

Azara



User's Guide

TABLE OF CONTENTS

Chapter 1, Tenant Management

1.1	Map View	1-3
1.1.1	Map View	1-3
1.1.2	Floor Plan View	1-6
1.2	Dashboard	1-11
1.2.1	Dashboard Configuration	1-11
1.2.2	Location Based Services Widgets	1-16
1.3	Monitor	1-27
1.3.1	Monitor Summary	1-27
1.3.2	Monitor Access Points	1-28
1.3.3	Monitor Clients	1-34
1.3.4	Monitor Rogues	1-38
1.3.5	Monitoring Event Logs	1-42
1.4	Reports	1-44
1.4.1	Generated Reports	1-44
1.4.2	Manage Reports	1-45
1.4.3	Scheduled Reports	1-48
1.5	Tools	1-50
1.5.1	Packet Capture	1-50
1.5.2	Wireless Debug Log	1-53
1.5.3	Ping/Traceroute	1-56
1.6	Configuration	1-58
1.6.1	Configuring Tenant Networks	1-58
1.6.2	Configuring Sites	1-77
1.6.3	Managing Inventory/Devices	1-84
1.6.4	Configuring Tenant Users	1-98
1.6.5	Configuring Tenant Preferences	1-100
1.6.6	Licensing	1-105
1.6.7	Captive Portal	1-107

Appendix A, Customer Support

CHAPTER 1

TENANT MANAGEMENT

Tenants are consumers of Extreme Networks Azara Cloud system and use the deployed networks across their sites to provide Azara Cloud services to their clients. Access points are deployed at the Tenant's sites to provide Azara Cloud services.

Before Azara Cloud services can be provided to the Tenant's clients, the Tenant account must be created by the MSP. *Managed Services Providers* (MSPs) are Extreme Networks partners and re-sellers who re-brand (white label) Azara service for their end users. The MSP, if required, can also configure different settings on behalf of the Tenant.

The Tenant can configure different parameters to suit their usage requirements from their individual accounts. Generally, the process involves setting up the Network and SSIDs for the VLANs, creating different physical sites where access point can be deployed, add the purchased access point to the account and then assign sites to the access point where they are to be deployed.

After the initial setup, the Tenant can create and add Users to manage the network. Access restrictions can be set at create time for each user account. This controls user access to the Tenant's configuration, reports and tools.

Azara enables Tenants to have a complete and real-time monitoring capability of their network. **Map View** provides an overall view of all the sites deployed by the Tenant on a world map. The Tenant can use Map View to navigate directly to each site's summary information.

Azara's **Tenant Dashboard** is a fully customizable, widget based reporting and monitoring tool. Tenants can create multiple dashboards with different widgets to get a deep insight into their network's state and performance. Each dashboard can be used to view the network state or the state of an individual site.

Azara's **Monitor** screens provide a real-time snapshot of the Tenant's networks, sites and access points. Multiple filtering options are provided to drill-down to the detail of interest. Graphs, charts and filter options enable easy visualization of the state and to quickly identify and mitigate issues.

Azara's **Reports** are highly customizable, detailed and can be drilled-down to show data points of interest to Tenants. Reports can be run on schedule with configurable periods. Reports can be stored on the Azara Cloud server and also mailed to the Tenant.

Azara provides simple **Tools** such as Ping and Traceroute, Packet Capture and Wireless Debug Log to trouble shoot local networking issues.

1-2 Azara User's Guide

This chapter is organized as follows:

- *Map View*
 - *Dashboard*
 - *Monitor*
 - *Reports*
 - *Tools*
 - *Configuration*
-

1.1 Map View

▶ [Tenant Management](#)

Map view displays a visual representation of the Tenant's sites on an interactive map. Use the view to quickly view the sites managed by this Tenant and to quickly navigate to a site to view further details about it.

Click on the map marker to get a summary of the site as a bubble. The information provided include the site's floor plan, summary, the number of access point on this site and their status.

For more information on map view, refer to the following:

- [Map View](#)
- [Floor Plan View](#)

1.1.1 Map View

▶ [Map View](#)

In a multi-site environment, the Azara Dashboard UI **Map View** provides a system-wide network visual overview as well as overviews of individual sites.

At the system level, the Map View displays the geographical location of each site for immediate visualization of the entire network. It also displays the status of the access point (online or offline), number of connected clients, site status (online or offline) and the number of access point down.

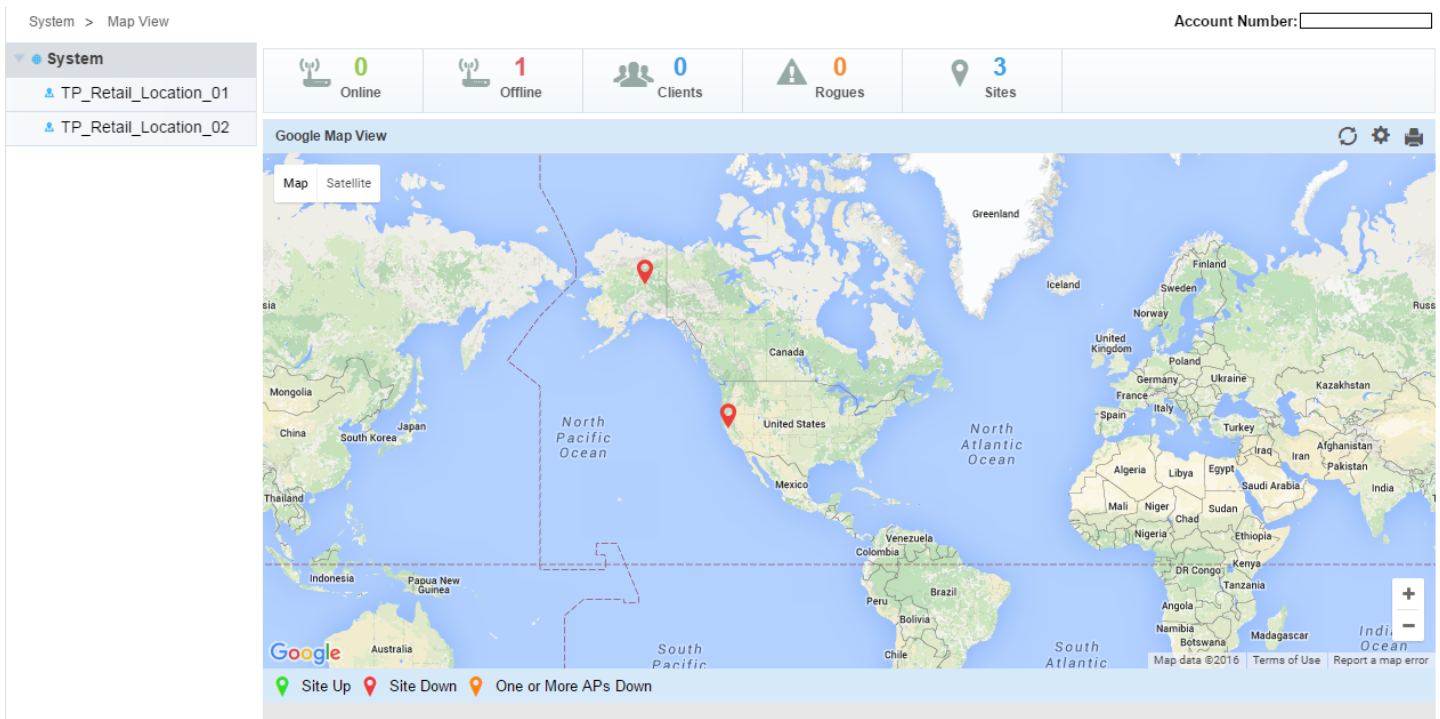


Figure 1-1 Tenant Map View - Geographic View

Use the **MAP/Satellite** button located at the top right of the screen to toggle between geographic and satellite map data. The following is satellite map imagery of the network displayed in the preceding image.

1-4 Azara User's Guide

System > Map View Account Number:


System

- TP_Retail_Location_01
- TP_Retail_Location_02

0 Online	1 Offline	0 Clients	0 Rogues	3 Sites
--------------------	---------------------	---------------------	--------------------	-------------------

Google Map View Refresh Settings Print

Map Satellite



Map data ©2016 Imagery ©2016 NASA, TerraMetrics Terms of Use Report a map error

Site Up Site Down One or More APs Down

Figure 1-2 Tenant Map View - Satellite View

At the site level, the Map View displays uploaded facility floor map(s).

1.1.1.1 Placing Sites Using Map View

▶ [Map View](#)

Sites can be dragged and dropped on the Map View screen. If a site has been created, but no geo location information provided, the Map View screen can be used to locate the site on the map.

To locate a site on the map view:

1. From the Map View screen, select the  icon. The following screen displays:

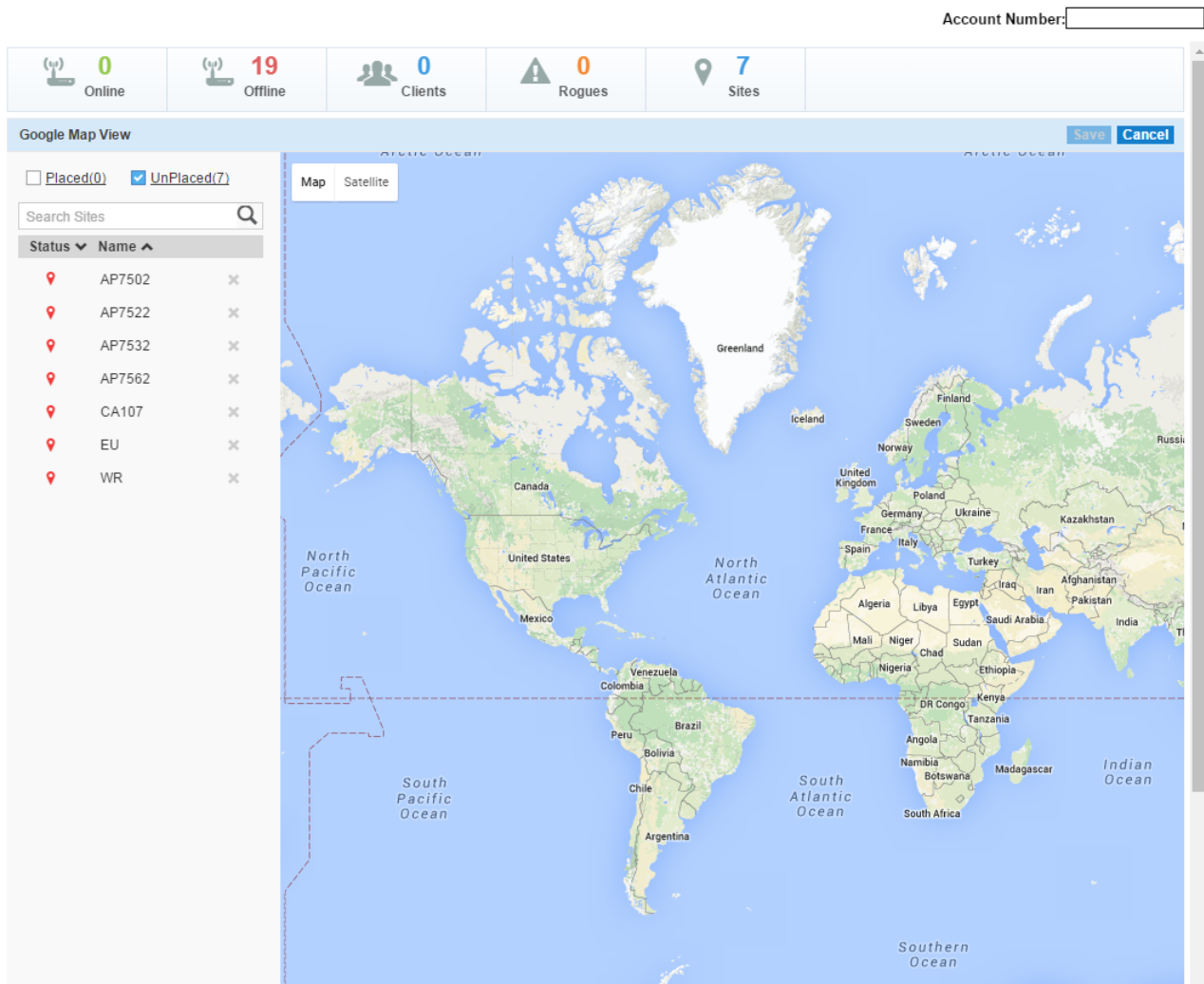


Figure 1-3 Map View - Configure screen

By default, the screen displays a list of all sites created but not placed on the map. Use the **Placed** check box at the top left of the screen to display the placed sites.

