CMX Dashboard Visitor Management

Cisco CMX Dashboard Visitor Management is a guest access solution based on Mobility Services Engine (MSE), Cisco Wireless LAN Controller (WLC) and Lightweight Access points (AP). Visitor Management is an intuitive captive portal for the Wi-Fi needs of the customers. A captive portal is designed to provide best experience for both mobile and laptop users.

Note CMX Visitor Management is a Demo feature that will not be supported by Cisco TAC. It is recommended for use in the lab environment and not in production networks. This is turned on by default and requires additional configuration to make it operational.

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 Management" operation from the Super Admin role.

Prerequisite for the Visitor Management

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

Complete the following steps:

Step 1 Open the Cisco WLC browser, click **WLAN** in the menu at the top, and click **New** on the upper right side.

Step 2 Choose WLAN as the Type. Select a profile name and WLAN SSID for web passthrough. You can use web pass for both the Profile Name and WLAN SSID. Please do not configure any security settings for the layer 2.

Step 3 Click **Apply** in the upper right corner.

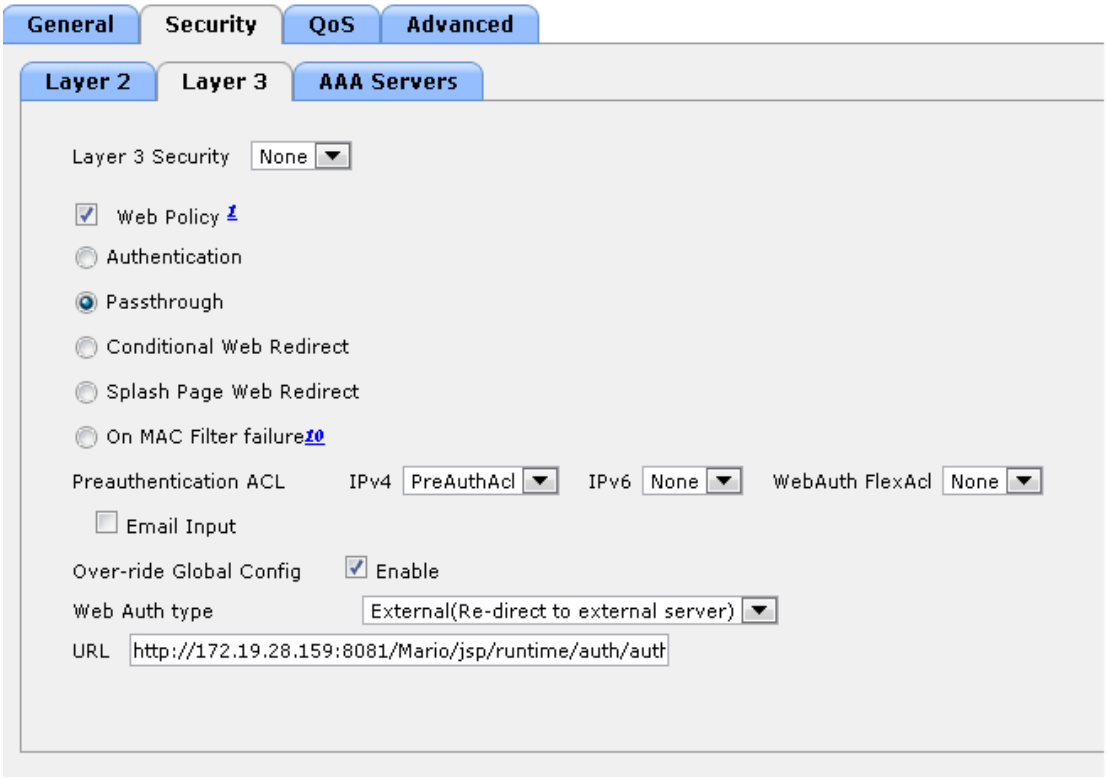
Step 4 A new **WLANs > Edit** window appears.

Step 5 Check the status box of the WLAN to enable the WLAN. From the Interface menu, select the name of the VLAN interface that you created previously.

Note Leave the default value for the other parameters on this screen.

Step 6 Select the Security tab. Go to the Layer 3 tab. Following figure shows the configuration.

Figure 12-1 Web passthrough setting



Step 7 Check the **Web Policy** check box. Click **Passthrough**.

Step 8 Check the **Enable** check box adjacent to Over-ride Global Config.

Step 9 Set the preauthentication ACL.

Step 10 Choose the web authentication as external from the Web Auth type drop-down list.

Step 11 Enter the URL of the splash page in URL.

