CHAPTER 11

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

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:

a. 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.

b. 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.

c. 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.

d. 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**.

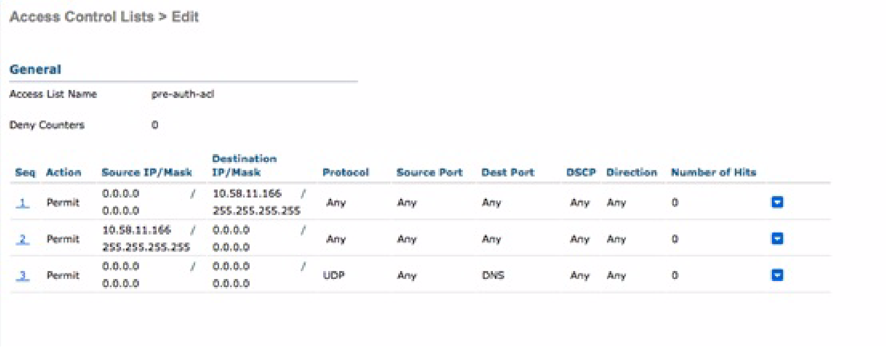
Configuring WLAN for Web Passthrough Authentication

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.

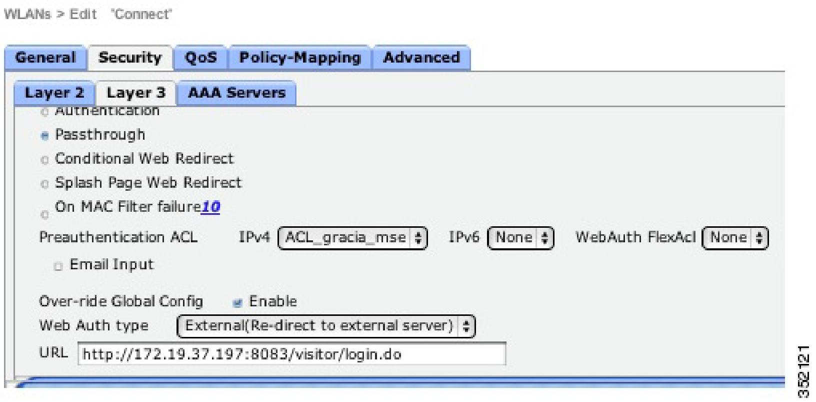
Step 5 From the Layer 2 Security drop-down list, choose **None**.

Step 6 Click **Apply**.

Figure 11-2 Layer 2 Setting

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

Figure 11-3 Web Passthrough Setting



○ Authentication
● Passthrough
○ Conditional Web Redirect
○ Splash Page Web Redirect
○ On MAC Filter failure10

Preauthentication ACL IPv4 ACL_gracia_mse IPv6 None WebAuth FlexAcl None

□ Email Input

Over-ride Global Config ☑ Enable
Web Auth type External(Re-direct to external server)
URL http://172.19.37.197:8083/visitor/login.do

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 filed 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

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” sword//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

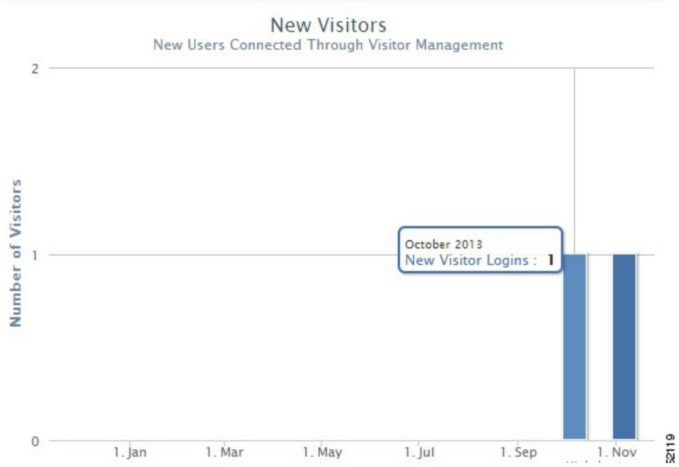
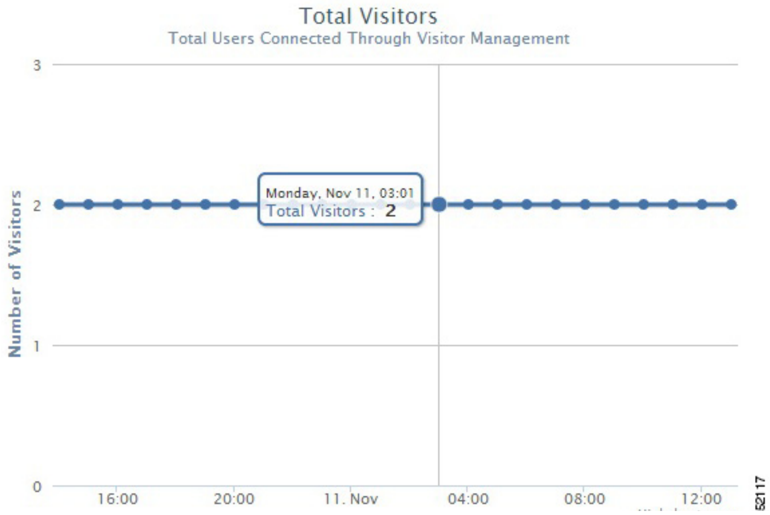