2. To place a site on the map, zoom to the appropriate location on the Map view. Once the site has been located on the map, select the correct site from the list on the left of the screen and drag it to the location.

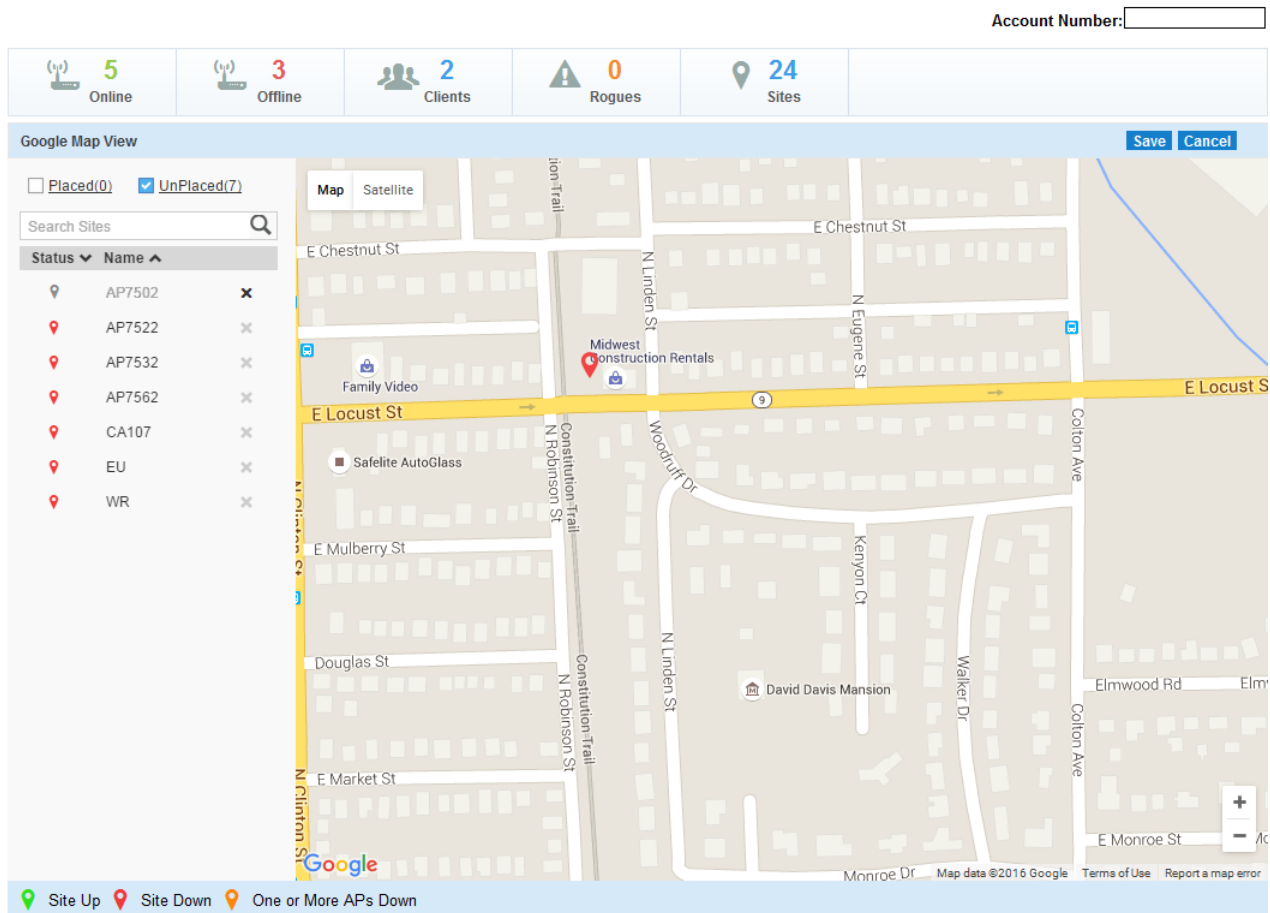


Figure 1-4 Map View - Configure - Place Site

3. To remove a newly added site from the map, select the “X” button located next to the site’s name in the list to the left of the screen. The site’s map marker is immediately removed from the screen.
4. Select **Save** from the top right to save this information. Select **Cancel** to exit this screen without saving the changes.

1.1.2 Floor Plan View

► Map View

The Floor Plan view displays a floor plan of the Tenant site. Each site’s floor plan must be uploaded to Azara Cloud and associated with the appropriate site before it can be displayed.

The Floor Plan view provides a highly customizable display of the Tenant’s site overlaid on a floor map. The administrator can choose from a large set of data points to display. Each of the selected data points are overlaid on the site’s floor map for a visualization of the current state of the site.

Floor plans are loaded and associate with the site from the **Configuration > Sites** screen. Multiple floor plans can be associated with a site. The floor plan view screen is only available when at least one (1) floor plan is associated with a site.

A floor map is interactive, allowing an administrator to embed any network or RF-specific attributes of an access point and its connected clients. Network-specific information can be optionally displayed, including RF channel assignments, SNR, retries, power, throughput and connected client count.

Before using the Floor Plan view, the site’s access points have to be placed on the floor plan. Use the icon located towards the top right of the screen to display a screen from where the access point can be placed on the floor map.

Use the **RF Quality Index** fields to quickly identify access points with poor RF quality. The labels are color coded to display the access point's RF quality based on the signal strength of its connected clients and their retry rates. Use the tool's sliders to filter access points with poor RF quality and show additional RF parameters (retry rates, throughput and connected clients).

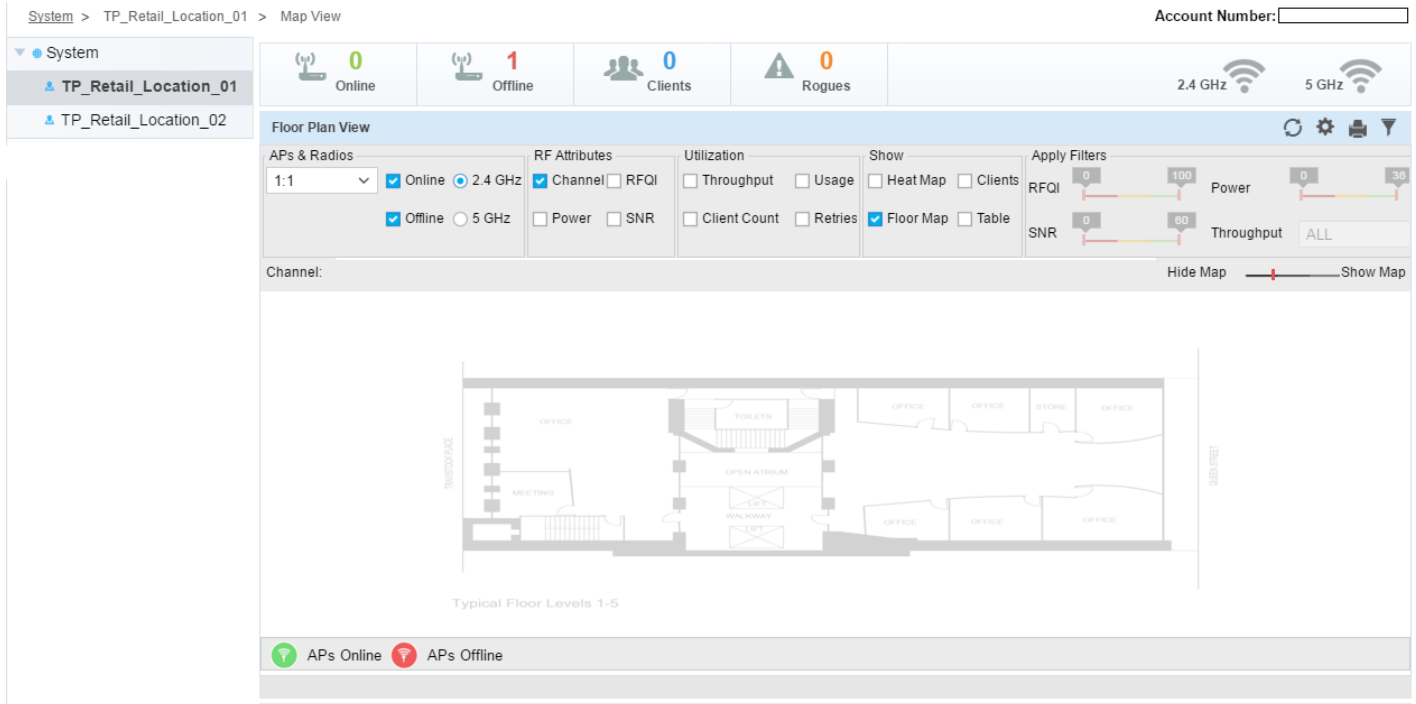


Figure 1-5 Tenant Map View - Floor Plan View

The site-level floor plan view can be customized to display the following:




APs & Radios: Online	Select or clear this option to either display or hide online access points and radios on the site map. Use this option to filter online versus offline device radios to help assess areas of coverage strength and weakness.
APs & Radios: Offline	Select or clear this checkbox to display or hide detected (but offline) access points and their radios on the site map.
APs & Radios: 2.4 GHz / 5 GHz	Select either the 2.4 GHz or 5 GHz option to define the RF band to filter and display on the site map.
RF Attributes: Channel	Select or clear this option to display or hide RF channels on the site map. Use this data to determine whether additional channel assignments are needed to better segregate client traffic in specific, highly impacted, areas of a floor map.
RF Attributes: Power	Select or clear this checkbox to display or hide power levels on the site map.
RF Attributes: RFQI	Select or clear this checkbox to display or hide a RF quality index. The RF quality index reflects network signal strength for the selected site.
RF Attributes: SNR	Select or clear this checkbox to display or hide <i>signal-to-noise ratio</i> (SNR) information on the site map. This information helps to determine the site's overall level of device interference and whether radio compensations are required.
Utilization: Throughput	Select or clear this checkbox to display or hide data-throughput speed on the site map.

1-8 Azara User's Guide

Utilization: Client Count	Select or clear this checkbox to display or hide adopted client counts on the site map. Use this information to assess the site's overall client load and distribution.
Utilization: Usage	Select or clear this checkbox to display or hide data usage (throughput) information on the site map. Periodically check this value to determine whether certain times of the day require greater coverage for resource requesting clients.
Utilization: Retries	Select or clear this checkbox to display or hide client connection retry information. When selected, the system periodically determines whether a particular site stands out in respect to large numbers of client connection attempts and retries.
Show: Heat Map	Select or clear this checkbox to display or hide RF heat map information. Heat map can be either for <i>Coverage</i> or <i>Noise</i> . The heat map displays RF coverage based on a color code, from red to green, indicating signal strength and is a means or visually indicating areas of good and bad radio coverage in specific areas on the floor map.
Show: Floor Map	Select or clear this checkbox to display or hide RF floor map information. The floor map, if uploaded, shows the site's geographical location and map.
Show: Clients	Select or clear this checkbox to display or hide client deployment information, represented by blue dots per client on the site map.
Show: Table	Select or clear this checkbox to display or hide RF attributes for each access point and radio within the site.
Apply Filters: RFQI	If selecting <i>RF Attributes: RFQI</i> , use the slider to filter the information displayed to fit the quality index ratio selected. This filter is disabled if <i>RF Attributes: RFQI</i> is not selected.
Apply Filters: SNR	If selecting <i>RF Attributes: SNR</i> , use the slider to filter the information displayed to fit the signal-to-noise ratio selected. This filter is disabled if <i>RF Attributes: SNR</i> is not selected.
Apply Filters: Power	If selecting <i>RF Attributes: Power</i> , use the slider to filter the information displayed to fit the power selected. This filter is disabled if <i>RF Attributes: Power</i> is not selected.
Apply Filters: Throughput	If selecting <i>Utilization: Throughput</i> , use the Throughput drop-down menu to select the unit in which throughput is displayed. Units are selectable in ranges from 1 kbps to 1000 Gbps.

Use the **Hide Map-Show Map** control function to adjust the transparency of the underlying floor map. Sliding the control towards the **Show Map** label darkens the underlying floor map. Sliding the control towards the **Hide Map** label lightens the underlying floor map.

Use the following table to understand the functions of other icons on this screen.


	Refresh - Use this button to refresh the data on this screen.
	Show/Hide Filter Criteria - Use this button to show or hide the different filter criteria.
	Print - Use this button to create an output of this screen for printing.

1.1.2.1 Placing Access Points Using Floor Map View

► *Floor Plan View*

Access points can be dragged and dropped on the Floor Map View screen. If an access point has been created, but not placed on the floor map, use the Floor Map View screen to place the access point on the site.

