auth Type drop-down list. This redirects clients to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box.



Note The external redirection URL should point to Visitor Connect captive portal URL.

- Step 12** Enter the URL of the splash page in the URL text box. For example, you can enter:
http://<MSE>:8083/visitor/login.do
- Step 13** Click **Apply** to commit your changes.
- Step 14** Click **Save Configuration** to save the changes.



Note Visitor Connect redirection requires special configuration on WLC for iOS devices and you can do it using this command: `Config network web-auth captive-bypass disable.`

Social Application Configuration

**Note**

The client authentication fails if the MSE has a private IP address and the MSE IP Address is used in the social application configuration. To fix the problem, assign a DNS name for MSE and use the MSE DNS Name instead of MSE IP address in the social application configuration. Make sure that MSE DNS name is used as the external portal URL in the guest SSID configuration.

The social authentication requires venue owners to create an application on social network provider such as Facebook, LinkedIn, and Google+. Once the social application is created, it provides an application ID and secret key that is required by the CMX Visitor Connect to successfully authenticate the visitors.

While creating social application, the venue owner has to provide the following information:

- Authorized Redirect URIs: *http://<mse>:8083/visitor/social.do*
- Javascript API Domains: *http://<mse>*

For more information on how to create social applications, refer to these resources:

- Facebook application ID and Secret key, see the following URL:
<http://www.youtube.com/watch?v=orx7bhEBUP4>

**Note**

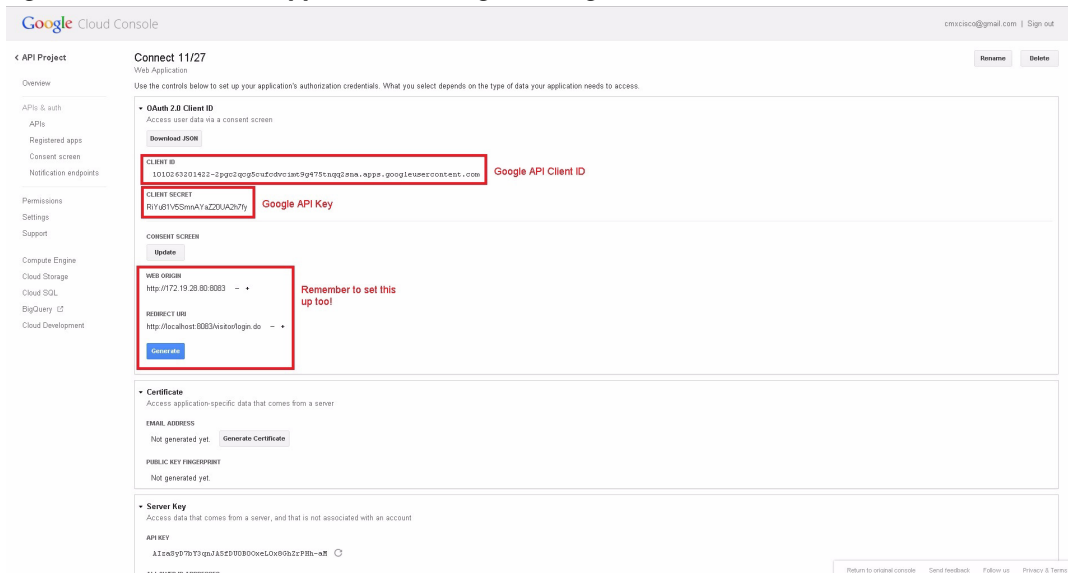
Disable the Sandbox Mode from the Facebook Developers page while creating Facebook application ID and secret key.

- LinkedIn API key and Secret, see the following URL:
http://www.youtube.com/watch?v=_J2ejcxg6NQ
- Google+ Client ID and Secret, see the following URL:
<http://www.youtube.com/watch?v=o425vQXpigw>

**Note**

You need to enable Google Cloud Storage JSON API in order to get the API key that is required in the CMX Visitor Connect Splash template set up. To activate this, click **Activate** that is next to Google Cloud Storage JSON API in the Services tab (see [Figure 11-4](#)).

Figure 11-4 Social Application Setting for Google+



Configuring CMX Visitor Connect



Note

Only the Super Administrator can access the CMX Visitor Connect.

To configure the Visitor Connect, follow these steps:

- Step 1** Choose **Settings > Roles** from the left sidebar menu.
- Step 2** Click **Super Admin**.
The Select Operations group box appears.
- Step 3** Ensure that Visitor Connect is available in the Existing Operations field. If it is not available, click **Visitor Connect** to highlight from the Available Operations field and choose **>> (Add)**.
- Step 4** Click **OK**.