Figure 11-6 Hourly Trend for Total Visitors



- 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

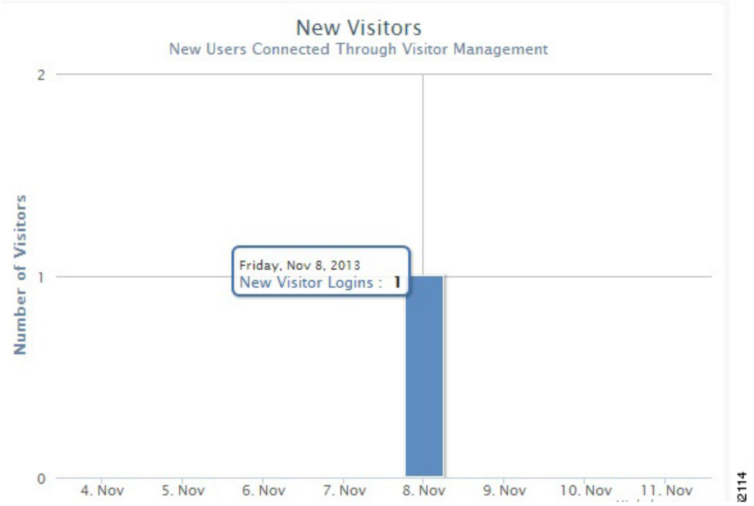
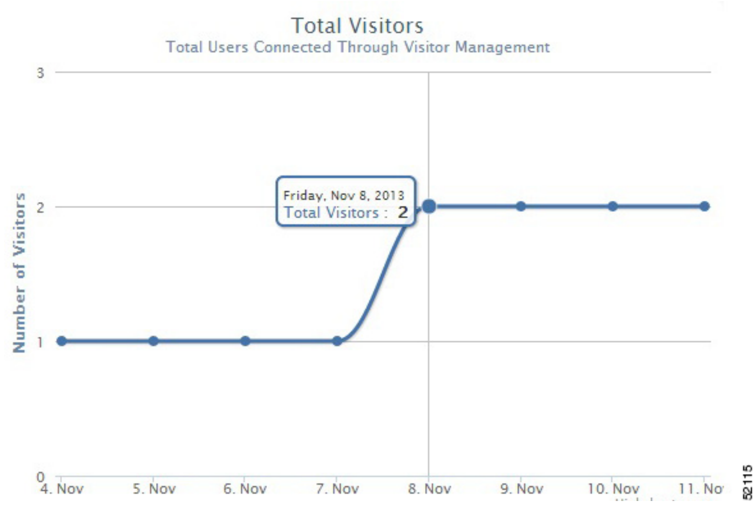