For example you can enter the URL - http://172.19.28.159:8081/Mario/jsp/runtime/auth/authLoginForm.html

Step 12 Click **Apply** in the upper right corner.

For Visitor Management to work the user has to enable the CMX Dashboard service.

For more information on the web passthrough and WLAN configuration, see *Cisco Wireless LAN Controller Configuration Guide Release 7.4*.

Visitor Management as Captive Portal

Captive portal is a solution aimed at providing access to wireless network to a customer at a venue. The customer needs to register with the information such as name, phone number, and email ID. Customer has to agree to the 'Acceptable Usage Policy'. This is one time registration. Then the wireless network is accessible. The web page on the captive portal is called Splash page.

CMX Dashboard Visitor Management is a captive portal.

Visitor Management is based on web pass-through methodology of providing guest access using Cisco WLC and APs. The admin user of the CMX Dashboard can customize the guest user experience by creating the flow of web pages that you want the user to visit. After that the customer can access the network at the venue.

As a captive portal, you can customize the Visitor Management with different splash pages. You can have customized templates.

Following is the flow of webpages:

1. Guest registration
2. View, and acceptance of the Acceptable Use Policy
3. Advertisement - This is optional
4. Welcome page with Social Network Authentication to provide a personalized browsing experience

With Visitor Management, you can create different Splash pages for different locations and provide Wi-Fi user experience at a specific venue.

Visitor Management recognizes a new user and a previous user and requests for registration for a new user only.

Visitor Management setting

Following are the three sections of the Visitor Management menu:

- Template Fields
- Social Connectors
- Splash Templates

Template Fields

In Template Fields, you can create a Splash template field. It is basically a type of information of the customer that you want to collect.

For example the fields can be Email, Name, Phone number, and the venue name where the customer has visited.

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

Step 1 Go to **Visitor Management > Template Fields** from the left side bar menu.

Step 2 Click **Create New Splash Template Field**.

Step 3 In Name, enter the name of the field you want to create.

Step 4 Select the type of the field from Type. There are two types of fields - Text and List.

Step 5 If you want to have the data in text, select Text. If you want to have the customer information for specific venue or a building, select List.

Step 6 Click **Submit**. If you want to cancel the creation of field, click **Cancel**.

Step 7 If you want to edit a template field, go to **Visitor Management > Template Fields**. Select the field from the list in the Splash Template Fields box. Click **Edit**. After the changes, click **Submit**.

Step 8 If you want to If you want to delete a template field, go to **Visitor Management > Template Fields**. Select the field from the list in the Splash Template Fields box. Click **Delete**. Click **OK** on the Delete Confirmation dialog box.

Social Connectors

The Visitor Management enables the venue owner to offer the access to the wireless network to customers using the social networking platforms such as Facebook, Google+, and LinkedIn.

The venue or store owner can provide an option to the customers to log in and access the Wi-Fi network at the venue using the credentials of the social networking sites. The venue owner needs to create an application for the CMX Visitor Management on the company's Facebook or Google+ page. This process generates the application keys and or the ID. The ID and the keys are important while creating a new social connector on the CMX dashboard.

Note To know how to configure social connector, see http://vimeo.com/59204177 - How to obtain Facebook App Key, http://vimeo.com/59204895 - How to get Google Client ID, and http://vimeo.com/59204949 - How to LinkedIn API Key.

On the CMX Dashboard the admin user can assign an account to a Social Connector.

The customer can provide the following information during the registration process at the venue.

- Website URL for the CMX Visitor Management (http://<NAME>:8080/Mario/jsp/runtime/auth/guestSocialLoginForm.html)
- Javascript API Domains (http://<NAME>)

After the social application is set up, you can generate the API Keys. You can then enter the API keys into Social Connector on the CMX Visitor Management.

You can use the social connector in the Social Authentication tab in the Splash Templates menu.

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

Creating Social Connector

Complete the following steps to create a social connector:

Step 1 Go to **Visitor Management > Social Connector** from the left side bar menu.

Step 2 Click **Create New Social Connector**. Add/Edit Social Connectors group box appears.

Step 3 In Connectors Name, enter the name that you want to give to the social connector.

Step 4 Choose the type of account from the Select Account drop-down list.

Step 5 In Facebook APP ID, enter the ID that you received while creating application for the Facebook site.

Step 6 Enter the key that you received while creating application for the Linked site in LinkedIn API Key.

Step 7 Enter the Google client ID and key in Google API Client and Google API Key respectively.

Step 8 Click **Submit**.

Editing Social Connector

Complete the following steps to edit a social connector:

Step 1 Go to **Visitor Management > Social Connector** from the left side bar menu.

Step 2 In Social Connectors group box, the list of all the connectors appears.