Template Fields

Using Template Fields, you can create various user input fields and splash template fields like email ID, name, phone number, etc.

This section contains the following topics:

- [Creating a splash Template Field, page 11-9](#)
- [Editing the Splash Template Field, page 11-9](#)
- [Deleting the splash Template Fields, page 11-9](#)

Creating a splash Template Field

To create a splash template field, complete the following steps:

-
- Step 1** Choose **Visitor Connect > Splash Templates** from the left side bar menu.
 - Step 2** Click **Create New Splash Template Field**.
 - Step 3** Enter the name of the field you want to create in the Name text box.
 - Step 4** Select the field type: **Text** and **List**.
 - Step 5** Click **Submit** to apply your changes, or **Cancel** to discard the creation of field.
- The newly added field appears in the Splash Template Fields group box.
-

Editing the Splash Template Field

To edit the splash template fields, follow these steps:

-
- Step 1** Choose **Visitor Connect > Template Fields** from the left sidebar menu.
 - Step 2** Highlight the field that you want to edit in the splash Template Fields group box and click **Edit**.
 - Step 3** Make the necessary changes in the Add/Edit Splash Template Field group box and click **Submit**.
-

Deleting the splash Template Fields

To delete the splash template fields, follow these steps:

-
- Step 1** Choose **Visitor Connect > Template Fields** from the left sidebar menu.
 - Step 2** Highlight the field that you want to delete in the splash Template Fields group box and click **Delete**.
 - Step 3** Click **OK** to confirm the deletion in the Delete Confirmation group box, or cancel to close the page without making any changes.
-

Social Connectors

The Visitor Connect enables the venue owners to offer Wi-Fi access to their customers using the social network authentication. This requires venue owners to create an application on the social network sites such as Facebook, Google+, and LinkedIn. See the [Social Application Configuration](#) for more information.

**Note**

You can use Facebook, Google+, and LinkedIn sites to create social connectors. The visitors can use credentials for any one of these connectors.

- [Configuring the Social Connector, page 11-10](#)
- [Editing Social Connector, page 11-10](#)
- [Deleting Social Connector, page 11-10](#)

Configuring the Social Connector

You can use the social connector menu to create multiple social connectors. To configure the social connector, follow these steps:

-
- Step 1** Choose **Visitor Connect > Social Connector** from the left side bar menu.
 - Step 2** Click **Create New Social Connector**.
The Add/Edit Social Connectors group box appears.
 - Step 3** Enter the social connector name in the Connector Name text box. You can create a maximum of 10 social connectors.
 - Step 4** Choose an account from the Account drop-down list.
 - Step 5** Enter the Facebook APP ID that you received after creating Facebook application in the Facebook APP ID text box.
 - Step 6** Enter the LinkedIn API ID that you received in the LinkedIn API Key text box.
 - Step 7** Enter the Google Client ID in the Google API Client ID text box.
 - Step 8** Enter the Google API Key in the Google API Key text box.
 - Step 9** Click **Submit**.
-

Editing Social Connector

To edit a social connector, follow these steps:

-
- Step 1** Choose **Visitor Connect > Social Connector** from the left side bar menu.
 - Step 2** Click to highlight a social connector entry in the Social Connectors group box and click **Edit**.
 - Step 3** Make the necessary changes in the Add/Edit Social Connectors group box and click **Submit**.
-

Deleting Social Connector

To delete a social connector, follow these steps:

-
- Step 1** Choose **Visitor Connect > Social Connector** from the left side bar menu.
 - Step 2** Click to highlight a social connector entry in the Social Connectors group box and click **Delete**.

- Step 3** Click **OK** to confirm the deletion, or cancel to close the page without making any changes.
-

Splash Templates

You can create location aware splash templates to serve different locations or zones. You can create multiple splash templates and assign them to different Points of Interest.

- [Creating a Splash Template, page 11-11](#)
- [Assigning a Splash Page Template to a Points of Interest or Floor, page 11-12](#)

Creating a Splash Template

To create a splash template, follow these steps:

-
- Step 1** Choose **Visitor Connect > Template Fields** from the left side bar menu.
- Step 2** Click **Create New Splash Template**.
The Add/Edit Splash Template wizard appears.
- Step 3** In the Template Name text, enter a name for the splash page.
- Step 4** From the Template Background drop-down list, choose a predefined background for your splash page. To set the background of your choice, choose Custom from the Template Background drop-list and click **Click to upload an image** to upload an image for the splash page background.
- Step 5** From the Form Fields list, choose the field(s) that you want to include in the splash page. These are fields that you created using Splash Template Fields menu.
- Step 6** Provide details for the splash fields that you choose in the Form Fields list. For template fields of type List, provide the list of choices you want to provide.
- Step 7** In the Terms and Conditions text box, enter the terms and conditions that you want to display in the splash page.
- Step 8** In Header text box, enter any welcome information for the customer. For example you can enter 'Welcome to XYZ mall'.
- Step 9** In Footer text box, you can enter any disclaimer. For example you can enter 'This is a complementary Wi-Fi network, we do not save your data'.
- Step 10** Click **Next** to configure advertisements that you want to display in the splash page.
- Step 11** In the Ad Script text box, provide html script that points to the advertisement server or static HTML pages, or HTML page with animated graphics.
This is a sample advertisement configuration that points to a YouTube URL: `<iframe width="853" height="480" src="//www.youtube.com/embed/uIDx3eUZ-vw" frameborder="0" allowfullscreen></iframe>`.



Note Advertisement is an optional step. If you do not specify any URL for the advertisement, the advertisement page will be skipped during the guest on boarding.

- Step 12** Click **Next** to configure social authentication for visitors log in.

**Note**

Social authentication is optional. If you do not select any social connector, the Social Authentication page is skipped during the guest onboarding.

- Step 13** In the Header text box, enter the information that you want to display in the Social authentication page. For example, you can enter 'Congratulations! You are on the Wi-Fi network of XYZ'.
- Step 14** From the Social Connector drop-down list, choose the social connector. This is the list of the connectors that you created in the **Visitor Connect > Social Connectors**.
- Step 15** Select the corresponding authentication type from Social Auth check box.
- Step 16** Enter the information in the footer text box.
- Step 17** Click **Submit**.

Assigning a Splash Page Template to a Points of Interest or Floor

You can assign a specific Splash Page Template to a Points of Interest or a floor. This enables the venue owners to give location aware network access to the customer.

To assign a splash page template to a floor, follow these steps:

- Step 1** Choose Points of Interest from the left sidebar menu.
- Step 2** In the right pane, choose PointOfInterests > System Campus > desired *Building* > desired *Floor*.

**Note**

If you assign a splash template to a building, all the floors defined under that building inherits the splash template. If you have a splash template defined at both building and floor, the floor splash template is used.

- Step 3** Click **Edit Floor**.
- Step 4** From the Splash Template drop-down list, choose the splash page template.
- Step 5** Click **Submit**.

Visitor Connect Report

Monitor the Visitor Details

To monitor the visitor details, follow these steps:

- Step 1** From the left side bar menu, select Reports.
The Services, Message, Domain Metrics, and Visitor Connect tabs appear.
- Step 2** To monitor the visitor details, click **Visitor Connect**.

- To view the hourly based trend for new visitors and total visitors connected through Visitor Connect, click **Hourly** and choose the start date and time and end date and time.

Figure 11-5 Hourly Trend for New Visitors

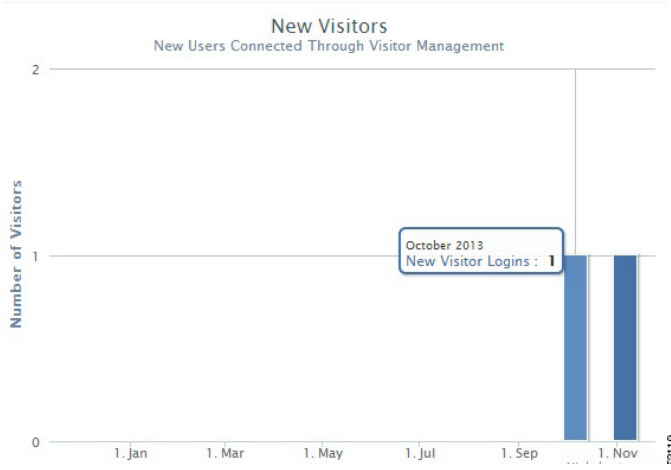
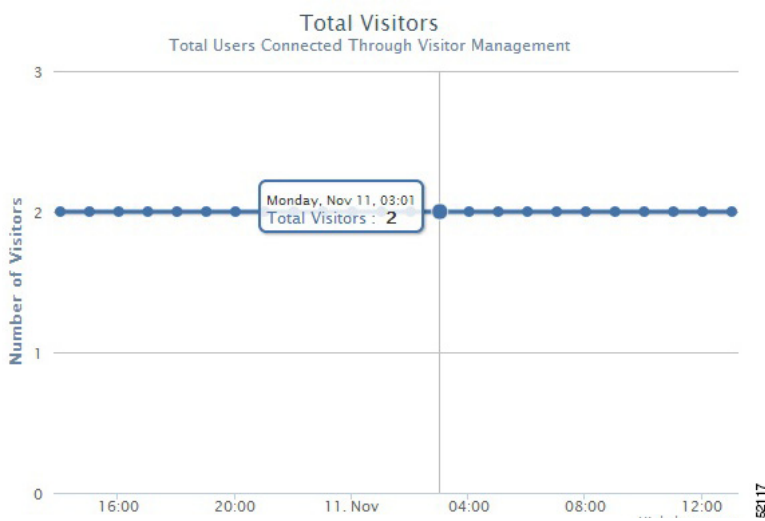