Figure 11-8 Daily Trend for Total Visitors



- 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

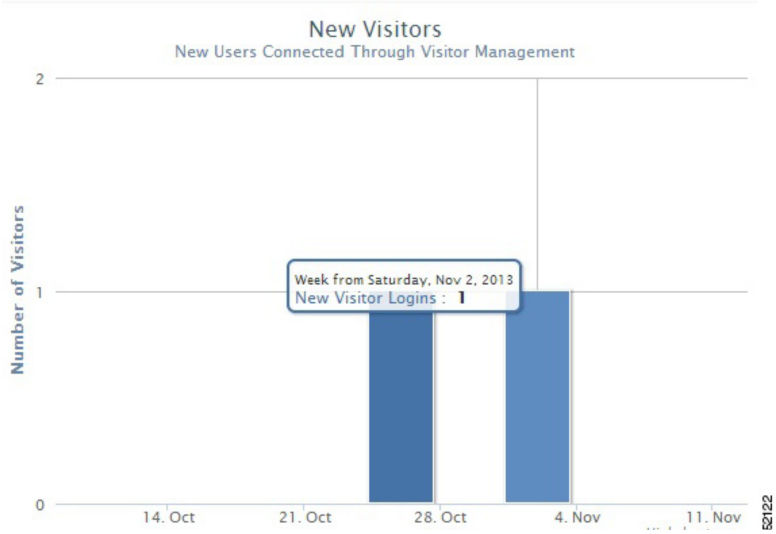
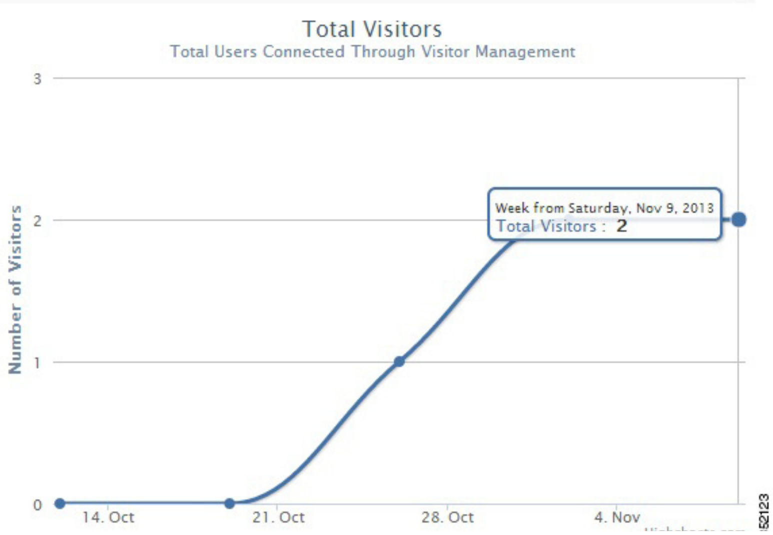


Figure 11-10 Weekly Trend for Total Visitors



- 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

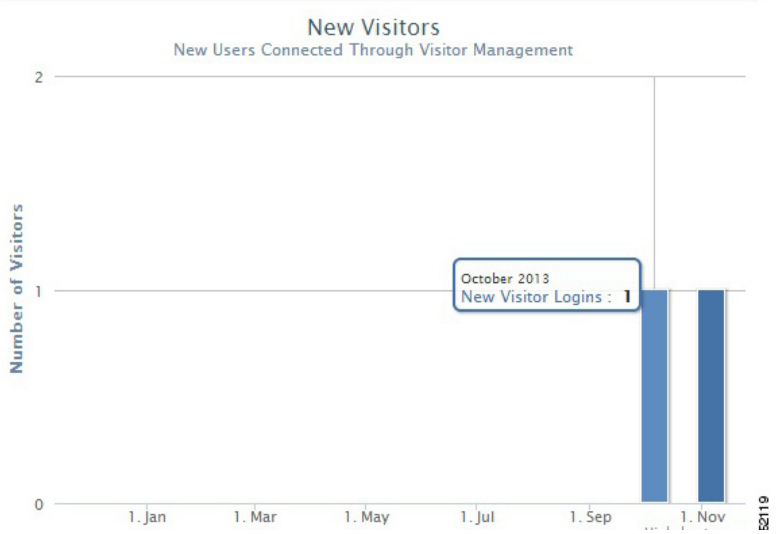
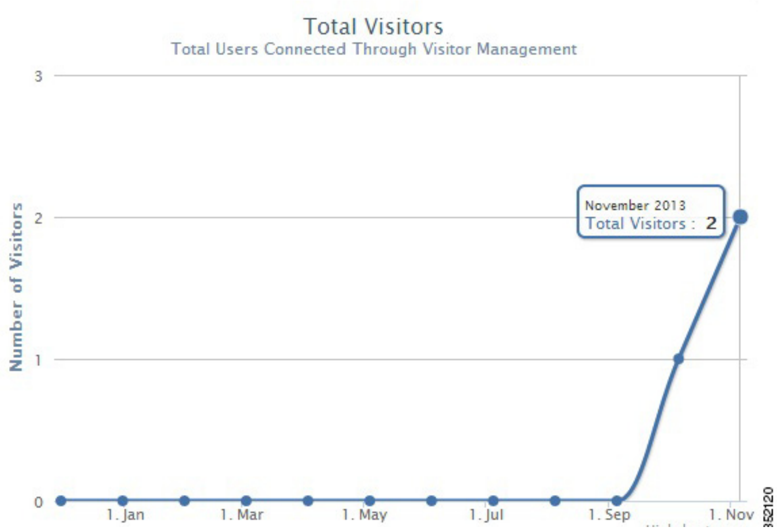


Figure 11-12 Monthly Trend for Total Visitors



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.