

ARISTA

Guest Manager User Guide 5.5

Arista Networks

www.arista.com

DOC - 05290-02

Headquarters	Support	Sales
5453 Great America Parkway Santa Clara, CA 95054 USA		
408 547-5500	408547-5502 866 476-0000	408 547-5501 866 497-0000
www.arista.com	support-wifi@arista.com	sales@arista.com

© Copyright 2022 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista Networks and the Arista logo are trademarks of Arista Networks, Inc in the United States and other countries. Other product or service names may be trademarks or service marks of others.

Contents

Intended Audience	6
Product and Documentation Updates	6
Contact Information	6
What's New	7
New Features in 5.3	7
New Features in 5.1	7
New Features in 5.0	7
New Features in 4.9.4	9
New Features in 4.9.3	9
New Features in 4.9	11
New features in 4.8	11
New features in 4.7	12
Introduction to Guest Manager	13
About Guest Manager	13
Features and Functionality	13
Guest Manager Workflow	17
Guest Manager Terminology	17
For the Foursquare plug-in	18
For the Facebook plug-in	18
For the Twitter plug-in	19
For the LinkedIn plug-in	19
For the Google plug-in	19
For the Okta plug-in	20
Accessing Guest Manager	20
Configure SMS and E-mail Settings	20
SMS Service Configuration	20
=<sms_content>	22
Email Service Configuration	23
Configuring Email Service with SMTP Details	24
Add a Server	26
Synchronize Server Information	27
View Portal Configuration	30
Creating a Portal	32

Modify Portal	33
Configure Quality of Service for Plug-In	35
Assign Campaign to Portal	37
Interception	38
Configure Interception	38
Configure Social Media Plug-Ins on a Portal	39
Configure Facebook Plug-In	39
Configure Twitter Plug-In	40
Configure LinkedIn Plug-In	41
Configure Google Plug-In	42
Configure Foursquare Plug-In	43
Configure Instagram Plug-In	44
Configure Okta Plug-In	44
Configure Guestbook Plug-In on a Portal	46
Enable Self-Registration	48
Enabling Self-Registration	49
Self-Registration by SMS	52
Wi-Fi Login Experience for Self-Registered Guest Users	53
Configure SMS Plug-In on a Portal	55
Download SMS Logs	60
Download SMS Logs for a Specific Date Range	62
Account Health	62
Configure Web Form Plug-In on a Portal	62
Configure RADIUS plug-in	63
Configure SSID Profile in Wireless Manager	64
Delete Portal	66
Notifying Third-Party Endpoints	67
Validating With Third-Party Endpoints	68
How does validation work?	68
Add Endpoint	68
Edit Endpoint	70
Delete Endpoint	71

Configuring Endpoint in Portal Plug-In	71
Create Guest Users	73
Edit Guest Users	76
Import Guest Users	78
Export Guest Users	79
Enable Guest Users	79
Disable Guest Users	80
Delete Guest Users	80
Change Account Expiry for Guest User	82
Create Guest Batch	82
Edit Guest Batch	85
Export Guest Batch	87
Delete Guest Batch	87
Send Email to Guest Users	88
Send Email to Guest Batch	88
Configure Email Content	89
Sort Guest Batch Information	89
Sort Guestbook User Information	91
Filter Guest Batch Information	91
Filter Guestbook User Information	91
Set Password	93
About Dashboard	94
Dashboard Widgets	95
Download Dashboard as PDF File	99
Schedule Dashboard Report	100
Schedule One-Time Dashboard Report from the Dashboard tab	100
Schedule One time Dashboard Report from the Reports Tab	101
Schedule Recurring Dashboard Report	103
Edit Dashboard Report Schedule	106

Delete Dashboard Report Schedule	106
Download Scheduled Dashboard Report	106
Location-Aware Analytics	108
Graph Configurations	109
Demographic Analytics	110
View Guest Profile Information	114
Sort Guest Profile Information	116
Filter Guest Profile Information	117
Contains.	117
Presence Analytics	117
Proximity-based Analytics using Floor Map	120
Wi-Fi Usage Analytics	123
Conversion Analytics	125
Loyalty Analytics	112
Download Analytics Graphs	114
Interception Analytics	114
Download Guest Wi-Fi Access Logs	117
Download User Audit Logs	118
Create Custom Report	120
Schedule Custom Report	121
Download Custom Report	122
Duplicate Custom Report	122
Email Custom Report	123
Delete Custom Report	123

About the Guide

This guide explains the basic operations that a user can perform using the Guest Manager. For information on using individual services provided by Arista Networks, refer to the respective service user guides.

Important! Please read the EULA before installing Guest Manager. You can download and read the EULA from <http://www.arista.com/en/support/product-documentation>. Installing the server constitutes your acceptance of the terms and conditions of the EULA mentioned above in this document.

Intended Audience

This guide is intended for anyone who wants to access and configure the Guest Manager.

Product and Documentation Updates

To receive important news on product updates, please visit our website at <http://www.arista.com>. We continuously enhance our product documentation based on customer feedback.

Contact Information

Arista Networks

5453 Great America Parkway

Santa Clara, Mountain View, CA 95054

Tel: 408 547-5500

For technical support, send an email to support-wifi@arista.com .

What's New

This section describes features that are new in the current and few of the immediate past releases of Guest Manager.

New Features in 5.5

The section lists all the features developed in the 5.5 release:

Updated client association charts in the GM UI for clients with randomly assigned MAC addresses	When clients with randomly assigned MAC addresses connect to the GM, GM uses an approximation algorithm to identify such clients. GM then displays a percentage approximation of such clients in all the client-association charts, instead of displaying the actual count.
---	---

New Features in 5.4

The section lists all the features developed in 5.4 release:

Social Data Retention Policy	Keeping the security parameters intact, Arista has introduced data retention policy to avoid storing user data through any social media plugin. Customers providing guest manager access to their users need to register their own version of social media apps through their account. The users can login through their credentials but no detail will be stored, thus, safeguarding their privacy.
Self-Registration Enhancement	A new field has been added for "Host kdjjsd sksdn lsddb shdb ljshsdbdf lssdbdf lshsdbf lshdsdbf LDBDFIUHDHFWEJBWB WIWHFIHB IWUIDHFB

New Features in 5.3

The section lists all the features developed in 5.3 release:

Okta Integration

Users can be authenticated and granted access to the Internet using Okta. Okta is an identity management service that is primarily built for the enterprise cloud but it is also compatible with many on-premises applications. Using Okta, users can authenticate and manage employee access to

any application or device (network access).

New Features in 5.1

The section lists all the features developed in 5.1 release:

Social Data Retention Policy

Keeping the security parameters intact, Arista has introduced data retention policy to avoid storing user data through any social media plugin. Customers providing guest manager access to their users need to register their own version of social media apps through their account. The users can login through their credentials but no detail will be stored, thus, safeguarding their privacy.

Self-Registration Enhancement

A new field has been added for "Host" in the approval email sent during the self-registration host approval. This will help the default email approver to know the context of the person hosting the guest.

New Features in 5.0

This section lists all the new features that were developed in the 5.0 release.

Key Based Guest Login

This feature by captive portal will enable the login support of multiple users with a single pre-shared key. A single passphrase can be configured in Canvas while making splash pages.

HTTP Pre-Validation for Guest Users

HTTP Pre-Validation helps the customers to validate their guest to grant internet access. The customers can pre-validate using their own validation systems like CRM or any third party validation system. An extra step for validation lets the customer have their own security settings.

Google Plugin Enhancements

Google login can be restricted to a set of users defined by the admin with Google hosted domain accounts.

Host Approval Enhancements for Self- Registration

The existing Self-Registration module of Guestbook plugin has been enhanced to create flexibility in the host approval workflow for guest users. By configuring the host settings, the host will only receive a notification about a guest requesting internet access. While, the approve/ reject authority remains with the configured approvers.

Introduction to Guest Manager

Guest Manager is a hosted service managed by Arista Networks. It enables you to provide guest users access to the Internet through your Wi-Fi setup by using a customized captive portal.

The guests can log in to the Wi-Fi setup by either using their social media account or through an account credential provided by you.

This chapter covers the following topics.

- [About Guest Manager](#)
- [Features and Functionality](#)
- [Guest Manager Workflow](#)
- [Guest Manager Terminology](#)

About Guest Manager

Guest Manager enables you to analyze the various stats and demographic profiles of guest users who access your Wi-Fi setup. You can obtain the user profiles by using social media plug-ins or through entries from a private guest book.

Users can access the Wi-Fi through custom captive portals created in Guest Manager. These portals can be configured to enable users to access the Wi-Fi by using their social media credentials or by using user accounts that you have created in the portal guest book.

Guest Manager leverages some of the features from the Wireless Manager. You must, therefore, have a Wireless Manager account to use Guest Manager. Guest Manager integrates with the Wireless Manager and fetches the visibility and association analytics data to chart some of the graphs.

Features and Functionality

Some of the important features of the Guest Manager are as follows:

Hosted Service

Guest Manager is provided as a cloud hosted service that is managed by Arista Networks. This relieves you of some of the responsibilities of provisioning and managing the service.

Multiple Custom Captive Portal

Guest Manager allows you to create multiple custom captive portals. Guest users connecting to your Wi-Fi network can be redirected to the captive portal. Users must authenticate

	<p>themselves through the portal before accessing the internet.</p>
Internet Access Using Social Media Account	<p>Guest users can access your Wi-Fi setup by using their social media account credentials. The social media plug-ins can be configured on the custom captive portals.</p>
Internet Access Using a Private Guestbook	<p>Guest users can also access Wi-Fi by authenticating with a guest user account, which you create in the private guest book. The guest book can also include other user-specific information.</p>
Click-Through and Web Form Internet Access	<p>You can also configure a custom portal to provide guests Internet access without using any authentication. This is possible only if you include the click-through plug-in for the portal. You can also configure the portal to request some basic user information through a Web form before granting Internet access.</p>
Internet Access Using an SMS Code	<p>You can configure a custom portal such that the guests provide their mobile/cellphone number to obtain a code through SMS, which they can then use to log into the portal and access the Internet.</p>
SMTP Integration	<p>You can configure an SMTP server in your Wireless Manager setup to send account details through e-mail to users defined in the guest book.</p>
Wireless Manager Integration	<p>Guest Manager integrates with Wireless Manager and fetches the visibility and association analytics information.</p>
Dashboard	<p>The dashboard provides analytical and statistical information related to demographic data about visitors in and around the store, visitors using guest Wi-Fi, demographic data of visitors using guest Wi-Fi, store footfall, dwell time and new users versus repeat users.</p> <p>The higher management can take appropriate business decisions by taking a quick look at the dashboard.</p>

Location-Aware Analytics	Guest Manager provides location-aware social, visitor, usage, loyalty, and conversion analytic information through different graphs.
Social Analytics	Guest Manager helps you analyze your guest Wi-Fi usage by providing you with numeric and graphical representation of the number of guest users based on the social media account that they used to access the Internet. You can also view pie charts depicting the guest users' age and gender distribution over a specific period of time.
Visitor Analytics	Guest Manager displays graphs representing the visitor distribution by days and locations, and visitor dwell time by days and locations.
Wi-Fi Usage Analytics	Guest Manager provides you with the graphs that represent the data received, transmitted, and total data exchange by days and location.
Loyalty Analytics	Guest Manager charts store and brand loyalty graphs representing the frequency of guest visits.
Conversion Analytics	Guest Manager provides conversion analytic graphs that depict how many guests got converted, that is, visited the store, based on the RSSI value.
Zoning Analytics using Floor Map	Guest Manager displays the AP-wise visitor distribution and dwell time for a location floor based on the proximity of visitors to APs deployed on the location floor.
Interception Analytics	Guest Manager displays the website intercepted, the duration time of their engagement, and the location.
Third Party Integration for Real-time Guest Profile Information	Guest Manager can integrate with third party applications and send real-time guest profile information to these applications. Based on this information, the guest can be provided with offers or personalized messages.
Reports Management	Guest Manager enables the creation of custom PDF reports. A custom report can contain

sections with data from various analytics charts.

Guest Manager Workflow

When guests try to access the Internet through an access point (AP) in your Wi-Fi environment, the Guest Manager portal page is displayed. This is a captive portal requesting guests for authentication credentials. The portal provides the guest with the option of authenticating with their social media account.

The image below gives you an insight into how Guest Manager works.

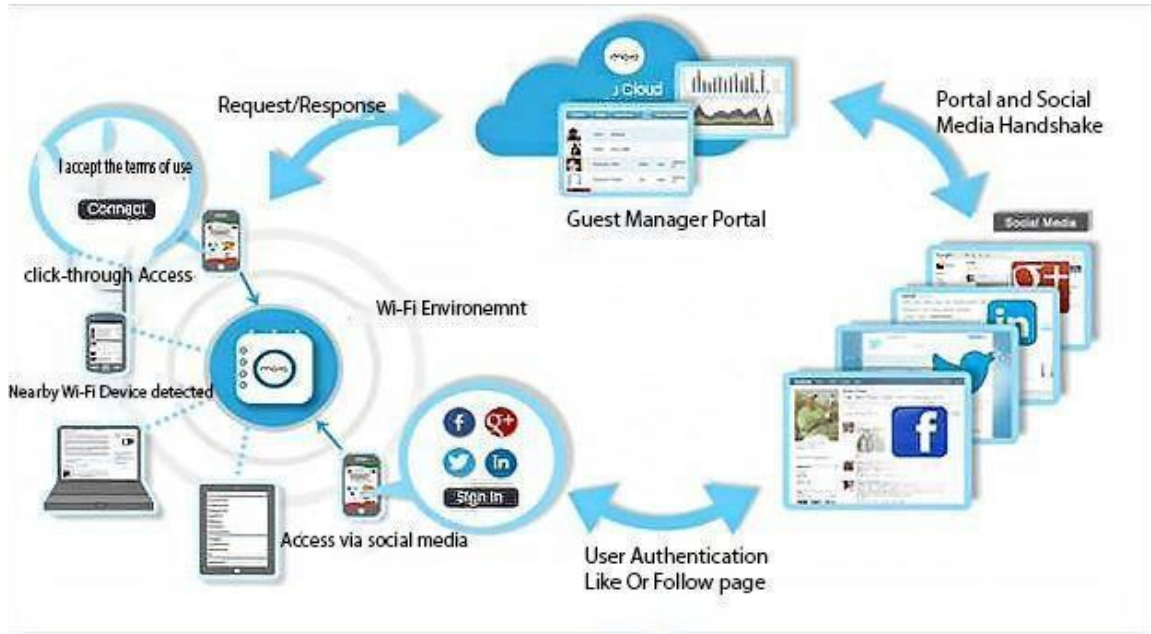


Figure 1: Guest Manager Workflow

If guests choose a social media, the portal redirects the users to the social media login. The guests then authenticate with their social media account credentials. The social media validates the user account credentials. If successful, the portal and the social media exchange certain information and perform a handshake.

The guest users are then requested whether they would like to share some of the information in their social media account with your social media App. If accepted, the social media checks whether guests Like or Follow your page on the social media and, if not, requests guests to Like or Follow your page.

The AP then opens the gate for the users to access the Internet.

Guest Manager Terminology

Here are certain terminologies that are specific to Guest Manager.

Before you proceed with using the Guest Manager, we would like you to get familiarized with the following terms in the context of Guest Manager.

Portal	This is a captive portal enabling you to authenticate guests who use your Wi-Fi setup.
Portal Bundle	A portal bundle is a set of files that define your splash page.
Splash Page	This is the landing page of the portal that guests see when they access your Wi-Fi setup.
Shared Secret	This is the passphrase used for secure communication between the access point (AP) and the portal.
Redirect URL	The URL of the page to which a guest must be redirected to on successful authentication from the splash page.
Login Timeout (mins)	The time duration in hours:minutes after which the user session expires and requires the guest to login again.
Blackout Time (mins)	The time duration in minutes, for which the user has to wait before logging in again after a session timeout.
Max. Upload Bandwidth	The maximum upload bandwidth, in Kbps, for the portal.
Max. Download Bandwidth	The maximum download bandwidth, in Kbps, for the portal.

Also, good to know are some of the plug-in specific terms.

For the Foursquare plug-in

Following are the terminologies for the Foursquare plug-in

Client ID	This is the identifier provided by Foursquare to communicate with the Foursquare application that uses OAuth 2.0 protocol to call Foursquare APIs.
Client Secret	Secret or passphrase that the portal uses to connect to and communicate securely with Foursquare.

For the Facebook plug-in

Following are the terminologies for the Twitter plug-in

App ID	This is ID of your Facebook App.
--------	----------------------------------

App Secret This is the secret or passphrase that the portal uses to connect to and communicate securely with the Facebook App.

Like Page Your Facebook page with the 'Like' button. You can configure the plug-in on the portal such that guests must like your Facebook page before they access the Wi-Fi.

For the Twitter plug-in

Following are the terminologies for the Twitter plug-in

Consumer Key This is the key provided by Twitter to communicate with the Twitter API.

Consumer Secret This is the secret or passphrase that the portal uses to connect to and communicate securely with Twitter.

Follow Page Your Twitter page with the 'Follow' button. You can configure the plug-in on the portal such that guests must follow you on Twitter before they access the Wi-Fi.

For the LinkedIn plug-in

Following are the terminologies for the LinkedIn plug-in

API Key This is the client identification provided by LinkedIn to communicate with the LinkedIn API.

API Secret This is the secret or passphrase that the portal uses to connect to and communicate securely with LinkedIn.

Follow Page Your LinkedIn page with the 'Follow' button. You can configure the plug-in on the portal such that guests must follow you on LinkedIn before they access the Wi-Fi.

For the Google plug-in

Following are the terminologies for the Google plug-in

Client ID This is an identifier provided by Google to communicate with the Google application that uses OAuth 2.0 protocol to call Google APIs.

Client Secret	This is the secret or passphrase that the portal uses to connect to and communicate securely with Google.
API Key	This is an API key generated by Google for each project and is used to communicate with other APIs enabled in the project.
Restricted login to Google Hosted Domains	This text box is to provide the list of Google Hosted Domains restricted to the set of guest users defined by the admin who will be allowed access. To enable the domains listed, select the checkbox for adding their email addresses.

For the Okta plug-in

Following are the terminologies for the Okta plug-in

Client ID	This is the identifier provided by Foursquare to communicate with the Foursquare application that uses OAuth 2.0 protocol to call Foursquare APIs.
Client Secret	Secret or passphrase that the portal uses to connect to and communicate securely with Foursquare.
Org Domain	Provide the domain where the Okta application is hosted.

Accessing Guest Manager

To access Guest Manager, log in to Launchpad with your credentials and access the Guest Manager service.

On successful login as an Administrator user, the Guest Manager Dashboard is displayed. Users with the Operator role can have access only to the guestbook grid. Analytics and Marketing users can have access to the Analytics, Dashboard, and Reports tab.

Configure SMS and E-mail Settings

Guest user can register through SMS or Email on the splash page of the captive portal, if the appropriate plugins are included. However, the administrator must configure the SMTP and Email settings in Guest Manager for this functionality to work.

SMS Service Configuration

You can configure an SMS service for your Guest Manager account from the SMS Service Configuration section under **Admin > SMS and Email Settings**. You can map the portal with the SMS service.

To configure SMS service, you must have an administrator role.

1. Click **Admin**.
2. Click on **SMS and Email Settings**.
A list of SMS/MMS accounts is displayed by default.
3. Click New Account to create a new SMS/MMS account.


For Twilio, provide the following details:

Option	Description
Username	The user name for your MSG91 user account.
Password	Password for the MSG91 user account.

Option	Description
Sender ID	A user-defined ID to be used to send SMS to the guest. This ID is used as the sender ID for the SMS. That is, the guest will receive the SMS with sender as this ID. The ID must be of 6 characters in length and can only contain letters from A through Z. For example, ATNSMS.
SMS Route	Whether the SMS should be sent through the Transactional route or the Promotional route. If the SMS contains any promotional content, then it cannot be sent through the Transactional route. If such a message is sent through the Transactional route, the message delivery fails. There are certain policies you must adhere to for sending promotional messages, which you can obtain from the MSG91 Website.

For Custom service provider, provide the following details.

Option	Description
Service URL	The URL of the SMS endpoint along with the GET parameters as name value pairs. It is mandatory that the URL has <sms_content> and <to_number> tags as placeholders for the fields that represent message content and destination number, respectively. For example: <code>https://custom.service.com/sms/?username=johnsmith&password=P@ssw0rd&to=<to_number>&body=<sms_content</code>

 *Note: Ensure that you take care of the following:*

- *Any invalid characters entered in the API Endpoint URL, for example (n), will be replaced with '_'.*

Option	Description
	<ul style="list-style-type: none"> '#' present in the API Endpoint URL will lead the URL after the '#' to be treated as a fragment. Any variables within the fragment will not be replaced.

- Click **New Account** to create a new SMS/MMS account.

Option	Description
Account SID	The account SID associated with your Twilio account.
Auth Token	The auth token for your Twilio account.
Twilio Number	A number or short code that you have purchased for your Twilio account.


- Click **Test Account Settings** to test the SMS service configuration.
- Click **Save**.

Email Service Configuration

In order to connect to the Wi-Fi services, the Guest user has to register through SMS or Email. The administrator has to configure these settings for the user. You can configure an e-mail service for your Guest Manager account from the Email Service Configuration section under Settings. The e-mail service can be configured to use your in-house SMTP server or the Email service.

To configure the e-mail service with Email, you must have the administrator role.

- Click **Admin**.
- Click **Settings** and then click **SMS and Email Settings**.
- Select the **Email** tab

 *Important: The Email Configuration information is Read Only if you have enabled PII related options in Launchpad. For more information refer Table 1 PII related impact in Guest Manager 4.5.*

- Enter the configuration information.

Option	Description
Email Service Type	Select Email.
From Email ID	The e-mail address from which the e-mails would be sent for your Guest Manager account.

Option	Description
From Name	Sender name to be used in the e-mail messages sent from your Guest Manager account.
Return Email ID	The e-mail address to which e-mail service related failure messages, such as e-mail bounce, must be sent to.

5. Click **Verify**.

You must verify the return e-mail ID. On clicking Verify, an e-mail with a link is sent to this address. You must open this e-mail and click the sent link to complete the verification process. If the e-mail address is not verified, the e-mail service configuration will be incomplete and no e-mails can be sent from your Guest Manager account.

6. Click **Send Test Email** to test the e-mail service configuration.

7. Click **Save**.

Configuring Email Service with SMTP Details

You must have an Administrator role to configure the Email settings with SMTP details

Do the following tasks to configure an Email service with SMTP details.

1. Click **Admin**.
2. Click **Settings** and then click **SMS and Email Settings** tile.
3. Select the **Email** tab.
4. Enter the configuration information.

Option	Description
Email Service Type	Select SMTP Configuration.
From Email ID	The e-mail address from which the e-mails would be sent for your Guest Manager account.
From Name	Sender name to be used in the e-mail messages sent from your Guest Manager account.
Return Email ID	The e-mail address to which e-mail service related failure messages, such as e-mail bounce, must be sent to.

Server Host	The IP address or the host name (FQDN) of the SMTP server.
--------------------	--

Option	Description
Server Port	The port for the SMTP service. The port number would vary based on the Connection Security setting.
Login Method	The login method configured on the SMTP server.
Login Username	The user name to log in to the SMTP server for e-mail service.
Login Password	The password for the SMTP server user account.
Connection Security	Whether or not connection security is enabled. If enabled, whether to use SSL or TLS.

5. Click **Send Test Email** to test the e-mail service configuration.
6. Click **Save**.

Integrating Wireless Manager

Guest Manager integrates with the Guest Manager Server to fetch information about the user account.

Guest Manager integrates with Guest Manager Server to fetch the following information:

- Locations defined in the Wireless Manager
- Arista devices listed under each location
- Visibility and association analytics generated on the server.

The information fetched is based on the user account used to add the Guest Manager Server to Guest Manager. Only the location and devices visible to the user account is fetched. Therefore, ensure that you provide a user account that has access to all the locations. The information from the Server is synchronized in Guest Manager periodically. By default, the synchronization occurs daily at 00:00 hours GMT.



Important: Guest Manager supports Wireless Manager Server 6.7 Update 4 and above.

Releases prior to 6.7 Update 4 are not supported.

This chapter covers the following topics:

- [Add Server](#)
- [Synchronize Server Information](#)

Add a Server

You must have the Administrator user role to add a Server.

To add a server, perform the followings tasks:


1. Click **Admin** and then click **Servers**. The Servers page is displayed.
2. Click **New Server**.
3. Provide the server information.

Option	Description
Display Name	The display name for the server. This is a mandatory field.
Server Hostname/IP Address	The IP address or host name of the Server. This is a mandatory field.
Username	The user account to access the server. Ensure that the user has access to all locations. If not, graphs for locations on which the user does

Option	Description
	not have access will not be generated. This is a mandatory field.
Password	The password for the user account. This is a mandatory field.

4. Click **Test and Save** to check whether Guest Manager is able to connect to the Server. Test and save only checks whether Guest Manager can reach the Server over the network and saves the server settings.

The server is added to Guest Manager and is listed on the Servers page.

 *Important: Guest Manager does not try to connect to the server when you add the server. Neither does Guest Manager check the version of Server. If the server information provided is incorrect or if the server is of a version prior to Server 6/7 Update 4, then the data synchronization operation fails. Ensure that you provide the correct server information and that the server version is 6.7 Update 4 or later.*

If you have already added one or more Server at an earlier date and now adding another Server, then ensure that you manually sync the existing servers after adding the new Server. This is to ensure that the analytics information in the graphs is not stale and includes the latest information from all the servers.

After a server is added, the server information can be edited by clicking the edit icon corresponding to the server details on the table under the Servers section of the Dashboard tab.

You can also delete a server added to your Guest Manager account by clicking the delete icon corresponding to the server details on the table under the Servers section of the Dashboard tab.

Synchronize Server Information

Guest Manager synchronizes the relevant data from the Server after the server is added. After the first synchronization cycle, the data from the server is synchronized daily at 00:00 hours GMT.

The data synchronization time can be configured in Guest Manager.

To configure the synchronization time, perform the following tasks:

1. Click **Admin** and then click **Servers**. The **Servers** page is displayed.
2. Click **Sync Settings**. The Sync Settings window is displayed.
3. Select the time of the day when the synchronization should occur in **Time**. The time-zone is same as that set for your Guest Manager user account.
4. Click **Save**.

All servers added to your Guest Manager account are queued for synchronization at the configured sync time. Guest Manager synchronizes the servers as and when a process thread becomes free. However, no specific order is defined for synchronizing the servers.

You can perform an unscheduled or manual synchronization by clicking **Sync Now**. Clicking Sync Now queues the servers added to your Guest Manager account for synchronization.

The latest synchronization time and status is updated in the table under the Servers section on the Dashboard tab.

If a synchronization operation fails (say due to network failure or server down-time), then Guest Manager waits for 5 minutes before queuing the server for synchronization operation. If the re-synchronization fails, then this process is repeated until the synchronization operation succeeds.

Portal Management

After you have created users in your Guest Manager account, you must create and configure one or more portals. The guest users authenticate in to your Wi-Fi setup through a portal. The portals can be configured with a combination of plug-ins for authenticating the guests and provide Internet access.

Guest Manager provides the following plug-ins:

Social Media	Social media plug-ins allow guests to authenticate with their social media account credentials. Guest Manager supports Facebook, Twitter, LinkedIn, Instagram, Google, and Foursquare.
Guestbook	Guest book helps you to maintain a private list of guest users who can access your Wi-Fi setup. Guests can authenticate using this plug-in by entering the account credentials provided by you. These credentials are defined by you in the Guest Manager.
Click-through	This plug-in enables a guest to access Internet without any authentication. You can configure your portal page such that the guest must first accept some Terms and Conditions before obtaining Internet access.
SMS	The SMS plug-in enables a guest to obtain an Internet access code through SMS on the mobile/cellphone number provided by him on the portal page.
Web Form	This plug-in can be considered as an enhanced form of click-through, wherein the guest must fill a form on the portal page before obtaining the Internet access.
RADIUS plugin	The RADIUS plug-in enables guests to obtain Internet access after using the username and password configured on the corresponding RADIUS server.

You must have an Administrator role to create and manage portals. After you configure the portal in Guest Manager, you must configure the SSID profile in the Wireless Manager to update the captive

portal and walled garden settings. These settings ensure that the guest is redirected to the captive portal when they connect to the SSID and also enable social media access for user authentication before enabling Internet access.

A social media plug-in can be configured to send real-time guest user profile information to a third party application when a guest logs in successfully using the plug-in. Based on the information, a personalized message or some personalized offers can be presented to the guest.

A portal must have a splash page and an optional landing page. Splash pages and landing pages can be designed and managed through Canvas. Once created, the pages can be associated with a campaign defined in Canvas, a web app that enables you to design onsite guest engagement campaigns. A campaign must be published before it can be associated with a portal in the Guest Manager. To publish a campaign it must have a splash page. A published campaign can contain only one active splash page and one active landing page.

This chapter covers the following topics.

- [View Portal Configuration](#)
- [Create Portal](#)
- [Modify Portal](#)
- [Assign Campaigns to Portal](#)
- [Guest Engagement](#)
- [Configure Social Media Plug-ins on a Portal](#)
- [Configure Guestbook Plug-In on a Portal](#)
- [Configure SMS Plug-In on a Portal](#)
- [Configure Web Form Plug-In on a Portal](#)
- [Configure SSID Profile in Wireless Manager](#)
- [Delete Portal](#)

View Portal Configuration

The Portals page provides a quick overview of the portals created in your Guest Manager account.