Figure 11-6 Hourly Trend for Total Visitors



- To view daily trend for new visitors and total visitors, click **Daily** and choose the start date and end date.

Figure 11-7 Daily Trend for New Visitors

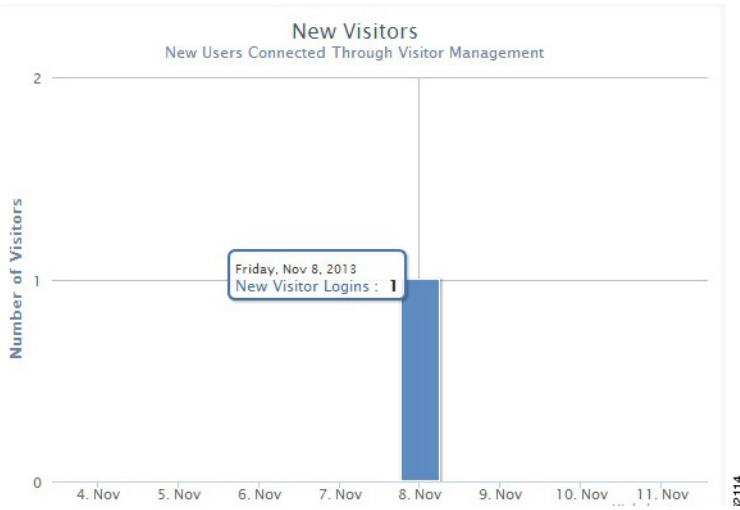
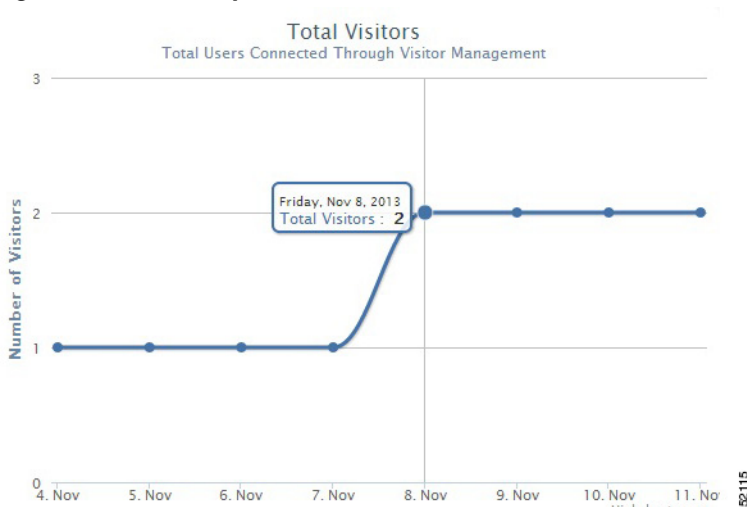


Figure 11-8 Daily Trend for Total Visitors



- To view weekly trend for new visitors and total visitors, click **Weekly** and choose the start date and end date.

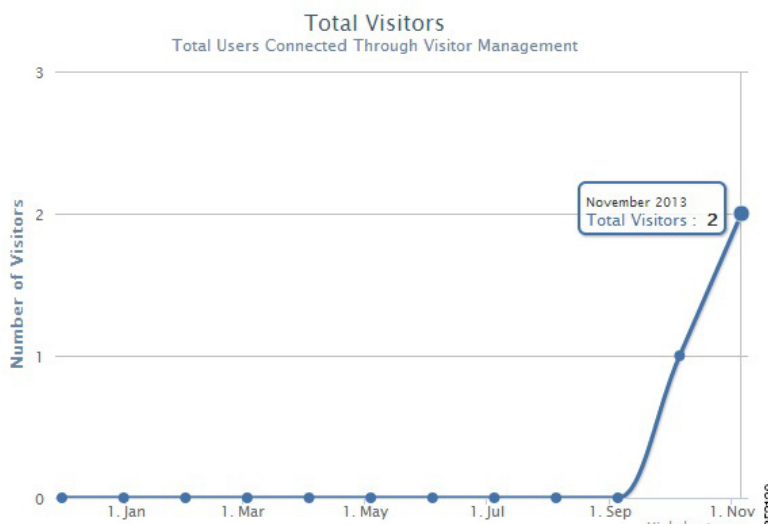
Figure 11-9 Weekly Trend for New Visitors



Figure 11-10 Weekly Trend for Total Visitors



- To view monthly trend for new visitors and total visitors, click **Monthly** and then choose the month.