To place an access point on a site's floor map:

1. From the Floor Map View screen, select the  icon. The following screen displays:

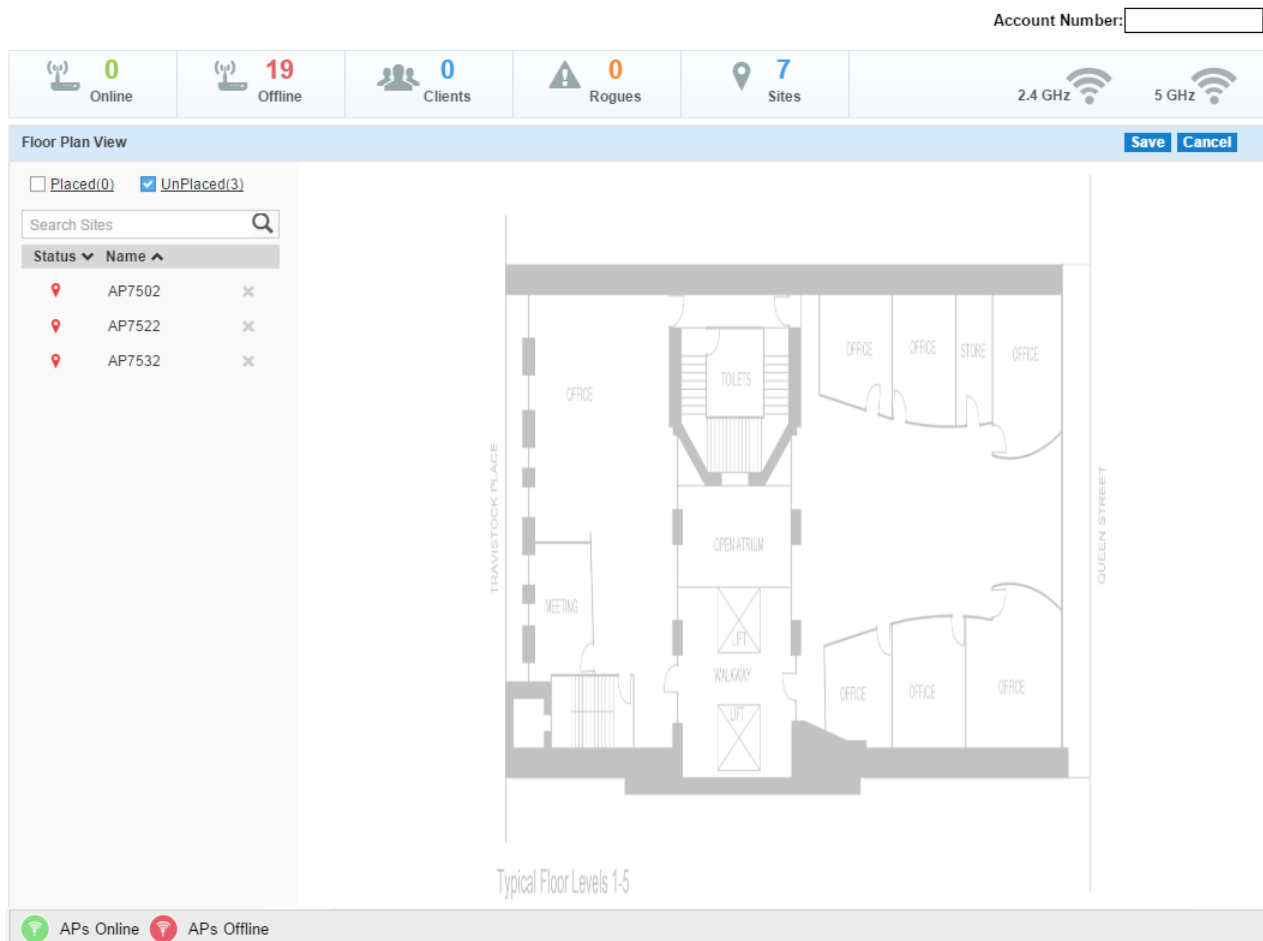


Figure 1-6 Floor Map View - Configure screen

By default, the screen displays all access points that are assigned to this site but not placed on the floor map. Use the **Placed** check box at the top left of the screen to display placed access points.

2. To place an access point, drag the access point from the list on the left of the screen to its intended location on the map. Repeat the process for additional access points as required.

1-10 Azara User's Guide

Account Number:

0 Online 19 Offline 0 Clients 0 Rogues 7 Sites 2.4 GHz 5 GHz

Floor Plan View Save Cancel

Placed(0) UnPlaced(3)

Search Sites

Status	Name	
	AP7502	
	AP7522	
	AP7532	

Typical Floor Levels 1-5

APs Online APs Offline

Figure 1-7 Floor Map View - Configure - Place Access Point

3. To remove a newly added access point, select the "X" button located next to the access point's name in the list to the left of the screen. The access point's map marker is immediately removed from the screen.
4. Select **Save** from the top right to save this information. Select **Cancel** to exit this screen without saving the changes made to this screen.

1.2 Dashboard

▶ [Tenant Management](#)

The Dashboard is a completely customizable, configurable screen that provides a Tenant administrator or user a widget based window to view the status of the Tenant's network and sites.

Use the provided widgets to get detailed and drilled-down information on the Tenant network and the dashboard as a container to display these widgets.

Widgets are classified according to the data they access and display. Categories include Utilization, RF (Radio Frequency), Clients, Security, Captive Portal and Application Visibility. Widgets from any of these categories can be combined to create the Dashboard.

Dashboards provide the display layout for the widgets. Layouts are available for different combinations of number of widgets and their possible physical positions on the dashboard. Tenant administrators can select the layout appropriate for their requirements.

Dashboards provide comprehensive data filtering capability, based on time duration of the data to be displayed, that is applied to all the widget included in the dashboard. Also, data can be further filtered on a per widget basis if the widget supports applying such a filter.

The same dashboard displays data at the System level and for the individual sites too.

Multiple dashboards can be created with different combinations of layouts and widgets. A maximum of 32 dashboards can be created for each Tenant.

For more information, refer the following:

- [Dashboard Configuration](#)
- [Location Based Services Widgets](#)

1.2.1 Dashboard Configuration

▶ [Dashboard](#)

Use the Dashboard screen to create customized presentations of specific Tenant data. The Dashboard contains tools, layouts and widgets to customize the Tenant's data display. Create new dashboards as needed to fit your network's analytic requirements.

Dashboard enables Tenant administrators to review and troubleshoot Azara Cloud network operation. Additionally, the Dashboard allows an administrative review of the network's topology, an assessment of network's component health and a diagnostic review of device performance.

By default, a blank Dashboard named *Dashboard1* is available and can be customized immediately. To add a new dashboard, click the + icon located to the right.

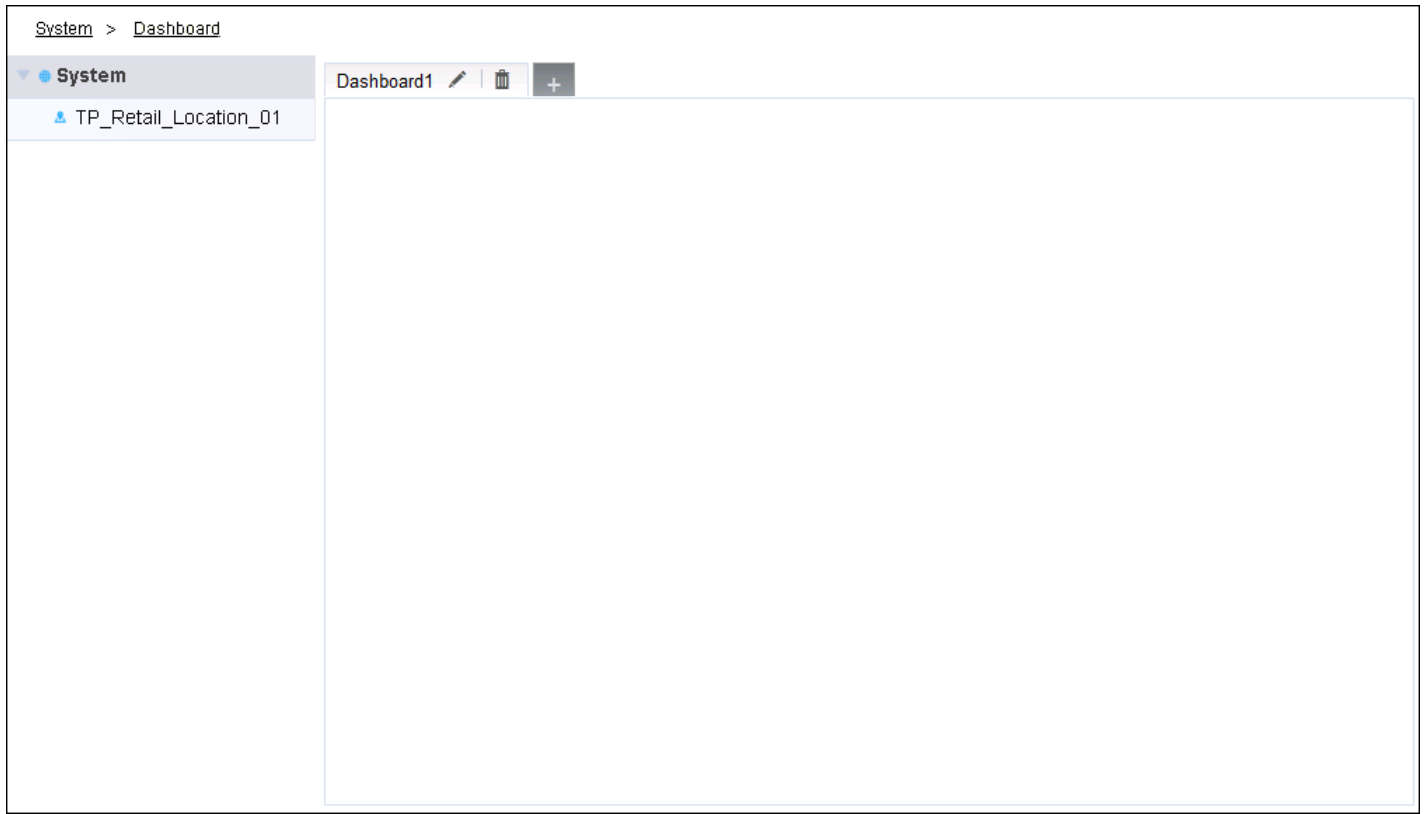


Figure 1-8 Tenant Dashboard View - Blank Dashboard

To rename the dashboard, double-click the dashboard's label and edit it. To delete a dashboard, click the **Trash** icon located to the right of each dashboard's tab.

To edit a dashboard, click the  icon located to the right of the dashboard's name.