When you click Portals, a list of portals with the following fields is displayed on the Portals page.

Portal List Information	
Portal name	The name of the portal.
Active plugins	List of plug-ins that have been enabled for this portal.
Splash Page	Click Show to view the Splash Page URL for the portal. You are presented with the following fields: <i>Splash Page URL</i> : Splash page URL of the portal on the Guest Manager server. This is an auto-generated

field. Ensure that you are

Portal List Information	
	<p>using the correct splash page URL by verifying it with the value of the Splash Page URL field. CDN Splash Page URL: This URL is shown only if a CDN is configured on the Guest Manager server. The Splash page URL of the portal on a remote Guest Manager server can be cached on a Content Delivery Network (CDN) server. The CDN Splash Page URL is the URL for this cached copy of the portal splash page on the CDN server. It is auto-generated and cannot be edited. This URL can be used when faster rendering of the splash page is desirable and the splash page does not change very often. If the splash page changes very often, it is recommended to use the Splash page URL instead of the CDN Splash Page URL.</p> <p><i>Shared Secret:</i> The passphrase for secure communication between the portal and the access point. This is configured in the Settings tab for the portal.</p>
Active	Indicates whether the portal is active or inactive.

In the Portals page, click the portal name link from the list of portals to view detailed information about the portal.

The configuration information of the selected portal is displayed on the Settings tab.

The following table describes the information displayed under Basic Settings tab-

Portal Configuration Information	
Field	Description
Portal name	Name of the portal.
Display Name	Name of the portal to display on the Guest Manager.

Shared Secret	The passphrase for secure communication between the access point and the portal. You must configure Shared Secret on the SSID in Wireless Manager and the portal.
Active	Indicates whether the portal is active or inactive.

Portal Configuration Information	
Field	Description
Sign out Popup	Whether to display a sign out popup to a guest user on signing in to the portal. By default, this option is selected.
Skip Splash page	If this option is selected, Guest Wi-Fi users will see the splash page only the first time they access the Internet. The authentication method is recorded and the guests are not shown the splash page on their subsequent visits within the duration specified. This setting is not applicable if the guest uses Clickthrough or RADIUS plug-in for authentication.
Duration	This option is displayed after selecting the Skip Splash page option. It is the number of days for which the returning guest Wi-Fi user will not have to authenticate through the splash page. The default value is 1 day and maximum value is 90 days.

You can view the individual plug-in configuration information for the portal by clicking the plug-in name on the Plugin Configuration tab. The QoS settings for the plug-ins can be viewed on the Plug-in QoS tab.

Creating a Portal

After you have created users in your Guest Manager account, you must create and configure one or more portals.

You can create one or more captive portals through which guest users can authenticate into your Wi-Fi setup.


1. Click **Portals**. The page lists the details of the portals created in your account.
2. Click **New Portal** under the basic settings tab and enter the following information:

Option	Description
Portal Name	Name of the portal. This is a mandatory field.
Display Name	Name of the portal to display on the Guest

Option	Description
Shared Secret	<p>Manager.</p> <p>The passphrase for secure communication between the access point and the portal. If</p>
Active	<p>Indicates whether the portal is active or inactive.</p>
Sign out Popup	<p>Whether to display a sign out popup to a guest user on signing in to the portal. By default, this option is selected.</p>
Skip Splash page	<p>If this option is selected, Guest Wi-Fi users will see the splash page only the first time they access the Internet. The authentication method is recorded and the guests are not shown the splash page on their subsequent visits within the duration specified. This setting is not applicable if the guest uses Clickthrough or RADIUS plug-in for authentication.</p>
Duration	<p>This option is displayed after selecting the Skip Splash page option. It is the number of days for which the returning guest Wi-Fi user will not have to authenticate through the splash page. The default value is 1 day and maximum value is 90 days.</p>

3. Click **Save**. The portal is created but not configured.
4. On the **Settings** tab, click the icons for the portal plug-ins to activate the respective plug-ins on this portal. At least one plug-in must be selected to complete the portal creation.
5. Click **Save**. The new portal is created with a default campaign.

The portal is configured with the default campaign, which has the default splash page.

 *Important: If you have activated plug-ins other than the Clickthrough plug-in in the portal, then the splash page in the default campaign must be modified to include the selected plug-ins. This can be done with Canvas.*

Modify Portal

After a portal is created, you can update the portal-specific information anytime. For example, you might want to activate or deactivate plug-ins in an existing portal or you want to deactivate a portal that is currently not in use.

You must have the Administrator role to perform the following steps:

1. Click **Portals**. Click the Portal Name corresponding to the portal that you want to edit.
2. Update the name of the portal that you want to edit.

Option	Description
Portal name	Name of the portal.
Display Name	Name of the portal to display on Guest Manager.
Shared Secret	The passphrase for secure communication between the access point and the portal. If a shared secret is configured on the SSID in Wireless Manager, you must configure the same shared secret in the portal.
Active	Whether to activate or deactivate the portal.
Sign Out Popup	Whether to display the sign out popup to a guest user on signing in to the portal. By default, this option is selected. Deselect the check box if you do not wish to display the sign out popup to a guest user.
Skip Splash page	If this option is selected, Guest Wi-Fi users will see the splash page only the first time they access the Internet. The authentication method is recorded and the guests are not shown the splash page on their subsequent visits within the duration specified. This setting is not applicable if the guest uses Clickthrough or RADIUS plug-in for authentication.
Duration	This option is displayed after selecting the Skip Splash page option. The number of days, the returning guest Wi-Fi user will not have to authenticate through the splash page. The default value is 1 days and maximum value is 90 days.

3. Click the icons for the portal plugins to activate or deactivate the respective plugins on this portal.
4. Click **Save**.

On successful modification of the portal information, the updated details are listed in the table on the Portals page.

Configure Quality of Service for Plug-In

You can configure the quality of service parameters such as Login Timeout (in mins), Blackout Time (mins), upload and download bandwidths, and redirect URL for each plug-in selected in a portal.

The URL of the page to which the guest user must be redirected to on successful login from the portal is the redirect URL.

The redirect URL could be a custom URL, Campaign URL or Third-party URL.

Custom Redirect URL

Select the Custom option for Redirect URL, and enter an HTTP or HTTPS URL to redirect the guest user opting to log in through the plug-in for which the Redirect URL is being configured. The guest user is redirected to the specified URL when he or she authenticates successfully by using the plug-in. Guest Manager does not send analytics data to the custom URL when this option is selected.

Campaign Redirect URL

Select Campaign if you want the plug-in to have a custom landing page as specified in the campaign. This can be used when you want to display offers to guests logging in through a specific plugin. You must have the required Campaign published through Canvas to be able to select a Campaign here. The guest user is redirected to the landing page of the selected Campaign on successful login.

Third-party Redirect URL

Guest Manager redirects the guest user to the redirect URL specified in the third-party endpoint specified here. Guest Manager sends guest user related analytics data to the third-party endpoint based on the key-value pairs defined in the endpoint. You must have the corresponding third-party analytics endpoint configured with method type as 'Redirect' before you can select the Redirect URL as third-party. Refer to [Configure End Points for Third Party Integration](#) to configure endpoints for third party integration.

Based on the analytics data, a personalized message or a personalized offer can be presented to the guest on the redirect URL



*Important: If the redirect URL has not been configured, the user is redirected to the Redirect URL specified in the SSID profile in Wireless Manager. If a redirect endpoint has been assigned to the **Redirect URL** under **Plug-in QoS** tab, this URL has a higher precedence than the redirect URL in the SSID profile in the Wireless Manager.*

If QoS settings have also been defined in the SSID profile applied to the Arista device then the plugin QoS settings get the highest precedence followed by QoS settings defined in the SSID profile applied to the Arista devices.

To configure quality of service parameters, perform the following steps:

1. Click **Portals**.
2. Click the portal name for which you want to configure the quality of service.
3. Click the **Plug-in QoS** tab. The list of enabled plug-ins is seen on this tab.
4. Specify the QoS parameter values.

Option	Description
Login Timeout (mins)	The time period, in minutes, after which the guest user session for the portal expires. The user must re-authenticate with his login credentials if he wants to continue using the Wi-Fi service. A value of zero indicates that the user session does not timeout and the user must explicitly log out from the portal. A non-zero timeout configured on the portal takes precedence over the timeout configured on the SSID profile in the Wireless Manager.
Blackout Time(mins)	The time period in minutes for which a user cannot log in to the portal after his last successful login has timed out. A value of zero indicates no blackout time. The blackout time, including zero value, configured on the portal takes precedence over the blackout time configured on the SSID profile in Wireless Manager.
Max Download Bandwidth (Kbps)	Maximum download bandwidth, in Kbps, for this plug-in on the portal.
Max Upload Bandwidth (Kbps)	Maximum upload bandwidth, in Kbps, for this plug-in on the portal.
Redirect URL---Third Party Endpoint (Notify)	On successful authentication, the Notification Parameters will be sent to the End Point

Option	Description
	URI of the third-party end point by using the configured Method Type.
<ol style="list-style-type: none"> 5. Click the edit icon (pencil) corresponding to the plug-in for which you want to configure the Redirect URL and select the type of Redirect URL along with the third-party endpoint notification. 6. If the value of the Redirect URL is Custom, enter an HTTP or HTTPS URL. If the value of the Redirect URL is Third-Party, select the appropriate third-party endpoint. If the value of the Redirect URL is Campaign, select the required Campaign. 7. Click the update icon (tick mark) to save the changes. 	

Assign Campaign to Portal

After you create a portal and configure the plugins on it, you must configure the portal to ensure that your custom login page is displayed when guest users access the portal. This is the portal splash page.


A campaign is the container for splash pages and landing pages designed using Canvas. You must associate an appropriate campaign with the portal so that the published splash page in the campaign associates with the portal.

You can modify the splash page of the portal through the Canvas app. Click Manage Campaigns on the Campaigns tab of portal page to access the Canvas app. The app enables you to create campaigns and add guest authentication and engagement content to the campaigns.

You must have the Administrator role to assign a campaign to the portal.

1. Click **Portal**.
2. Click the portal name for which you want to upload a custom portal bundle.
3. Click the **Campaigns** tab. For a new portal, the default campaign is selected, by default.
4. Select the campaign from the list of available campaigns. The thumbnails for the published splash page and landing page for the campaign are displayed.
5. Click Save.

The published splash page of the campaign is associated with the portal.

 *Note: If the published splash page in the selected campaign contains plug-ins that are not configured on the portal, then such plug-ins would not work and guest Wi-Fi users might see an error. You must manually configure the required plug-ins for the portal to ensure an error-free guest Wi-Fi user experience.*

Interception



Based on your Canvas subscription, you can create coupons and text messages (advertisements) and add these to a campaign. Such content can be used for Interception through MMS or SMS.



When a guest user connects to your Wi-Fi network, based on the specific Website that guests access over the Wi-Fi, you can engage them by using targeted marketing with the help of coupons and text messages. For example, in the case of a retail establishment, such targeted marketing can be used as a way to promote goods and services in the establishment based on what the guest is currently trying to look for on the Internet when using the guest Wi-Fi network.

The user can analyze the reports and based on these reports the user can offer better promotional offers.

Configure Interception

You must have the guest user's mobile number to configure this feature.

1. Click **Portals**.
2. Click the portal name for which you want to upload a custom portal bundle. A set of four tabs is displayed.
3. Click the **Campaigns** tab. The default campaign is selected, by default.
4. Click **Manage Campaigns**. By default, the page for basic campaigns is selected.
5. Click the Menu icon () to display the left panel, and select **Pro Campaign**.
6. Click the Interception icon (). The Interception page is displayed.
7. Specify the following Interception parameters.

Option	Description
On/Off	Whether the Interception feature should be activated or not.
Websites to intercept	The list of website that needs to be intercepted.
Content	You can prioritize whether to send an SMS or an MMS by drag and drop.  <i>Note: The MMS feature is available only in USA.</i>
Do not resend content within	The number of days after which the content is resent to the guest user.  <i>Note: Only one message per day is sent to the user, irrespective of the number of websites and the number of visits on that particular day. This</i>

Option**Description**

avoids flooding of messages to the guest user.

8. Click **OK** to save the settings.


The campaign must be associated with a portal, which is then configured on an SSID to enable Interception.


Configure Social Media Plug-Ins on a Portal

You can configure social media plug-ins on your captive portal. This release of Guest Manager supports Facebook, Twitter, LinkedIn, Google social media plug-ins and Foursquare as well.

You must have the Administrator role to configure the social media plug-ins. You can reconfigure existing configured plug-ins by performing the same tasks listed here.

Before you configure a social media plug-in you must ensure that you have created your application/ project in the social media. The user will now only input his values and no value will be stored. The fields will be either null or with dash.

 *Note: For Google plugin, login has been restricted only to Google hosted domain accounts.*

 *Note: You can only configure the plug-ins that are selected for the portal. You can select or enable the plug-ins for the portal in the Settings tab.*

Configure Facebook Plug-In

To configure the Facebook plug-in, perform the following steps.

1. Click **Portals**.
2. Click the portal name for which you want to configure the Facebook plug-in.
3. Click the **Settings** tab. Click the Facebook icon to enable the Facebook plug-in for the portal.
4. Click the **Plug-in Configuration** tab. The icons for various plugins are seen on this tab.
5. Click the Facebook icon. The Facebook icon is available only if the Facebook plug-in was selected during the portal creation. If not, you must first edit the portal to include the Facebook plug-in. The Facebook plugin details are displayed.
6. Provide the Facebook plug-in information.

Option**Description**

App ID

App ID provided by Facebook to communicate with the Facebook API.

App Secret

App secret that Guest Manager uses to connect to Facebook App.

Option	Description
Display Like Page	Whether the guests must Like your Facebook page when they authenticate using their Facebook account credentials. If selected, a notification with a Like button (a thumbs-up icon) is displayed requesting the user to Like the Facebook page. If you select this, the Likes check box under Extend User Profile Permissions is automatically selected.
Like Page URL	The Facebook page that guests see and can 'Like'.
Extend User Profile Permissions	Whether you want to ask the guest user for permission to access additional information such as email address, birthday, and location. If selected, the user is asked for permissions to access above-mentioned information from the user profile. Select the check boxes for the information fields (Email address, Birthday, Likes, Location) that you want to request access for from the guest user.

7. Click **Save**.
8. Click **Preview Like Page** to preview the 'Like' page to be seen by the guest.

The Facebook plug-in configuration data is displayed on the Facebook page of the selected portal.

Configure Twitter Plug-In

You can configure Twitter plug-ins on your captive portal. You must have the Administrator role to configure the Twitter plug-ins. Before you configure the Twitter plug-in you must ensure that you have created your application/ project in the social media.

To configure the Twitter plug-in, perform the following steps.

1. Click **Portals**.
2. Click the portal name for which you want to configure the Twitter plugin.
3. Click the **Settings** tab. Click the Twitter icon to enable the Twitter plug-in for the portal.
4. Click the **Plug-in Configuration** tab.
5. The icons for various plugins are seen on this tab.
6. Click the Twitter icon.

The Twitter icon is available only if the Twitter plug-in was selected during the portal creation. If not, you must first edit the portal to include the Twitter plug-in.

The Twitter plugin configuration details are displayed.

7. Provide the Twitter plug-in information.

Option	Description
Consumer Key	Key provided by Twitter to communicate with the Twitter API.
Consumer Secret	Secret that Guest Manager uses to connect to Twitter.
Display Follow Page	Whether the guests must Follow you on Twitter when they authenticate using their Twitter account credentials. If selected, a notification with a Follow button is displayed requesting the user to Follow the Twitter page.
Follow Page URL	The Twitter page that the guests can see and 'Follow'.

8. Click **Save**.

The Twitter plug-in configuration data is displayed on the Twitter page of the selected portal.

Click **Preview Follow Page** to preview the 'Follow' page to be seen by the guest.

Configure LinkedIn Plug-In

You can configure LinkedIn plug-ins on your captive portal. You must have the Administrator role to configure the LinkedIn plug-ins. Before you configure the LinkedIn plug-in you must ensure that you have created your application/ project in the social media.

To configure the LinkedIn plug-in, perform the following steps:

1. Click **Portals**.
2. Click the portal name for which you want to configure the LinkedIn plug-in.
3. Click the **Settings** tab. Click the LinkedIn icon to enable the LinkedIn plug-in for the portal.
4. Click the **Plug-in Configuration** tab.
5. The icons for the various plugins are seen on this tab.
6. Click the LinkedIn icon. The LinkedIn icon is available only if the LinkedIn plug-in was selected during the portal creation. If not, you must first edit the portal to include the LinkedIn plug-in. The LinkedIn plugin configuration details are displayed.
7. Provide the LinkedIn plug-in information.

Option	Description
App ID	App ID provided by Facebook to communicate with the LinkedIn API.
Secret Key	Secret that Guest Manager uses to connect to LinkedIn.
Display Follow Page	Whether the guests must Follow you on LinkedIn when they authenticate using their

Option	Description
Follow Page URL	LinkedIn account credentials. If selected, a notification with a Follow button is displayed requesting the user to Follow the LinkedIn page.
Extend User Profile Permissions	The Follow page to be displayed to the guest. Select the additional user details you wish to select from the user profile on LinkedIn like Email Address, Phone Number, and Full Profile. The user is notified whether he would like to share the requested information (basic and additional details). If the user denies the request, the log in fails.

8. Click **Save**.

The LinkedIn plug-in configuration data is displayed on the LinkedIn page of the selected portal.

Configure Google Plug-In

To configure the Google plug-in, perform the following steps:

1. Click **Portals**.
2. Click the portal name for which you want to configure the Google plug-in.
3. Click the **Settings** tab. Click the Google icon to enable the Google plug-in for the portal.
4. Click the **Plug-in Configuration** tab.
5. The icons for various plugins are seen on this tab.
6. Click the Google icon. The Google icon is available only if the Google plug-in was selected during the portal creation. If not, you must first edit the portal to include the Google plug-in. The Google plugin configuration details are displayed
7. Provide the Google plug-in information.

Option	Description
Client ID	Identifier provided by Google to communicate with the Google application that uses OAuth 2.0 protocol to call Google APIs.
Client Secret	Secret or passphrase that the portal uses to connect to and communicate securely with Google.
API Key	An API key generated by Google for each project and is used to communicate with other APIs enabled in the project.

Option	Description
Extend User Profile Permissions	Select the additional user details you wish to select from the user profile on Google which includes Email Address and Advanced Profile. The login request is restricted to users with accounts in the Google Hosted domains. The user is notified whether he would like to share the requested information (basic and additional details). If the user denies the request, the log in fails.

8. Click **Save**.

The Google plug-in configuration data is displayed on the Google page of the selected portal.

Configure Foursquare Plug-In

To configure the Foursquare plug-in, perform the following steps.

1. Click **Portals**.
2. Click the portal name for which you want to configure the Foursquare plug-in.
3. Click the **Settings** tab. Click the Foursquare icon to enable the Foursquare plug-in for the portal.
4. Click the **Plug-in Configuration** tab. The icons for various plug-ins are seen on this tab.
5. Click the Foursquare icon. The Foursquare icon is available only if the Foursquare plug-in was selected during the portal creation. If not, you must first edit the portal to include the Foursquare plug-in. The Foursquare plug-in configuration details are displayed.
6. Provide the Foursquare plug-in information.

Option	Description
Client ID	Identifier provided by Foursquare to communicate with the Foursquare application that uses OAuth 2.0 protocol to call Foursquare APIs.
Client Secret	Secret or passphrase that the portal uses to connect to and communicate securely with Foursquare.

7. Click **Save**.

The Foursquare plug-in configuration data is displayed on the Foursquare page of the selected portal.

Configure Instagram Plug-In

You can configure Instagram plug-ins on your captive portal. You must have the Administrator role to configure the Instagram plug-ins. Before you configure the Instagram plug-in you must ensure that you have created your application/ project in the social media.

To configure the Instagram plug-in, perform the following steps.

1. Click **Portals**.
2. Click the portal name for which you want to configure the Instagram plug-in.
3. Click the **Settings** tab. Click the Instagram icon to enable the Instagram plug-in for the portal.
4. Click the **Plug-in Configuration** tab.
5. The icons for various plug-ins are seen on this tab.
6. Click the Instagram icon. The Instagram icon is available only if the Instagram plug-in was selected during the portal creation. If not, you must first edit the portal to include the Instagram plug-in. The Instagram plug-in configuration details are displayed.
7. Provide the Instagram plug-in information.

Option	Description
Client ID	Identifier provided by Instagram to communicate with the Instagram application that uses OAuth 2.0 protocol to call Instagram APIs.
Client Secret	Secret or passphrase that the portal uses to connect to and communicate securely with Instagram.

8. Click **Save**.

The Instagram plug-in configuration data is displayed on the Instagram page of the selected portal.

Configure Okta Plug-In

To configure the Okta plug-in, perform the following steps.

1. Click **Portals**.
2. Click the portal name for which you want to configure the Okta plug-in.
3. Click the **Settings** tab. Click the Okta icon to enable the Okta plug-in for the portal.
4. Click the **Plug-in Configuration** tab. The icons for various plug-ins are seen on this tab.
5. Click the Okta icon. The Okta icon is available only if the Okat plug-in was selected during the portal creation. If not, you must first edit the portal to include the Okta plug-in. The Okta plugin details are displayed.
6. Provide the Okta plug-in information.

Option	Description
Client ID	Client ID provided by Okta to communicate with the Okta API.

Option	Description
App Secret	App secret that Guest Manager uses to connect to the Okta application.
Org Domain	The domain where the Okta application is hosted.

7. Click **Save**.

8. Click **Preview Like Page** to preview the 'Like' page to be seen by the guest.

The Facebook plug-in configuration data is displayed on the Facebook page of the selected portal.

Configure Guestbook Plug-In on a Portal

You can also maintain a private guest book and allow users to log in to your Wi-Fi setup with guest user account credentials defined by you. The guest book can also include other user-specific information.

You can select the fields to be displayed while creating guest users in the guestbook for a portal from a predefined list of fields. You can also choose which of these fields should be mandatory while adding or editing guestbook user accounts.

You can enable self-registration so that guest users are able to register themselves on the portal.

You can limit the number of devices through which a guest user can log in to his guest user account. This is optional. The device limit can be set at the Guestbook portal level, guest batch level, and the guest user level. If all or two of these device limits are set, the device limit set at the

user level has the highest priority followed by the device limit at the guest batch level. The device limit at the guestbook portal level has the lowest priority among the three levels.

The User tab consists of the following details:

- User Account
- User Profile
- Quality Of Service Settings

The fields available for the user account, user profile, and Quality Of Service Settings are as follows:

User Account	User Profile	Quality Of Service Settings
Username	First Name	Login Timeout
Password	Last Name	Blackout Time
Timezone	Company	Max. Download Bandwidth
Valid From	Address	Max. Upload Bandwidth
Valid To	Host	
Email	Notes	
Device Limit		
Login Count Limit		
SSID Name		
SSID Key		

The fields Username, Password and Email are displayed, by default. All the three fields are mandatory.

For details on guestbook management, refer to the [Guestbook Management](#) chapter.

To configure the Guestbook plug-in on the portal, you must have the Administrator role.

1. Click **Portals**.
2. Click the portal name for which you want to configure the Guestbook plug-in.
3. Click the **Settings** tab. Click the Guestbook icon to enable the Guestbook plug-in for the portal.
4. Click the **Plug-in Configuration** tab. Click the Guestbook icon. The Guestbook plug-in configuration details are displayed. The Guestbook icon is available only if the Guestbook plug-in was selected during the portal creation. If not, you must first edit the portal to include the Guestbook plug-in.

5. Select the Delivery Medium as Email or SMS or both. You have to configure the Email and SMS accounts if you have selected Email or SMS as your delivery medium. For details on configuring the Email and SMS settings, refer to [Configure SMS and Email settings](#)

6. Select **Self-Registration** check box if you want to allow users to register themselves. For details on self-registration, refer to the [Enable Self-Registration](#) section.
7. Select the account validity in days or hours. This is the duration for which the guest account is valid, starting from the time of activating, registering, or reactivating the account using one-time password.
8. Select the Device Limit. This is the maximum number of devices through which the user can simultaneously log in to Guest Manager. The default value is N/A, which means that there is no limit on the number of devices for simultaneous user login.
9. Select the fields that must be displayed and the required fields in the guest user profile during the creation of the guest user account.
10. Enter or modify the Email Subject and Email Body if you have selected Email as your delivery medium. Ensure that you retain the {username}, {password}, and {expiration_time} parameters.
11. Enter or modify the SMS content if you have selected SMS as your delivery medium. Ensure that you retain the {username}, {password}, and {expiration_time} parameters.
12. Click **Save**.

Enable Self-Registration

Guest users can register themselves by enabling self-registration in the guest book configuration for a portal.


The guest user's email ID can be specified as the user ID when the guest registers himself or herself. If the portal guestbook configuration enables the guest user to set the password, the guest user can also set his password. This password can be set only once and cannot be changed after it has been set by the user. An e-mail with a one-time password (OTP) is sent to the guest user. The user must set the password within 10 minutes of receiving the OTP as the OTP expires in 10 minutes.

If the guest user is not allowed to set the password, the e-mail sent to the user contains a system-generated password that the user must use to log in to the portal.

You can restrict self-registration to a selected set of host domains. When a guest user attempts to register himself or herself, the host's domain name is evaluated against the list of domains configured for the portal. If the host domain matches a domain in the domain list configured under Plug-in Configuration for the portal, the guest Wi-Fi user name, password and expiry date are sent to the host through e-mail. The guest user can obtain his or her login credentials from the host.


A self-registering user is not allowed to set or reset his or her password or reactivate an expired account, when the guest user login is restricted to allowed host domains.

Guest users that register themselves must log in to Guest Manager within the account expiry duration. If they fail to do so, the guest user account expires. You could allow guest users to reactivate their expired accounts. Such guest users can be provided with a link to reactivate their accounts on the splash page. The reactivated account is valid from the date and time of reactivation for the duration based on the Account Validity specified in the Plug-in Configuration tab.


 *Important: If self-registration is disabled after being enabled for a while, the administrator must make sure that the splash page is modified to accommodate this change.*

Enabling Self-Registration


Guest users can register by themselves when you enable self-registration in the guest book configuration for a portal. The guest user's email ID can be specified as the user ID during the registration process.


 *Note: A self-registering user is not allowed to set or reset the password or reactivate an expired account, when the guest user login is restricted to allowed host domains.*

When you enable Self-Registration you can select all or any of the following options:

Option	Description
Host Email Settings	<p>These are the settings required if you have selected Email or SMS as your delivery medium. Refer Wi-Fi Login Experience for Self-Registered Guest Users on page 46 section to know the Wi-Fi login experience for self-registered guest Wi-Fi users based on the options selected for the Guestbook plugin.</p> <p> <i>Note: A self-registering user is not allowed to set or reset his or her password or reactivate an expired account, when the guest user login is restricted to allowed host domains.</i></p>
Domain Restriction	<p>Enter details if you want to restrict self-registration to a selected set of host domains. When a guest user attempts to register, the host's domain name is evaluated against the list of domains configured for the portal. If the host domain matches a domain in the domain list configured under Plug-in Configuration for the portal, the guest Wi-Fi user name, password and expiry date are sent to the host through e-mail. The guest user can obtain the login credentials from the host. This is a mandatory option if you have selected Host Email Settings.</p>
Approver Email	<p>Enter details if you want to send Wi-Fi access approval email to the host email address provided by the guest and to any other approver email addresses that are configured. The request for Wi-Fi access approval email</p>

Option	Description
	will have hyperlinks for approval and rejection and can be used only once by any one of the host or the approvers.
Allow host to approve Wi-Fi access for guest	If you do not select this setting, the host will only receive a notification about a guest requesting internet access. While, the approve/reject authority remains with the configured approvers. If selected, the host will need to approve the guest users for access.
Allow guest Wi-Fi users to skip host's email on splash page	Select this option so that the guest user need not enter the host email address on the splash page. The approval email will be sent to the email addresses configured in Approver Email field. If this option is selected, at least one email address must be added under Approver Email.
Auto Login after Registration/Approval	Select this option to automatically log in the self-registered guest Wi-Fi user for the first time. If this option is selected, the guest Wi-Fi user gets immediate access to Wi-Fi on successful registration. Refer Wi-Fi Login Experience for Self-Registered Guest Users on page 46 section to know the Wi-Fi login experience for self-registered guest Wi-Fi users based on the options selected for the Guestbook plugin.
Show Credentials Page	Select the Show Credentials Page option if you want to redirect the guest user to a page with the login credentials on successful registration. If the Host Email Settings are configured, the self-registered guest is redirected to the credential page after host approval. Refer Wi-Fi Login Experience for Self-Registered Guest Users on page 46 section to know the Wi-Fi login experience for self-registered guest Wi-Fi users based on the options selected for the Guestbook plugin.
Login Count Limit	You can enforce the number of times a guest Wi-Fi user can use the login credentials.