Figure 11-11 Monthly Trend for New Visitors**Figure 11-12 Monthly Trend for Total Visitors**

Step 3 Table at the bottom of the page lists the registration information about the active visitors based on the splash template configuration. This information in the table can be sorted and filtered.

Step 4 Click **Export to CSV** to export the visitors details.



HTTP Proxy

Currently, CMX Dashboard relies on HTTP traffic flows to provide value added services and messages to the customer at the venue.

One of the main components of the CMX Dashboard is script insertion component.

The router intercepts the HTTP traffic and the CMX Dashboard inserts a script at the end of the HTTP traffic.

The HTTP Proxy is enabled on the Mobility Services Engine.

HTTP Proxy on the MSE terminates all HTTP traffic intercepted using Policy Based Routing (PBR) and acts as a forward proxy by pulling contents on behalf of wireless clients.

HTTP Flow

The following is the flow of HTTP traffic generated from a wireless client and the interactions of the various components.

1. Client browser makes HTTP request to the web server. The router intercepts and forwards to the proxy service.
2. Proxy terminates the previous connection and opens another to the web server.
3. Proxy inserts a script tag with CMX Dashboard server IP and the client IP.
4. Proxy responds with altered HTML payload.
5. Client browser intercepts the script tag and sends a request to CMX Dashboard server.
6. CMX Dashboard server asks the client location from the Context Aware Service (CAS) server.
7. CAS Server responds with the client location.
8. CMX Dashboard serves the advertisement to client browser using location and campaign information.

HTTP Proxy Service

The following are the important functional components of the HTTP Proxy:

- HTTP Proxy Service:

- It is the proxy service that
- Receives the redirected end-user HTTP requests,
- Terminates the TCP stack, and
- Inserts the Banners in the returning HTTP traffic
- Redirection Router:

The router is in the data path of the end-user's traffic to the Internet. It intercepts and redirects the end-user's HTTP traffic to the MSE HTTP Proxy service.

This redirection takes place by either of the following:

- Policy Based Routing (PBR) — It operates at the L2 level addresses.
- L4-Redirect functionality available on higher end routers — It operates at the L3 and L4 level addresses. (For example: ASR1000 with ISG functionality).

**Note**

The Wi-Fi device of the customer must be on different subnet than that of the HTTP Proxy.

Deployment Types

Following are the two types of the MSE deployment:

- MSE Centralized Deployment

In this deployment there is a single MSE package. In this software package the HTTP proxy service is a part of the MSE image.

- MSE Flex Deployment

In this deployment there are two packages - a MSE package and a Cloud connector package. The HTTP proxy is part of the Cloud connector package. This software is deployed on ISR routers with UCS E-series blades.

Configuration on the MSE

The Mobility Services Engine is a platform for hosting multiple mobility applications.

The simplest deployment model of a CMX Dashboard solution can be a PBR router and a single MSE running both CMX Dashboard sub-services and CAS.

The MSE framework supports starting and stopping the CMX Dashboard services. By default, both the platform and proxy sub-services are started by the framework. For deployment models where the proxy is not running on the MSE, you can disable the proxy sub-service.

You can enable the HTTP proxy service on the MSE with PBR interception on L2 adjacent router then MSE receives the HTTP data traffic. The user may want to separate the management and data traffic.

**Note**

To setup the Proxy use the Proxy Configuration tab in PI. You can choose a CMX Dashboard MSE IP to communicate the Proxy MSE so the Proxy can insert the script from that CMX Dashboard MSE.

Enabling DNS and Default Domain Name via MSE Console

The HTTP proxy requires the DNS and domain name to be configured in the proxy configuration file. The proxy startup script uses the values from the MSE Linux host. These values can be configured by the MSE setup script.

The command is:

```
/opt/mse/setup/setup.sh
```

**Note**

If not set, the MSE Proxy service takes the default values to the DNS of 8.8.8.8 and default domain name as cisco.com



CMX Cloud Connector

The Cisco Integrated Services Router (ISR G2) is a branch router that transforms service delivery for cloud, multimedia applications, and mobile devices. ISR G2 routers are multiple services or integrated services routers.