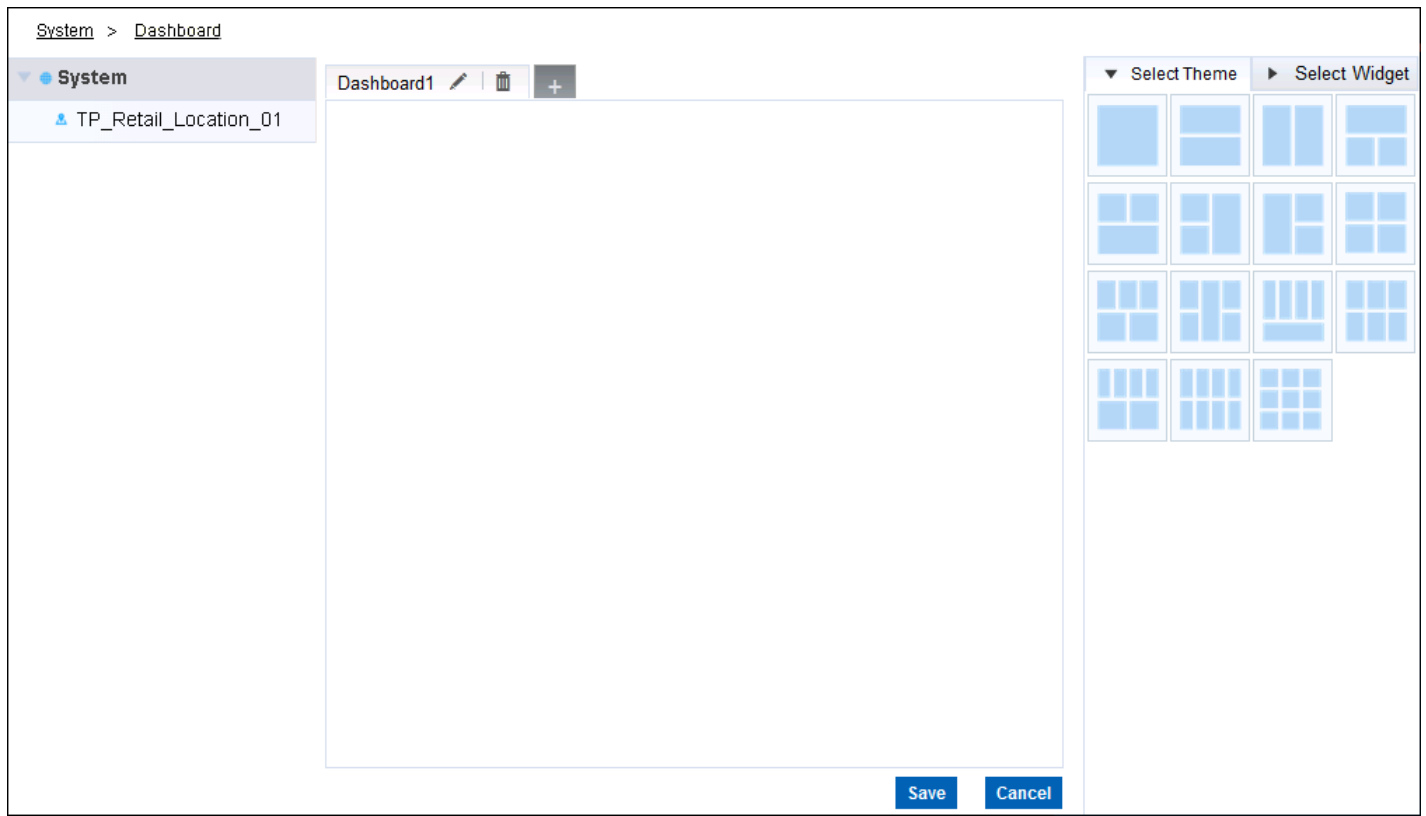


Figure 1-9 Tenant Dashboard View - Edit Dashboard

To customize the dashboard:

1. Select one of the available layouts from the **Select Theme** tab on the right of the screen and drag it to the empty dashboard. The theme is applied to the dashboard. When a theme is applied, the filtering criteria buttons are automatically added to the dashboard.

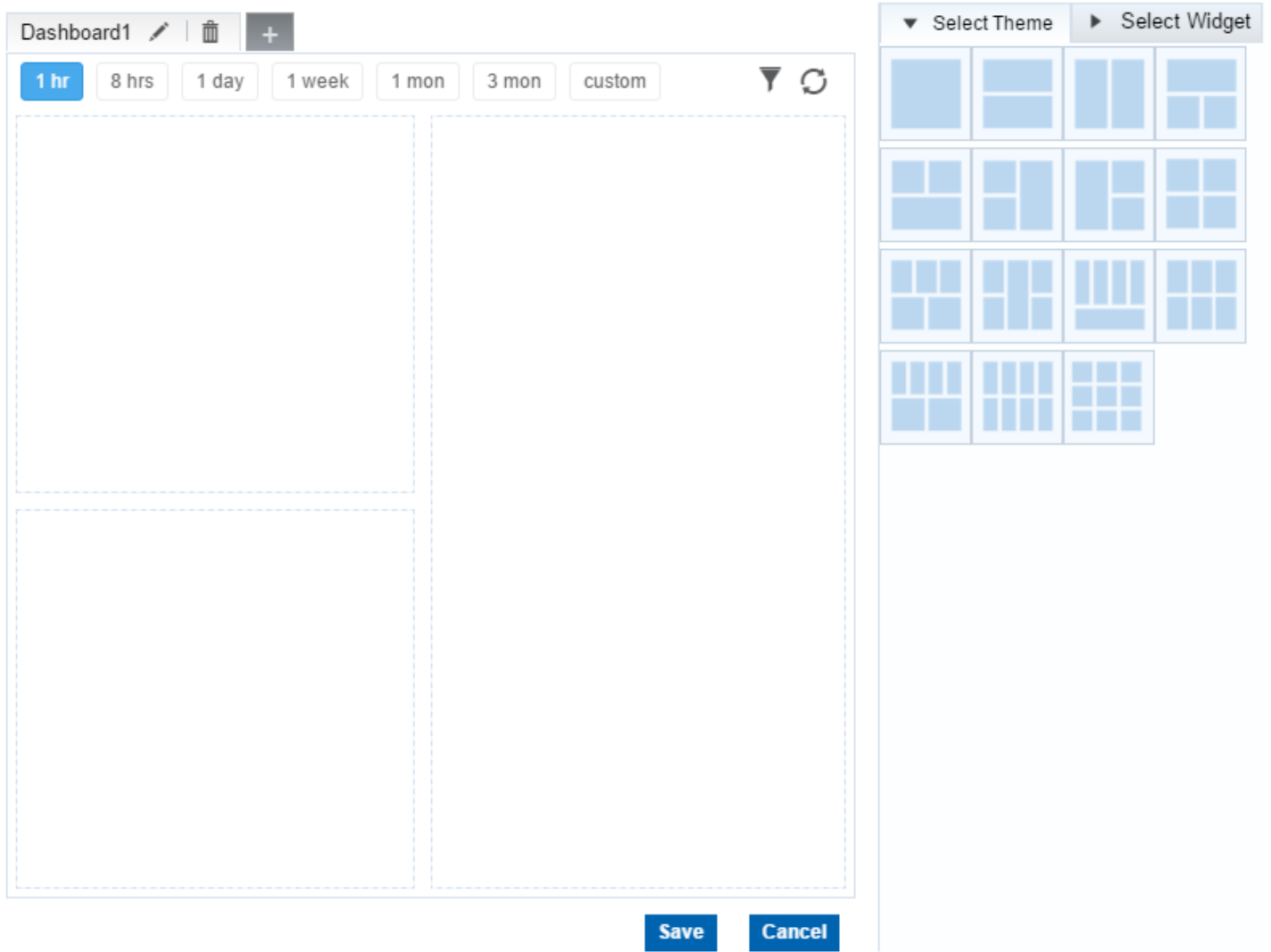


Figure 1-10 Tenant Dashboard View - Theme Applied

2. Select the **Select Widget** tab. From the available options, select a widget and drag it to one of the empty positions in the Dashboard.

Widgets are grouped under the following categories:

Utilization	This set of widgets enables tracking of utilization metrics such as client count and various top 10/bottom 10 counts.
RF	This set of widgets enables tracking of Radio Frequency metrics such as RF quality, RF health, channel utilization, various top 10/bottom 10/worst 10 metrics. This group also includes various Smart-RF metrics.
Location Based Services	This set of widgets enable tracking of visitors to your location using Azara's Location Based Services. For more information, see Location Based Services Widgets on page 1-16 .
Clients	This set of widgets enable tracking of client distribution based on different parameters.
Security	This set of widgets provide security related information including Rogue AP metrics & WIPS events.

Captive Portal	This set of widgets provide captive portal related information on guest users such as associated guests, their duration and login type.
Application Visibility	This set of widgets provide application visibility metrics.

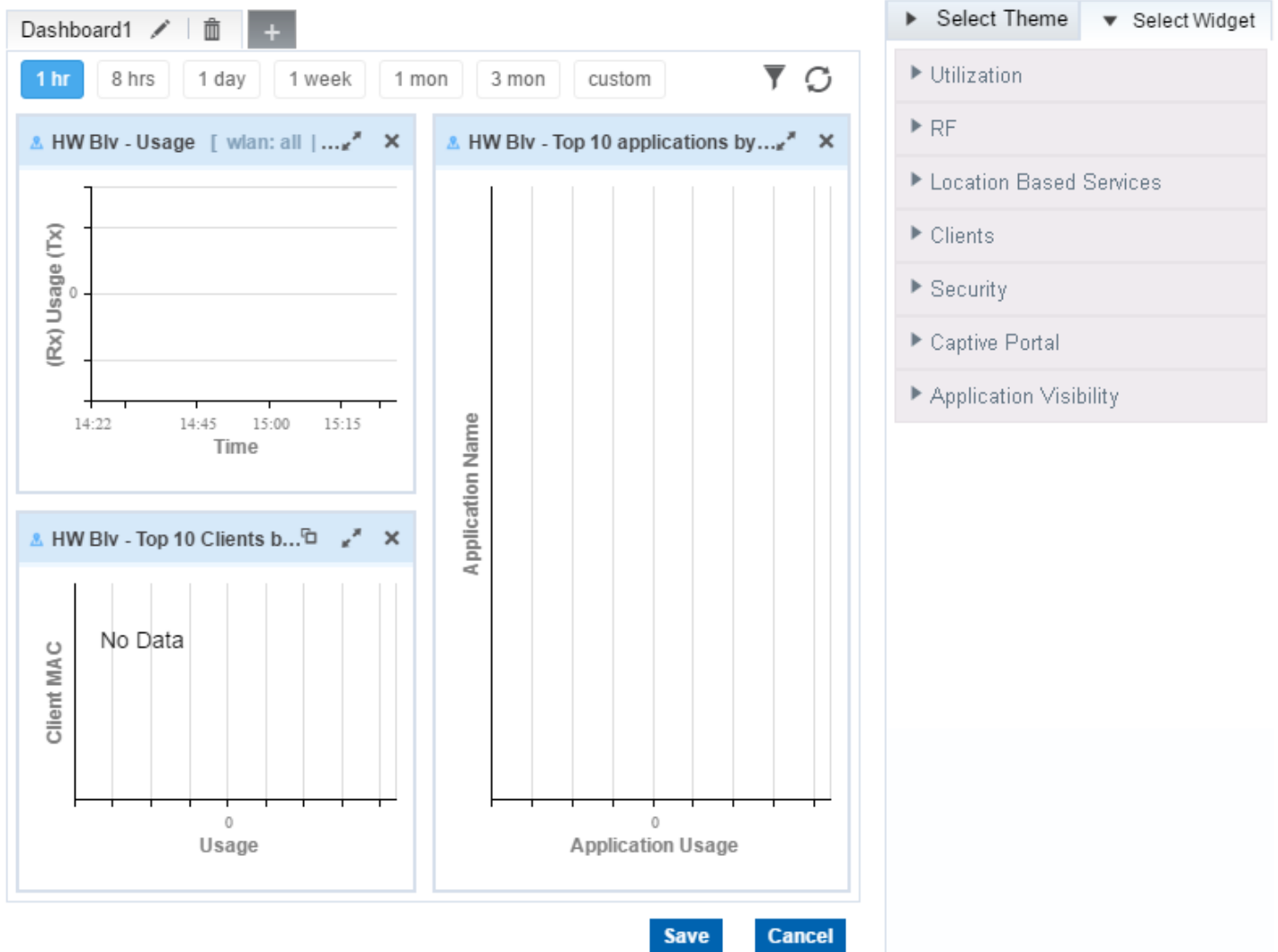


Figure 1-11 Tenant Dashboard View - Completed Dashboard

- Once all the required widgets are in place, select the **Save** button to save the dashboard. If required, select the **Cancel** button to exit without customizing the dashboard.

1.2.2 Location Based Services Widgets

► [Dashboard](#)

This section explains the various *Location Based Services* (LBS) widgets that can be included in the dashboard. Use these widgets to get a variety of device visit information at your location. LBS enables you to get a comprehensive view of device visits to your site, including different types of visit counts, visit engagement counts and visit lengths.

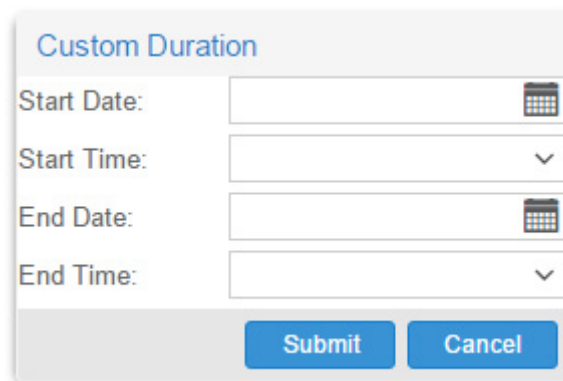
The following is a glossary of the terms used in the LBS widgets.

- **User** – Any mobile device observed by the LBS through the deployed sensors.
- **Passerby** – A device that is observed by the LBS is classified as a *Passerby* device if it meets any one of the following criteria:
 - The device is observed at a RSSI value less than -85dbm
 - The device is observed once at a RSSI value of -85dbm or more.
- **Visitor** – A device that is not classified as a *Passerby* device is considered a Visitor. Visitor devices are further classified as:
 - **Bounced Visitor** – A device that is observed by LBS for a duration of five (5) minutes or less.
 - **Engaged Visitor** – A device that is observed by LBS for a duration of above five (5) minutes.
 - **First Time Visitor** – A device that is observed by LBS for the first time at the specified site in a period of three (3) months.
 - **Repeat Visitor** – A device that is observed by LBS more than once in three (3) consecutive months.