Option	Description
	 <i>Note: If the account is valid and the user has crossed the login count limit, the user will not be allowed to log in.</i>
Allow Self-registered User to Set Password	<p>If you select this option, the guest user can also set the password. This password can be set only once and cannot be changed after it has been set by the user. An e-mail with a one-time password (OTP) is sent to the guest user. The user must set the password within 10 minutes of receiving the OTP as the OTP expires in 10 minutes. If the guest user is not allowed to set the password, the e-mail sent to the user contains a system-generated password that the user must use to log in to the portal.</p>
Enable Forgot Password Link	<p>If you select this option, a Forgot Password link is displayed to the guest users. The check box is disabled if Domain Restriction check box is enabled.</p>
Allow to Activate Expired Account	<p>If you select this option, self-registered guest users will be provided with a link to re-activate their account, if expired. Guest users that register themselves must log in to Guest Manager within the account expiry duration. If they fail to do so, the guest user account expires. You could allow guest users to reactivate their expired accounts. Such guest users can be provided with a link to reactivate their accounts on the splash page. The reactivated account is valid from the date and time of reactivation for the duration based on the Account Validity specified in the Plug-in Configuration tab.</p>

 *Note: If self-registration is disabled after being enabled for a while, the administrator must make sure that the splash page is modified to accommodate this change.*

Self-Registration by SMS

To enable self-registration by SMS and configure the parameters do the following tasks:

1. Click the portal name on which you want to enable self-registration for Guestbook plug-in.

2. Click the **Plug-in Configuration** tab. The icons for various plug-ins are seen on this tab.
3. Click the Guestbook icon. The Guestbook plug-in configuration details are displayed. The Guestbook icon is available only if the Guestbook plug-in was selected during the portal creation. If not, you must first edit the portal to include the Guestbook plug-in.
4. Select the Self Registration check box, if you want to allow a guest to register by himself.
5. Select **SMS**.
6. The SMS/MMS account displays the chosen SMS service for that plugin.
 Note: The Guest user receives an OTP for logging in. The validity of the OTP is 10 minutes.
7. Select the Allow Self-registered User to set password check box if you want the guest user to set his own password when he activates the account. The check box is disabled if Domain Restriction check box is enabled.
8. Select the Enable Forgot Password link check box to display a Forgot Password link to guest users. The check box is disabled if Domain Restriction check box is enabled.
9. Select the **Allow to Activate Expired Account** check box. The check box is disabled if Domain Restriction check box is enabled.
10. Select the account validity in days or hours. This is the duration for which the guest account is valid, starting from the time of activating, registering, or reactivating the account using one-time password.
11. Click **Save**.

Wi-Fi Login Experience for Self-Registered Guest Users

This topic lists the Wi-Fi login experience for self-registered guest Wi-Fi users based on the options selected for the Guestbook plugin.

The following table lists options selected for the Guestbook plugin:

Host Email Settings	Auto Login after Registration/ Approval	Show Credentials Page	Results
Disabled	Enabled	Disabled	The guest user is logged in automatically on successful registration.
Disabled	Enabled	Enabled	The guest user is directed to the credentials page and after clicking Continue , is logged in to the Wi-Fi network.

Enabled

Enabled

Disabled

- If the host approves the request within 5 minutes of the registration, the guest user is logged in to the Wi-Fi network.
- If the host approves the request after 5 minutes, the guest user is redirected to the

Host Email Settings	Auto Login after Registration/Approval	Show Credentials Page	Results
			splash page. The guest user has to enter the credentials received through Email or SMS.
Enabled	Enabled	Enabled	<ul style="list-style-type: none"> If the host approves the request within 5 minutes of the registration, the guest user is directed to the credentials page, and after clicking Continue is logged in to the Wi-Fi network. If the host approves the request after 5 minutes, the guest user is directed to the credentials page. The user must click Login and enter the credentials on the splash page to connect to the Wi-Fi network.
Enabled	Disabled	Disabled	The guest user is successfully registered and the credentials are mailed through the selected medium by Email or SMS.

Configure SMS Plug-In on a Portal

The SMS plug-in enables a guest to obtain an Internet access code through SMS on a mobile/cellphone number and use this code to access the Internet. If the SMS plug-in is configured on the portal, guests can enter the mobile number on which they wish to receive an Internet access code through SMS.

The SMS is sent through an account created on Twilio (<http://www.twilio.com/>), MSG91 (<https://msg91.com/india/>), or a custom service provider and configured in the plug-in.

You must select the SMS plug-in for the portal during portal creation or edit the portal to include the plug-in. You must also create an account in MSG91 and buy SMS or create an account in Twilio and buy numbers or short codes. If you are using any other service provider, ensure that the basic requirements to use the service, such as getting an account subscription, purchasing SMS packs, or procuring numbers or short codes, are met.

To configure the SMS plug-in on the portal, you must have the administrator role.

1. Click **Portals**.

2. Click the portal name for which you want to configure the SMS plug-in.
3. Click the **Settings** tab. Click the SMS icon to enable the SMS plug-in for the portal.
4. Click the **Plug-in Configuration** tab.
5. The icons for various plugins are seen on this tab.

6. Click the SMS icon. If not, you must first edit the portal to include the SMS plug-in. The SMS plug-in configuration details are displayed.
7. Under Service Configuration select the service provider.
8. Based on the service provider selected, provide the appropriate account information.

- For Twilio, provide the following details.

Option	Description
Account SID	The account SID associated with your Twilio account.
Auth Token	The auth token for your Twilio account.
Twilio Number	A number or short code that you have purchased for your Twilio account.

- For MSG91, provide the following details.

Option	Description
Username	The user name for your MSG91 user account.
Password	Password for the MSG91 user account.
Sender ID	A user-defined ID to be used to send SMS to the guest. This ID is used as the sender ID for the SMS. That is, the guest will receive the SMS with sender as this ID. The ID must be of 6 characters in length and can only contain letters from A through Z. For example, ATNSMS.
SMS Route	Whether the SMS should be sent through the Transactional route or the Promotional route. If the SMS contains any promotional content, then it cannot be sent through the Transactional route. If such a message is sent through the Transactional route, the message delivery fails. There are certain policies you must adhere to for sending promotional messages, which you can obtain from the MSG91 Website.

- For Custom service provider, provide the following details.

Option	Description
Method Type	The method type can be either GET, PUT or

POST. When the method is GET, the URL

Option	<p>Description</p> <p>of the SMS endpoint along with the GET parameters as name value pair. When the method type is PUT or POST the parameters will be defined in the response body. The response body may contain information about the users or other parameters.</p>
Service URL	<p>The URL of the SMS endpoint along with the GET parameters as name value pairs. It is mandatory that the URL has <sms_content> and <to_number> tags as placeholders for the fields that represent message content and destination number, respectively. The SMS endpoint</p> <p>For example: <code>https://custom.service.com/sms/?username=johnsmith&password=P@ssw0rd&to=<to_number>&body=<sms_content></code></p> <p>Note: Ensure that you take care of the following:</p> <ul style="list-style-type: none"> • Any invalid characters entered in the API Endpoint URL, for example (\n), will be replaced with '_'. • '#' present in the API Endpoint URL will lead the URL after the "#" to be treated as a fragment. Any variables within the fragment will not be replaced.
Request Headers	<p>The request header contains the parameters in case the method type is GET for the SMS endpoint.</p>
Request Body	<p>The Request Body can be set when method type is POST / PUT. The dynamic parameters (to_number, sms_content) can be included using the tags <to_number> and <sms_content> in the Request Body.</p>
Success Response Codes	<p>This is a comma-separated list of the possible HTTP response codes on successful execution of the API. eg. 200,201.</p>

Provide the SMS settings information.

Option	Description
Validation Endpoint	Select the Validation endpoint when you want to access guest Wi-Fi. The validation tab validates the guest Wi-Fi user before the OTP is sent.
Device Limit	The maximum number of devices through which a guest user can simultaneously log in with a single user account. The default value is N/A, which means that there is no such device limit.
SMS content	The message content for the SMS. Ensure that you include the text ' <code> ' in the message, as shown in the sample message. This is replaced with the code generated for Internet access.
Login Code Length	The number of characters in the code.
Login Code validity Period	The time duration in minutes for which the code is valid.
Max attempts to resend SMS	The maximum number of times the code can be resent to the guest.
Minimum interval to resend SMS	The time interval in seconds after which the portal checks with the guest, if he has not logged in to the Wi-Fi, whether he would like the SMS with the same code to be resent.

9. Click **Save**.

Download SMS Logs

You can download the logs to obtain the detailed information about which code was sent to which number and how many times, the last login status, and other information such as the client and AP MAC address.

To download the SMS logs for specified hours, days or months before Guest Manager system date, do the following:

1. Click Admin and then click **Logs**.
2. Under **SMS Logs**, select **Last** and specify the number of hours, days or months for which you want to download the Wi-Fi access logs. Also select the unit of measurement of time as hours, days or months.
3. Click **Download** to download logs for the specified time duration.

Option	Description
Service Provider	The service provider used to send the SMS. This can be Twilio, MSG91, or a custom service provider.
From	The Twilio number or short code configured or the MSG91 sender ID configured on the plug-in.
Mobile No	The mobile number provided by the guest for receiving the SMS with Internet access code.
Login Code	The generated Internet access code sent through SMS to the mobile number.
Send Count	The number of times the SMS was sent to the mobile number.
Authentication Count	The number of times the mobile number and the Internet access code were used for logging into Wi-Fi. If the mobile number-access code combination was used from multiple clients to access the Internet, then each login is accounted for separately. Also, if the Login Timeout is lesser than the Code Validity Time, then the mobile number-access code combination can be used to log in again into the Wi-Fi after the session times out. In this case, each such login is accounted for separately.
Last Login Status	The value can be 0 or 1. The value 0 indicates the code was not used for authentication. The value 1 indicates the code was used for authentication.
Last Send Error State	The error in SMS delivery to the mobile number, if any. If the last sent SMS was delivered successfully to the mobile number, then this field is blank.
Last Send Time	The time when the last SMS with the Internet access code was sent to the mobile number.
Client MAC List	The list of MAC address of all clients used to generate the Internet access code with the mobile number and MAC address of all clients

Option	Description
	used to access the Internet with the mobile number-access code combination.
AP MAC	The MAC address of the AP (access point) that the clients connected to.
AP SSID Profile	The name of the SSID profile applied on the AP.

Download SMS Logs for a Specific Date Range

You can download SMS logs for a specific date range.


To download the SMS logs for a specific date range, do the following:

1. Click the Admin tab and then click **Logs**.
2. Under **SMS Logs**, select **Custom** and specify the from and to date and time for which you want to download the access logs. Use the calendar icon and clock icon to select the date and time respectively.
3. Click **Download** to download logs for the specified time duration.

Account Health

The health of your MSG91 or Twilio account is displayed under **Test Account Settings** under the Plugin Configuration tab.

You must click the SMS icon to view the SMS configuration details. You can check the account health by clicking **Test Account Health**. You must provide your mobile number and click **Send SMS** to test the account health. Any configuration issues with the account and issues with delivery of the SMS are reflected in the Account Health.

 *Note: The health of the Custom service provider's account can be checked by referring to the service provider's response provided in the **Service Response** text box.*

Configure Web Form Plug-In on a Portal

You can configure the portal such that the guest must provide some personal information before obtaining Internet access. This can be achieved by using the Web Form plug-in. The plug-in obtains the user information and provide Internet access to the guest without any authentication.

This plug-in can be considered as an enhanced form of click-through plug-in, where the guest obtains Internet access without any authentication but has to provide some personal information first. You must select the Web Form plug-in for the portal during portal creation or edit the portal to include the plug-in.

To configure the Web Form plug-in on the portal, you must have the administrator role.

1. Click **Portals**.
2. Click the portal name for which you want to configure the Web Form plug-in.

3. Click the **Settings** tab. Click the Web Form icon to enable the Web Form plug-in for the portal.
4. Click the **Plug-in Configuration** tab. The icons for various plug-ins are seen on this tab.
5. Click the Web Form icon.

The Web Form icon is available only if the Web Form plug-in was selected during the portal creation. If not, you must first edit the portal to include the Web Form plug-in.

The Web Form plugin configuration details are displayed.

6. Provide the timeout interval information.

Option	Description
Username	User name of the guest user
First Name	First name of the guest user.
Last Name	Last name of the guest user.
Gender	Gender of the guest user.
Birth Day	Day of birth of the guest user.
Birth Month	Month of birth of the guest user.
Birth Year	Year of birth of the guest user.
Email	E-mail address of the guest user.
Phone	Phone number of the guest user.
Location	Location of the guest user.

7. **Validation Endpoint** For pre-validating the guest users, customers can select the Validation Endpoint checkbox mentioned in the Third Party Integration step.
8. Select **Passphrase for guest users** to provide a single pre-shared key for all the users to login in the specified splash page.
9. Click **Save**.

The Web Form plug-in is configured.

Configure RADIUS plug-in

With the RADIUS plug-in, guest users can obtain access to the Wi-Fi network by their username and password that is configured on a RADIUS server. Guests are authenticated by the RADIUS server, which informs the AP about the successful login.

To configure the Radius plug-in on the portal, you must have an administrator role.

1. Click **Portals**.
2. Click the portal name for which you want to configure the RADIUS plug-in.
3. Click the **Settings** tab. Click the RADIUS icon to enable the RADIUS plug-in for the portal.

The RADIUS plug-in does not require any further configuration in Guest Manager. You can configure as many plug-ins in Guest Manager, however, RADIUS plug-in is shown on the splash page, only if you have configured the RADIUS settings in the Captive Portal section of the SSID profile in Wireless Manager, else the other configured plug-ins will be shown on the splash page. Refer the Wireless Manager User Guide for more details.

The RADIUS plug-in is mutually exclusive from the other plug-ins.

Configure SSID Profile in Wireless Manager

Deploying your captive portal means ensuring that the guests are redirected to the captive portal splash page when they connect to the access point.

This can be achieved by configuring the SSID profile in Wireless Manager.

1. Log in to the Wireless Manager. Ensure that you log in as an Administrator.
2. Click **Configuration**, and then click **Wi-Fi Access**.
3. Select the SSID profile that you wish to edit and click **Edit**.
4. Expand the **Captive Portal** section.
5. Check the **Enable Captive Portal** option if it is not checked.
6. Select the **External Splash Page for Sign-in/Click-through** option for all the other plug-ins.
7. Select the **External Splash page with RADIUS authentication** option for the Radius plug-in..
8. Enter the splash page URL for your captive portal, check the shared secret option, and enter the shared secret for the captive portal. You can obtain this by clicking the **Show** link on the **Portals** page of Guest Manager. Ensure that the shared secret is same as that provided during the portal creation.



Important: Enter the RADIUS settings if you have opted for the RADIUS plug-in. Refer Wireless Manager. User Guide for more details.

9. Add the following destinations to the Walled Garden.
 - googleapis.com
 - gstatic.com
10. Due to some third-party application issues, some of the plug-ins do not respond properly on Apple iOS clients. To work-around these issues, you must add the following entries in the walled garden for enabling the captive portals to function properly on Apple iOS clients:
 - appleiphonecell.com
 - captive.apple.com
 - itools.info
 - ibook.info
 - airport.us
 - thinkdifferent.us

11. Add the following destinations to the Authenticated sites, so that the guest user renders the Splash page.

Plug-In	Authentication sites
Facebook	<ul style="list-style-type: none">• facebook.com• facebook.net• fbcdn.net
Twitter	<ul style="list-style-type: none">• twitter.com• twimg.com• akamaihd .net
LinkedIn	<ul style="list-style-type: none">• linkedin.com• licdn.com• akamaihd.net
Vimeo	<ul style="list-style-type: none">• vimeo.com• vimeocdn.com• google-analytics.com• akamaihd .net
PollDaddy	polldaddy.com
Youtube	<ul style="list-style-type: none">• youtube.com• googlevideo.com• ytimg.com• google.com• googleusercontent.com (for thumbnail images)• lh5.googleusercontent.com (for thumbnail images)
Instagram	<ul style="list-style-type: none">• instagram.com• akamaihd.net
Foursquare	<ul style="list-style-type: none">• foursquare.com• 4sqi.net
Okta	<ul style="list-style-type: none">• okta.com

12. Click **Save**.

Delete Portal

You can delete a portal if you no longer require it. If you do not want to delete the portal that is currently not required, you can deactivate it.

To deactivate a portal, you must edit the portal. To know more about modifying a portal, see the [Modify Portal](#) section of this chapter.

You must have the Administrator role to delete a portal.

1. Click **Portals**. The tab Guest Manager lists the details of the portals created in your account.
2. In the Portals list, click Delete icon corresponding to the portal that you want to delete. A message prompting you to confirm deletion is displayed.
3. Click **OK** to confirm the portal deletion.

On successful deletion of the portal, the portal details are removed from the table under the Portals section of the Dashboard page.

Integrating Third-Party Endpoints

Integrating with Third-Party endpoints is an available option when a user wants to connect with the guest Wi-Fi.

Third party is here to exchange information between the servers or in simpler words to give or receive data. This two-way communication only happens when the guest Wi-Fi connects. The communication happens by either providing Notification or Validating the request for accessing guest Wi-Fi.

Notification service takes place after the user has logged in to the server while Validation service happens when the user tries to connect to the server for gaining access to the guest Wi-Fi.

Notifying Third-Party Endpoints

Guest Manager provides a mechanism to send real-time guest profile information to third party applications as soon as a guest user accesses a portal and successfully authenticates using one of the plug-ins defined on the portal.

This works for all the plug-ins like SMS, Guestbook, Facebook, LinkedIn, Google, Twitter, Foursquare, Instagram or Clickthrough. The third-party application can store it for future use. This information is sent in the form of key-value pairs and can be stored in any desired format, JSON, XML, or in a database by the third-party application. An appropriate code or module on the third-party application can handle how these key-value pairs must be treated. The information sent to the third-party plugins can be different for different plugins.

Guest Manager provides a predefined set of values for a guest profile based on the information it captures. The individual fields in the guest profile information can be mapped to relevant keys or field names in a third-party application. Keys are the identifiers derived from the third-party application to which you want to associate this information to form a key-value pair.

To send guest profile information to a third-party application, you must configure the third-party endpoints in the Guest Manager. An endpoint is the destination, say a service running on a server, to which the guest profile information is to be sent. When you configure the endpoint, you specify the destination URI, the HTTP method to use for data transfer, and the information (key-value pairs) to be sent to this endpoint. You can add, edit, and delete third-party endpoints from **Admin>Third Party Integration** in Guest Manager.

After you define the endpoints, you must configure them in the respective plug-in QoS on the portal. This helps Guest Manager to send the requested key-value pairs to the appropriate endpoint when a user authenticates from the portal splash page using the plug-in.

Validating With Third-Party Endpoints

To secure the Wi-Fi access granted to the guest users, an extra step for validation has been added. The validation is needed to give the customer an upper hand to allow only authenticated users to have access to the Wi-Fi. So, an external HTTPS endpoint has been added to pre-validate the Wi-Fi access for SMS plugin specifically.

The Validation node validates the data sent from the user side. The user makes a request to login to access Wi-Fi through SMS plugin. Once he does so, he will be sent the request and then the validation process comes into action. It will further make a request to the server and send the guest user details. If the details are successfully authenticated the server sends a successful message 200 OK ensuring that the user will be able to login.

For the Validation node, we will have a Raw body and request headers along with Form-data. Raw body contains the parameters that are to be defined quoted in parentheses. Raw body only emerges when the call is POST call. While Guest Manager server tries to connect with the third party and there is failure in receiving response, it submits the request again after trying for the specified response time. The server can retry to establish connection but the maximum count for retry is only 3. Though there will be no retry for failure in connection establishment.

How does validation work?

The authentication process is done by specifying certain primary parameters which will perform the authentication process. In case of SMS plugin, we need a valid phone number of the user which will receive an OTP or any authenticated code that will validate the user. This can be a combination of two or more than two parameters also. It depends on the customer and its customized splash page.

For example, if a user logs in to the portal and needs to access the guest Wi-Fi in a particular office area. He is then asked to provide a valid phone number and an insurance id. These two unique primary factors define the user and the information is sent to the server. The server then sends an OTP via SMS plug-in to user's phone number. Once the details have been put in, the authentication process takes place and a corresponding success or failure message is thrown based on which the guest user can login.

Add Endpoint

You can add endpoints for third-party integration with Guest Manager. The guest profile information can be sent to the endpoint using the HTTP GET and HTTP POST methods or the redirect method. You can send guest profile information that is collected by Guest Manager and custom data where you can specify your own key and corresponding value for the key.

When adding an endpoint, you must enter at least one notification parameter for the endpoint. If you select the parameter type as **Guest Manager**, you must select a value from the predefined list of values.

If you select the HTTP GET method or redirect, the key-value pairs are appended to the endpoint URL. If you select HTTP POST, the key-value pairs are sent as encoded form-data. A Notification Preview is presented on the bottom of the page as you enter the key-value pairs. This is a preview

of the actual form in which the data will be sent to the third-party application using an HTTP request. The Validation Preview has a header tab and request body. The request body parameter generates only when the call is POST Call and for SMS plugin specifically.

To add an endpoint, perform the following steps.

1. Click the **Admin** tab and then click the **Third Party Integration** tile.
2. Click **Add Endpoint**.
3. Provide the endpoint details.

Option	Description
Service	The service type can be either Validation or Notification.
Name	A user-defined name of the endpoint.
End Point URI	The URI of the endpoint. This is URI to which the key-value pairs will be sent. This could be a service listening for requests and handling the incoming key-value pairs. This is a pre-validation done by the customers.
Description	An optional description about the endpoint.
Method Type	You can select only one method for an endpoint. Select GET, POST, or Redirect option. If you select the HTTP GET method or redirect, the key value pairs are appended to the endpoint URL. If you select HTTP POST, the key-value pairs are sent as encoded form-data. If you select the Redirect option, you must select the third-party endpoint as the Redirect URL in the respective plug-in QoS tab of the portal.
Response Timeout	The timeout, in seconds, for which Guest Manager keeps the data in its cache for sending it to the endpoint. After the timeout period, the data is deleted from the cache. The default value is 10 seconds. Response timeout can have a maximum value of 60 seconds.
Retry Count	This is an integer value that specifies the number of times server will try reconnecting to the third-party server. The maximum retry count is 3.
Notification Preview	Preview the Requested URI and encoded form data.

4. Click **Add new row** to add Notification Parameters as specified in the table below. Repeat this step to add multiple parameters.

Option	Description
Parameter Type	The type of parameter to pass to the third- party application. Select Guest Manager if you want to pass a parameter captured by the Guest Manager. To send custom key-value pairs, select the Custom option. You can

Option	Description
	include a mix for Custom and Guest Manager notification parameters.
Key	The key name to which the corresponding value will be associated. You can define key names that map with the appropriate fields or attributes defined in the third-party application.
Value	The parameter to pass to the third-party application. For a Guest Manager parameter, select a predefined value from the drop-down list that will be mapped to the corresponding key. If the parameter type is Custom, you can enter any string here.

5. For Validation purposes, we will also have a raw body section where we will define the JSON parameters in parentheses. The possible values for the parameters will be as mentioned:

portal_name	visit_count	birth_day	email
ap_mac	private_data	friends_count	languages
first_name	plugin_name	last_visit	birth_month
gender	ap_ssid	membership_id	followers_count
location	last_name	client_mac	date_created
phone_number	picture_url	username	marketing_optin
birth_year	login_location	age_range	

The parameters must be specified within parentheses under raw-body.

Once the SMS login is done, success or failure messages are sent, and the user is granted access.

Edit Endpoint

An endpoint is the destination to which the guest profile information is sent. When you configure the endpoint, you specify the destination URI, the HTTP method to use for data transfer, and the information to be sent to this endpoint.

If you change the HTTP method from Redirect to any other value in the endpoint, then the endpoint is automatically deleted from the Redirect URL of the plug-ins in which it is configured.

To edit an endpoint, perform the following steps:

1. Click the **Admin** tab and then click the **Third Party Integration** tile.

2. Click the name of the endpoint you wish to edit.
The endpoint configuration is displayed.
3. Make the required changes to the endpoint configuration.
4. Click **Save**.

The changes made to the endpoint will take effect in the subsequent guest user authentication using the corresponding plug-in on the portal splash page.

Delete Endpoint

Any third-party endpoint that is no longer required can be deleted from Guest Manager. If you delete an endpoint, it is removed from all the plug-ins on which it was configured.

To delete an endpoint, perform the following steps.

1. Click the **Admin** tab and then click the **Third Party Integration** tile to view a list of existing endpoints.
2. Click the delete icon for the endpoint to delete.
A message prompting you to confirm the deletion appears.
3. Click **Delete** on the confirmation message to delete the endpoint.

The endpoint is deleted and removed from the table on the Third Party Integration page. The endpoint is also removed from the corresponding portal plug-ins.

Configuring Endpoint in Portal Plug-In

After you define a third-party endpoint, it must be configured in the portal plug-in. Guest Manager then sends the notification parameters (guest profile information) configured in the endpoint to the third-party application. For the SMS plugin, validation parameters are sent to a third-party application.

To configure the endpoint in the portal plug-in:

1. Click the **Portals** tab.
2. Click the portal name for which you want to configure the endpoints. The portal details are shown on the screen.
3. Click the Plug-in QoS tab of the portal.
4. Click the edit icon corresponding to the plug-in for which you want to configure the endpoint.
5. Specify the configured endpoint in **Third Party Endpoint (Notify)**.
If you have selected **Redirect** as the Method Type in the endpoint, then select **Third-party** from the Redirect URL drop-down list and then specify the endpoint as the redirect URL.
6. Click the Update icon to save the changes.

Guestbook Management

A guest book is a private list of guest users to whom you have provided access to your Wi-Fi setup. When a user wants to access the Internet through your Wi-Fi setup, they can either login with their social media account or request for a guest user account.

This guest user account information is stored in the guest book of the portal. You can obtain user-specific information and add it to the user profile when creating a user account. To manage the guest book, you must have either the Administrator role or the Operator role.

This chapter covers guestbook management features for Guest Manager users and includes the following topics.

- [*Create Guest Users*](#)
- [*Enable Self-Registration*](#)
- [*Edit Guest Users*](#)
- [*Import Guest Users*](#)
- [*Export Guest Users*](#)
- [*Enable Guest Users*](#)
- [*Disable Guest Users*](#)
- [*Delete Guest Users*](#)
- [*Create Guest Batch*](#)
- [*Edit Guest Batch*](#)
- [*Export Guest Batch*](#)
- [*Delete Guest Batch*](#)
- [*Send Email to Guest Users*](#)
- [*Send Email to Guest Batch*](#)
- [*Sort Guestbook User Information*](#)
- [*Filter Guestbook User Information*](#)
- [*Sort Guest Batch Information*](#)
- [*Filter Guest Batch Information*](#)

To know about configuring the Guestbook for a portal, with reference to what user information can or must be added during guest user creation, see [*Configure Guestbook Plug-In on a Portal*](#).

Create Guest Users


You can create guest user accounts on your portal and provide these details to guest users who want to access the Internet through your Wi-Fi setup

. Alternatively, you can allow guest users to register themselves, and optionally, set their own password. This is called self-registration. For information on enabling self-registration, refer to [Enable Self-Registration](#).

To create a guest user account, perform the following tasks:

1. Click **Portals**.
2. Click the portal name for which you want to configure the Guestbook plug-in. A set of four tabs is displayed. The tabs displayed are Settings, Plug-in Configuration, Plug-in QoS, and Campaigns.
3. Click the **Plug-in Configuration** tab. The icons for various plug-ins are seen on this tab.
4. Click the Guestbook icon. The Guestbook plug-in configuration details are displayed. The Guestbook icon is available only if the Guestbook plug-in was selected during the portal creation. If not, you must first edit the portal to include the Guestbook plug-in.
5. Click the **View Guest Users** link. The Users and Batches tabs are displayed.
6. In the Users tab, click **New User**. The fields for a new user are displayed
7. Provide the user account details.

Option	Description
Username	Name of the guest user account. This is generated randomly. Alternatively, you can enter a username of your choice here.
Password	Password for the guest user account. This can be generated randomly. Click Random to generate a random password. Alternatively, enter a desired password here.
Timezone	Reflects the various timezones that you need to select from.
Expiration Date (valid from and valid to)	Date and time of expiration of guest user account. The guest will not be able to use this account beyond this date. Click the calendar icon and the clock icon to select the expiration date and time respectively.
Email	The e-mail address of the guest user to which the user account information will be sent, if the e-mail service is configured on the Guest Manager account.

Option	Description
Device Limit	The maximum number of devices through which a guest user can simultaneously log in with a single user account. The default value is N/A, which means that there is no such device limit. The device limit can be set at the Guestbook plug-in level, guest batch level and the guest user level. If all or two of these device limits are set, the device limit set at the user level has the highest priority followed by the device limit at the guest batch level. The device limit at the guestbook plug-in level has the lowest priority among the three levels.
Login Count Limit	The number of times the guest user can log in from the splash page using a specific set of credentials. This option is also available when you configure the Guestbook plugin. The value mentioned while creating a guest user takes precedence over the value mentioned while configuring the Guestbook plug-in.  <i>Note: If the account is valid and the user has crossed the login count limit, the user will not be allowed to log in.</i>
SSID Name	SSID Name for the AP that has been assigned.
SSID Key	SSID Key for the AP that has been assigned.