You can insert a service module in this router, one such module is UCSE (Unified Computing System E-series) server. The UCSE server is a blade server. It has x86 processor and you can have virtualization environment such as VMware ESXI 5.1. You can install applications and operating systems on it.

You can run virtual machine on the ESXI. The virtual machine is a cloud connector in case of the CMX Dashboard. This connector is called the CMX Dashboard Cloud Connector.

The centralized set-up for the CMX Dashboard has the MSE. In the decentralized set-up for the CMX Dashboard, the MSE and ISR G2 router exchange the data. The ISR G2 router along with the CMX Dashboard Connector interacts with the MSE in the cloud.

The CMX Dashboard Connector intercepts the WAN traffic and inserts a Java response script into the HTTP response and they are converted in the ads and services for the end user.

Prerequisites for the CMX Dashboard Connector

Following are the prerequisites for the CMX Dashboard Connector to operate:

- You have ISR G2 router with IOS version - 15.3-M0.2 and any upcoming rebuilds of this release version. For example - 15.3(3)M1 & 15.3(3)M2.



Note The IOS version with OnePK support is needed.

- You have the UCSE module pre-installed with VMware ESXI 5.1.
- You have installed the UCSE module inside the ISR router.
- You have configured the UCSE parameters such as IP address and networking through Cisco Integrated Management Controller (CIMC) GUI.
- You can access the ESXI on the UCSE module through VMware VSphere client.

**Note**

ISR G2 Routers that support the CMX Dashboard are series 2911, 2921, 2951, 3925, 3945.

The following is the Hardware Comparison Matrix for the UCS E-Series:

Parameter	UCS-E140S	UCS-E140D(P) / UCS-E160D(P)
Processor	Intel Xeon (Sandy Bridge) E3-1105C (1 GHz)	Intel Xeon (Sandy Bridge) E5-2428L (2 GHz) / E5-2418L (1.8 GHz)
Core	4	4 / 6
Memory	8 - 16 GB DDR3 1333MHz	8 - 48 GB DDR3 1333MHz
Storage	200 GB- 2 TB (2 HDD) SATA, SAS, SED, SSD	200 GB- 3 TB (3 HDD*)SATA, SAS, SED, SSD
RAID	RAID 0 & RAID 1	RAID 0, RAID 1 & RAID 5*
Network Port	Internal: 2 GE Ports External: 1 GE Port	Internal: 2 GE Ports External: 2 GE Ports PCIE Card: 4 GE or 1 10 GE FCOE

CMX Dashboard Connector

The CMX Dashboard Connector software is provided as a single .ova file. The open virtualization format works on top of the ESXI 5.1.

The .ova file provides a Linux-based runtime environment to host the cloud connectors. The environment uses the Kernel version - 2.6.32.46.cge (Montavista). The environment hosts only the CMX Dashboard Connector. It comes bundled with this connector hosting infrastructure.

The Linux-based connector hosting infrastructure has the following administrative interfaces:

- VGA (Video Graphics Array) console that uses VSphere
- SSH that uses SSH client
- WEB UI that uses Web browser

Initial Setup

The CMX Dashboard .ova file is deployed on top of the ESXI using VMware VSphere Client. You can either point to the hypervisor directly or through vCenter. You can then access the VGA console of the virtual machine.

Complete the following steps:

Step 1 For setting up OnePK on the router use the following commands:

```
Re:
onep
datapath transport gre sender-id 1 interface Vlan1
transport type tcp
!
```

Step 2 Log in the VMware VSphere Client using your credentials. The CMX Dashboard .ova file is deployed and you get access to the VGA console.

Step 3 To install the Linux-based connector hosting environment, enter install in boot.

Step 4 After a few seconds, initial configuration of the system takes place. You can organize the parameters such as admin users, networking setup, and time zones.

Step 5 Set the password for the shell user and management interface user.



Note You can re-run the setup utility to change configured parameters by issuing 'setup' at the shell. After initial networking setup, you can access the shell through SSH client.

Step 6 Go to Configuration tab. Select Networking in the Hardware group box. vSwitch Properties box appears. Select vSwitch.

Step 7 Set the MTU at 1700 in the vSwitch properties box.

Web based Management UI

Installation of the .ova file on top of ESXI hypervisor initiates the C3 hosting component. The initial setup has configuration of the hosting environment, Linux networking and Web browser access. After the setup, Management Web UI is accessible from a browser.



Note Use https (port 443) with the IP address specified during initial setup. Ignore Certificate errors, no publicly recognized certificate is provided.



Note The supported Google Chrome versions for the Management UI are chrome version 21 to version 28. Other browsers supported are Internet Explorer and Mozilla Firefox.