Data Filtering

Data displayed in the LBS widgets can be filtered on the time duration (last 1 Hour/8 Hours/1 Day/1 Week/1 Month/3 Months and custom). LBS data is displayed with a granularity of 1 hour or 1 day. When data is requested for 1 Hour, 8 Hours or 1 Day, the granularity of display is 1 hour. So, for 8 Hours, 1 hour data is displayed for the last 8 hours. Similarly, when data is requested for 1 Week, 1 Month or 3 Months, the granularity of display is 1 day. For example, for 1 Month, daily data is displayed for the last 30 days.

Use the *Custom* filter to fetch and display data for a particular period of interest. When the **Custom** button is selected, the following dialog displays.



The image shows a dialog box titled "Custom Duration". It contains four input fields: "Start Date:" with a calendar icon, "Start Time:" with a dropdown arrow, "End Date:" with a calendar icon, and "End Time:" with a dropdown arrow. At the bottom of the dialog are two buttons: "Submit" and "Cancel".

Use the fields in the dialog to set the duration of interest. The data granularity will be according to the duration set in the above fields. For more information on data display granularity, see the next section [Data Display](#).

Data Display

For the LBS widgets that display summary data, like *Visit Opportunity*, *Engaged Visits*, values greater than or equal to ten thousand (10,000) is displayed concisely with the suffix 'K'. For example, if the actual value is 11,215, then the displayed value will be 11.21K. Hover your mouse over the widget to view the precise value for these widgets. Similarly, the widgets will display a concise value with the suffix 'M' for values over a million (1,000,000).

The following widgets are available for use:

- *Visit Opportunity*
 - *Visits by Count*
 - *Visitor Type in Percentage*
 - *Engagement*
 - *Mean Visit Length*
 - *Loyalty*
 - *Repeat Visitor Rate*
 - *First Time Visitors*
 - *Repeat Visitors*
 - *Engaged Visits*
 - *Bounced Visits*
 - *Passers By*
 - *Engagements*
-

1.2.2.1 Visit Opportunity

▶ Location Based Services Widgets

This widget displays a count of devices observed at the selected site for the selected time period. This includes all the different kinds of visitors: *Bounced*, *Engaged* and *Passerby*.



Figure 1-12 Location Based Services - Visit Opportunity widget

For more information on how data is displayed in this widget, see [Data Filtering on page 1-16](#).

1.2.2.2 Visits by Count

▶ Location Based Services Widgets

This widget displays a graph of the different types of device visits to the selected site. If a device is seen multiple times, each visit is classified and counted individually. Visits are classified as *Passerby*, *Bounced* and *Engaged Visits* and is displayed as a line graph over time. Hover over each data point in the graph to view detailed information for that time period.

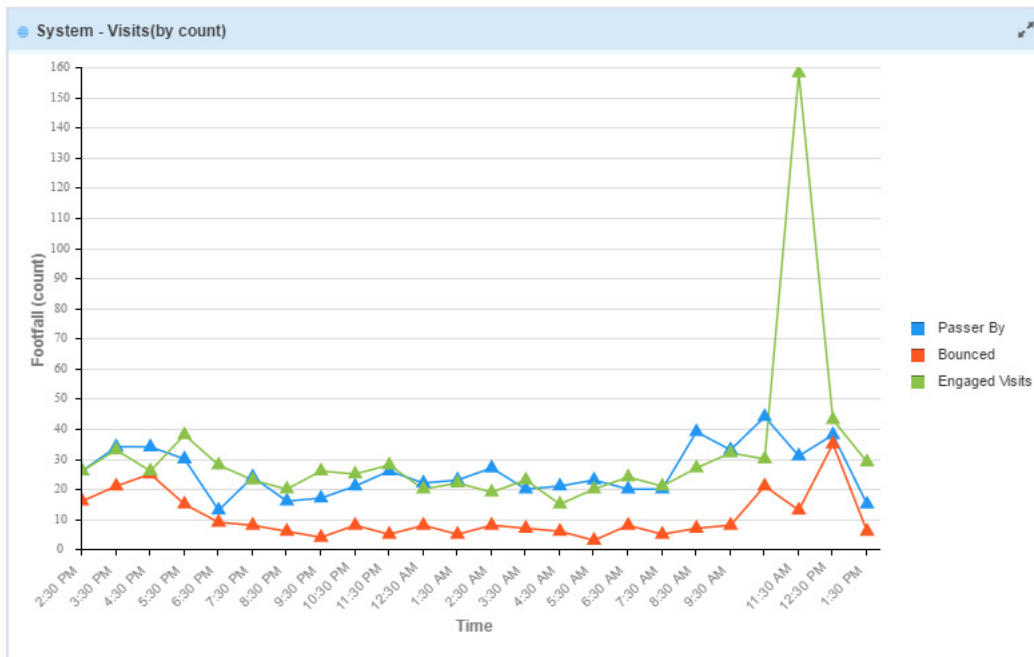


Figure 1-13 Location Based Services - Visits by Count widget

For more information on how data is displayed in this widget, see [Data Filtering on page 1-16](#).

1.2.2.3 Visitor Type in Percentage

▶ *Location Based Services Widgets*

This widget displays a graph of the different types of device visits as percentage of total visits. The visits are classified as *Passerby*, *Bounced* and *Engaged Visits* displayed as a bar graph over time. Hover over each bar in the graph to view detailed information for that time period.

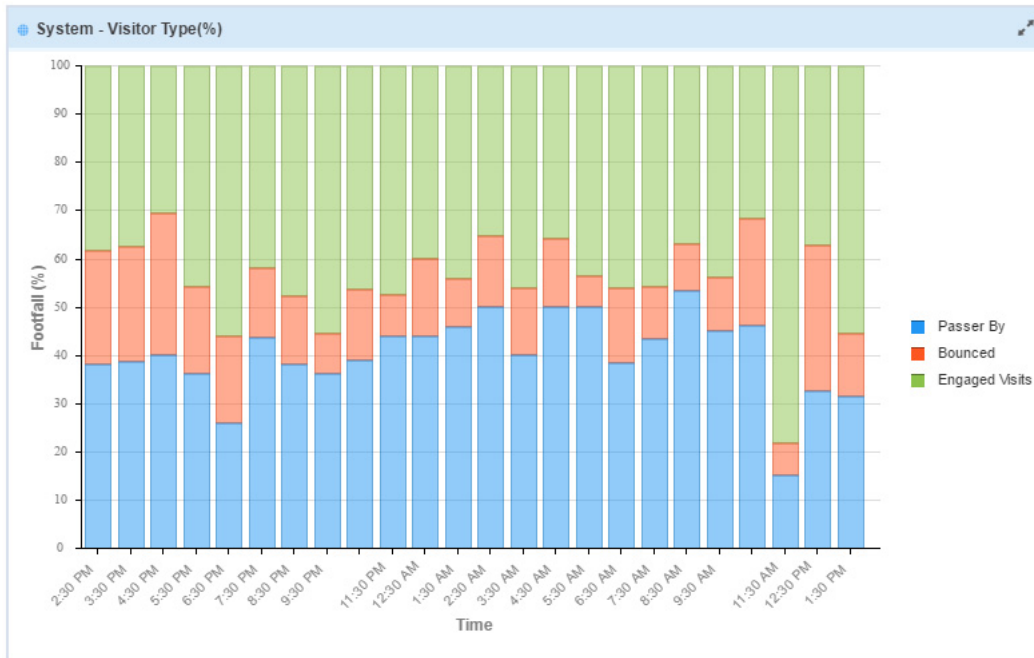


Figure 1-14 Location Based Services - Visitor Type in Percentage widget

For more information on how data is displayed in this widget, see [Data Filtering on page 1-16](#).

1.2.2.4 Engagement

▶ Location Based Services Widgets

This widget displays a graph of engaged visits classified according to the length of time they are engaged with the site. The visits are classified in these groups: *5-20 minutes*, *20-60 minutes*, *1-6 hours* and *greater than 6 hours*. Bounced visits are displayed in the *less than 5 minutes* group. Hover over each bar in the graph to view detailed information for that time period.

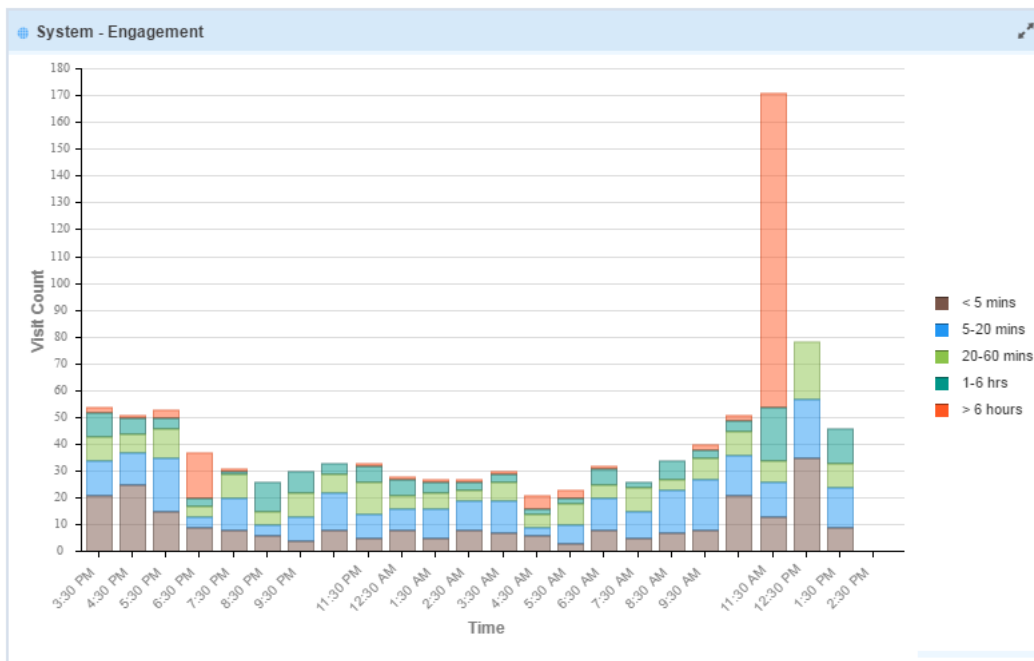


Figure 1-15 Location Based Services - Engagement widget

For more information on how data is displayed in this widget, see [Data Filtering on page 1-16](#).

1.2.2.5 Mean Visit Length

▶ *Location Based Services Widgets*

This widget displays a graph of the average visit duration to the selected site. This value is displayed over time. Mean visit length measures the average time a device remains in the site. Hover over each data point in the graph to view detailed information for that time period.

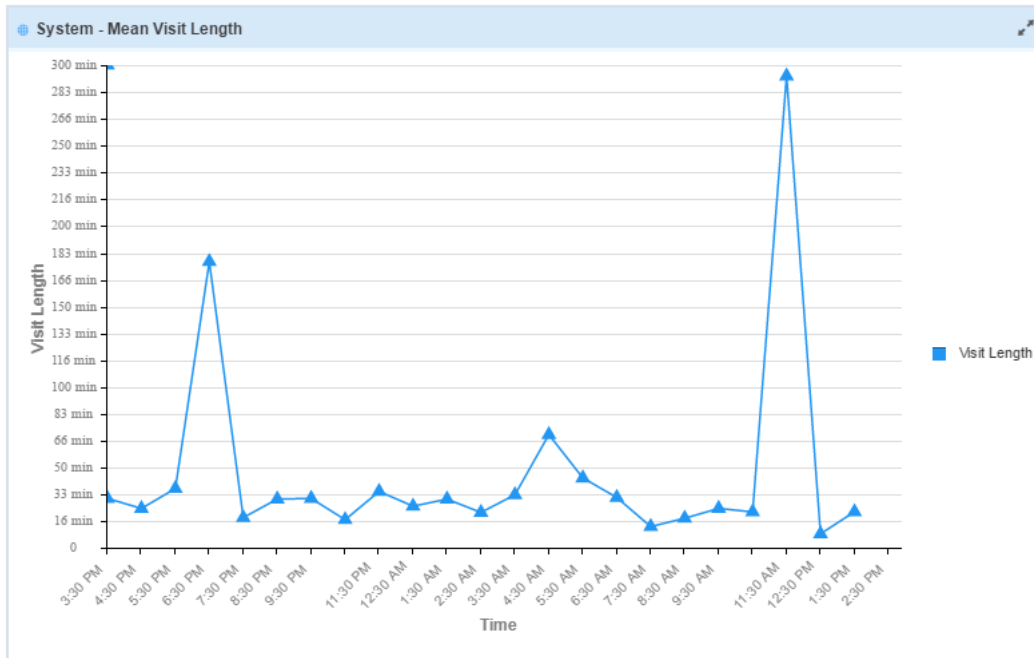


Figure 1-16 Location Based Services - Mean Visit Length widget

For more information on how data is displayed in this widget, see [Data Filtering on page 1-16](#).