8. Provide the Quality of Service Settings for the portal.

Option	Description
Login Timeout	The time period, in hours: minutes, after which the guest user session for the plug-in expires. The user must re-authenticate with his login credentials if he wants to continue using the Wi-Fi service. A value of zero indicates that the user session does not timeout and the user must explicitly log out from the portal. A non-zero timeout configured on the plug-in takes precedence over the timeout configured on the portal.
Blackout Time	The time period in minutes for which a user cannot log in to the portal after his

Option	Description
	last successful login has timed out. A value of zero indicates no blackout time. The blackout time, including zero value, configured on the plug-in takes precedence over the blackout time configured on the portal.
Max Download Bandwidth	The maximum download bandwidth, in Kbps, for the guest user.
Max Upload Bandwidth	The maximum upload bandwidth, in Kbps, for the guest user.

9. Provide the User Profile information. There are two check boxes available for the available fields. Select the **Display** check box for the fields to display and select the **Mandatory** check box if you want to make the field mandatory. The following table explains the fields available for a user profile:

Option	Description
First name	First name of the guest user. If this is not provided and there is a mention of the variable <i>first_name</i> in the email content, a blank value is seen in the e-mail.
Last name	Last name of the guest user. If this is not provided and there is a mention of the variable <i>last_name</i> in the email content, a blank value is seen in the e-mail.
Company	Company name of the guest user.
Phone	Phone number of the guest user.
Address	Postal address of the guest user.
Host	Name of the guest.
Notes	Notes that you might want to add for this user profile.

10. Click **Save**.

The guest user is created.

11. To add the user and send the guest user account details through e-mail, click **Save and Email**.

The guest user is created and the guest user account details are sent to the configured guest book user.

The guest user is added to the guestbook of the portal.


Edit Guest Users

You can modify guest user accounts on your portal after they are created.

To modify a guest user account, perform the following tasks:

1. Click **Portals**.
2. Click the portal name for which you want to configure the Guestbook plug-in. A set of four tabs is displayed. The tabs displayed are Settings, Plug-in Configuration, Plug-in QoS, and Campaigns.
3. Click the **Plug-in Configuration** tab. The icons for various plug-ins are seen on this tab.
4. Click the Guestbook icon. The Guestbook plug-in configuration details are displayed. The Guestbook icon is available only if the Guestbook plug-in was selected during the portal creation. If not, you must first edit the portal to include the Guestbook plug-in.
5. Click the **View Guest Users** link. The Users and Batches tabs are displayed.
6. In the **Users** tab, click the username link for the user to edit.
7. Provide the new user account details in the User Account

tab. Option	Description
Username	Name of the guest user account.
Password	Password for the guest user account.
Expires At	Date and time of expiration of guest user account. The guest will not be able to use this account beyond this date. Click the calendar icon and the clock icon to select the expiration date and time respectively.
Email	The e-mail address of the guest user to which the user account information will be sent, if the e-mail service is configured on the Guest Manager account.
Device Limit	The maximum number of devices through which a guest user can simultaneously log in with a single user account. The default value is N/A, which means that there is no such device limit. The device limit can be set at the Guestbook portal level, guest batch level and the guest user level. If all or two of these device limits are set, the device limit set at the guest user level has the highest priority followed by the device limit at the guest batch level. The device limit at the guestbook portal level has the lowest priority among the three levels.

Option	Description
Login Count Limit	<p>The number of times the guest user can log in from the splash page using a specific set of credentials. This option is also available when you configure the Guestbook plugin. The value mentioned while creating a guest user takes precedence over the value mentioned while configuring the Guestbook plug-in.</p> <p> <i>Note: If the account is valid and the user has crossed the login count limit, the user will not be allowed to log in.</i></p>
SSID Name	SSID Name for the AP that has been assigned.
SSID Key	SSID Key for the AP that has been assigned.
8. Provide the Quality of Service Settings.	
Option	Description
Login Timeout	<p>The time period, in hours: minutes, after which the guest user session for the plug-in expires. The user must re-authenticate with his login credentials if he wants to continue using the Wi-Fi service. A value of zero indicates that the user session does not timeout and the user must explicitly log out from the portal. A non-zero timeout configured on the plug-in takes precedence over the timeout configured on the portal.</p>
Blackout Time	<p>The time period in minutes for which a user cannot log in to the portal after his last successful login has timed out. A value of zero indicates no blackout time. The blackout time, including zero value, configured on the plug-in takes precedence over the blackout time configured on the portal.</p>
Max Download Bandwidth	The maximum download bandwidth, in Kbps, for the guest user.
Max Upload Bandwidth	The maximum upload bandwidth, in Kbps, for the guest user.
9. Provide the User Profile information.	

Option	Description
First name	First name of the guest user. If this is not provided and there is a mention of the variable <i>first_name</i> in the e-mail content, a blank value is seen in the e-mail.
Last name	Last name of the guest user. If this is not provided and there is a mention of the variable <i>last_name</i> in the e-mail content, a blank value is seen in the e-mail.
Company	Company name of the guest user.
Address	Postal address of the guest user.
Host	Name of the guest.
Notes	Notes that you might want to add for this user profile.

The fields displayed and the required fields in the user profile are configured in the guestbook plug-in of the portal.

10. Click **Save**. To modify the user information and send the updated guest user account details through e-mail, click **Save and Email**.

The guest user account information is updated in the guestbook of the portal.

Import Guest Users

You can import guest user accounts from a CSV file in to your portal. A sample CSV file is shown

Username	Password	First Name	Last Name	Email	Departme	Company	Work Pho	Home Phc	Mobile Ph	Address	City	State	Country	Zip
conference20	Zwqjepe	John	Doe	jdoe@ent.com			304-890-8877			12, Chagri	Beachwood	CA	USA	12345
conference19	SJEWhde	Will	Smith	wsmith@ent.com			509-902-3333			202, Niaga	Niagara Falls	NY	USA	34567
conference18	Wkjdpqe	Diane	Woods	dwoods@ent.com						396, Frami	Boston	MA	USA	30512

below:



Important: The CSV file to be imported should contain the data in the format as seen above.

The field names seen for the personal and business information of the guest user must be present in the first row of the CSV file.

If any of the fields have been specified as mandatory fields under **Portals > Guestbook > Configuration**, the respective values for these fields must be present for correct import of the data from the CSV file.

To import guest user accounts, perform the following tasks:

1. Click **Portals**.
2. Click the portal name for which you want to configure the Guestbook plug-in. A set of four tabs is displayed. The tabs displayed are Settings, Plug-in Configuration, Plug-in QoS, and Campaigns.
3. Click the **Plug-in Configuration** tab. The icons for various plug-ins are seen on this tab.

4. Click the Guestbook icon. The Guestbook plug-in configuration details are displayed. The Guestbook icon is available only if the Guestbook plug-in was selected during the portal creation. If not, you must first edit the portal to include the Guestbook plug-in.
5. Click the **View Guest Users** link. The Users and Batches tabs are displayed.
6. In the Users tab, select **Import User(s)** from the **More** list.
7. Browse and select the required CSV file.
8. Click **Import**. To import the users and send an e-mail with the account information to the respective users, whose e-mail address is available in the imported list, click **Import and Email Users**.

The guest user accounts from the CSV file are added to the guestbook of the portal.

Export Guest Users

You can export one or more guest user accounts in your portal to a CSV file.

To export guest user accounts, perform the following tasks:

1. Click **Portals**.
2. Click the portal name for which you want to configure the Guestbook plug-in. A set of four tabs is displayed. The tabs displayed are Settings, Plug-in Configuration, Plug-in QoS, and Campaigns.
3. Click the **Plug-in Configuration** tab. The icons for various plug-ins are seen on this tab.
4. Click the Guestbook icon. The Guestbook plug-in configuration details are displayed. The Guestbook icon is available only if the Guestbook plug-in was selected during the portal creation. If not, you must first edit the portal to include the Guestbook plug-in.
5. Click the **View Guest Users** link. The Users and Batches tabs are displayed.
6. If you want to export only specific user accounts, then you must first select the user accounts.
7. In the Users tab, select **Export Selected User(s)** from the **More** list. If you want to export all guest user accounts, select **Export All Users** from the **More** list.

The guest user accounts are exported to a CSV file, users.csv, and downloaded on to your computer device.

Enable Guest Users

You can enable guest user accounts that are created on your portal. Guest user accounts that are currently not required can be disabled and re-enabled at a later time.

To enable one or more guest user accounts, perform the following tasks:

1. Click **Portals**.
2. Click the portal name for which you want to configure the Guestbook plug-in. A set of four tabs is displayed. The tabs displayed are Settings, Plug-in Configuration, Plug-in QoS, and Campaigns.
3. Click the **Plug-in Configuration** tab. The icons for various plug-ins are seen on this tab.

4. Click the Guestbook icon. The Guestbook plug-in configuration details are displayed. The Guestbook icon is available only if the Guestbook plug-in was selected during the portal creation. If not, you must first edit the portal to include the Guestbook plug-in.
5. Click the **View Guest Users** link. The Users and Batches tabs are displayed.
6. In the Users tab, select the disabled guest user accounts that you want to re-enable.
7. Select **Enable User(s)** from the **More** list. The guest user accounts are enabled.

Disable Guest Users

You can disable guest user accounts that are created on your portal. Guest user accounts that are currently not required can be disabled and re-enabled at a later time.

To disable one or more guest user accounts, perform the following tasks:

1. Click **Portals**.
2. Click the portal name for which you want to configure the Guestbook plug-in. A set of four tabs is displayed. The tabs displayed are Settings, Plug-in Configuration, Plug-in QoS, and Campaigns.
3. Click the **Plug-in Configuration** tab. The icons for various plug-ins are seen on this tab.
4. Click the Guestbook icon. The Guestbook plug-in configuration details are displayed. The Guestbook icon is available only if the Guestbook plug-in was selected during the portal creation. If not, you must first edit the portal to include the Guestbook plug-in.
5. Click the **View Guest Users** link. The Users and Batches tabs are displayed.
6. In the Users tab, select the active guest user accounts that you want to disable.
7. Select **Disable User(s)** from the **More** list. The guest user accounts are disabled.

Delete Guest Users

You can delete guest user accounts from your guestbook for the portal when they are no longer required.

To delete guest user accounts, perform the following steps:

1. Click **Portals**.
2. Click the portal name for which you want to configure the Guestbook plug-in. A set of four tabs is displayed. The tabs displayed are Settings, Plug-in Configuration, Plug-in QoS, and Campaigns.
3. Click the **Plug-in Configuration** tab. The icons for various plug-ins are seen on this tab.
4. Click the Guestbook icon. The Guestbook plug-in configuration details are displayed. The Guestbook icon is available only if the Guestbook plug-in was selected during the portal

creation. If not, you must first edit the portal to include the Guestbook plug-in.

5. Click the **View Guest Users** link. The Users and Batches tabs are displayed.

6. In the Users tab, select the guest user accounts that you want to delete.
7. Select **Delete User(s)** from the **More** list.

The guest user accounts are deleted from the guestbook.

You can also delete individual guest user accounts by clicking the delete icon corresponding to the guest user in the table displayed on the Guestbook page of the portal.

Change Account Expiry for Guest User

You can change the account expiry date and time for a guest user.

To change the account expiry for a guest user, perform the following steps.

1. Click **Portals**.
2. Click the Plug-in **Configuration** tab. The icons for various plug-ins are seen on this tab.
3. Click the View Guest Users link.
4. Select the check box for the guest user whose account expiry is to be changed.
5. Click **More > Set Account Validity**.
6. Select the new date and time for account expiry and click Save. The new date and time of account expiry for the guest user is set.

Create Guest Batch


When you want to create a large number of guest user accounts for specific events, say a seminar or an event you have organized and want to provide Wi-Fi access to the guests, creating individual guest user accounts could take a lot of effort and time.

. In such cases, you can create a batch of guest user accounts.

To create a batch of guest user accounts, perform the following tasks:

1. Click **Portals**.
2. Click the portal name for which you want to configure the Guestbook plug-in. A set of four tabs is displayed. The tabs displayed are Settings, Plug-in Configuration, Plug-in QoS, and Campaigns.
3. Click the **Plug-in Configuration** tab. The icons for various plug-ins are seen on this tab.
4. Click the Guestbook icon.
The Guestbook plug-in configuration details are displayed. The Guestbook icon is available only if the Guestbook plug-in was selected during the portal creation. If not, you must first edit the portal to include the Guestbook plug-in.
5. Click the **View Guestbook** link. The Users and Batches tabs are displayed.
6. In the Batches tab, click **New Batch**. The Batch list is displayed.
7. Provide the user batch information.

Option	Description
Username Prefix	Prefix for the guest user accounts batch. This is applied to all the users in the batch.
Batch Type	Select Random Users to generate a random users in the guest user batch. Alternatively, select Incrementing Users to generate user names with the specified prefix and an incremental index in the batch.
Username Length	Length of the randomly generated username. This field is seen only if you select Random Users.
Password Length	Length of the password.
Start Index	The starting number that is appended for an incrementing user batch. This field is seen only if you select Incrementing users.
Number of Users	The number of users to create in the batch.
Expires At	Date and time of expiration of guest user accounts in the batch. The guests will not be able to use this account beyond this date. Use the calendar icon and the clock icon to select the expiration date and time respectively.
Batch Description	Description of the batch. Any text giving details of what the batch represents can be entered here. For instance, if the batch has been created for a conference, you can specify the details of the conference here.
Device Limit	The maximum number of devices through which a guest user can simultaneously log in with a single user account. The default value is N/A, which means that there is no such device limit. The device limit can be set at the Guestbook portal level, guest batch level and the guest user level. If all or two of these device limits are set, the device limit set at the guest user level has the highest priority followed by the device limit at the guest batch level. The device limit at the guestbook portal level has the lowest priority among the three levels.

Option	Description
Login Count Limit	<p>The number of times the guest user can log in from the splash page using a specific set of credentials. This option is also available when you configure the Guestbook plugin. The value mentioned while creating a guest batch takes precedence over the value mentioned while configuring the Guestbook plug-in.</p> <p> <i>Note: If the account is valid and the user has crossed the the login count limit, the user will not be allowed to log in.</i></p>

8. Configure the Quality of Service Settings.

Option	Description
Login Timeout	<p>The time period, in hours:minutes, after which the guest user session for the plug-in expires. The user must re-authenticate with his login credentials if he wants to continue using the Wi-Fi service. A value of zero indicates that the user session does not timeout and the user must explicitly log out from the portal. A non-zero timeout configured on the plug-in takes precedence over the timeout configured on the portal.</p>
Blackout Time	<p>The time period in minutes for which a user cannot log in to the portal after his last successful login has timed out. A value of zero indicates no blackout time. The blackout time, including zero value, configured on the plug- in takes precedence over the blackout time configured on the portal.</p>
Max Download Bandwidth	<p>The maximum download bandwidth, in Kbps, for the guest user.</p>
Max Upload Bandwidth	<p>The maximum upload bandwidth, in Kbps, for the guest user.</p>

9. Click **Save**.

The batch of guest user accounts is created in the guestbook of the portal. The guest user accounts created by the batch can be viewed by clicking **Users** on the Guestbook page.

Edit Guest Batch

After creating a batch, you can edit some of the batch information.

To edit a batch of guest user accounts, perform the following tasks:


1. Click **Portals**.
2. Click the portal name for which you want to configure the Guestbook plug-in. A set of four tabs is displayed. The tabs displayed are Settings, Plug-in Configuration, Plug-in QoS, and Campaigns.
3. Click the **Plug-in Configuration** tab. The icons for various plug-ins are seen on this tab.
4. Click the Guestbook icon. The Guestbook plug-in configuration details are displayed. The Guestbook icon is available only if the Guestbook plug-in was selected during the portal creation. If not, you must first edit the portal to include the Guestbook plug-in.
5. Click the View Guestbook link. The Users and Batches tabs are displayed.
6. In the Batches tab, click the Batch ID for the batch to modify.
7. Update the user batch information.

Option	Description
Expires At	Date and time of expiration of guest user accounts in the batch. The guests will not be able to use this account beyond this date. Click the calendar icon and clock icon to select the expiration date and time respectively.
Batch Description	Description of the batch. Any text giving details of what the batch represents can be entered here. For instance, if the batch has been created for a conference, you can specify the details of the conference here.
Device Limit	The maximum number of devices through which a guest user can simultaneously log in with a single user account. The default value is N/A, which means that there is no such device limit. The device limit can be set at the Guestbook portal level, guest batch level and the guest user level. If all or two of these device limits are set, the device limit set at the user level has the highest priority followed by the device limit at the guest batch level. The device limit at the guestbook portal level has the lowest priority among the three levels.
Login Count Limit	The number of times the guest user can log in from the splash page using a specific set of credentials. This option is also available when

Option

Description

you configure the Guestbook plugin. The value mentioned while creating a guest user takes precedence over the value mentioned while configuring the Guestbook plug-in. The range lies between 1 to 10000.

 *Note: If the account is valid and the user has crossed the login count limit, the user will not be allowed to log in.*

8. Update Quality of Service Settings, if required.

Option

Description

Login Timeout

The time period, in hours: minutes, after which the guest user session for the plug-in expires. The user must re-authenticate with his login credentials if he wants to continue using the Wi-Fi service. A value of zero indicates that the user session does not timeout and the user must explicitly log out from the portal. A non-zero timeout configured on the plug-in takes precedence over the timeout configured on the portal.

Blackout Time

The time period in minutes for which a user cannot log in to the portal after his last successful login has timed out. A value of zero indicates no blackout time. The blackout time, including zero value, configured on the plug- in takes precedence over the blackout time configured on the portal.

Max Download Bandwidth

The maximum download bandwidth, in Kbps, for the guest user.

Max Upload Bandwidth

The maximum upload bandwidth, in Kbps, for the guest user.

9. Click **Save**.

The batch of guest user accounts is created in the guestbook of the portal. The guest user accounts created by the batch can be viewed by clicking **Users** on the Guestbook page.

Export Guest Batch

You can export the guest user accounts created by a batch to a CSV file.

To export guest user accounts of a batch, perform the following tasks:

1. Click **Portals**.
2. Click the portal name for which you want to configure the Guestbook plug-in. A set of four tabs is displayed. The tabs displayed are Settings, Plug-in Configuration, Plug-in QoS, and Splash Page.
3. Click the **Plug-in Configuration** tab. The icons for various plug-ins are seen on this tab.
4. Click the Guestbook icon. The Guestbook plug-in configuration details are displayed. The Guestbook icon is available only if the Guestbook plug-in was selected during the portal creation. If not, you must first edit the portal to include the Guestbook plug-in.
5. Click the View Guestbook link. The Users and Batches tabs are displayed.
6. In the Batches tab, select the batch you want to export from the table displayed on the page.
7. Select **Export** from the **More** list.

The guest user accounts created by the batch are exported to a CSV file, *users.csv*, and downloaded on to your computer device.

Delete Guest Batch

You can delete a batch of guest user accounts from your guestbook for the portal when they are no longer required.

To delete a batch of guest user accounts, perform the following tasks.

1. Click **Portals**.
2. Click the portal name for which you want to configure the Guestbook plug-in. A set of four tabs is displayed. The tabs displayed are Settings, Plug-in Configuration, Plug-in QoS, and Splash Page.
3. Click the **Plug-in Configuration** tab. The icons for various plug-ins are seen on this tab.
4. Click the Guestbook icon. The Guestbook plug-in configuration details are displayed. The Guestbook icon is available only if the Guestbook plug-in was selected during the portal creation. If not, you must first edit the portal to include the Guestbook plug-in.
5. Click the View Guestbook link. The Users and Batches tabs are displayed.
6. In the Batches tab,
7. Select the batches that you want to delete.
8. Select **Delete** from the **More Actions** list.
9. Click **OK** to confirm the batch deletion.

The batches and the corresponding guest user accounts are deleted from the guestbook.

You can also delete an individual batch and the guest user accounts created by the batch by clicking the delete icon corresponding to the batch in the table displayed on the Guestbook page of the portal.

Send Email to Guest Users

You can also send e-mail to a list of guest users and guest batches at the same time by using the **Send Email** option from the **More Actions** list.

To send e-mail to multiple guest users at the same time

1. Click **Portals**.
2. Click the portal name for which you want to configure the Guestbook plug-in. A set of four tabs is displayed. The tabs displayed are Settings, Plug-in Configuration, Plug-in QoS, and Splash Page.
3. Click the **Plug-in Configuration** tab. The icons for various plug-ins are seen on this tab.
4. Click the Guestbook icon. The Guestbook plug-in configuration details are displayed. The Guestbook icon is available only if the Guestbook plug-in was selected during the portal creation. If not, you must first edit the portal to include the Guestbook plug-in.
5. Click the View Guestbook link. The Users and Batches tabs are displayed.
6. In the Users tab, select the guest user accounts from the table displayed.
7. Select **Send Email** from the **More** list.
8. Click **OK** to confirm the send e-mail action.

An e-mail with the account information is sent to a guest user only if the corresponding e-mail address is provided for the guest user account.

Send Email to Guest Batch

You can also send e-mail to a list of guest users and guest batches at the same time by using the **Send Email** option from the **More Actions** list.

To send e-mail to one or more batch of users at the same time

1. Click **Portals**.
2. Click the portal name for which you want to configure the Guestbook plug-in. A set of four tabs is displayed. The tabs displayed are Settings, Plug-in Configuration, Plug-in QoS, and Splash Page.
3. Click the **Plug-in Configuration** tab. The icons for various plug-ins are seen on this tab.
4. Click the Guestbook icon. The Guestbook plug-in configuration details are displayed. The Guestbook icon is available only if the Guestbook plug-in was selected during the portal creation. If not, you must first edit the portal to include the Guestbook plug-in.
5. Click the View Guestbook link. The Users and Batches tabs are displayed.
6. In the Batches tab, select the guest batches from the table displayed.
7. Select **Send Email** from the **More** list.

8. Click **OK** to confirm the send e-mail action.

For a guest batch, you must manually add the e-mail address for each user account created by a guest batch before sending e-mail to the batch of guest user accounts.


Configure Email Content

You can configure the content of the email. The body of the e-mail comprises a subject and the actual message.

Typically, the message would have a personalized greeting, the login credentials, and a message for the user.

You can include the following pre-defined variables in curly brackets in the e-mail content.

- **first_name** - The value for this variable is derived from the First Name field of the guestbook user profile. If this is an optional field and has not been specified, a blank value is passed to the email content.
- **last_name** - The value for this variable is derived from the Last Name field of the guestbook user profile. If this is an optional field and has not been specified, a blank value is passed to the email content.
- **username** - The value for this variable is derived from the UserName field of the guestbook user account information.
- **password** - The value for this variable is derived from the Password field of the guestbook user account information.
- **expiration_time** - The value for this variable is derived from the Expires At field of the guestbook user account information.

 *Important: The {first_name} and the {last_name} have to be specified manually in the email body. The {username}, {password} and {expiration_time} are present, by default, in the message body.*

You can format the message contents using the formatting tool bar seen above the message body.

You can insert an image in the message content by clicking the  icon. You can insert a

hyperlink in the message content by clicking the  icon.

The following image displays a sample email content.

Sort Guest Batch Information

The list of guest batches in a guest book is visible in a tabular format under the Users tab. You can sort this information on different fields.

To sort a Guest batch, do the following tasks:

1. Click the name of the field on which you want to sort the information. The field is alphabetically

sorted.

2. To reverse the sort order, click the field name again.

Sort Guestbook User Information

The list of guest users in a guest book is visible in a tabular format under the Users tab. You can sort this information on different fields.

To sort the guest user information, do the following tasks:

1. Click the name of the field on which you want to sort the information.
2. To reverse the sort order, click the field name again.

Filter Guest Batch Information

You can filter guest batch information on a field to view information that matches the filter applied to a field in the Batches tab for a guest book.

To filter guest batch information, perform the following steps.

1. Click **Portals**.
2. Click the Portal name and click the **Plug-in Configuration** tab.
3. Click **Guestbook** and then click the **View Guest Users** link.
4. Click the down arrow next to the field name on the **Guestbook>Batches** tab.
5. Click the Filter option. A small window appears for the filter text.
6. Select the filter criterion and enter the substring or string on which you want to filter the information in the text box below the filter criterion.
7. Click the Filter button.

The information is filtered based on the substring or the string entered.

To clear the filter applied to the guest batch information, perform the following steps.

8. Click **Portals**.
 9. Click the Portal name and click the **Plug-in Configuration** tab.
 10. Click **Guestbook** and then click the **View Guest Users** link.
 11. Click the down arrow next to the field name on the **Guestbook>Batches** tab.
 12. Click the Filter option for the field on which the filter is applied. A small window appears for the filter text.
 13. Click the Clear button.
- The filter is removed.

Filter Guestbook User Information

You can filter guest user information on a field to view information that matches the filter applied to

a field in the Users tab for a guestbook

To filter guest user information, perform the following steps.

1. Click **Portals**.
2. Click the Portal name and click the **Plug-in Configuration** tab.
3. Click Guestbook and then click the **View Guest Users** link.
4. Click the down arrow next to the field name on the **Guestbook>Users** tab.
5. Click the Filter option. A small window appears for the filter text.
6. Select the filter criterion and enter the substring or string on which you want to filter the information in the text box below the filter criterion.
7. Click the Filter button. The information is filtered based on the substring or the string entered.
To clear the filter applied to the guest user information, perform the following steps.
8. Click **Portals**.
9. Click the Portal name and click the **Plug-in Configuration** tab.
10. Click Guestbook and then click the **View Guest Users** link.
11. Click the down arrow next to the field name on the **Guestbook>Users** tab.
12. Click the Filter option for the field on which the filter is applied. A small window appears for the filter text.
13. Click the Clear button.
The filter is removed.

Set Password

You may set password in a single instance for selected guest users.

To set a common password for the guest user accounts, perform the following steps:

1. Click **Portals**.
2. Click the portal name for which you want to configure the Guestbook plug-in. A set of four tabs is displayed. The tabs displayed are Settings, Plug-in Configuration, Plug-in QoS, and Splash Page.
3. Click the **Plug-in Configuration** tab. The icons for various plug-ins are seen on this tab.
4. Click the Guestbook icon. The Guestbook plug-in configuration details are displayed. The Guestbook icon is available only if the Guestbook plug-in was selected during the portal creation. If not, you must first edit the portal to include the Guestbook plug-in.
5. Click the **View Guest Users** link. The Users and Batches tabs are displayed.
6. In the Users tab, select the guest user accounts that you want to set the password.
7. Select **Set Password** from the **More** list.
A common password is set for the selected users.

Dashboard

The dashboard offers a graphical view of the daily, weekly and monthly statistics about the people visible in and around the store.

These people use Wi-Fi enabled devices. They might or might not be using the guest Wi-Fi services offered by your store.


This chapter covers the following topics.

- [About Dashboard](#)
- [Dashboard Widgets](#)
- [Download Dashboard as PDF File](#)

About Dashboard

The dashboard provides a quick overview of the statistics related to demographic data about visitors using guest Wi-Fi, store footfall, dwell time and new users versus repeat users for the last day, last week, and the last month for the location selected in the location tree.

The dashboard provides a quick overview of the statistics related to demographic data about visitors using guest Wi-Fi, store footfall, male users vs female users, dwell time and new users versus repeat users for the last day, last week and the last month for the location selected in the

location tree. You can show or hide the location tree by clicking the  Description: location.png icon on the top left side of the location tree. You can search for a location by typing the search string in the search box above the location tree.

You must be an analyst or an administrator to view the dashboard. You are presented with the last day dashboard when you log in to Guest Manager as an analyst or an administrator. You can view the last week or last month statistics on the dashboard by clicking **Last Week** or **Last Month** respectively.

For each of the statistics, a percentage rise or fall is presented in comparison with the data for the previous day, week or month. Green and red arrowheads represent the upward and downward trend in percentage respectively.

If you are viewing the last day statistics, the trend is for the last day as compared to the previous working day. This is a percentage increase or decrease for the respective number of guest users for the last day as compared to the day before the last day.

If you are viewing the last week statistics, the trend is for the last week as compared to the statistics for the week before the last week.

The graphs can be useful to observe trends such as customer loyalty, new customers, average dwell time in the store etc. Management decisions can be taken based on these trends. The data

available is for conversion chart, Wi-Fi users, Male users vs Female users, New Vs Repeat users, and Dwell Time.

- The Conversion chart displays the percentage of users which entered the store to use the Wi-Fi as to guest users accessing Wi-Fi from outside. The conversion ratio is calculated and displayed.
- Demographics shows us the percentage of male and female users for different age bars.
- New vs Repeat users shows the percentage of users who were new to the store or who have frequently visited the store. The repeated user frequency is also shown through a pie chart. The pie chart depicts the most likely event of a user to visit the store again. New vs Repeat users is the ratio of total time span from current date to first time he visited the store as to the number of time he has visited the store in between.
- Dwell time displays an average dwell time of the users along with the percentage of guest users who used the Wi-Fi for particular durations.

The statistics seen on the dashboard are for the selected location. When a location has sub-locations represented by sub-folders, the aggregated user data for the selected location having sub-locations is displayed.

You can define a schedule to generate location-specific dashboard report for the last day, last week or last month.

A date is displayed at the top of the dashboard. This is the last date for which the data is available. The duration that you select for the charts is with reference to this date as the last date. For instance, if you choose to view dashboard data for the last week when the data availability date is June 26, 2018, dashboard data is displayed for the week June 20, 2018 to June 26, 2018. You can also select a custom date for the dashboard data. The charts are then populated for dates based on the custom date as the last date. If you choose to view dashboard data for the last week and the custom date is June 22, 2018, the dashboard data is displayed for the week June 16, 2015 to June 22, 2018. The custom date can be a date before the data availability date or the same as the data availability date.