Through this UI you can manage and configure the following:

- Hosting infrastructure
- CMX Dashboard connector
- HTTP proxy service

CMX Dashboard Connector Configuration

The web UI has the following three tabs:

- Connectors
- HTTP Proxy
- System Info

The About tab displays the Cisco Cloud Connector Management box. The current release information and the host name are displayed.

Connectors

The following figures show the Connector Configuration.

Figure B-1 Connector Configuration-1

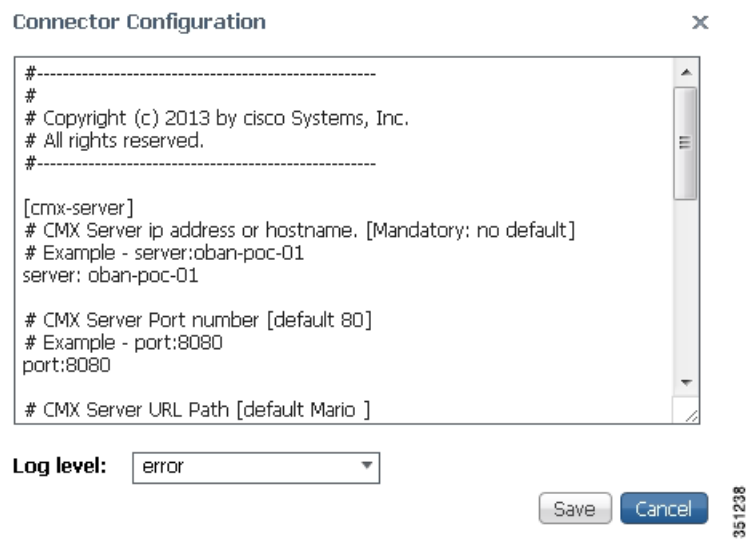


Figure B-2 Connector Configuration-2

Connector Configuration

```
# CMX Server URL Path [default Mario ]
# Shouldn't start with "/" and end with "/" but can contain it in
between
# Examples - "Mario", "service/v1/Mario"
path:"service/v1/Mario"

[cmx]
# Domain white list (regex) to apply CMX feature. [default NULL]
# If left blank, all domains will be processed.
# Example - domains: .*\.ebay\.com, .*\.edu, .*\.cisco\.*
domains:


# Domain black list (regex) to skip CMX feature [default NULL]
# Excluded domains are skipped even if "domains" filter matches.
# Example - excludedDomains: .*\.google\.com, my\.*\.com
excludedDomains:
```

Log level: error

Save Cancel

351238

Complete the following steps to configure the CMX Dashboard Connector:

-
- Step 1** Log in to the Management UI through a web browser. Click the Connectors tab. The CMX Dashboard Connector is in deployed state by default.
- Step 2** Before stating the connector, configure HTTP proxy. See Appendix A- HTTP Proxy.
- Step 3** To start the CMX Dashboard Connector, click **Start**.
- Step 4** To configure the CMX Dashboard server, click **Configuration**.
- Step 5** Enter the server details in CMX server ip address or host name. For example the server can be server:oban-poc-01.
- Step 6** Enter the port details in CMX server port number.
- The path of the URL in CMX server URL path, by default is 'Mario'.
-
-  **Note** Do not enter the URL path with '/' in the beginning or at the end.
-
- Step 7** In Domain white list, enter the names of the domains where you want the CMX Dashboard feature to appear. If you do not specify the names of the domains, all the domains are processed. For example, the included domain names can be `*\ebay\.com, *\cisco\.com`.
- Step 8** In Domain black list, enter the names of the domains where you do not want the CMX Dashboard feature to appear. Excluded domains are avoided even if the 'domains' filter matches. For example, excluded domain names can be `*\google\.com, *\my\.com`
- Step 9** In Content Type Filter, enter text or html.
- Step 10** In URL white list, enter the URLs where you want to the CMX Dashboard feature to appear.
- Step 11** From the Log level drop-down list, choose level of the log for the CMX Dashboard connector.

**Note**

You can view and download the logs from the Connectors tab. Click Show Log and then click **Download** in the Connectors logs box.

To check up the C3 hosting component following are the debug commands:

```
isr-3945-zs# show onep datapath
VM Tport State Prt/Eth Misordered packets
1 GRE up
  Local-addr: 192.0.2.1 0x8921 1
  Remote-addr: 198.51.100.1 0x8921 0
isr-3945-zs#
```

HTTP Proxy

To configure the HTTP Proxy and OnePK, click **HTTP Proxy**.