1.2.2.6 Loyalty

▶ Location Based Services Widgets

This widget displays a graph of the number of *First Time* visits and *Repeat* visits over time. Hover over each data point in the graph to view detailed information for that time period.

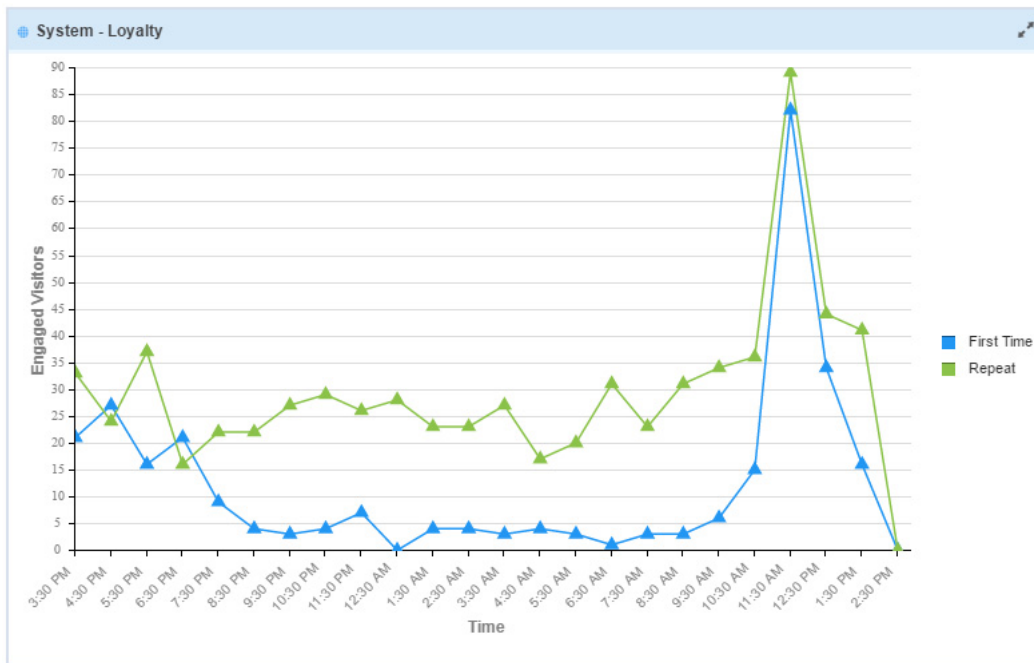


Figure 1-17 Location Based Services - Loyalty widget

For more information on how data is displayed in this widget, see [Data Filtering on page 1-16](#).

1.2.2.7 Repeat Visitor Rate

▶ [Location Based Services Widgets](#)

This widget displays a graph of the number of *First Time* visits and *Repeat* visits as a percentage of *Engaged* visits mapped over time. Hover over each bar in the graph to view detailed information for that time period.

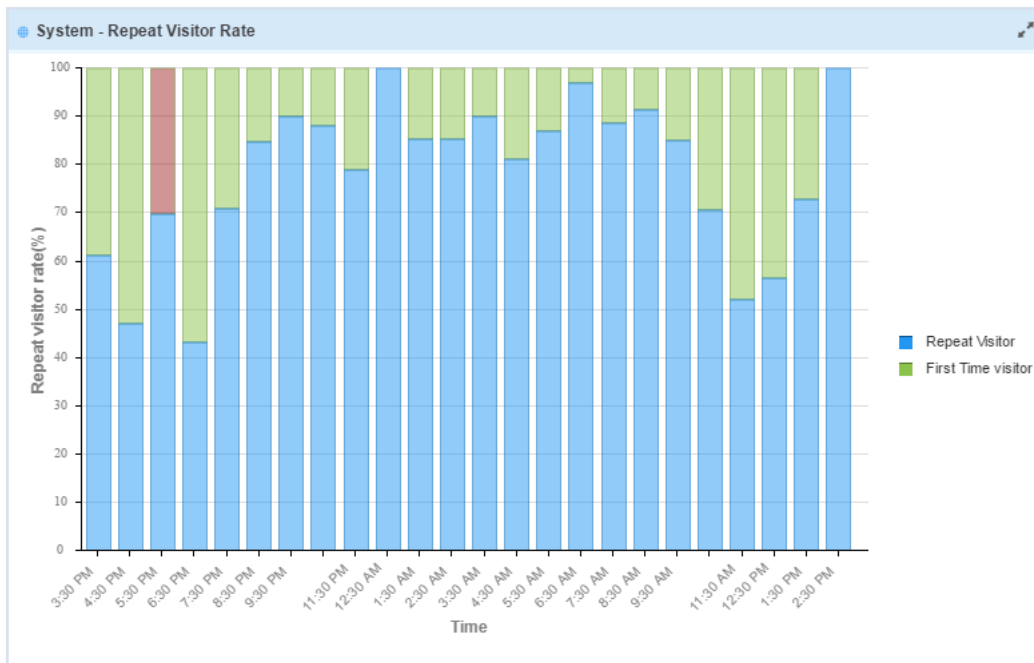


Figure 1-18 Location Based Services - Repeat Visitor Rate widget

Repeat visits are tracked over a period of three (3) consecutive months.

For more information on how data is displayed in this widget, see [Data Filtering on page 1-16](#).

1.2.2.8 First Time Visitors

▶ [Location Based Services Widgets](#)

This widget displays the total number of *First Time* visits for the selected time duration.

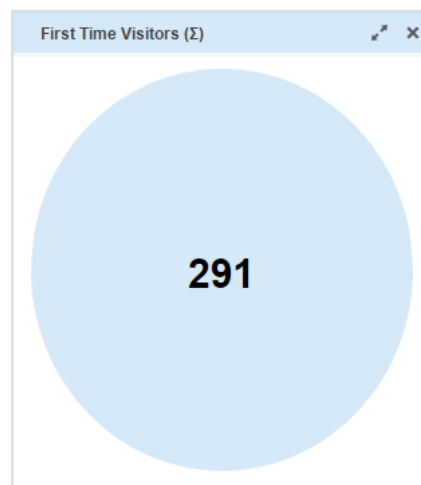


Figure 1-19 Location Based Services - First Time Visitors widget

For more information on how data is displayed in this widget, see [Data Filtering on page 1-16](#).

1.2.2.9 Repeat Visitors

▶ [Location Based Services Widgets](#)

This widget displays the total number of *Repeat* visits for the selected time duration.

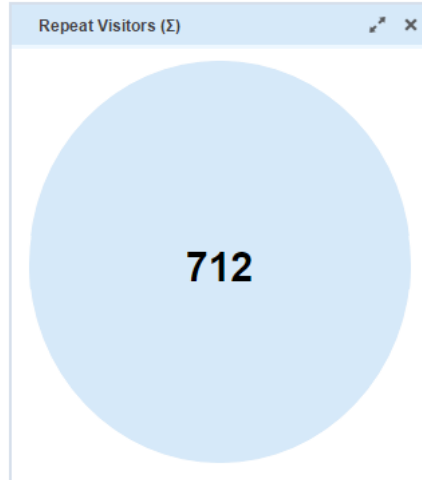


Figure 1-20 Location Based Services - Repeat Visitors widget

For more information on how data is displayed in this widget, see [Data Filtering on page 1-16](#).

1.2.2.10 Engaged Visits

▶ [Location Based Services Widgets](#)

This widget displays the total number of *Engaged* visits to the site for the selected time duration.

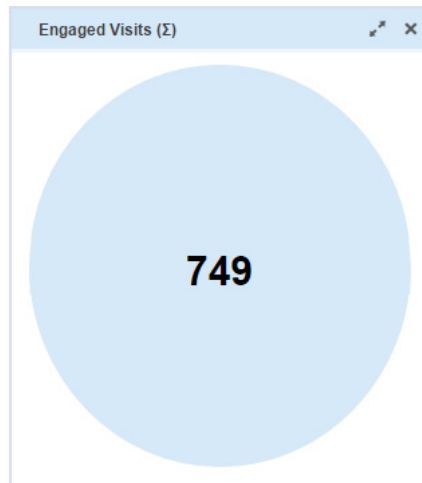


Figure 1-21 Location Based Services - Engaged Visits widget

For more information on how data is displayed in this widget, see [Data Filtering on page 1-16](#).

1.2.2.11 Bounced Visits

▶ Location Based Services Widgets

This widget displays the total number of *Bounced* visits to the site for the selected time duration.

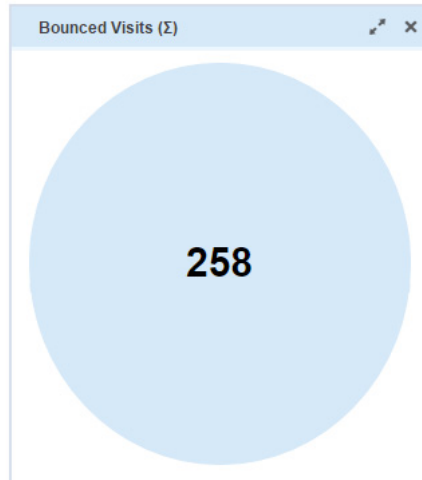


Figure 1-22 Location Based Services - Bounced Visits widget

For more information on how data is displayed in this widget, see [Data Filtering on page 1-16](#).

1.2.2.12 Passers By

▶ Location Based Services Widgets

This widget displays the total number of passers by observed by the LBS for the site for the selected time duration.

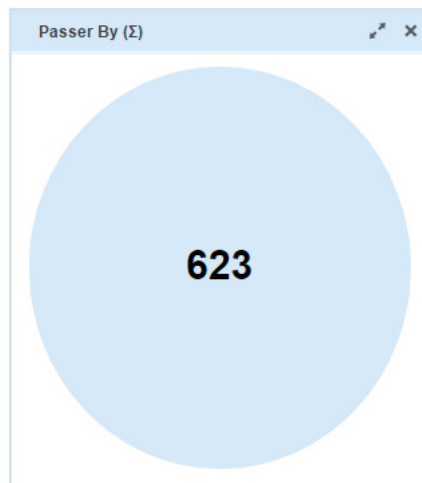


Figure 1-23 Location Based Services - Passers By widget

For more information on how data is displayed in this widget, see [Data Filtering on page 1-16](#).

1.2.2.13 Engagements

▶ *Location Based Services Widgets*

This widget displays a graph of all device visits observed by the LBS across all the sites for the Tenant. Hover over each section in the graph to view detailed information for that visitor engagement time period.

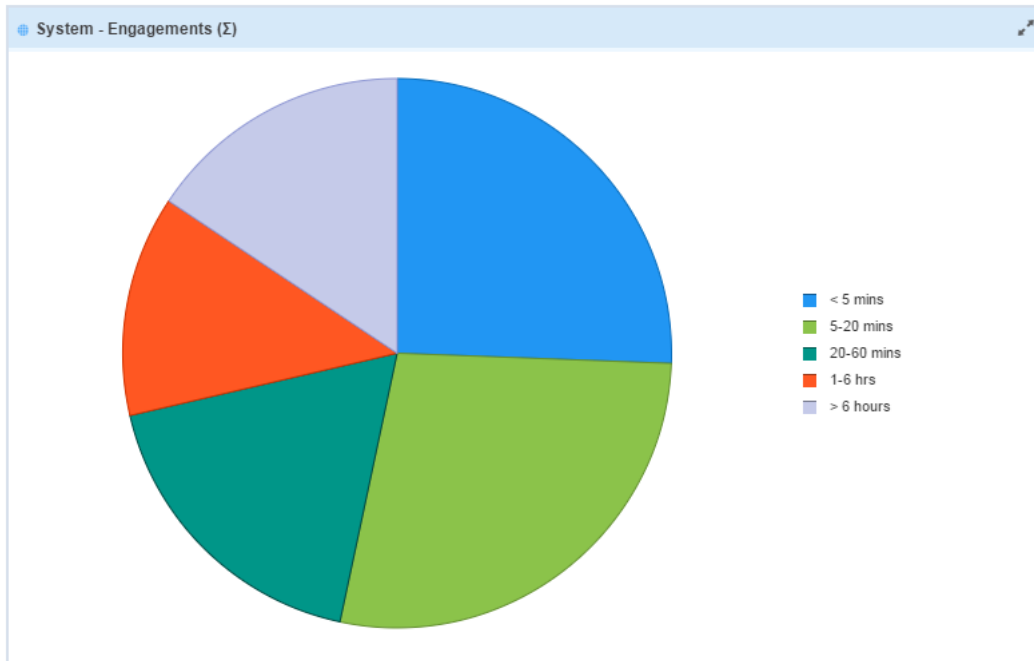


Figure 1-24 Location Based Services - Engagements widget

For more information on how data is displayed in this widget, see [Data Filtering on page 1-16](#).