To reset the custom date back to the default data availability date, click the date and then click the *Reset to Default* link.

Dashboard Widgets

The dashboard has 5 widgets. They are as follows.

Conversion: This widget presents the statistics related to the people with Wi-Fi enabled devices, but not connected to the Wi-Fi service offered by the store. The Conversion widget presents the total number of people with Wi-Fi enabled devices in and around the store, the number of visitors with Wi-Fi enabled devices present inside the store. The percentage of the storefront conversion displayed in this widget represents the number of visitors inside the store as compared to the number of people inside and around the store.

The following image illustrates the **Conversion** widget.

Conversion



Figure 2: Conversion

Wi-Fi users: The Wi-Fi Users widget presents the total visible visitors inside and outside the store, the total users who have used Wi-Fi, and the percentage of the visitors using the guest Wi-Fi out of the total users.

The following image illustrates the **Wi-Fi Users** widget.

Wi-Fi Users



Figure 3: Wi-Fi Users

Demographics: The Demographics widget displays the percentage of male users and the percentage of female users who are using the guest Wi-Fi through a social media plugin. This widget also presents a bar graph with an age group wise percentage for each gender. This data is derived from the social media sites used by the guest Wi-Fi users to log in to Guest Manager. This data is provided directly by the user in case of Web Form.

The following image illustrates the **Demographics** widget.

Demographics



Figure 4: Demographics

New Vs Repeat Users: The New Vs Repeat Users widget displays the total number of Wi-Fi users using the guest Wi-Fi, along with the percentage of new and repeat Wi-Fi users. It also presents the average number of days between repeat visits for repeat users.

The following image illustrates the **New Vs Repeat Users** widget.

New Vs. Repeat Users



Figure 5: New Vs. Repeat Users

Dwell Time: Dwell time is the time for which a user is visible to the access points installed in the store. The dwell time widget displays a bar graph of the percentage of visitors for different time-ranges. The unit of measurement for the time range is minutes. The widget also displays the average dwell time in minutes.

The following image illustrates the **Dwell Time** widget.

Dwell Time

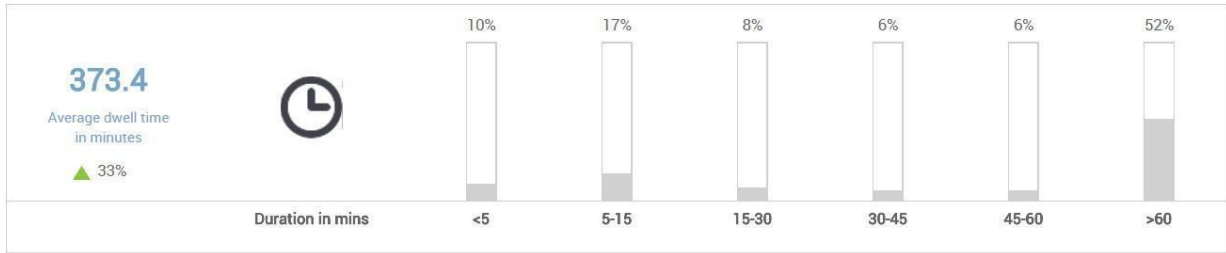



Figure 6: Dwell Time

Download Dashboard as PDF File

The dashboard contents for a particular day, week or month can be saved for future use. The dashboard can be downloaded as a PDF file. The contents of the PDF file are exactly the same as that of the dashboard.

You must be an analyst or an administrator to download the dashboard as a PDF file.

To download the dashboard for the last day, last week or last month, perform the following steps.

1. Click the Dashboard icon and then click **Last Day**, **Last Week**, or **Last Month**.
2. Click . The Schedule Report and Download Report buttons appear.
3. Click **Download Report** to download the dashboard in PDF format.

Manage Dashboard Report Schedules

You can schedule the automatic generation of the dashboard for the last day, last week or last month for a specific location. The output is a dashboard report in PDF format.

This file can be sent over e-mail to any number of e-mail addresses mentioned in the report schedule. The PDF report file is zipped before it is attached to the e-mail.

To ensure delivery of e-mails, you must configure the e-mail settings appropriately in **Admin > Settings > Email Settings**. The e-mail settings must be configured in one of the following ways.

- If the Email Service Type is **SMTP Configuration**, the **From Email ID** and **Return Email ID** must be specified.
- If the Email Service Type is **Email**, the **Return Email ID** must be specified.

If the e-mail settings are not configured correctly, the reports are not saved for delivery and an error occurs.

Schedule Dashboard Report

The schedule for a dashboard report can be a one-time schedule or a recurring schedule.

There are two ways to schedule a dashboard report.

- From the **Dashboard** tab
- From the **Reports** tab

Schedule One-Time Dashboard Report from the Dashboard tab


If you wish to generate the dashboard report only once, you can use the One Time option. If you activate the schedule while adding it, the report is generated per the given date and time. If the schedule is not activated, the report is not generated unless you activate the schedule.

You must be an analyst or administrator to schedule dashboard reports.

If you have already selected a location and are viewing the dashboard for the location and wish to define a schedule, you can add the schedule through the dashboard.



Alternatively, if you want to define a schedule for a location, you must first select the location and then navigate to the Reports tab (or the Dashboard tab) and add the schedule for the dashboard report for this location.

To add the schedule from the Dashboard tab, perform the following steps.

1. Click **Dashboard** and then click the  icon. The Schedule Report and Download Report buttons appear.
2. Click **Schedule Report**.

3. Under New Reporting Schedule, configure the schedule for the

report. Option	Description
Report Name	The name for the schedule
Email Addresses	A comma-separated list of e-mail addresses where the dashboard report is to be sent.
Duration	The duration for the dashboard. Select the Last Week option to schedule e-mail delivery for the last week dashboard report. Select the Last Day option to schedule for e-mail delivery for the last day dashboard report. Select the Last Month option to schedule e-mail delivery for the last month dashboard report.
Schedule Active	Select this check box to activate the schedule. If you want to simply add the schedule and activate it at a later point, keep the check box clear.

4. Select the One Time option.
5. Select the date and time by clicking the  and the  to configure the date and time of the schedule.
6. Click **Save** to save the schedule.

Schedule One time Dashboard Report from the Reports Tab

If you wish to generate the dashboard report only once, you can use the One Time option. If you activate the schedule while adding it, the report is generated per the given date and time. If the schedule is not activated, the report is not generated unless you activate the schedule.



To add the schedule from the Reports tab, perform the following steps.

1. Select the location.
2. Click **Reports** and then click **New Schedule**.
3. Under New Reporting Schedule, configure the schedule for the

report. Option	Description
Report Name	The name for the schedule.
Email Addresses	A comma-separated list of e-mail addresses where the dashboard report is to be sent.
Duration	The duration for the dashboard. Select the Last Week option to schedule e-mail delivery for the last week dashboard report. Select the

Last Day option to schedule for e-mail delivery for the last day dashboard report. Select the

Option	Description
	Last Month option to schedule e-mail delivery for the last month dashboard report.
Schedule Active	Select this check box to activate the schedule. If you want to simply add the schedule and activate it at a later point, keep the check box clear.

4. Select the One Time option.
5. Select the date and time by clicking the  and the  to configure the date and time of the schedule.
6. Click **Save** to save the schedule.


Schedule Recurring Dashboard Report

If you wish to generate the dashboard report at regular intervals, you must use the recurring option. If you activate the schedule while adding it, the report is generated per the given date and time. If the schedule is not activated, the report is not generated unless you activate the schedule.

If you have already selected a location and are viewing the dashboard for the location and wish to define a schedule, you can add the schedule through the dashboard.

Alternatively, if you want to define a schedule for a location, you must first select the location and then navigate to the Reports tab (or the Dashboard tab) and add the schedule for the dashboard report for this location.





To add the schedule from the Dashboard tab, perform the following steps.

1. Click **Dashboard** and then click the  icon. The Schedule Report and Download Report buttons appear.
2. Click **Schedule Report**.
3. Under New Reporting Schedule, configure the schedule for the report.

Option	Description
Report Name	The name for the schedule.
Email Addresses	A comma-separated list of e-mail addresses where the dashboard report is to be sent.
Duration	The duration for the dashboard. Select the Last Week option to schedule e-mail delivery for the last week dashboard report. Select the Last Day option to schedule for e-mail delivery for the last day dashboard report. Select the Last Month option to schedule e-mail delivery



for the last month dashboard report.

Option	Description
Schedule Active	Select this check box to activate the schedule. If you want to simply add the schedule and activate it at a later point, keep the check box clear.



- Select the Recurring option.
 - Select the frequency of report generation in Repeat Every. Specify the number of days, weeks or months after which the report should be generated.
 - Select the date and time for Start Schedule by clicking the  and  the icons to configure the start date and time of the schedule.
 - Select the date and time for End Schedule by clicking the  and the  icons to configure the end date and time of the schedule.
 - Click **Save** to save the schedule.
- To add the schedule from the Reports tab, perform the following steps.

- Select the location.
- Click **Reports** and then click **New Schedule**.
- Under New Reporting Schedule, configure the schedule for the report.

Option	Description
Report Name	The name for the schedule.
Email Addresses	A comma-separated list of e-mail addresses where the dashboard report is to be sent.
Duration	The duration for the dashboard. Select the Last Week option to schedule e-mail delivery for the last week dashboard report. Select the Last Day option to schedule for e-mail delivery for the last day dashboard report. Select the Last Month option to schedule e-mail delivery for the last month dashboard report.
Schedule Active	Select this check box to activate the schedule. If you want to simply add the schedule and activate it at a later point, keep the check box clear.

- Select the Recurring option.
- Select the frequency of report generation in Repeat Every. Specify the number of days, weeks or months after which the report should be generated.
- Select the date and time for Start Schedule by clicking the  and  the icons to configure the start date and time of the schedule.

Description: time_icon.jpg

15. Select the date and time for End Schedule by clicking the  and the  Description: time_icon.jpg icons to configure the end date and time of the schedule.

16. Click **Save** to save the schedule.

Edit Dashboard Report Schedule

You can edit the previously created dashboard report schedules.

Remember that the location for a report schedule cannot be edited. It is a read-only field that is populated based on the location selected by you while adding the schedule.

To edit a dashboard report schedule, perform the following steps.

1. Select the location.
2. Click **Reports** and then click the Report Name link for the schedule to be edited.
3. Make the required changes.
4. Click **Save**.

Delete Dashboard Report Schedule

You can schedule the automatic generation of the dashboard for the last day, last week or last month for a specific location. The output is a dashboard report in PDF format.

You can delete individual dashboard report schedules.

To delete a dashboard report schedule, perform the following steps.

1. Select the location.
2. Click **Reports** and then click the  icon for the schedule to be deleted.
3. Click **Delete** when asked to  confirm the deletion of schedule.

Download Scheduled Dashboard Report

You can download the dashboard report from the Reports tab. The duration for which this report is generated is based on the duration specified in the schedule.

The report is generated with respect to current system time. For instance, if the duration specified in the schedule is Last Week, the downloaded report is for the last week with respect to the current system time.

To download the dashboard report, perform the following steps.

1. Select the location.
2. Click **Reports** and then click the  icon for the report zip file to be downloaded.

The report is downloaded to the default downloads folder.

Analytics

Guest Manager integrates with Wireless Manager and fetches the visibility and association analytics information from the Wireless Manager. Guest Manager analyzes guest user information for each portal and provides graphical and tabular representations of this data.

Guest Manager integrates with Wireless Manager and provides various location-aware analytic graphs. After you add Wireless Manager to Guest Manager and the information from the Wireless Manager is synchronized, the analytic graphs in Guest Manager are charted.

To view analytics information, click **Analytics**.



Important: You must add Wireless Manager information in Guest Manager to obtain and view the analytic graphs. If the Wireless Manager is not added, no analytics information will be collected and displayed in Guest Manager.


This chapter covers the following topics:


- [Location-Aware Analytics](#)
- [Graph Configurations](#)
- [Demographic Analytics](#)
- [View Guest Profile Information](#)
- [Presence Analytics](#)
- [Proximity based Analytics using Floor Map](#)
- [Wi-Fi Usage Analytics](#)
- [Engagement Analytics](#)
- [Download Analytics Graphs](#)

Location-Aware Analytics

Guest Manager integrates with Wireless Manager and provides various location-aware analytics graphs. Every page on the **Analytics** tab is divided into two panes.

The left pane of the page displays a location tree with each Wireless Manager added to Guest Manager. Under each server, the various folders and locations defined are listed in the tree. When you select or click a node on the tree, the right pane displays the graphs for the selected duration based on the information fetched from the Server (as of the last successful synchronization operation). The graphs are plotted for the sub-tree of the selected node. You can see multiple graphs or charts on the right pane.

You can show or hide the location tree by clicking the  icon. You can search for a location by typing the search string in the search box above the location tree.

 *Important: If you have selected the root location of a Wireless Manager and you have changed the display name of this location in Guest Manager, the analytics graph displays the original name of the root location (that is, root location name on the Wireless Manager on the X-axis. This happens only when you have selected the root location of the Server in the Guest Manager location tree while viewing the location-aware analytics.*

Graph Configurations

Guest Manager Analytics represents the data in line graphs, pie charts, and bar graphs.

Important! If you have enabled MAC randomization, then some of the graphs and charts appear with different configurations and some charts are removed from the UI as they are not relevant. For more information, see the [Clients with Random MAC Addresses](#) section.

A date is displayed at the top of the analytics charts. This is the last date for which the data is available. The duration that you select for the charts is with reference to this date as the last date. For instance, if you choose to view analytics data for the last week when the data availability date is June 26, 2015, analytics data is displayed for the week June 20, 2015 to June 26, 2015. You can also select a custom date for the analytics data. The charts are then populated for dates based on the custom date as the last date. If you choose to view analytics data for the last week and the custom date is June 22, 2015, the analytics data is displayed for the week June 16, 2015 to June 22, 2015. The custom date can be a date before the data availability date or the same as the data availability date.

To reset the custom date back to the default data availability date, click the date and then click the *Reset to Default* link.

Some of the configuration information for these charts are listed below:

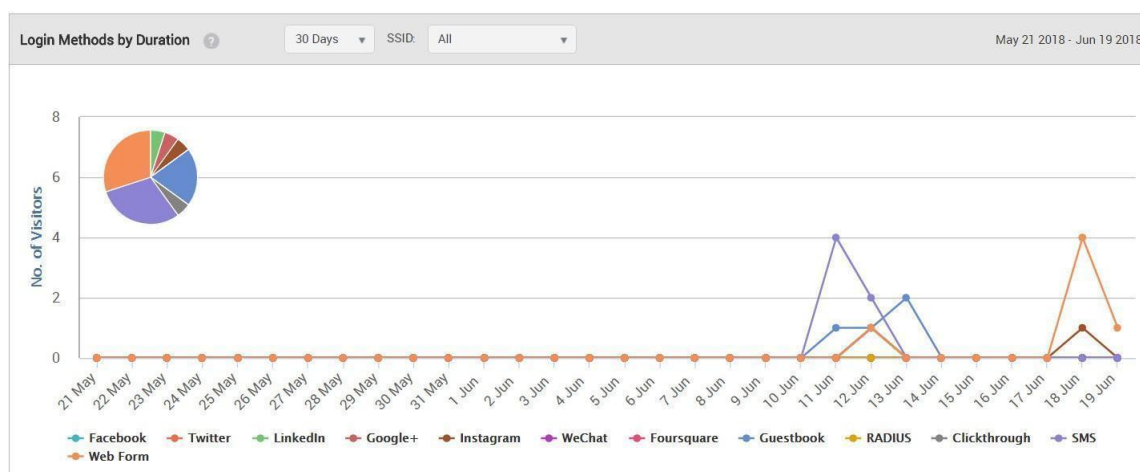
- All the graphs are followed by a legend. You can select or deselect an item from being displayed in the graph by clicking it in the legend.
- Day-wise graphs (line graphs and some bar graphs) can be configured to display the data for 7, 14, 30, 60, 90, 180, and 365 days. For 7, 14, and 30 days graph durations, the data is plotted for each day. For 60, 90, and 180 days graph durations, the aggregated data for each week during the specified duration is plotted. For 365 days graph duration, monthly aggregated data is displayed.
- Clicking or hovering the mouse over a line, bar, or pie in the graph provides more information about the plotted data as a tool tip.
- You can click a sector in pie chart to pull it out slightly from the pie chart. This is useful if you want to highlight a specific sector in your printed graph.
- You can click and drag the mouse over a specific area of a line or bar graph to zoom-in the selected section of the graph.

Demographic Analytics

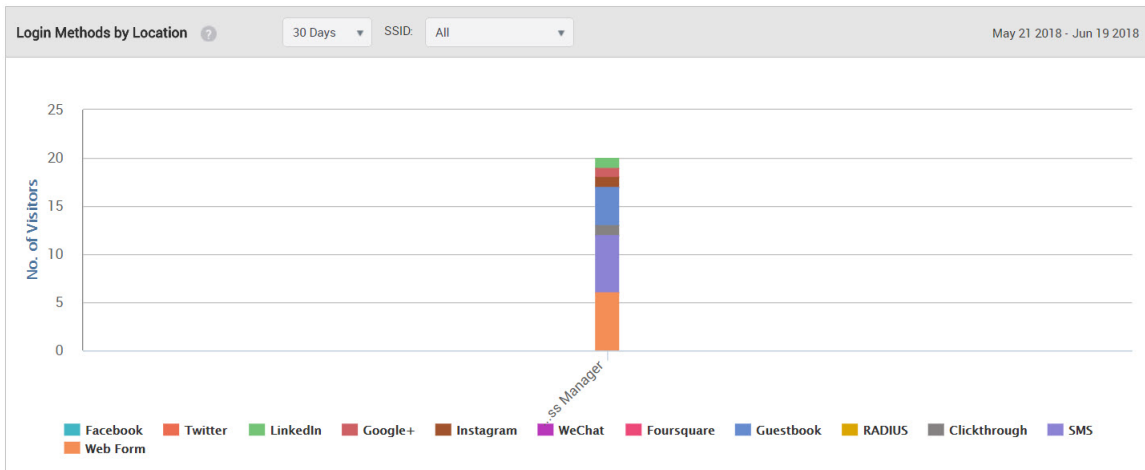
Guest Manager provides the social analytic information for guest users who use the Wi-Fi by authenticating with their social media account. Guest Manager retrieves some user-specific information from the social media account that they use to authenticate with the Guest Manager.

Guest Manager provides location-wise social analytic graphs and portal-wise visitor log information. Click **Demographics** under **Analytics** to view demographic analytics information. Guest Manager analyzes guest information for the users who use their social media account and represent this data in the following graphs:

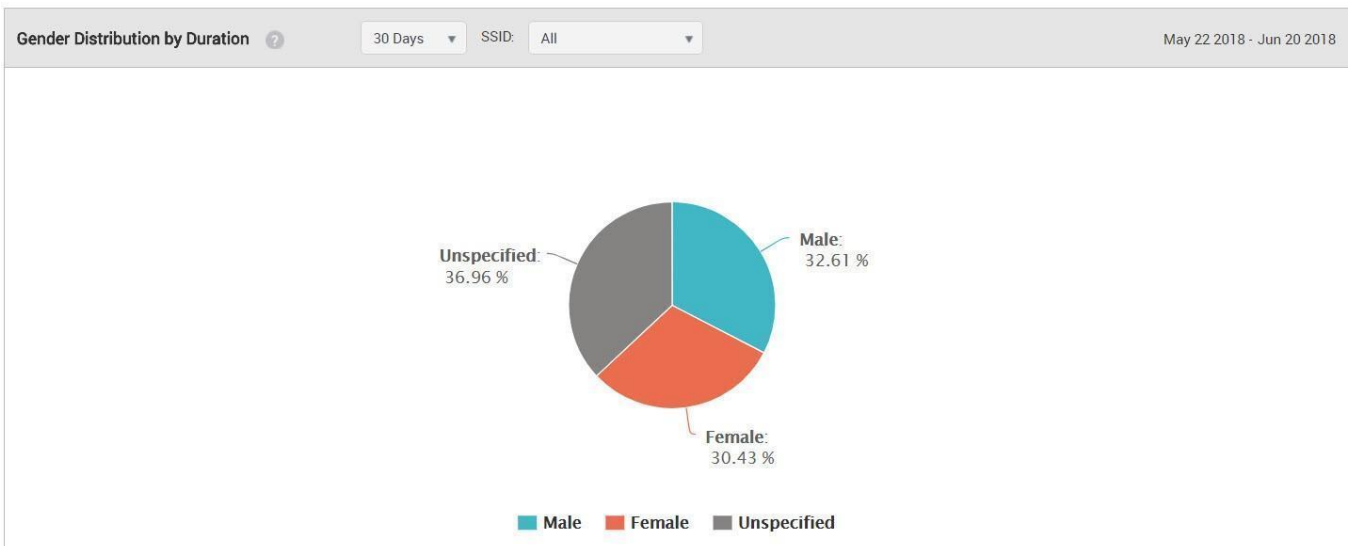
- Login Methods by Duration: Line graphs charting login method wise visitors (guests) accessing the Wi-Fi. For the location selected on the left pane, the line graph shows the number of visitors for each plug-in (social media, guest book, and click-through) during the specified duration for the selected SSID based on the data availability date or custom date selected by you. To select the date, click the date seen on the top of the Analytics page. A pie chart representation of the distribution is also seen for the selected duration and SSID. By default, the graph and pie chart are based on last 7 days of data (with the date seen on top of the Analytics page as the last date) for all the SSIDs defined on the servers is displayed.



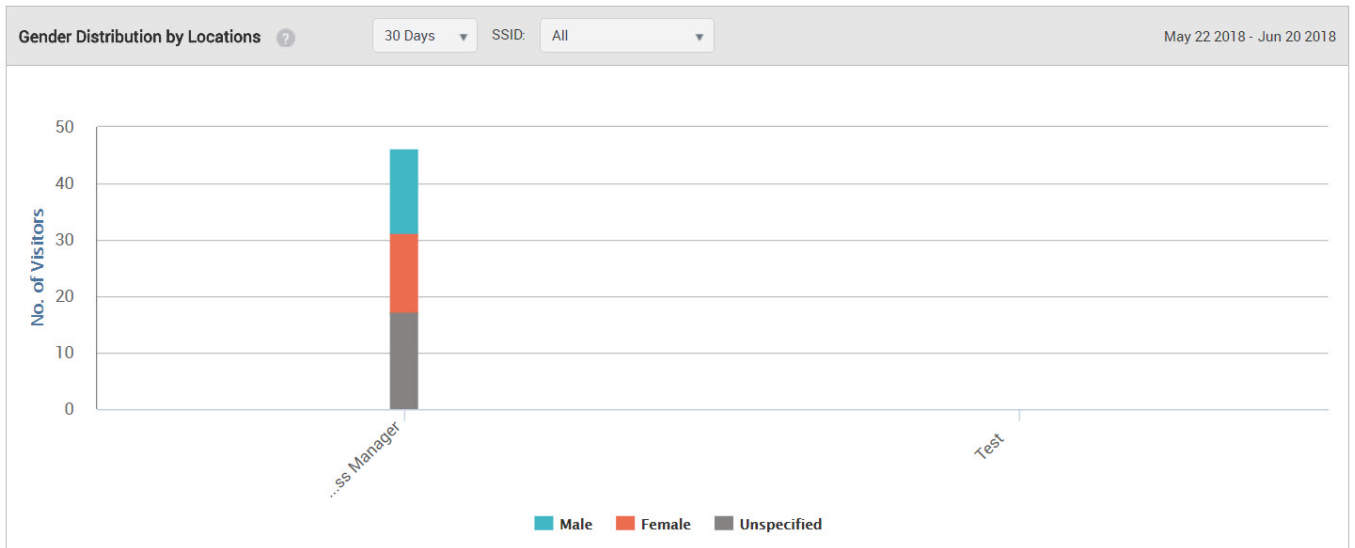
- Login Methods by Location: A bar graph showing the login method wise percentage of guests for the selected location and its child locations that have accessed the Wi-Fi during the specified time duration for the selected SSID.



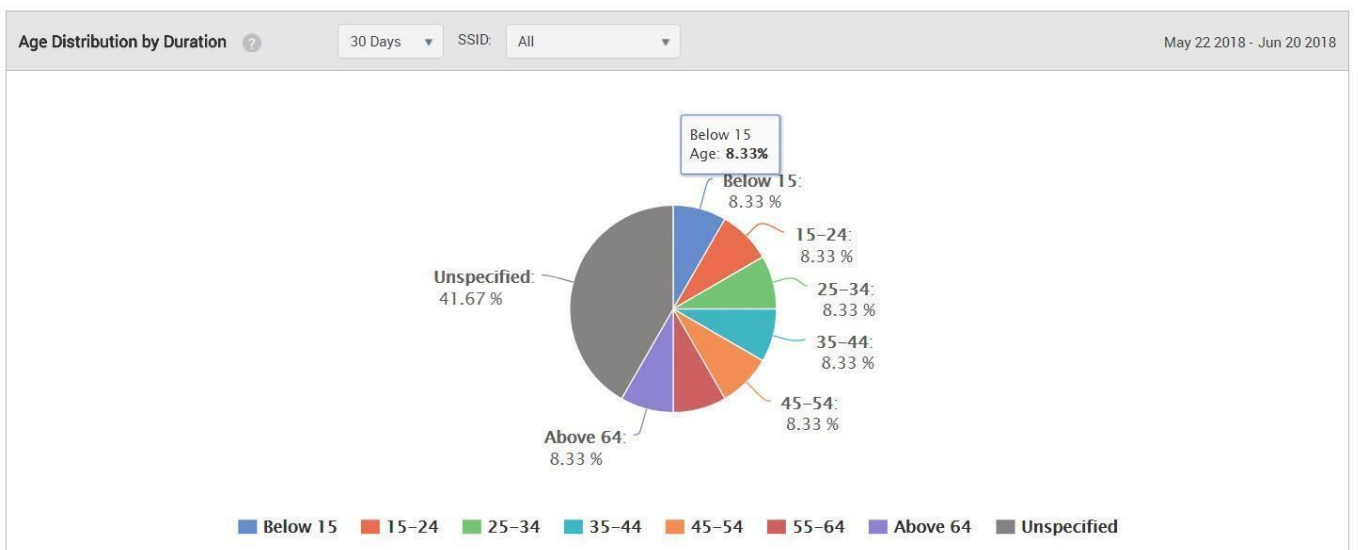
- Gender Distribution by Duration: A pie chart showing the gender-wise percentage of guests that have accessed the Wi-Fi during the specified time duration for the selected SSID.



- Gender Distribution by Location: A graph showing the gender-wise percentage of guests for the selected location and its child locations that have accessed the Wi-Fi during the specified time duration for the selected SSID.



- Age Distribution by Duration: A pie chart showing the number of guests for different age ranges who have accessed the Wi-Fi during the specified time duration for the selected SSID.



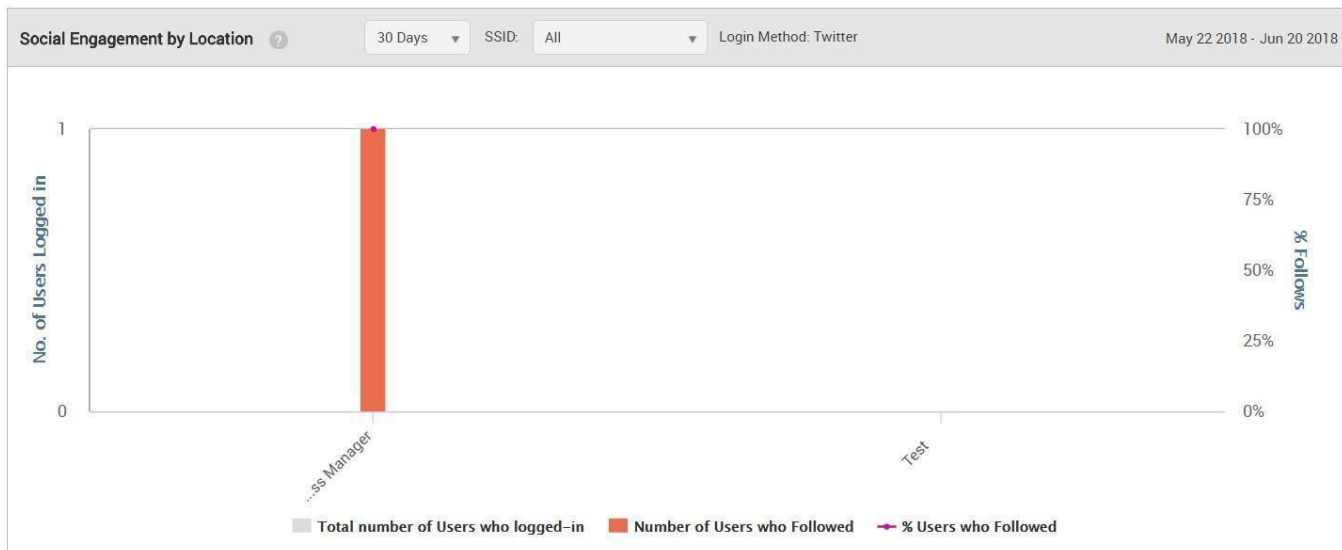
- Age Distribution by Location: A chart showing the number of guests for different age ranges that have accessed the Wi-Fi for the selected location and its child locations.