In the Router OnePK Settings group box complete the following steps:

-
- Step 1** Enter the IPv4 address of the VM host.
 - Step 2** Enter the user name and the password of the router.
Proxy filter port is as per the port details you entered in the Connectors tab.
 - Step 3** In Intercept Interface(s), enter the interface details to intercept the traffic.

**Note**

The interface is the gigabit ethernet interface. The traffic is going outward, so this interface is outgoing interface.

-
- Step 4** To intercept the traffic on the WAN side choose **WAN** from the Connected to drop-down list. To intercept the traffic on the LAN side choose **LAN** from the Connected to drop-down list.
 - Step 5** From the Log level drop-down list, choose level of the log. Click **Apply**.

**Note**

If you want to reorganize the configuration parameters, click **Reset**.

Figure B-3 HTTP Proxy

The screenshot displays two main configuration panels. The left panel, titled 'Router OnePK Settings', contains several input fields: 'IPv4 address' (209.165.200.225), 'User name' (alex), 'Password' (masked with dots), 'Proxy Filter Port' (80), 'Intercept Interface' (GigabitEthernet0/0/0.15), 'Connected to' (WAN), and 'Log Level' (error). Below these fields are 'Apply' and 'Reset' buttons. The right panel, titled 'HTTP Proxy Status', shows the 'OnePK connection status' as 'Disconnected' with a red status icon. The 'Proxy daemon running status' is 'Running'. Below these are statistics: 'Forced restart count' (0), 'Transformation match' (0), 'Transformation completed' (0), and 'Transformation skipped' (0). A 'Refresh' button is located at the bottom right of this panel. A vertical ID '351707' is visible on the far right edge of the interface.

In the HTTP Proxy Status group box, the status of the OnePK connection changes to connected. The status of the Proxy daemon changes to running.



Note To reload the settings, click **Refresh**.

You can view the forced restart count.

You can also view the counts of the transformation match, completed transformation, along with skipped transformation. After the HTTP traffic starts, these counts increase.



Note The HTTP Proxy information doesn't reload automatically; click **Refresh** to view the up-to-date information.

System Information

To monitor the performance of the entire system and to view the details of system parameters, click the System Info tab.

The VM Host Info pane shows the following details:

- Host name
- Uptime
- System time
- Software version

The host information doesn't reload automatically; click **Refresh Stats** to view the up-to-date information.

The VM CPU & Processes pane shows the following details:

- The Intel processor details
- CPU Utilization
- Processes

Step 1 To view the currently running processes, click **Inspect**.

The VM Memory pane shows details of the used and available memory size. The VM Storage pane shows the details of the space used. You can view the destination IP addresses and mask in the VM Ip v4 routing pane.

The VM DNS and NTP settings show the domain, name server, and the NTP server.

Step 2 The VM Logs pane shows the current log level for the system. To change the log level, choose the type of the log from the Current log level drop-down list and click **Change**.

Step 3 The log names, log size and view options are shown as a table. Click **download**, against the log that you want to download and save.

Step 4 In case of performance issues of the system, you can contact Cisco Systems Technical Support with the information of the issue. Click **Generate snapshot file** to generate the issue snapshot. Click **download** to save the file.



Note To delete the snapshot file of an old issue, click **X**. To reload the list of the snapshot files, click **Refresh List**.

Step 5 If the system crashes, a core file is generated. The core name pane shows the list of the core files. Click download to save the core file.



Note To delete the core file of an old crash, click **X**. To reload the list of the core files, click **Refresh List**.

The VM Interfaces pane shows the following:

- List of network interfaces
- Data packets received
- Data packets transferred

Step 6 To log out of the management UI, click **Log Out**.



A

- Account Management [3-1](#)
- Adding a Point of Interest [4-1](#)
- Advertisement [6-4](#)
- Analytics and Reports [10-1](#)

B

- Banner [6-1](#)
- Banner to a campaign [7-2](#)
- Browser Simulator [9-1](#)
- Browsers Support [9-8](#)

C

- Campaign Management [7-1](#)
- Captive portal [11-1](#)
- CMX Dashboard [1-3](#)
- Creating an Account [3-1](#)
- Creating campaign [7-1](#)

D

- Domains [3-3](#)

H

- Hyper-local Search [8-1](#)

M

- Make a Wish [9-8](#)

- Map service [8-2](#)
- Message Management [6-1](#)
- Mobility Services Engine [2-1](#)

N

- Navigation Management [5-1](#)

O

- Offer message [6-3](#)

P

- Point of Interest [4-1](#)

R

- Roles [3-3](#)

V

- Visitor Connect [11-1](#)

W

- web banner [7-1](#)
- Welcome message [6-1](#)