1.3 Monitor

▶ [Tenant Management](#)

Use the different Monitor screens to view the various status of the Tenant's network.

The **Summary** tab displays a set of live graphs that lists the state of the Tenant's network. This tab displays a mix of graphs showing client information, RF information and access point information.

The **Access Points** tab displays a set of live graphs that lists the device details for the Tenant's network. For the network summary, this tab displays a summary of devices on the network as a whole. For an individual site, this tab displays a list of devices activated for that site.

The **Clients** tab displays a set of live graphs that lists the clients using the Tenant's networks. For the network summary, this tab displays a summary of usage and a brief clients summary. For an individual site, this tab displays a summary of usage and a set of tabs classifying the clients on this network.

The **Rogues** tab displays a set of live graphs of Rogue access points and un-sanctioned access points discovered in the Tenant's network.

The **Event Log** tab displays a live log of events on the Tenant's network. Use this tab to drill down to events of interest at the system level or at a site level. A large number of filter parameters are available for use to drill-down to the events of interest.

1.3.1 Monitor Summary

▶ [Monitor](#)

The *Monitor Summary* screen displays live data about the state of the Tenant's networks. By default, a system wide summary of all the Tenant's network is displayed. Use this screen to monitor the performance of the Tenant's network including the devices and clients that are members of the Tenant's network. Individual networks can be selected from the menu tree on the left of the screen. Summary information for the selected network is then displayed.

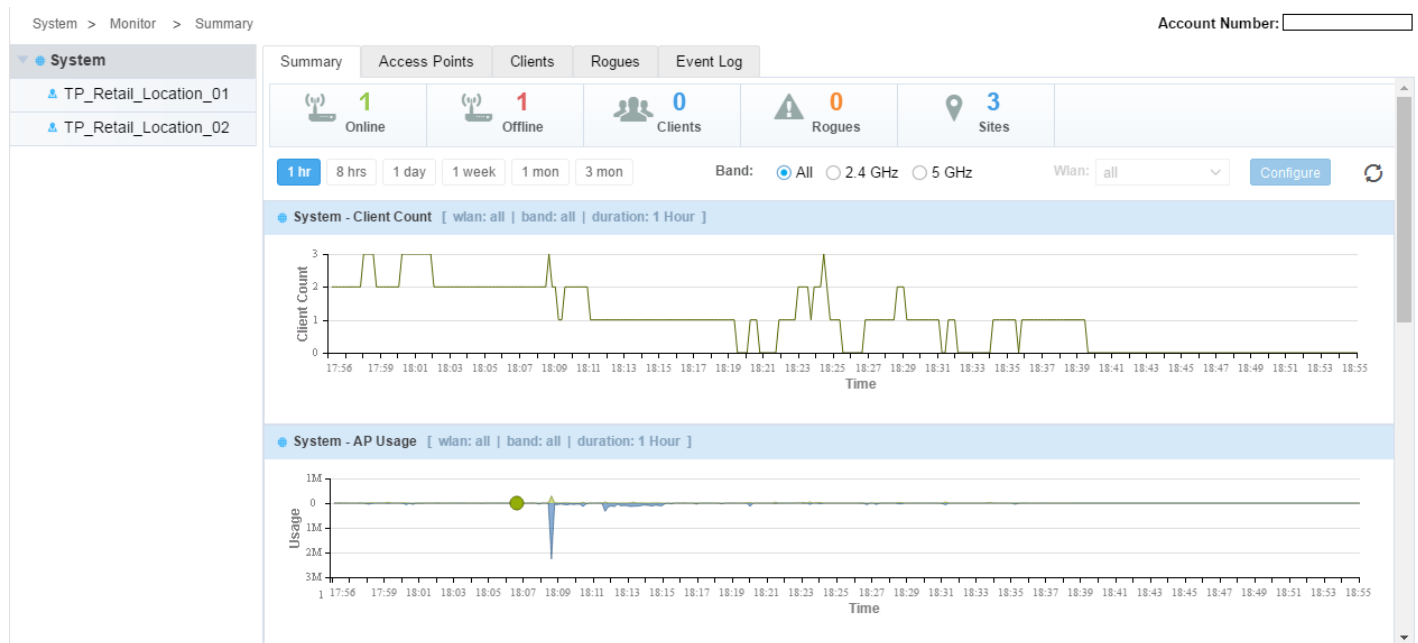


Figure 1-25 Tenant Monitor View - Monitor Summary

The *Summary* screen displays the following information:



NOTE: All the graphs on this screen can be filtered based on the available WLAN, the band of operation (2.4 GHz/5 GHz/all) and time duration (last 1 Hour/ 8 Hours/1 Day/1 Week/1 Month/3 Months). These filters are independent of each other and can be used together for fine grained control over the data being displayed.

The following graphs are displayed for both Summary information and for individual sites.

- **Client Count** displays the of number of clients on the network over time.
- **AP Usage** displays the access point usage in MB over time. Tx and Rx data is displayed over time.

The following graphs are displayed for the Tenant Summary:

- **Top Sites by Usage** displays the top sites by data usage in MBs.
- **Worst Sites by RF Quality** displays the 10 worst sites by their RF quality. Use this information to take action to improve the RF quality of these sites.
- **Top Sites by Client Count** displays a list of the top 10 sites by client count.
- **Worst Sites by Channel Utilization** displays a list of 10 worst sites by their channel utilization.
- **Top Applications by Usage** displays a list of the top 10 client applications by data usage. Use this information to assess if specific client applications are adversely impacting performance and warrant filtering.
- **Worst Sites by Retries** displays a list of 10 worst sites by number of retries. Use this information to identify the sites that have poor performance and then troubleshoot the issue causing the retries.

The following graphs are displayed at the site level.:

- **Top APs by Usage** displays top 10 access points deployed at the site by data usage.
- **Worst APs by RF Quality** display a list of the 10 worst access points deployed at the site by their RF quality. Use this information to improve performance of these access points.
- **Top APs by Client Count** displays a list of the top 10 access points by client count.
- **Worst APs by Channel Utilization** displays a list of the 10 access points deployed at the site with the maximum channel utilization.
- **Top Applications by Usage** displays a list of the top 10 client applications by data usage at a site. Use this information to assess if specific client applications are adversely impacting performance and warrant filtering.
- **Worst APs by Retries** displays a list of 10 worst access points deployed at a site by number of retries. Use this information to identify the access points that have poor performance and then troubleshoot the issue causing the retries.

Use the **Configure** button next to the WLAN drop-down to edit the configuration of the selected site. This button is only enabled when a site's information is viewed. It is not enabled at the system level.

1.3.2 Monitor Access Points

► *Monitor*

Monitor Access Point screen displays live data about the access point present in the Tenant's networks. By default, a system wide summary of all the Tenant's access points is displayed. Use this screen to monitor the performance of the Tenant's access points that are members of the Tenant's network. Individual networks can be selected from the menu tree on the left of the screen. Access point information for the selected network is then displayed.

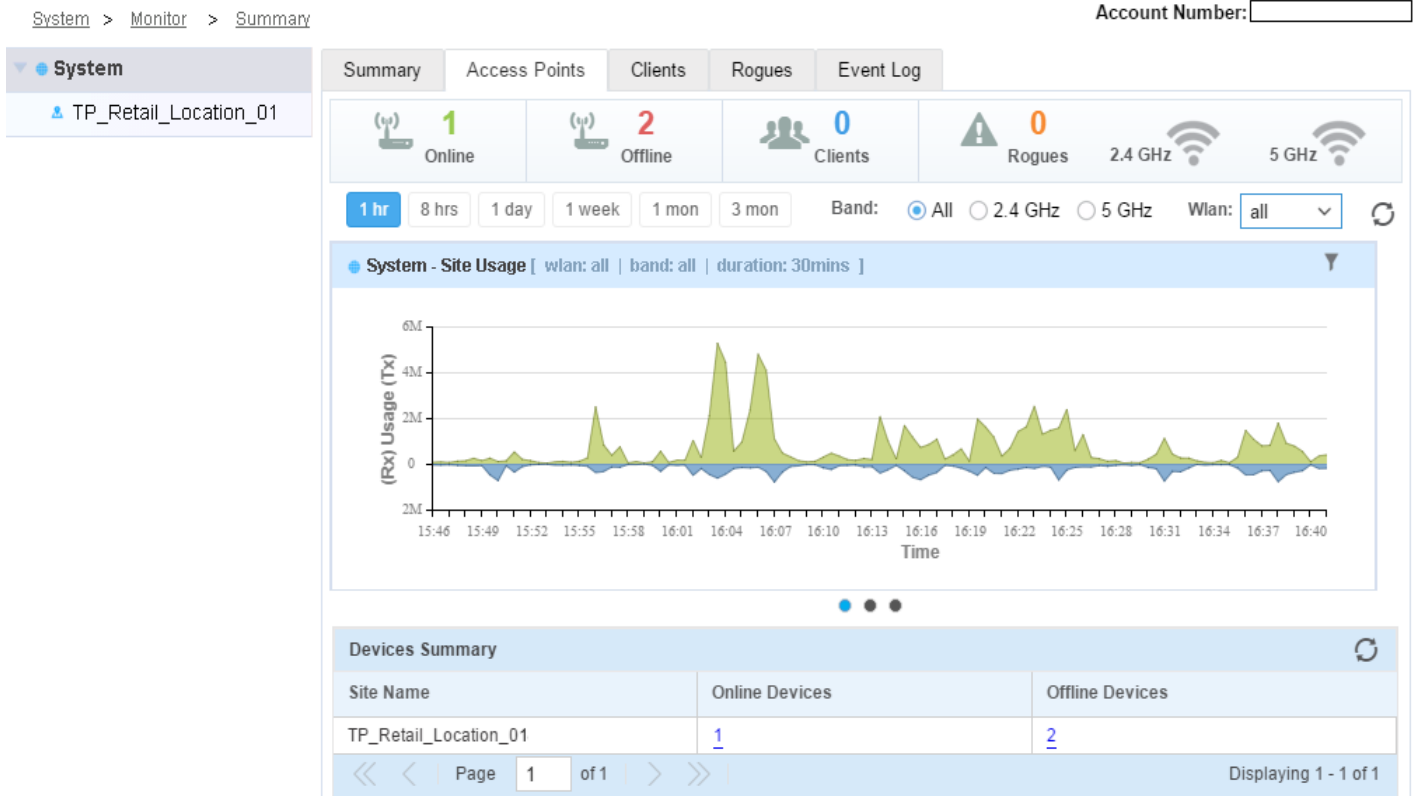




Figure 1-26 Tenant Monitor View - Monitor Access Points

The *Access Point* screen displays the following information:



NOTE: All the graphs on this screen can be filtered based on the available WLAN, the band of operation (2.4 GHz/5 GHz/all) and time duration (last 1 Hour/8 Hours/1 Day/1 Week/1 Month/3 Months). These filters are independent of each other and can be used together for fine grained control over the data being displayed. These filtering criteria are hidden by default. Use the  icon located to the top left of the graph title to display the filtering criteria.

Use the  buttons located below the graph panel to display three (3) different graphs. Depending on the context, the graphs display data for the whole system or for the selected site. The graphs are:

- **Site Usage** graph displays the bandwidth usage in MB over time. Tx an Rx data is displayed over time.
- **Client Count** graph displays the number of clients associated over time.
- **RF Quality** graph displays RF quality over time.

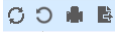




The **Devices Summary** table displays all the configured devices for the Tenant. This includes managed access point on the Tenant's network that are currently offline.

Site Name	Displays the site name.
Online Devices	Displays the number of online access points reported by the site as a link. Select the link to display the <i>Devices List</i> table which provides more information on each offline access point.
Offline Devices	Displays the number of offline access points reported by the site as a link. Select the link to display the <i>Devices List</i> table which provides more information on each offline access point.