- Social Engagement by Duration: A chart showing the number of guest users who logged using Twitter, and liked the page for the selected duration.



- Social Engagement by Location: A chart showing the number of guest users who logged using Twitter, and liked the page for a selected location.



View Guest Profile Information

The demographic analytics also provides profile information of all the visitors, which contains information about the guests who have accessed the Wi-Fi. To see the profile information of visitors or guests, click **Profiles** under **Analytics**. The profile information of guests or visitors is presented in a tabular format. The information displayed is the information that the guest user has allowed to be displayed.

When a user logs in to the Wi-Fi, he logs in through a plugin be it Social plugin, Guestbook or Webform. While logging through the plugin, the user will be asked to fill in various fields. Those fields will be displayed on the analytics chart of "Profiles" like profile picture, portal, plugin, gender or location. Some of the information is visible, by default. You can view additional fields by clicking the down arrow next to the field name in the table, click **Columns** and select the check boxes for the additional fields to view. The following table provides a description of the fields seen in the profile information and provides the following information.

Fields seen on Profiles Page	
Default Fields	
Profile Picture	The photograph of the guest. This is retrieved from the social media site based on the respective social media account the user uses to access the Wi-Fi.
Portal	The name of the portal used to access the Wi- Fi.

Plugin	Name of the plug-in used to authenticate.
---------------	---

Fields seen on Profiles Page	
User Name	Login name of the guest as mentioned on the social media account.
First Name	First name of the guest as mentioned on the social media account.
Last Name	Last name of the guest as mentioned on the social media account.
Gender	Gender of the guest as mentioned on the social media account.
Location	Location of the guest as mentioned on the social media account.
Login Location	Location of the AP to which the guest connected. This is the location defined in the Wireless Manager.
Email ID	E-mail id of the guest as mentioned on the social media account.
Age Range	Age range of the guest.
Number of Visits	Number of visits by the guest to the portal.
Additional Fields	
Phone number	Phone number of the guest as mentioned on the social media account.
Languages	Languages known to the guest as mentioned on the social media account.
Friends count	Number of friends the user has on the social media account.
Followers count	Number of followers as mentioned on the social media account
DOB day	Day of birth of the guest as mentioned on the social media account.

DOB month	Month of birth of the guest as mentioned on the social media account.
DOB year	Year of birth of the guest as mentioned on the social media account.
Date Created	Date of account creation.

Fields seen on Profiles Page	
Last authentication time	Date and time of the last visit by the guest to the portal.
Last Skip Time	Date and time of the last splash page skipped by the guest user.
Skip visit count	Number of time the guest user skipped the splash page.
Membership ID	Membership ID of the guest user
Marketing Opt-in	Marketing Opt-in if used by guest user.

The guest profile information can be downloaded as a CSV file by clicking the **Download CSV** button on the **Profiles** page.

The guest profile information is available for each location in the location tree. The guest profile information for upto 100 users can be displayed per page at a given time. If the number of guests for a location exceeds 1000, the profile information for the latest 1000 guests for that location is displayed under **Profiles**.

The following image illustrates the **Profiles** widget.

Profiles ▾

Download CSV ?
↻

Profile Picture	Portal	Plugin	User Name	First Name	Last Name	Gender	Login Location	Email ID	Last Authenti... Time	No. Of Visits
	Test_S-NS	Web Form	Vishal@test.co...				Test	Vishal@test.co...	Jun 19 2018 7:47 AM	1
	Test_S-NS	Web Form	sfsgfs@bcn.co...				user_9	sfsgfs@bcn.co...	Jun 19 2018 5:45 AM	1

Figure 7: Profiles

However, you can view the profile information of all the guests for a location by exporting this information to a CSV file by clicking the **Download CSV** button on the **Profiles** page. The CSV file includes the profile information of all the guests for a selected location and is not limited to a maximum value. You can download the CSV data for last **90 days**.

Sort Guest Profile Information

The profile information of guests is visible in a tabular format. You can sort this information on different fields.

To sort the profile information, do the following tasks:

1. Click the name of the field on which you want to sort the information. The field is alphabetically sorted.
2. To reverse the sort order, click the field name again.

Filter Guest Profile Information

You can filter guest profile information on a field to view information that matches the filter applied to the field.

To filter guest profile information, perform the following steps.

1. Click the down arrow next to the field name on the **Profiles** page.
2. Click the **Filter** option. A small window appears for the filter text.
3. Enter the substring or string on which you want to filter the information in the text box seen under **Contains**.
4. Click the **Filter** button.
The information is filtered based on the substring or the string entered.
To clear the filter applied to the guest profile information, perform the following steps.
5. Click the down arrow next to the field name on the **Profiles** page.
6. Click the **Filter** option. A small window appears for the filter text.
7. Click the **Clear** button.
The filter is removed.

Presence Analytics

Guest Manager integrates with Wireless Manager and fetches the visibility analytics information from the server. You can view the day and location-wise visitor distribution and visitor dwell time graphs from the **Presence** page on the **Analytics** tab.

Guest Manager provides you with the following visitor analytic graphs on the **Presence** page:

- **Footfall by Duration:** This is a bar graph that shows the number of visitors during different time splices of a day for the specified duration and at the selected location. The graph also plots the total number of visitors for each day at the selected location for the specified duration. The number even includes the guest users who haven't even accessed the Wi-Fi but were duly visible. The data displayed on the graph for each time splice is based on the time zone set for the location selected in the tree. That is to say, you select a node with multiple locations under it. The graph plots the total number of visitors for each day (based on the duration selected). The graph also plots the total number of visitors during a specific time period of the day (time splice). The total number of visitors for a specific time splice is calculated by aggregating the visitor count during the said time splice for each location based on the time zone of the location. We can access their presence for a span of 7 days, 30 days, 60 days, 180 days or 365 days. When you need a 7 day chart, you will easily be able to track the per day data of the visitors in and around the store from Monday to Sunday. But when you go for >60 days slot you will be able to see per week data for 60 days. And for 365 days you can view the per month data. The

granularity changes as per the data distribution for the duration. If a user accesses the Wi-Fi in a particular time slot like 8 am-12 pm multiple times, it will be counted as one visit for that time slot. But if he logs in under different time slots, he will be counted different for each time but for an overall view for the parent location, the guest user will be counted as one visitor. Similarly, If the person logs in through different devices in the same time slot or different slot, he will be counted as a different visitor each time as that login depends on the MAC address of the device. Different MAC addresses will count as different visitors.

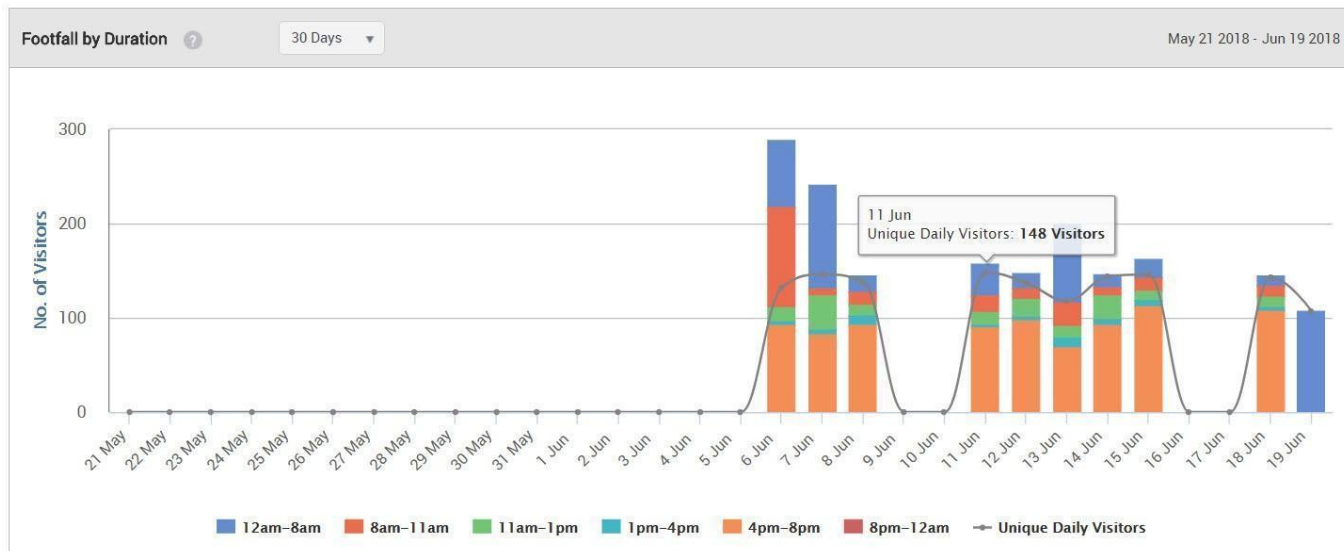


Figure 8: Footfall by Duration

- **Footfall by Locations:** This is a location-wise bar graph depicting the total number of visitors during different time periods of the day (time splice) aggregated for the specified duration. The data is plotted for the selected location and its immediate child locations. Assume, there is one root location also known as the parent location. The parent location has many child locations. For example, *Arista -- **Maharashtra-- ***Pune--- ****Alpha-- ****Gamma-- ****Beta-- ***Mumbai-- ***Kolhapur-- This is the location tree. Arista is the root location which has Maharashtra as the child. Which in turn has Pune, Mumbai, Kolhapur as its child nodes. Pune in turn has alpha, gamma, beta as its child locations. When the chart is made, we pick up a location. Suppose out of the folders, I picked up Pune as my location, now I will be able to see the visitors or clients as we know for Pune location as well as for its child location. So, we will get a chart for Pune+Alpha's visitors+Beta's visitors+Gamma's visitors. This chart will be an aggregation of the parent+child location.

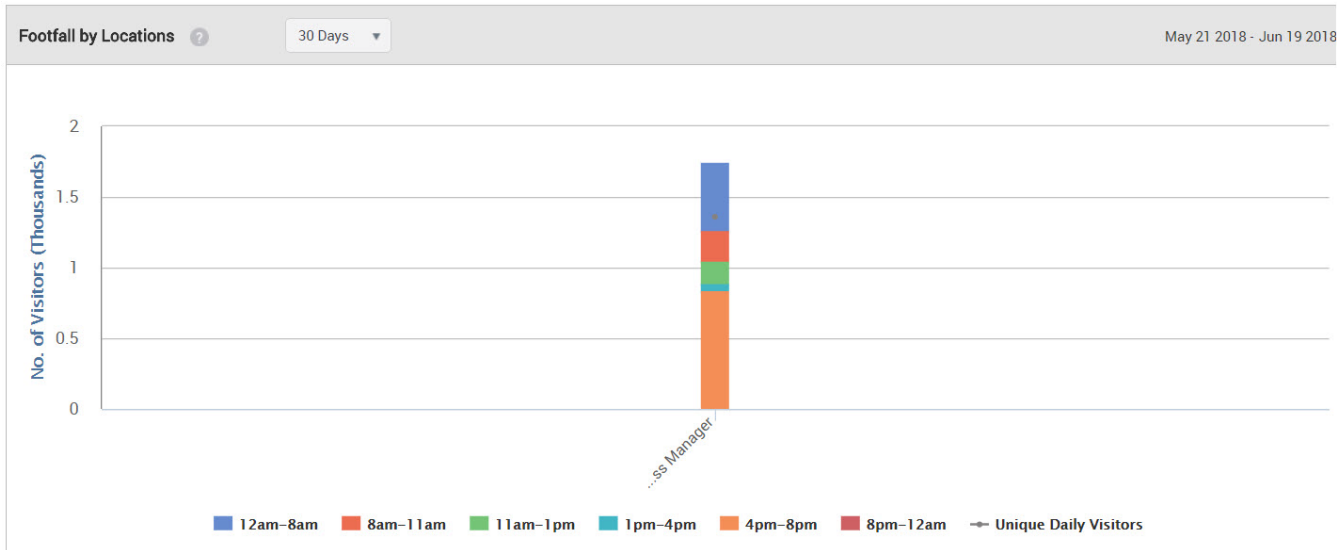


Figure 9: Footfall by Location

- Dwell Time by Duration: This is a bar graph showing total number of users who have accessed the Wi-Fi for different time periods during each visit for the specified duration and at the selected location. But the greater question arises how is this calculated?

The Dwell time depends on the RSSI value that we receive. The relative signal strength of the Wi-Fi is considered to be good the more its value is close to 0. So, when a client connects for a particular time slot its duration is mapped. This is again an aggregated data. Suppose, in the time slot of 8-11 am, a client logs in at 8-9 am for 4 minutes and again logs in from 9-10 am for 3 mins. If he does so, his total time slot will be 4+3= 7 minutes and will be depicted on the chart, accordingly.



Figure 10: Dwell Time by Duration

- **Dwell Time by Location:** This is a location-wise bar graph depicting the total number of users who have accessed the Wi-Fi for different time periods during each visit. The data is aggregated for the specified duration. The data is plotted for the selected location and its immediate child locations. Dwell time by location shows us the customers that have logged in at a particular location for a particular time slot. These values depend on the RSSI value. Let us take an example, There are 4 locations where Arista APs are placed- Alpha, Beta, Gamma, and Phi. Now, the customer is at Beta location but is visible to both the Beta and Alpha locations. Our problem begins how will we calculate which parameter to count. That is when RSSI values come into action. On location Alpha the RSSI values for customer is as follows: He logged in from 10:01 am - 10:05 am.

Sensor A detects For time = 10:01; RSSI value = -60 dbm, For 10:02; RSSI value = -40 dbm, For 10:03; RSSI value= -255 dbm, For 10:04; RSSI value= -30 dbm, For 10:05; RSSI value= -255 dbm. *Sensor B* detects only for the duration: 10:02- 10:04 where, For 10:02; RSSI value= -30 dbm, For 10:03; RSSI value= -255 dbm and For 10:04; RSSI value= -60dbm. Now, we calculate the best RSSI value for all the particular slots by comparing sensor A and B. The aggregated data comes For 10:01; RSSI value= -60 dbm, For 10:02; RSSI value= -30 dbm(out of -60 and -30,-30 is the best value), For 10:03; RSSI value= -255 dbm, For 10:04; RSSI value= -30dbm, For 10:05; RSSI value= -255 dbm. This is the aggregated data based on the best of RSSI values. We know the value -255 dbm means that no data came for these time slots. So, these time slots are automatically cancelled. Then as per what we receive, we have data only for 4 minutes. Based on data calculated on RSSI values we get the graph plotted.

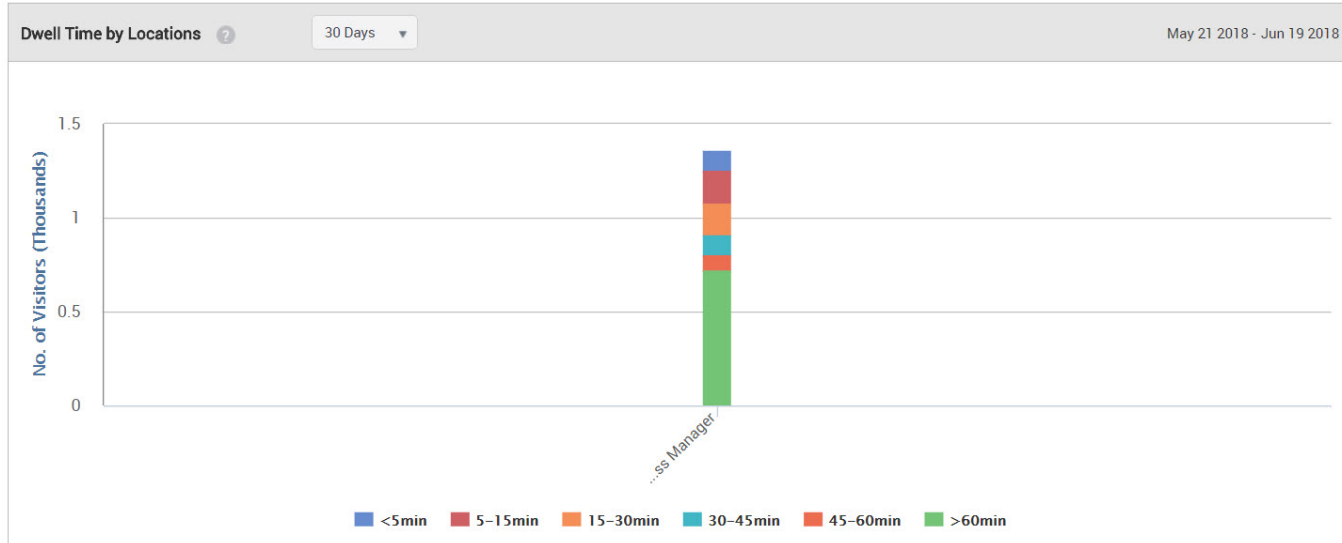


Figure 11: Dwell Time by Location

Proximity-based Analytics using Floor Map

You can view the AP-wise visitor distribution and dwell time for a location floor from the **Floor Map** page on the **Analytics** tab based on the proximity of visitors to the APs deployed on the location

floor. The graphical view on the **Floor Map** page displays the average number of visitors visible to the APs on the floor for the selected time slice or the average dwell time per AP for the selected time slice.

Floor Map gives us a full floor view of the location where the AP is located. This can only be viewed for the leaf locations under the parent locations. There is no aggregation of data. It is considered as Heat Map depiction of APs across the sections. The zone for each AP is represented by a circle. You can reduce or extend the zone by dragging the edge of the circle with the mouse. You cannot extend an AP zone beyond a signal strength of -90 dBm.

The floor map for the selected location floor is retrieved from CV-CUE.

When you click an AP on the floor map, the device MAC, radius of the AP zone and total visitors are displayed. If the AP has been present for only a part of the selected duration, a start date and end date is also seen with the above-mentioned details. Let us understand the concept with an example: Supposedly, you need the floor map of a floor in the mall. The mall is segregated into various sections including kids, shoes, and accessories section. Two of them have the company APs installed. The floor map will give us the total visitor count for each AP for the duration selected. The number of visitors increases as it is taken for a longer duration. More the visitors, the color automatically starts to change- for lesser number of visitors the color stays blue, with increase in visitors it continues to change to red or any other color. You can customize the radius of the visible AP circle. Increase it to see the visibility of users in that part. Floor map is calculated on the basis of location folders. When you select a location like AMC or AMC1, you will be redirected to the floor map of the location as been uploaded. The floor map depicts the APs that are planted across the floor. Each user is counted based on the unique MAC addresses of its device and his total visit time is calculated for a particular date, time slot, sensor and RSSI value. The range of the MAC address and time is looked upon for its unique visits. Based on the RSSI values the range is created. Suppose a range for -40 DBM is created, when we increase the range of the RSSI value to -50DBM or so the number of users change.

Guest Manager provides you with the following AP-based visitor analytic views for a location floor:

- **Visitor Distribution by AP:** This graphical representation shows the average number of visitors visible to the AP in the selected intra-day interval for the specified time period at the selected location floor. Visibility is partitioned on the density of users who are using the Wi-Fi. The visitors who can connect on a particular location are presented as an aggregated data and that is the footfall data aggregation by AP. By default, the intra-day interval is 'all day'. For visitor distribution or footfall, you can configure the minimum and maximum number of visitors per day for the average visitors view.

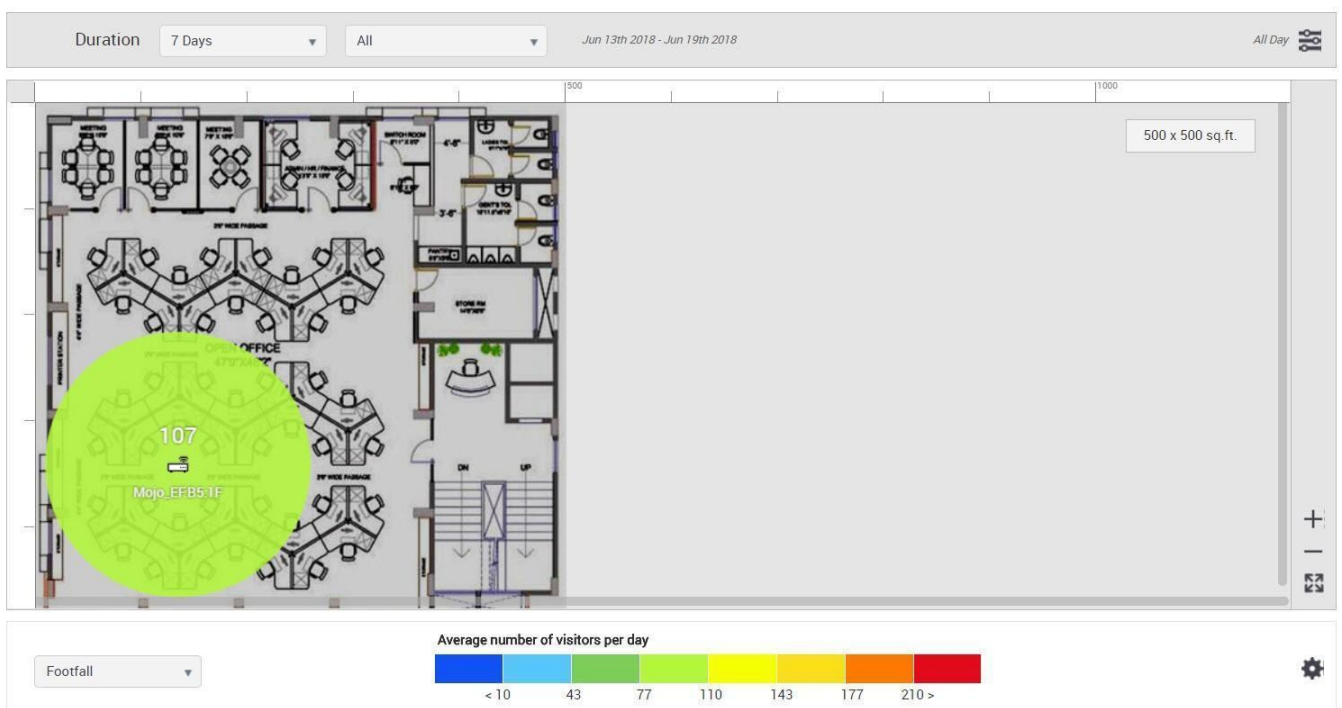


Figure 12: Footfall

- Dwell Time by AP: This graphical representation shows the average time spent by visitors in the AP zone in the selected intra-day interval for the specified time period at the selected location floor. The dwell time indicates the amount of time a guest user spends on a particular location near an AP. The amount of time gives the idea as to where does the guest user spends his larger amount of time. Floor Map gives us the view of the visitors according to the time spent too. When you choose the duration to be 7 days and a visitor visits each day on that particular location, he will be counted as 1 uniquely on each day. But if we see the floor map for a larger portion of time like for >90 days the user is then counted as 1 only. The data is an aggregation so the data for a user is not counted as a single user each time. By default, the intra-day interval is 'all day'.

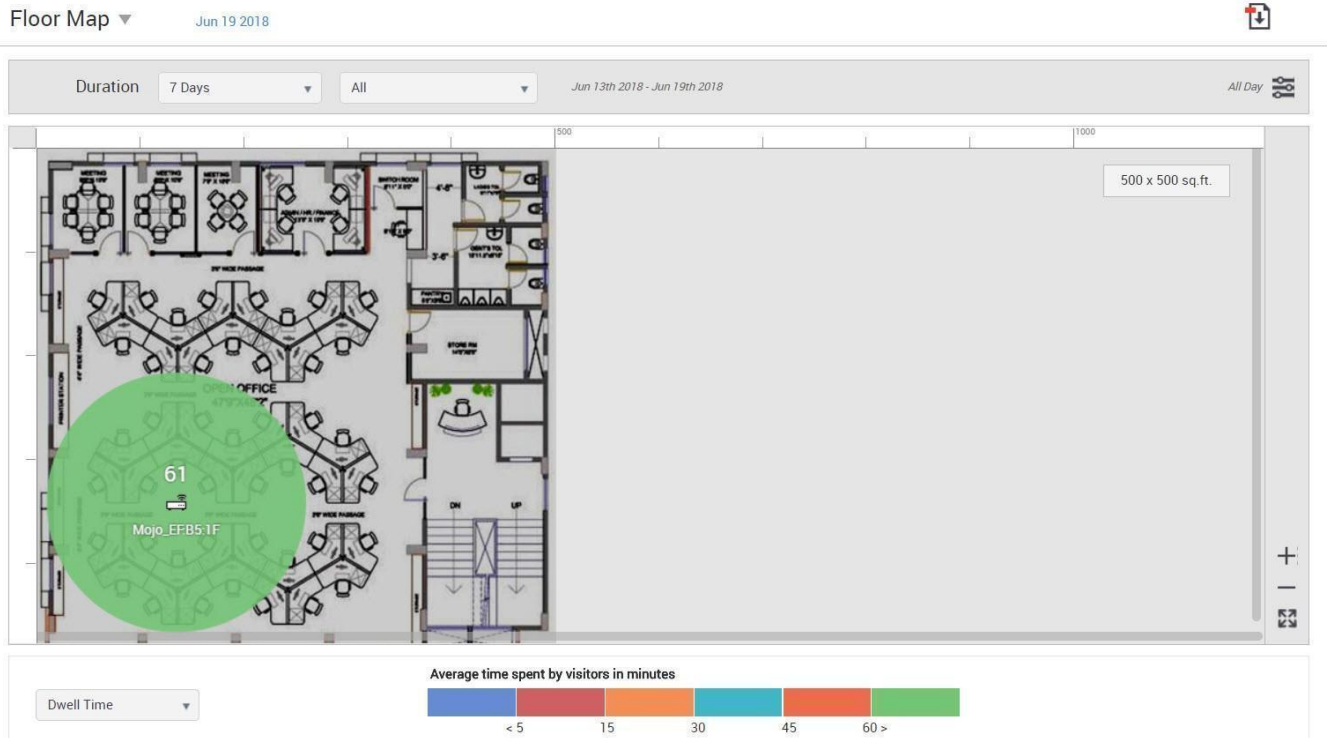


Figure 13: Dwell Time

Wi-Fi Usage Analytics

Guest Manager integrates with Wireless Manager and fetches the association analytics information from the server.

Guest Manager provides two graphs that show the data transfer by days and by location. You can view these graphs under **Analytics>Wi-Fi Usage**. The graphs are as follows:

- **Data Transfer by Duration:** This is a line graph that plots the data received transmitted and total data exchange over the specified duration at the selected location for the selected SSID.

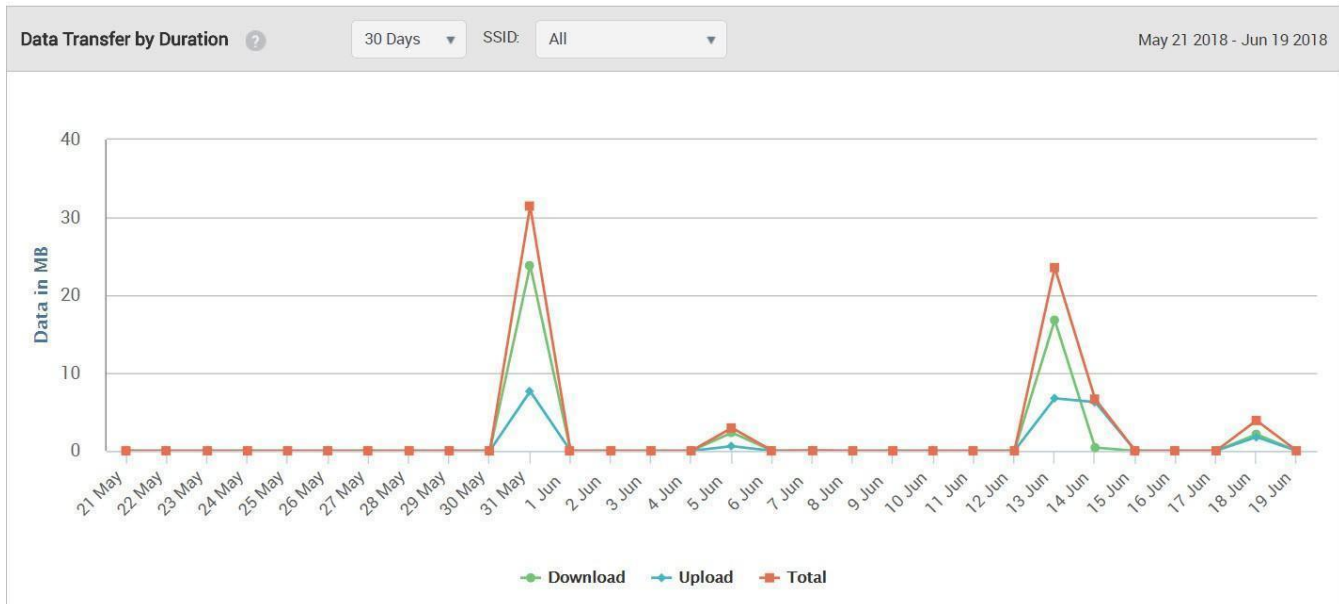


Figure 14: Data Transfer by Duration

- **Data Transfer by Location:** This is a bar graph that plots the data transmitted and received for the specified duration at the selected location and its immediate child locations for the selected SSID. When you select a particular location from the root folder, the chart depicts the total Wi-Fi usage done in that particular location. The line data shows the data that is being transferred from AP to the client(download data) and from the client to the AP(upload data). The data transferred can be chosen for a particular location along with its child locations, SSID or duration. An aggregated data for the location is presented.