Step 3 Select the connector that you want to edit. Click **Edit**.

Step 4 Make the changes in the Add/Edit Social Connectors group box. Click **Submit**.

Deleting Social Connector

Complete the following steps to edit a social connector:

Step 1 Go to **Visitor Management > Social Connector** from the left side bar menu.

Step 2 In Social Connectors group box, the list of all the connectors appears.

Step 3 Select the connector that you want to edit. Click **Delete**.

Step 4 Click **OK** in the Delete Confirmation dialog box.

Splash Templates

You can create the template for the splash pages for locations. The splash page shows its name and the names of the social connectors such as Facebook, LinkedIn, and Google+.

To create a splash template complete the following steps:

Go to **Visitor Management** > **Template Fields** from the left side bar menu.

Click **Create New Splash Template**.

There are three group boxes:

- Basic Authentication
- Ad Configuration
- Social Authentication

Step 1 In Basic Authentication, enter the name of the template in Template Name.

Step 2 Choose the type of the background from the Template Background drop-down list.

Note If you want to set the background of your choice, you can choose Custom from the list. To upload an image that you want to display, click Click to upload an image.

Step 3 Choose the name of the field from the Form Fields drop-down list. These are fields that you created using Template Fields menu. For example, the fields can be Email, Name, Phone number, and the venue name.

Note If it is a list field you need to add comma separated strings to prepare drop-down list.

Step 4 You can set the terms and conditions that you want to display in the Terms and Conditions editor.

Step 5 In Header enter the information for the customer. For example you can enter 'Welcome to XYZ mall'.

Step 6 In Footer, you can enter any disclaimer. For example you can mention 'This is complementary Wi-Fi network, we do not save your data'.

Step 7 Click **Next**.

Step 8 Enter the script of the advertisement in Ad Script in Ad Configuration box. You have to provide the html code or the iframe source of the video that you want to share as an advertisement in Ad Script.

For example, you can insert a video ad from YouTube. Ad script for such example is - <iframe width="853" height="480" src="//www.youtube.com/embed/uIDx3eUZ-vw" frameborder="0" allowfullscreen></iframe>.

Step 9 Click **Next**.

Step 10 In Social Authentication box, enter the information that you want to display in Header. For example you can enter 'Congratulations! You are on the Wi-Fi network of XYZ'.

Step 11 Choose the type of social connector from the Social Connector drop-down list. This is the list of the connectors that you created in **Visitor Management** > **Social Connectors**.

Step 12 Select the corresponding authentication type from Social Auth.

Step 13 Enter the information in the footer.

Step 14 Click **Submit**.

Assigning a Splash Page Template to a floor

You can assign a specific Splash Page Template to POI or a floor. This enables the venue owner to give 'location aware' network access to the customer.

You can assign a splash template to any map element such as system campus, floors, a building, a single campus, or to a single floor.

Complete the following steps to assign a splash page template to a floor:

Step 1 Go to Points of Interest on the left side bar menu of CMX Dashboard.

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 **Edit Floor** and from the Splash Template drop-down list choose the type of splash page template you want to assign.

Step 6 Click **Submit**.

Feature Information for the Cisco CMX Dashboard Configuration Guide

The following table lists the release history for CMX Dashboard. All the features of CMX Dashboard are new.

Feature Name	Release	Feature Information
Banner Management	7.5	Banner Management allows creation of different types of messages to interact with the customers at the stores or venues. This feature is introduced in this release.
Campaign Management	7.5	Campaign Management enables enterprises to create and implement various campaigns. This feature is introduced in this release.
Points of Interest (POI) Management	7.5	POI Management enables creation of various POIs such as campuses, venues, floors, or zones. This feature is introduced in this release.
Navigation Management	7.5	CMX Dashboard enables organization of the navigation of the zones of venue per need. This feature is introduced in this release.
Account Management	7.5	With Account Management you can create and assign accounts depending on the product or service. This feature is introduced in this release.
CMX Dashboard Reports	7.5	The CMX Dashboard enables the administration user in an enterprise to analyze the use of services and the customer behavior. This feature is introduced in this release.
Visitor Management	7.5	Cisco CMX Dashboard Visitor Management is a guest access solution based on Mobility Services Engine (MSE), Cisco Wireless LAN Controller (WLC) and Lightweight Access points. This feature is introduced in this release. This is a demo feature.
HTTP Proxy	7.5	CMX Dashboard has the HTTP traffic flows to provide value added services and messages to the customer at the venue. This feature is introduced in this release.
Cloud Connector	7.5	The CMX Dashboard Connector intercepts the WAN traffic and inserts a Java response script. This feature is introduced in this release.