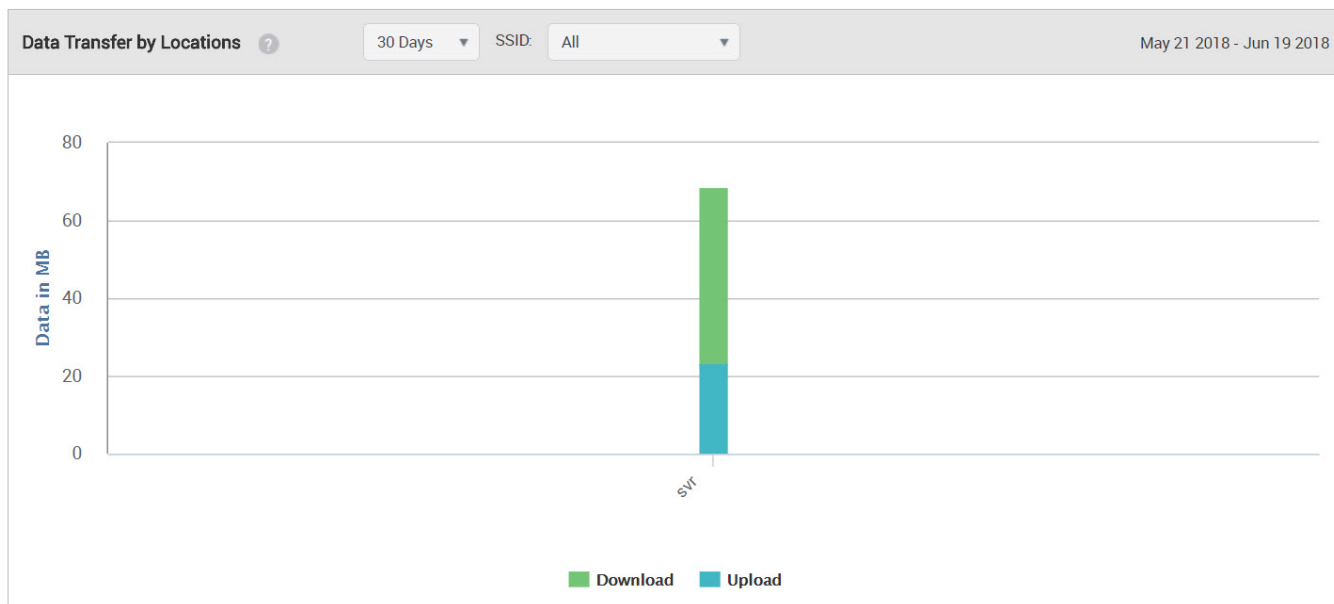


Figure 15: Data Transfer by Location

Conversion Analytics

Conversion Analytics comprises of loyalty analytics and conversion analytics.

You can view conversion analytics under **Analytics > Conversion**.

Guest Manager provides two conversion analytic graphs. The conversion graph plots the number of visitors or the number of visits inside a store.

Conversion shows us the data for the converted customers. Converted customers means the visitors who were visible around the store but chose to enter and use the Wi-Fi. Suppose, a shop in the mall has an AP. There are visitors all day long who choose to enter or who choose to just pass by or stay outside. We draft the charts for how many users actually came inside the store after analyzing the statistics. We have a configurable threshold RSSI value and a time slot in which it is converted. Suppose, the RSSI value is -70dbm and the time slot is 5 minutes. Greater than this RSSI value and a time greater than 5 minutes will fall in the court. The chart shows the number of visitors who are in and around the store for a duration. There is a red line that goes through the graph also known as the conversion factor. This red line is the percentage of the visitors who were actually converted which is calculated by : $\text{Inside}/(\text{inside}+\text{outside})\% = \text{conversion factor}$. Suppose, there are 50,000 visitors inside and 60,000 outside then the Conversion factor = $50,000/(50000+60000)*100 = 45\%$. So, the red line will go showing the conversion factor as 45% for the particular duration that we choose. Be it 7 days, 14 days, 30 days or more than that.

The RSSI threshold and the time duration are configurable. This can be configured in the **Conversion Thresholds** tab under **Admin > Settings**. Enter the required threshold value and time duration and click **Update**. The new threshold value and time duration will be used to chart the

graphs after the next successful synchronization of the servers. To immediately view the graphs with the updated thresholds, you must manually synchronize the servers. See [Synchronize Arista Server Information](#) for further server synchronization details.

- Conversion Factor by Duration: A day-wise bar graph showing the number of visitors/visits to the inside of the store and the number outside. Also a line graph plotting the percentage of visitors/visits that was converted, that is, the percentage of visitors/visits inside the store.



Figure 16: Conversion by Duration

- Conversion Factor by Location: A location-wise bar graph showing the number of visitors/visits to the inside of the store and the number outside. Also a line graph plotting the percentage of visitors/visits that was converted, that is, the percentage of visitors/visits inside the store.

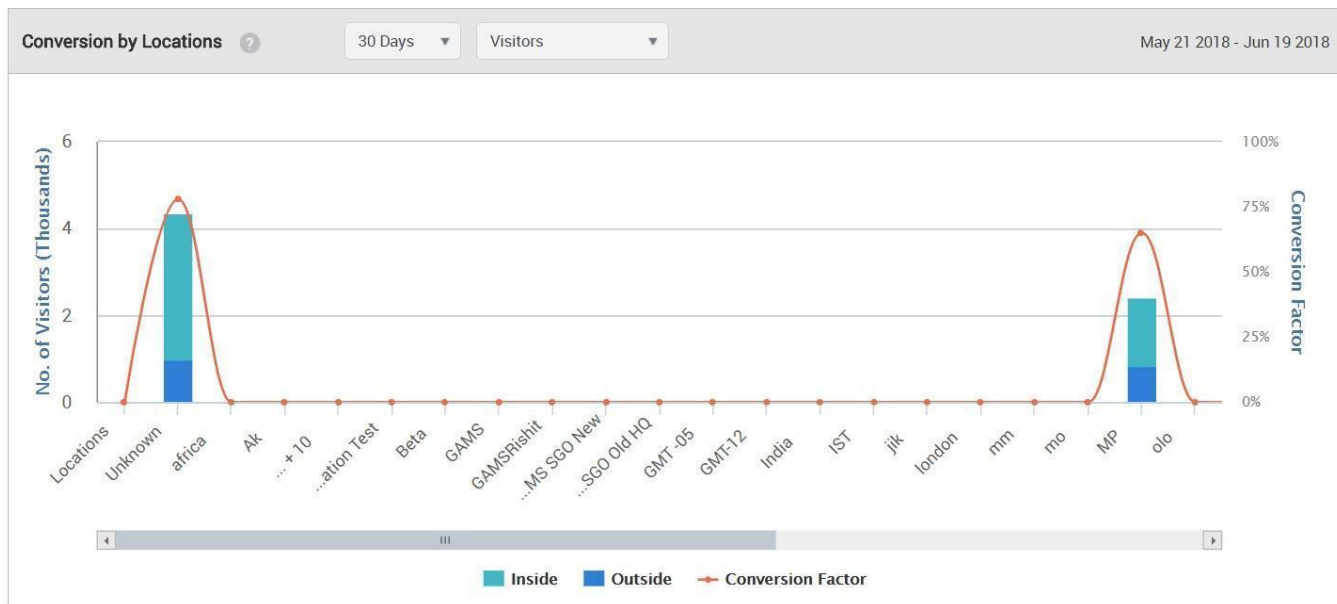


Figure 17: Conversion by Location

Loyalty Analytics

Guest Manager provides loyalty analytics which shows the number of visitors based on their frequency of visits at different stores and different brands.

You can view loyalty analytics under **Analytics > Conversion**. The following loyalty graphs are provided:

- Store Loyalty:** This is a bar graph that shows the number of visitors for different visit frequencies who have accessed the Wi-Fi one or more times during the specified duration at the selected location using the specified SSID. The graph plots the total number of guests based on the number of visits by each guest on different dates during the specified duration. That is to say, multiple visits by a user on a single day is accounted as 1 visit. The frequency of visits is plotted as shown in the following table.

Frequency	7 days/14 days	30 days
One-time	1 visit	1 visit
Infrequent	2 visits	2-4 visits
Frequent	3 visits	5-7 visits
Very frequent	4 visits	8-15 visits
Loyal	more than 4 visits	more than 15 visits

For the selected location, the bar graphs are displayed for each child location. Also, an aggregated pie chart for the selected location and its immediate children is displayed.

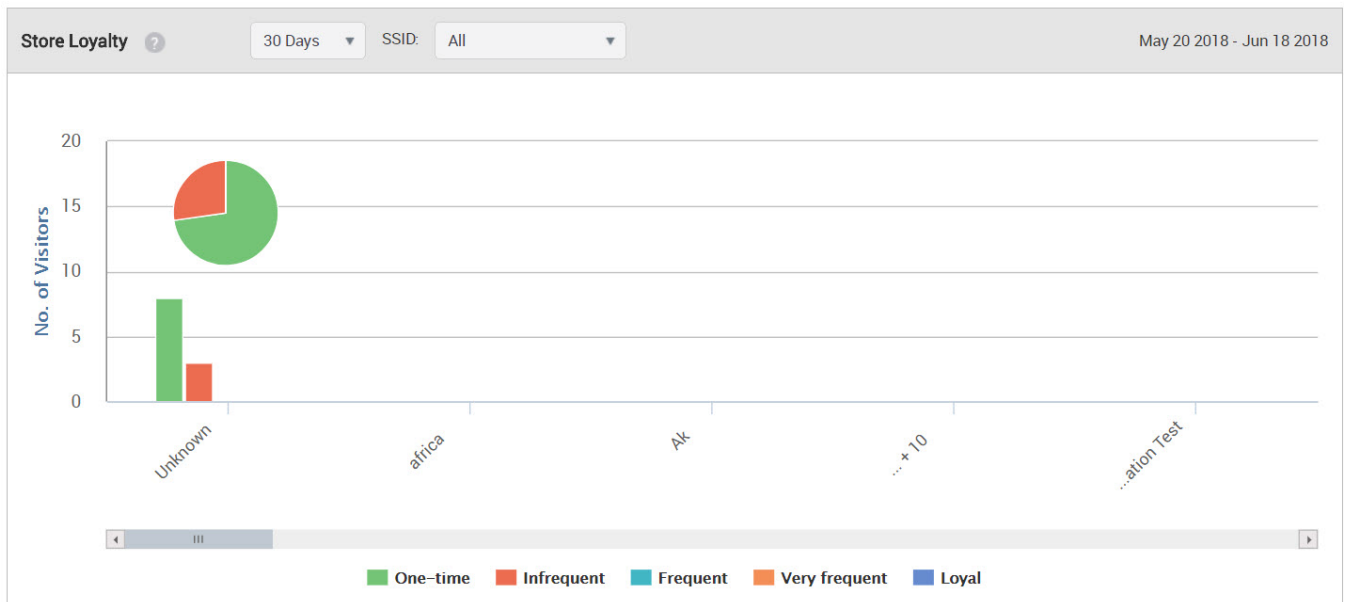


Figure 18: Store Loyalty

- **Brand Loyalty:** In the case of brand loyalty, the number of visitors for different visit frequencies is plotted based on the SSID accessed by the guest. The graphs are plotted based on the data from all locations and is not specific to the location selected on the tree. You can obtain the brand loyalty data for all SSIDs only at the root level. The data uniqueness is decided by combining the MAC address and the SSID. The visit frequency legend is same as that used for Store Loyalty. In the case of brand loyalty, the data used to plot the pie chart is an inclusive data for the selected location and not an aggregated one as in the case of store loyalty. For example:

1. If a client has connected to SSID1 many times at the same store (location) on the same day, then the contribution of client is considered as 1 visitor with 1 visit (ONE-TIME category on the chart) .
2. If a client has connected to SSID1 at store1 and also connected to SSID2 at store2 on the same day or different, the contribution of client is considered as 1 visitor with 1 visit at respective store.
3. If a client has connected to SSID1 at store1 and the same SSID at store2 on the same day or different, the contribution of client is considered as 1 visitor with 2 visits (INFREQUENT category on the chart) at both stores.

For Brand Loyalty graph, we are considering 'client MAC and SSID' as the key to find the number of visitors while location is used for calculating the number of visits. All the above mentioned behaviors are common when a single SGO is added or multiple SGOs are added to a customer. In order to find unique visitor we take all the added SGOs into considerations. As data displayed on the chart is calculated across all the added servers for the customer unlike all other charts where calculation is limited to just the location/server under consideration.

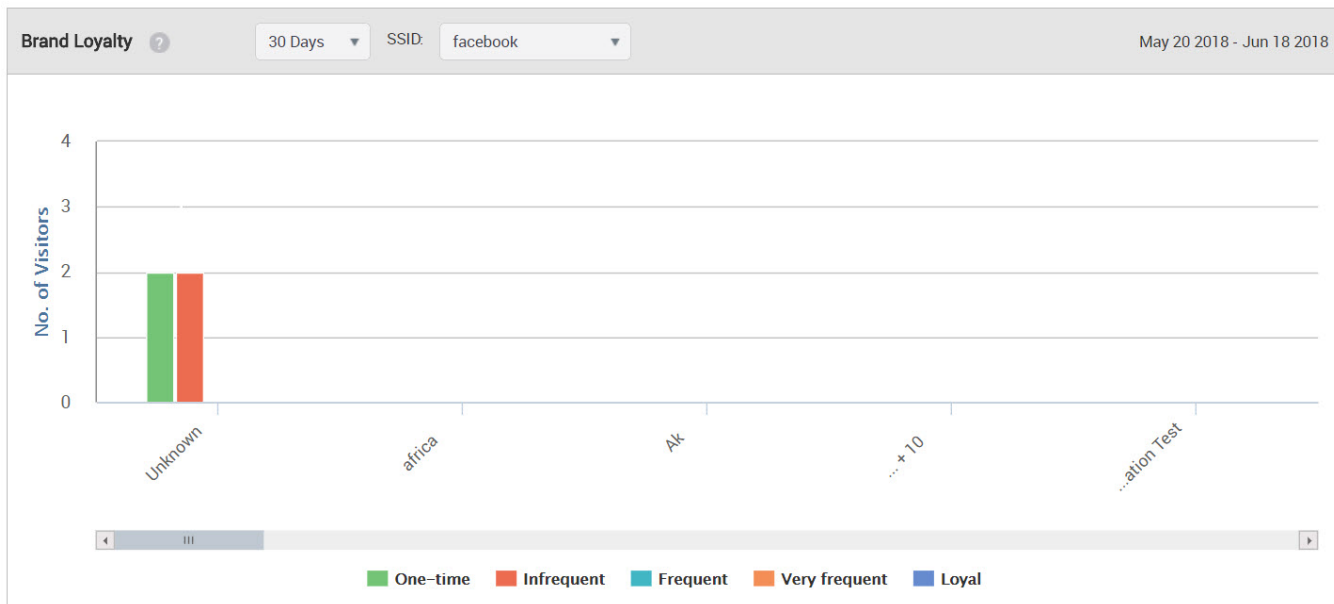


Figure 19: Brand Loyalty

Download Analytics Graphs

The analytics graphs that are presented on each of the Analytics pages can be downloaded in PDF format. This can then be viewed with a PDF viewer.

The PDF file contains graphs for the selected analytics page. If you are on the Conversion Analytics page and you download the PDF file, the file would contain the graphs for Conversion by Days, Conversion by Locations, Store Loyalty and Brand Loyalty, for the selected location. That is, the PDF file would contain exactly the same graphs that you see on the Conversion Analytics page.

To download an analytics graph, perform the following steps.

1. Click the **Analytics** tab.
2. Click the required Analytics option, that is, click Presence, Demographics, Profiles, Conversion, Interception or Wi-Fi Usage depending on what analytics information you want to download.

3.



Click the icon seen on the top right corner of the selected Analytics page. The PDF file is generated and downloaded to the default downloads folder.

Interception Analytics

Guest Manager provides three graphs that show the interception of guest users by days and by location.

Interception projects before us the website that were intercepted by the user while using the Wi-Fi at a particular location. For instance, we have a Cromia store, the Cromia store wants to know what

percentage of people use website like Amazon, Tech store or any other Gadget website on their phones. Based on the data they receive, they can trigger some related offers for the customers in their store which in turn helps to increase the sales. You can view these graphs under **Analytics > Interception**. The graphs are as follows:

- **Websites Intercepted:** This is a bar graph that plots the percentage of guest users accessing the Wi-Fi facility and the number of website intercepted.

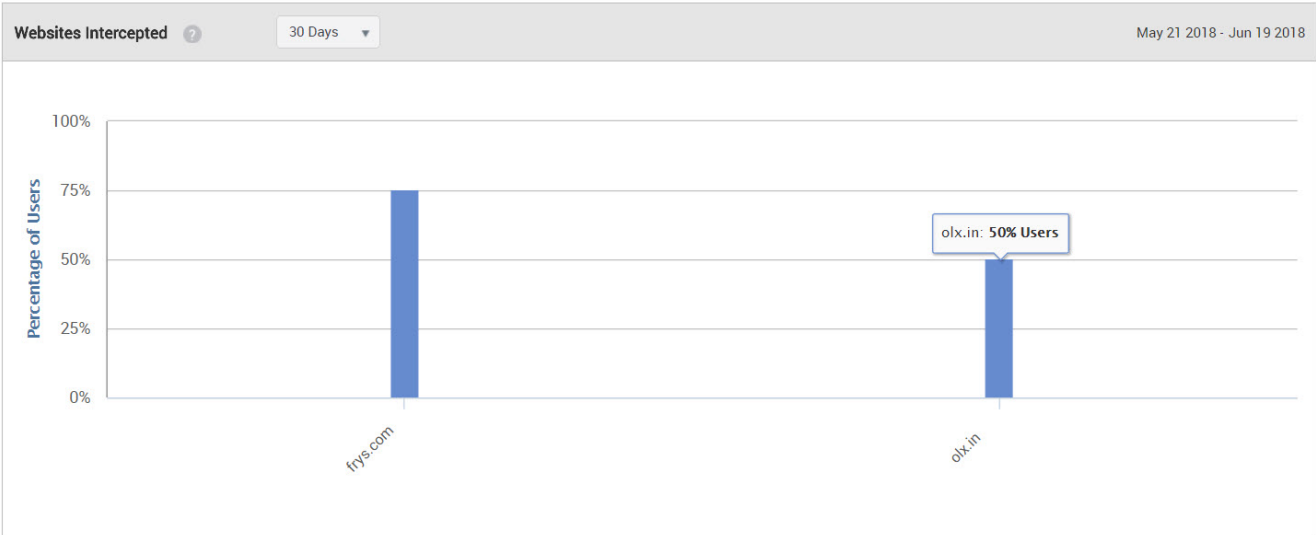


Figure 20: Websites Intercepted

- **Users Engaged by Duration:** This is a bar graph that plots the number of guest users who access the Wi-Fi facility and accessed the intercepted websites and the days they received SMS or MMS.

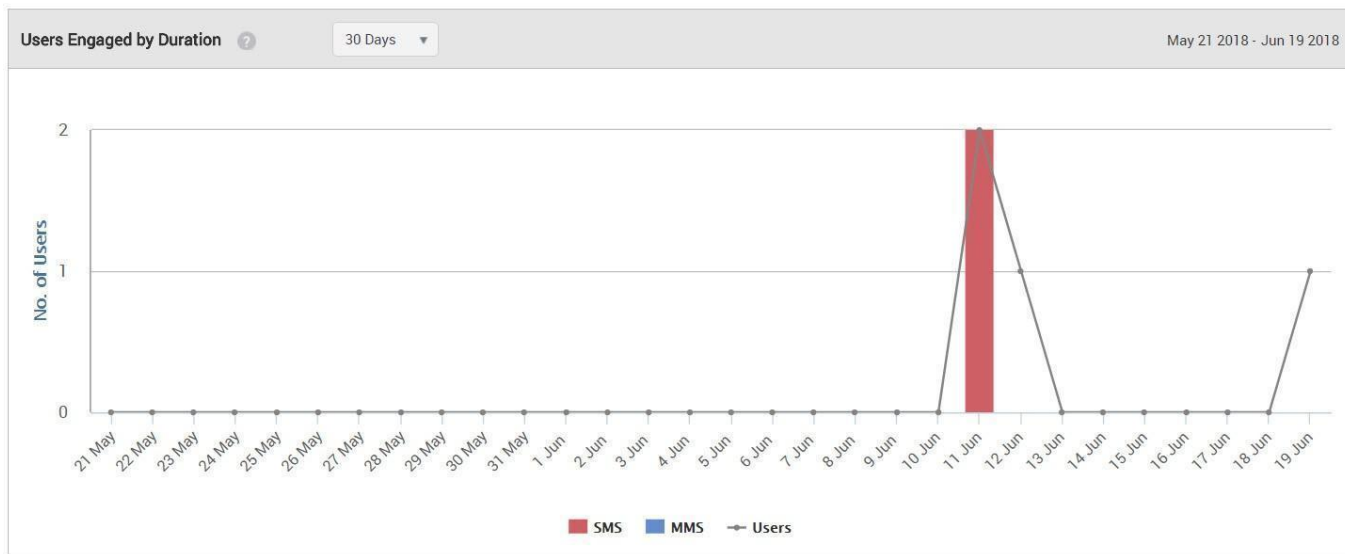


Figure 21: Users Engaged by Duration

- Users Engaged by Location: This is a location-wise bar graph that plots the number of guest users who accessed the Wi-Fi facility, intercepted by SMS or MMS.

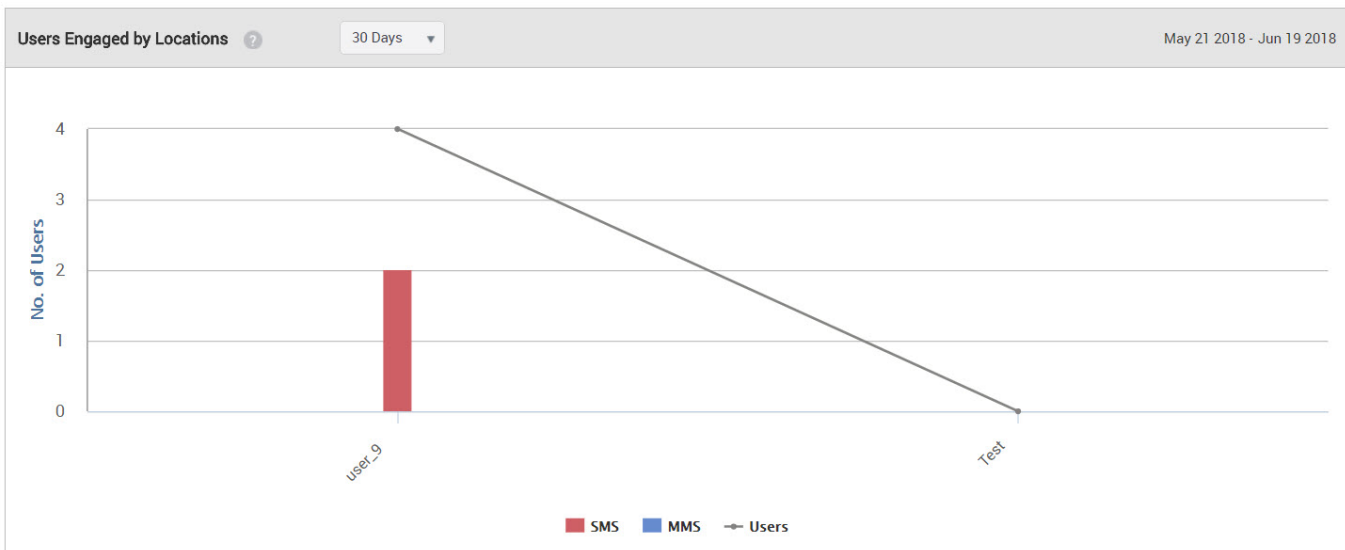


Figure 22: Users Engaged by Location

Clients with Random MAC Addresses

iOS, Android, and Windows OS have introduced the use of randomly generated, locally-administered MAC addresses for Wi-Fi clients. It is done to hide the hardware MAC for security reasons. As a result, identifying such devices by its MAC is not possible because the MAC address keeps changing with time. This resulted in problems with displaying some of the charts in the GM, which use MAC addresses as the primary means to uniquely identify a client.

When clients with random MAC addresses connect to an AP, the actual count and the absolute count of the clients are vastly different. Due to MAC Randomization, the same client can connect multiple times with an AP using MAC addresses in a shorter duration. The AP will consider such clients as different clients as the MAC addresses are different in every association. When clients with randomly assigned MAC addresses connect to the GM, GM uses an approximation algorithm to identify such clients. GM then displays a percentage approximation of such clients in all the client-association charts, instead of displaying the actual count.

The following table shows which charts are different or have changes when you enable the MAC Randomization feature. For graphs that are not mentioned in the table, you can assume that it is unchanged irrespective of whether Random MAC is enabled or disabled.

GM Charts	Change	Modification
Conversion	Yes	Shows only the total footfall.
WiFi Users	Yes	Shows only the percentage change in footfall instead of the absolute count.
New vs Repeat Users	Not available	Deleted from the GM UI when MAC Randomization is enabled.
Dwell Time	Yes	
Presence > Footfall by Duration	Yes	
Presence > Footfall by Location	Yes	
Presence > dwell time by duration	Yes	Shows an approximate percentage of clients instead of an absolute count.
Presence > dwell time by location	Yes	Shows an approximate percentage of clients instead of an absolute count.
Conversion > Conversion by Duration	Not available	Deleted from the GM UI when MAC Randomization is enabled.
Conversion > Conversion by Location	Not available	Deleted from the GM UI when MAC Randomization is enabled.

GM Charts	Change	Modification
Demographics > Login Methods by Duration	Yes	Converted the Y-axis into an approximate percentage count instead of an absolute count.
Demographics > Login Methods by Location	Yes	Converted the Y-axis into an approximate percentage count instead of an absolute count.
Demographics > Social Engagement by Duration	Yes	Converted the Y-axis into an approximate percentage count instead of an absolute count.
WiFi Usage > Social Engagement by Location	Yes	Converted the Y-axis into an approximate percentage count instead of an absolute count.
Floor Map	Yes	

The following charts are updated for MAC Randomization:

Conversion

This widget presents the statistics related to the people with Wi-Fi enabled devices, but not connected to the Wi-Fi service offered by the store. The Conversion widget presents the total number of people with Wi-Fi enabled devices in and around the store, the number of visitors with Wi-Fi enabled devices present inside the store. The percentage of the storefront conversion displayed in this widget represents the number of visitors inside the store as compared to the number of people inside and around the store.

The following image shows the **Conversion** widget.

Conversion

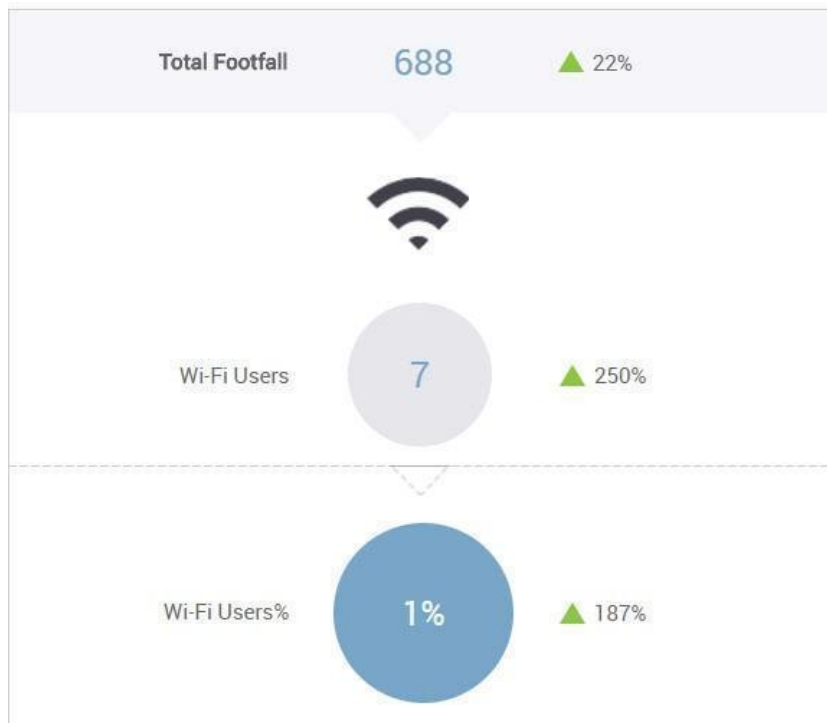


Wi-Fi Users

The Wi-Fi Users widget presents the total visible visitors inside and outside the store, the total users who have used Wi-Fi, and the percentage of the visitors using the guest Wi-Fi out of the total users.

The following image shows the **Wi-Fi Users** widget.

Wi-Fi Users

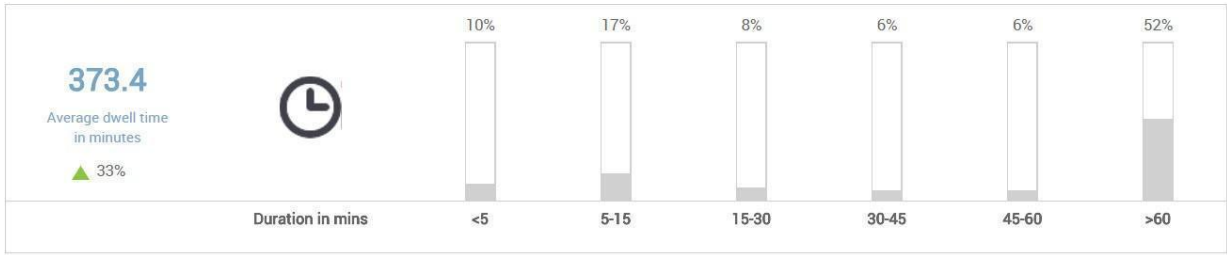


Dwell Time

Dwell time is the time for which a user is visible to the access points installed in the store. The dwell time widget displays a bar graph of the percentage of visitors for different time- ranges. The unit of measurement for the time range is minutes. The widget also displays the average dwell time in minutes.

The following image shows the **Dwell Time** widget.

Dwell Time

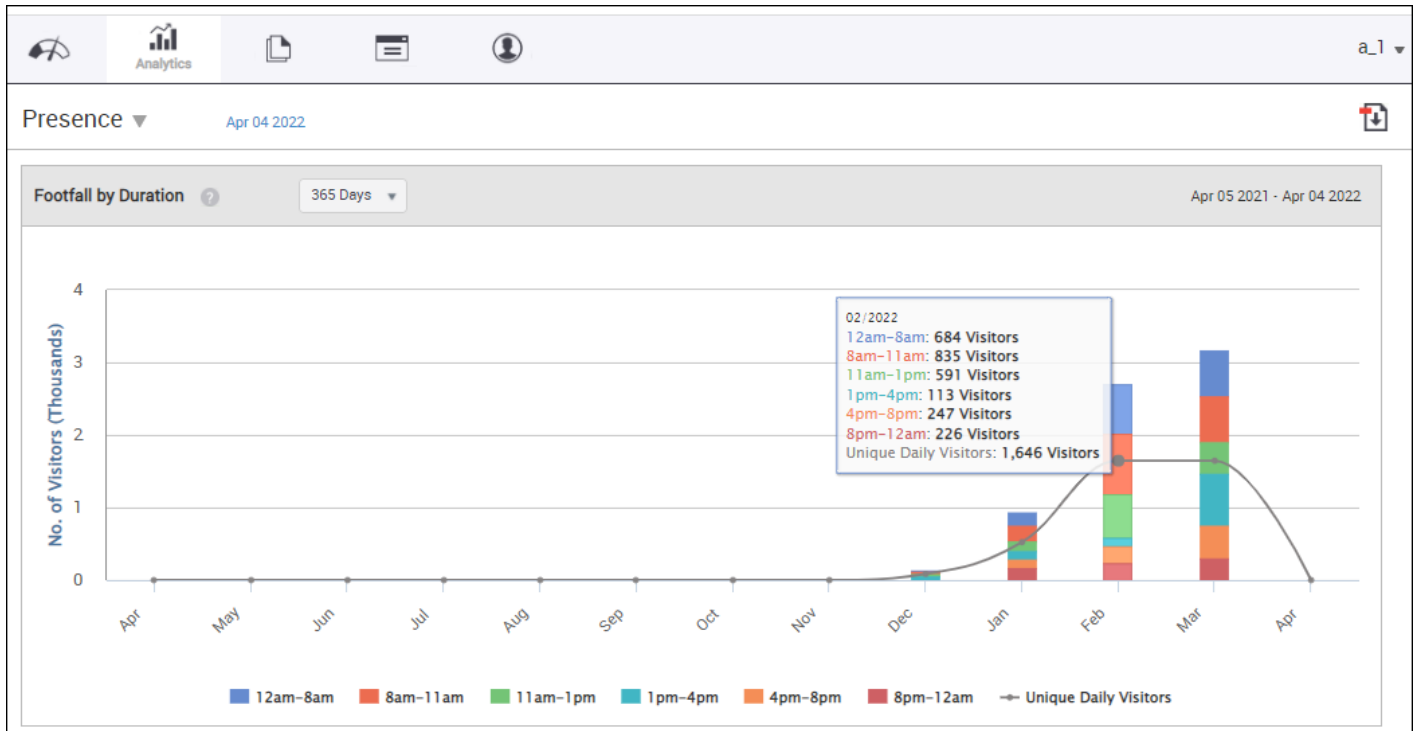


Footfall by Duration

This is a bar graph that shows the number of visitors during different time splices of a day for the specified duration and at the selected location. The graph also plots the total number of visitors for each day at the selected location for the specified duration. The number even includes the guest users who haven't even accessed the Wi-Fi but were duly visible. The data displayed on the graph for each time splice is based on the time zone set for the location selected in the tree. That is to say, you select a node with multiple locations under it. The graph plots the total number of visitors for each day (based on the duration selected). The graph also plots the total number of visitors during a specific time period of the day (time splice). The total number of visitors for a specific time splice is calculated by aggregating the visitor count during the said time splice for each location based on the time zone of the location. We can access their presence for a span of 7, 14, 30, 60, 90, 180, or 365 days.

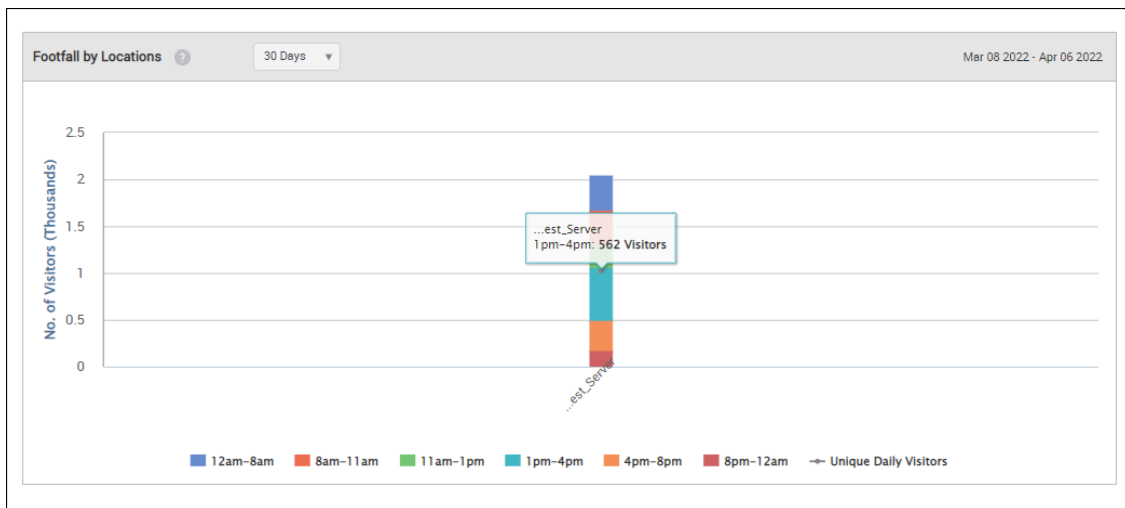
When you need a 7-day chart, you will easily be able to track the per day data of the visitors in and around the store from Monday to Sunday. But when you go for >60 days slot you will be able to see per week data for 60 days. And for 365 days you can view the per month data. The

granularity changes as per the data distribution for the duration. If a user accesses the Wi-Fi in a particular time slot like 8 am-12 pm multiple times, it will be counted as one visit for that time slot. But if he logs in under different time slots, he will be counted different for each time but for an overall view for the parent location, the guest user will be counted as one visitor. Similarly, If the person logs in through different devices in the same time slot or different slot, he will be counted as a different visitor each time as that login depends on the MAC address of the device. Different MAC addresses will count as different visitors. Due to MAC Randomization, the footfall count shown in chart is an approximation and not an absolute count.



Footfall by Locations

This is a location-wise bar graph depicting the total number of visitors during different time periods of the day (time splice) aggregated for the specified duration. The data is plotted for the selected location and its immediate child locations. Assume, there is one root location also known as the parent location. The parent location has many child locations. For example, *Arista -- **Maharashtra-- ***Pune--- ****Alpha-- ****Gamma-- ****Beta-- ***Mumbai-- ***Kolhapur-- This is the location tree. Arista is the root location which has Maharashtra as the child. Which in turn has Pune, Mumbai, Kolhapur as its child nodes. Pune in turn has alpha, gamma, beta as its child locations. When the chart is made, we pick up a location. Suppose out of the folders, you select Pune as my location. You can see the visitors or clients for Pune location as well as for its child location. So, you will see a chart for Pune+Alpha's visitors+Beta's visitors+Gamma's visitors. This chart will be an aggregation of the parent+child location. Due to MAC Randomization, the count shown in chart is an approximation and not an absolute count.



Dwell Time by Duration

This is a bar graph showing total number of users who have accessed the Wi-Fi for different time periods during each visit for the specified duration and at the selected location. Due to MAC Randomization, the count shown in chart is an approximation and not an absolute count.

The Dwell time depends on the RSSI value that we receive. The relative signal strength of the Wi-Fi is considered to be good the more its value is closer to 0. So, when a client connects for a particular time slot, its duration is mapped. This is again an aggregated data. Suppose, in the time slot of 8-11 am, a client logs in at 8-9 am for 4 minutes and again logs in from 9-10 am for

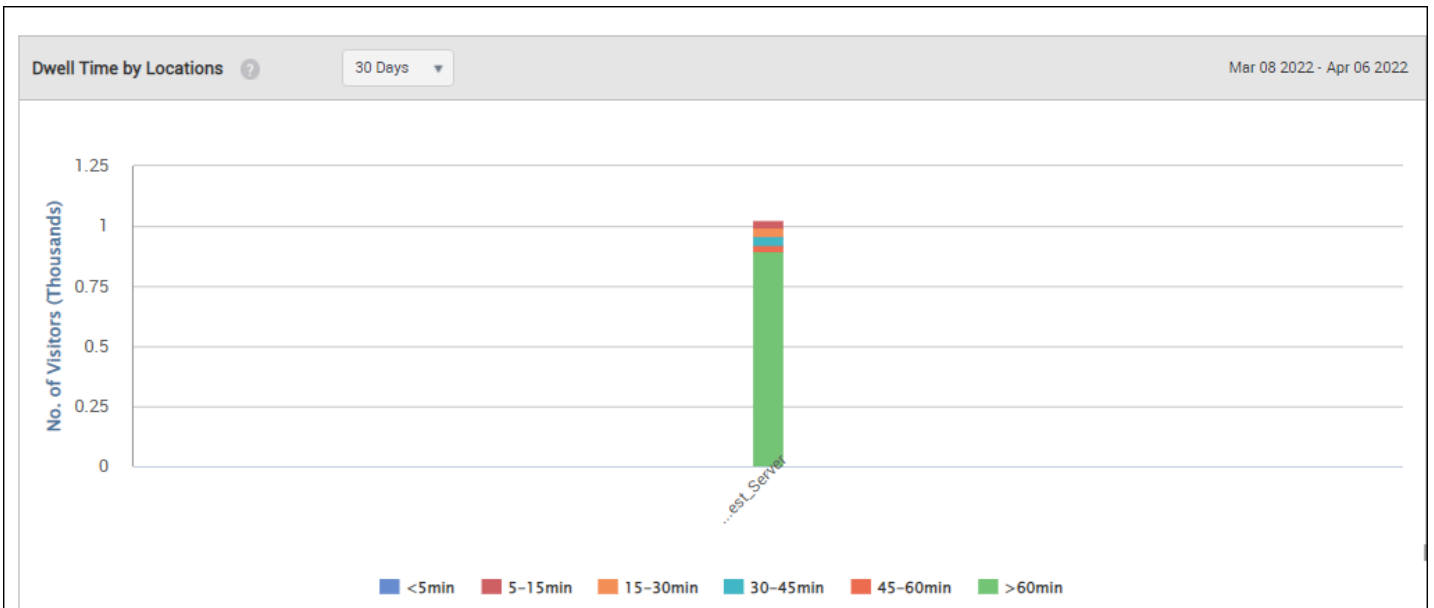
3 mins. If he does so, his total time slot will be 4+3= 7 minutes and will be depicted on the chart, accordingly.



Dwell Time by Location

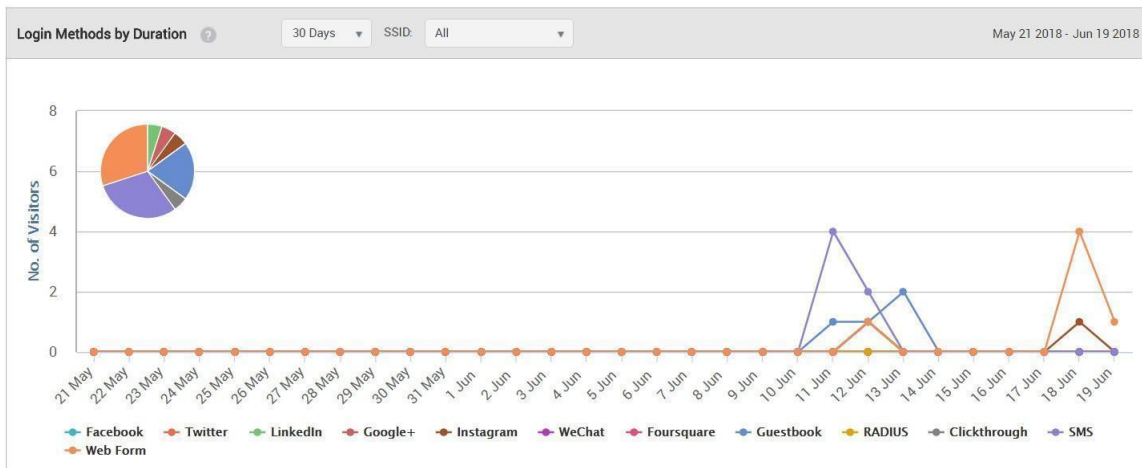
This is a location-wise bar graph depicting the total number of users who have accessed the Wi-Fi for different time periods during each visit. Due to MAC Randomization, the count shown in chart is an approximation and not an absolute count. The data is aggregated for the specified duration. The data is plotted for the selected location and its immediate child locations. Dwell time by location shows us the customers that have logged in at a particular location for a particular time slot. These values depend on the RSSI value. Let us take an example; suppose there are 4 locations where Arista APs are placed- Alpha, Beta, Gamma, and Phi. Now, the customer is at Beta location but is visible to both the Beta and Alpha locations. Our problem begins how will we calculate which parameter to count. That is when RSSI values come into action. On location Alpha, the RSSI values for customer is as follows: He logged in from 10:01 am - 10:05 am.

Sensor A detects For time = 10:01; RSSI value = -60 dbm, For time 10:02; RSSI value = -40 dbm, For time 10:03; RSSI value= -255 dbm, For time 10:04; RSSI value= -30 dbm, For time 10:05; RSSI value= -255 dbm. *Sensor B* detects only for the duration: 10:02- 10:04 where, For time 10:02; RSSI value= -30 dbm, For time 10:03; RSSI value= -255 dbm, and For time 10:04; RSSI value= -60dbm. Now, we calculate the best RSSI value for all the particular slots by comparing sensor A and B. The aggregated data comes For time 10:01; RSSI value= -60 dbm, For time 10:02; RSSI value= -30 dbm (out of -60 and -30,-30 is the best value), For time 10:03; RSSI value= -255 dbm, For 10:04; RSSI value= -30dbm, For 10:05; RSSI value= -255 dbm. This is the aggregated data based on the best of RSSI values. We know the value -255 dbm means that no data came for these time slots. So, these time slots are automatically canceled. Then as per what we receive, we have data only for 4 minutes. Based on data calculated on RSSI values we get the graph plotted.



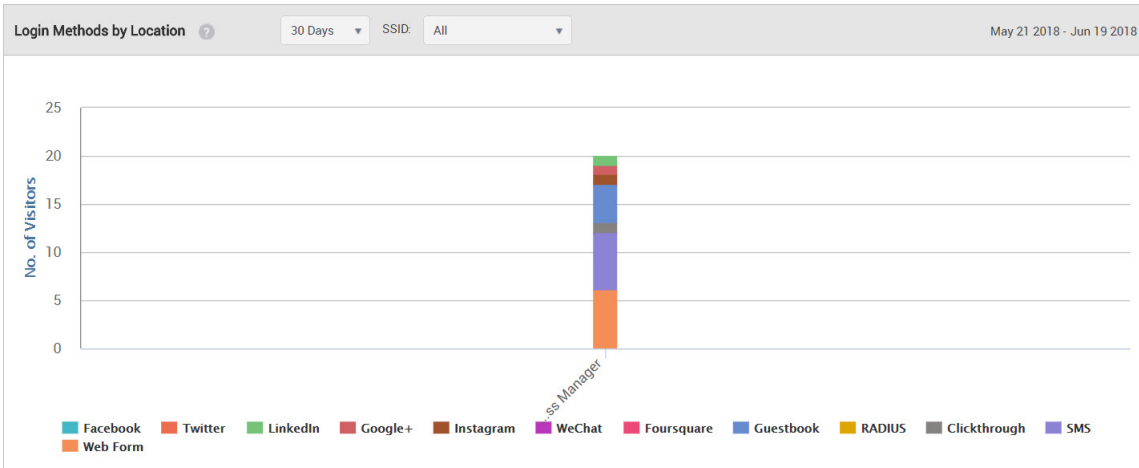
Login Methods by Duration

Line graphs charting login method wise visitors (guests) accessing the Wi-Fi. For the location selected on the left pane, the line graph shows the number of visitors for each plug-in (social media, guest book, and click-through) during the specified duration for the selected SSID based on the data availability date or custom date selected by you. Due to MAC Randomization, the count shown in chart is an approximation and not an absolute count. To select the date, click the date seen on the top of the Analytics page. A pie chart representation of the distribution is also seen for the selected duration and SSID. By default, the graph and pie chart are based on last 7 days of data (with the date seen on top of the Analytics page as the last date) for all the SSIDs defined on the servers is displayed.



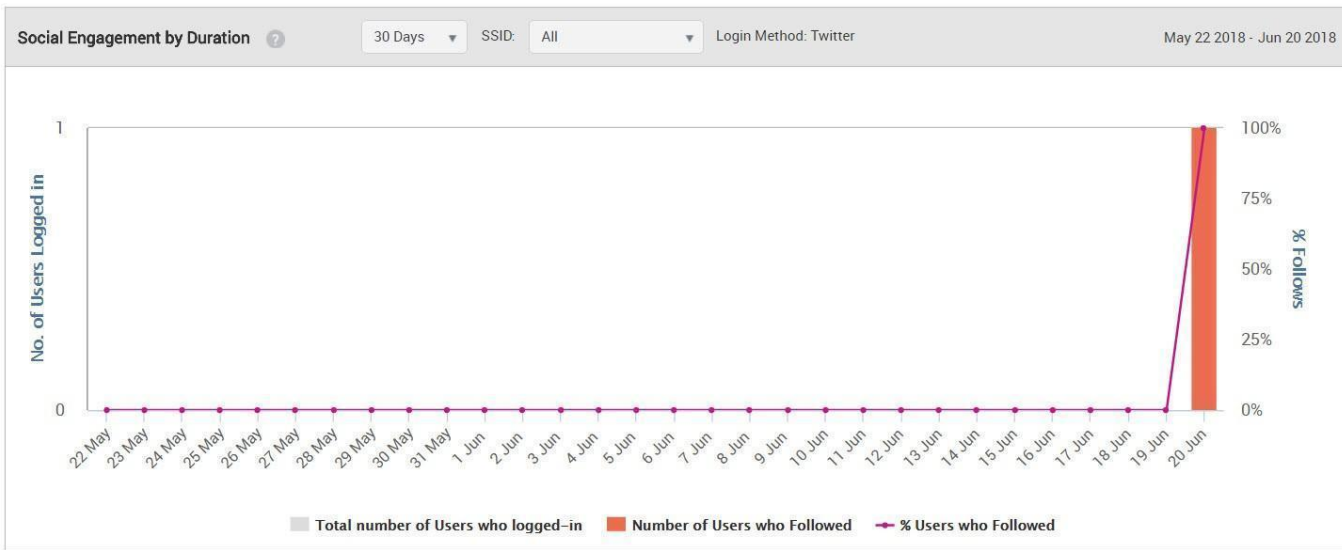
Login Methods by Location

A bar graph showing the login method wise percentage of guests for the selected location and its child locations that have accessed the Wi-Fi during the specified time duration for the selected SSID.



Social Engagement by Duration:

A chart showing the number of guests based on approximation who logged in using social media authentication, for example Twitter, and liked the page for the selected duration. The Y-axis also displays



Social Engagement by Location

A chart showing the number of guest users who logged in using social media authentication, for example Twitter, and liked the page for a selected location.

Social Engagement by Location ?

30 Days ▾

SSID: All ▾

Login Method: Twitter

May 22 2018 - Jun 20 2018



Log Management

Guest Manager provides a few log management features. The logs help you in analyzing the usage pattern of the Wi-Fi as well as the actions performed on your Guest Manager account.

This chapter covers the following topics.

- [*Download User Audit Logs*](#)
- [*Download Guest Wi-Fi Access Logs*](#)
- [*Download SMS Logs*](#)
- [*Download Payment Logs*](#)

Download Guest Wi-Fi Access Logs

The guest Wi-Fi access logs for all the portals can be downloaded from the Admin> Logs page. You must have the Administrator role to download the access logs.

You can download Wi-Fi access logs for the specified number of hours, days or months before the Guest Manager system date. Alternatively, you can specify a date range for which you want to download the Wi-Fi access logs.

To download the access logs for specified hours, days or months before Guest Manager system date, perform the following steps:

1. Click the **Admin** tab and then click **Logs**.
2. Under **WiFi Access Logs**, select **Last** and specify the number of hours, days or months for which you want to download the Wi-Fi access logs. Also select the unit of measurement of time as hours, days or months.
3. Click **Download** to download logs for the specified time duration.

To download the access logs for a specific date range, perform the following steps:

4. Click the **Admin** tab and then click **Logs**.
5. Under **WiFi Access Logs**, select **Custom** and specify the from and to date and time for which you want to download the access logs. Use the calendar icon and clock icon to select the date and time respectively.
6. Click **Download** to download logs for the specified time duration.

The following table describes the fields displayed on the Access Logs

page: Option	Description
Portal	Name of the portal accessed by the guest user.
Type	Type of access operation. This indicates whether it is a login, logout, portal access or

Option	Description
	gate access. Portal access entry is recorded when the user accesses the portal. A gate access entry is recorded when the access point opens the gate for the user to access the Internet.
Client IP	IP address of the client used by the guest user to connect to the access point.
Client MAC	MAC address of the client used by the guest user to connect to the access point.
AP MAC	MAC address of the access point used by the guest user to access Wi-Fi.
AP SSID	SSID of the access point accessed by the guest user.
AP IP	IP address of the access point accessed by the guest user.
AP Port	Port number used to communicate with the access point.
User Agent	User agent details of the browser used by the guest user to access Wi-Fi.
User URL	URL accessed by the guest user.
Username	The user account used to access the Wi-Fi followed by the plug-in name. In the case of the LinkedIn plug-in, the first name and last name of the guest user is displayed instead of the user account.
Message	Provides gateway access and log off URLs.
Date/Time	Date and time of access by the guest user

Download User Audit Logs

The audit logs provide information about the Guest Manager user activities. You must have the Administrator role to access the audit logs. Audit logs for self-registered users are retained for 30 days. These are the 'temp' type audit logs and they are deleted after 30 days of their creation.

To download the audit logs for specified hours, days or months before Guest Manager system date, perform the following steps.

1. Click the **Admin** tab and then click **Logs**.

2. Under **Audit Logs**, select **Last** and specify the number of hours, days or months for which you want to download the Wi-Fi access logs. Also select the unit of measurement of time as hours, days or months.

3. Click **Download** to download logs for the specified time duration.

To download the audit logs for a specific date range, perform the following steps

4. Click the **Admin** tab and then click **Logs**.

5. Under **Audit Logs**, select **Custom** and specify the from and to date and time for which you want to download the access logs. Use the calendar icon and clock icon to select the date and time respectively.

6. Click **Download** to download logs for the specified time duration.

The following table describes the information displayed in an Audit Logs CSV file.

Option	Description
Serial No	Running serial number.
IP Address	IP address of the computer device from which the operation was performed.
Operation Type and performed	Type of operation. The operation types logged are Create, Read, Update, Delete, and Other. Some operations, such as login and logout, are categorized as Other.
Date/Time	Date and time of the operation.
Username	User name of the Guest Manager user who performed the operation.
Portal Name	Name of the portal for which the operation was performed.
Role	Role assigned to the user in Guest Manager.

Reports Management

You can create custom reports for a location floor with Guest Manager versions 4.2 and above.

A report is made up of one or more segments. A segment represents a part of a report. A segment consists of a section, a chart for the selected section, and the duration for which the selected chart is to be populated in the report. The available sections are Dashboard, Demographics, Presence, Engagement, Wi-Fi Usage or Floor Maps. The other filters for the segment such as SSID or time range are made available based on the section selected for a segment. A custom report can contain up to 20 different segments.

This chapter covers the following topics

- [Create Custom Report](#)
- [Schedule Custom Report](#)
- [Download Custom Report](#)
- [Email Custom Report](#)
- [Duplicate Custom Report](#)
- [Delete Custom Report](#)

Create Custom Report

You can create one or more custom reports for a location floor. Each report can have segments with different filter criteria. A custom report can have one segment with a Dashboard section, one segment with a Floor Maps section, and one or more segments with the remaining sections.

The Demographics, Presence, Engagement, Wi-Fi Usage sections can be repeated in a custom report with different filters applied to each of the repeating sections.



Important: You cannot create a custom report unless a floor map has been attached to the location floor. The floor map is attached to a location floor through Wireless Manager.

To perform this task, you must have the Administrator, Analyst or Marketing Executive role assigned to you.

To create a report, perform the following steps.

1. Click the **Reports** tab.
2. Select the location floor for which you want to create the report.
3. Click **New Report**.
4. Enter the report name.
5. Click the **Add** icon to add a new segment.
6. Select the section.

7. Select the chart.
8. Select the duration.
9. Select the appropriate option from any other filters that appear.
10. Repeat steps 4 through 8 to add new segments to the report.
11. To delete a segment, click the **Delete** icon.
12. To duplicate the current segment, click the **Copy** icon.
13. Click **Save**.

Schedule Custom Report

Once a report is created and saved, you can add a schedule to the report to automatically generate the report at the specified frequency.

To perform this task, you must have the Administrator, Analyst or Marketing Executive role assigned to you.

To create a report, perform the following steps.

1. Click the **Reports** tab.
2. Select the location floor for which the report has been created.
3. Click the three dot menu for the report and click **Schedule**.
4. Enter the schedule details.

Option	Description
Frequency Type	One time and Recurring are the available options. Select One time to generate the report just once. Select Recurring to generate the report at regular intervals.
Repeat Every	Applicable if frequency type is Recurring. Select the interval at which you want to generate the report. The frequency could be daily, weekly or monthly. Select the number of days, weeks or months after which the report is to be generated.
Start Schedule	Start date of the schedule.
End Schedule	End date of the schedule.
Email Addresses	Comma-separated e-mail addresses to which the report is to be sent.

Option	Description
Active	Select the check box to activate the schedule. Deselect the check box to deactivate the schedule.

5. Click **Save**.

Download Custom Report

You can create custom reports for a location floor with Guest Manager versions 4.2 and above.

You can download a custom report.

To perform this task, you must have the Administrator, Analyst or Marketing Executive role assigned to you.

To create a report, perform the following steps.

1. Click the **Reports** tab.
2. Select the location floor for which the report has been created.
3. Click the three dot menu for the report and click **Download**.
4. Select Get Latest Report to get the latest report available on Guest Manager. Alternatively, you can specify a custom date. This is the end date up to which the report is generated. For instance, if the report duration is last 7 days then the custom date is considered as the seventh day.
5. Click Download.

The report is downloaded at the specified location.

Duplicate Custom Report

You can create a copy of an existing report and tweak it when you want a report that is similar to an existing report.

To perform this task, you must have the Administrator, Analyst or Marketing Executive role assigned to you.

To create a copy of an existing report, perform the following steps.

1. Click the **Reports** tab.
2. Select the location floor for which the report has been created.
3. Click the three dot menu for the report and click **Create a Copy**.
4. Enter a new name and click **Duplicate**.

Email Custom Report

You can e-mail a custom report to one or more e-mail addresses.

To perform this task, you must have the Administrator, Analyst or Marketing Executive role assigned to you.

To create a report, perform the following steps.

1. Click the **Reports** tab.
2. Select the location floor for which the report has been created.
3. Click the three dot menu for the report and click **Email**.
4. Select **Get Latest Report** to get the latest report available on Guest Manager. Alternatively, you can specify a custom date. This is the end date up to which the report is generated. For instance, if the report duration is last 7 days then the custom date is considered as the seventh day.
5. Enter comma-separated e-mail addresses to which the report is to be sent by e-mail.
6. Click **Email**.

Delete Custom Report

You can create custom reports for a location floor with Guest Manager versions 4.2 and above.

You can delete obsolete reports.

To perform this task, you must have the Administrator, Analyst or Marketing Executive role assigned to you.

To create a report, perform the following steps.

1. Click the **Reports** tab.
2. Select the location floor for which the report has been created.
3. Click the three dot menu for the report and click **Delete**.
4. Click **Delete** on the Delete Report message box.

The selected report is deleted.