1-30 Azara User's Guide

When the link in the **Online Devices** or **Offline Devices** fields in the **Devices Summary** is selected, the **Devices List** table displays. The table displays the following information for each access point:

Status	Displays the status of the access point. If an access point is up, a green icon along with the word "Online" is displayed. If an access point is not online, a red icon along with the word "Offline" is displayed.
Name	Displays the name assigned to the access point. The name displays as a link that can be selected to view the access point's summary information. See section Access Point Details on page 1-31 for more details.
Device Type	Displays the access point type. The supported access point types are: AP7502, AP7522, AP7532 and AP7562.
Clients	Displays the number of clients associated with the selected access point.
MAC Address	Displays the MAC address of the access point.
IP Address	Displays the IP address assigned to the access point as its network identifier. Displays N/A otherwise.
Site Name	Displays the name of the site where this access point is located physically.
Country Code	Displays the country code of the country where the access point is deployed.
Serial Number	Displays the unique hardware serial number assigned to each device during manufacture.

The group of icons  located to the top right of the Device List table are used to perform specific actions on the data displayed in this table. Use the  icon to refresh the data displayed in this table. Use the  to reset the table columns to default order if their order was changed. Use the  icon to print the information displayed in this table and is displayed in a new tab. Use the  icon to export the data displayed in the table.

1.3.2.1 Access Point Details

► [Monitor Access Points](#)

When the access point's **Name** in the **Device Summary** table is selected, the following screen displays:

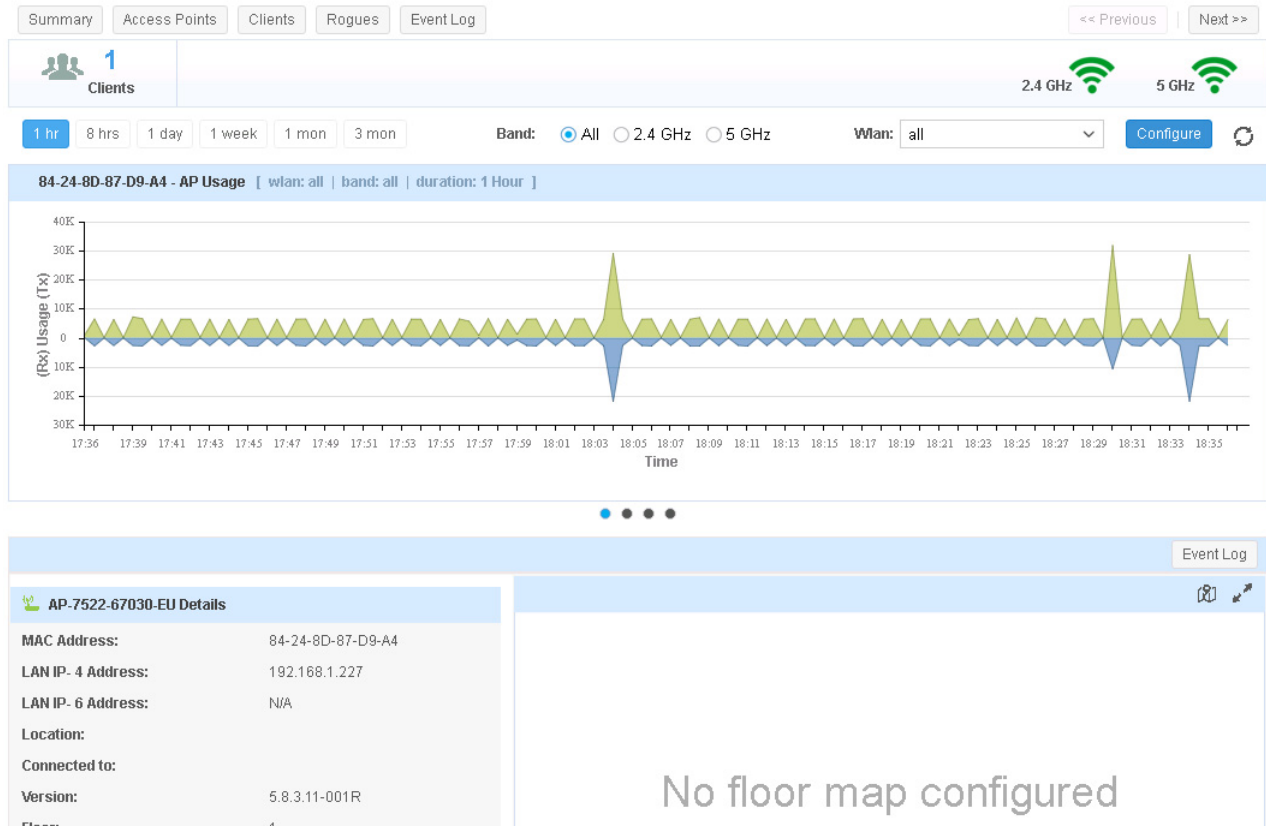


Figure 1-27 Tenant Monitor View - Monitor Access Points - Access Point Details screen


This screen displays a large amount of detailed information about the selected access point. The **AP Usage** graph displays the access point usage (Tx and Rx) over time.

Use the ● ● ● buttons located below the graph panel to display four (4) different graphs. The graphs are:

- **AP Usage** graph displays the bandwidth usage over time. Tx and Rx data are displayed over time.
- **Client Count** graph displays the number of clients associated over time.
- **RF Quality** graph displays RF quality over time.
- **Channel Utilization** graph displays the channel utilization percentage over time.
- The **Details** area displays detailed information about the access point. The following information is displayed for the access point:

MAC Address	Displays the MAC address of the access point.
LAN IP-4 Address	Displays the IPv4 address assigned to the access point as its network identifier. Displays N/A otherwise.
LAN IP-6 Address	Displays the IPv6 address assigned to the access point as its network identifier. Displays N/A otherwise.
Location	Displays the location of the access point. If the geolocation of the access point is configured, this information is displayed here.
Version	Displays the version of firmware installed on the access point.

Floor	Displays the floor where the access point is deployed in a multi-floored site.
Site Name	Displays the name of the site where this access point is located physically.
Country Code	Displays the country code of the country where the access point is deployed.
Serial Number	Displays the unique hardware serial number assigned to each device during manufacture.

- The **Floor Map** area displays a graphical floor map of the site with a overlay of the access point's location. This is only displayed if a floor map for the site is available and the access point has been placed on the floor map. Select the  icon located to the right to toggle this area between **Floor Map** and **Google Map**. When in **Google Map** view, the access point is placed on the Google Map if geolocation information is available for the site.
- The **Radio Details** table displays the following radio information:

Status	Displays the status of each radio on the access point.
MAC Address	Displays the radio's factory-assigned <i>Media Access Control</i> (MAC) address. The MAC address represents the radio's unique hardware network identifier.
Frequency	Displays the radio's frequency
Channel	Displays the radio's current channel of operation.
Clients	Displays the total number of clients on this radio.
Tx Power	Displays the Tx power for this radio.

- The **Wired Interface Details** table displays the following information:

Interface	Displays the interface name for each of the wired interface on the access point.
MAC Address	Displays the MAC address of the wired interface.
Operating Speed	Displays the operating speed of the wired interface. If the wired interface is not connected, displays N/A.
Tx	Displays the amount of data transmitted through this interface.
Rx	Displays the amount of data received through this interface.

- The **Top 10 Application by Usage** graph displays a graph of the top 10 applications by bandwidth usage.
- The **Current Client** table displays a list of all the associated clients for this access point. The following information is displayed for each client.

Status	Displays the associated status of the client.
MAC Address	Displays the MAC address of the client as a link. Select this link for more information on this client. See section Client Details on page 1-33 for more details.
Name	Displays the user assigned name for this client. If no name is assigned, then this field displays the MAC address of the client.
Vendor	Displays the manufacturer name for this client.

IP Address	Displays the IPv4 address assigned to this client.
User Name	If available, displays the username on this client.
WLAN	Displays the WLAN which this client uses.
Channel	Displays the channel which this client uses.

1.3.2.2 Client Details

► [Monitor Access Points](#)

When the **MAC Address** link in the **Current Client** table is selected, the following screen displays:

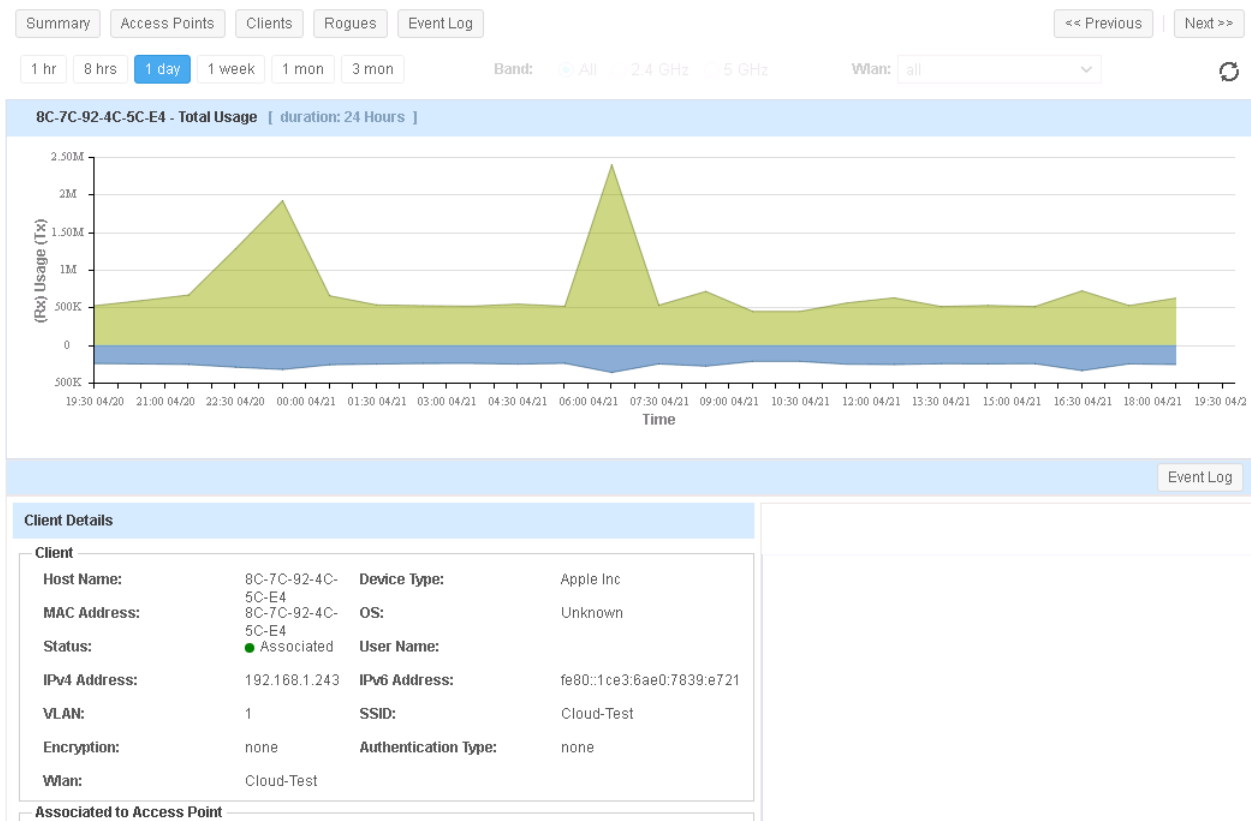


Figure 1-28 Tenant Monitor View - Monitor Access Points - Client Details screen

This screen displays a large amount of detailed information about the selected client. The **Total Usage** graph displays the client usage (Tx and Rx) over time.

- The **Client Details** area displays detailed client information. For each client, the following information is displayed:

Host Name	Displays the user assigned name for this client. If no name is assigned, then this field displays the MAC address of the client.
MAC Address	Displays the client's factory-assigned <i>Media Access Control</i> (MAC) address. The MAC address represents the client's unique hardware network identifier.
Status	Displays the associated status of the client.
IP Address	Displays the IPv4 address assigned to this client.

VLAN	Displays the VLAN assigned to this client.
Encryption	Displays the encryption scheme used on the WLAN used by the client.
WLAN	Displays the WLAN which this client uses.
Device Type	Displays the type of device. If a mobile device, displays the vendor name.
OS	If available, displays the Operating System installed on the client.
User Name	If available, displays the username on this client.
IPv6 Address	If assigned, displays the IPv6 address assigned to the client.
SSID	Displays the SSID used by the client.
Authentication Type	Displays the authentication type used on the WLAN used by the client.

- The **Floor Map** area displays a graphical floor map of the site with an overlay of the client's location. This is only displayed if a floor map for the site is available and the client's can be located on the floor map.
- The **Top 10 Application by Usage** graph displays a graph of the top 10 applications by bandwidth usage.

1.3.3 Monitor Clients

► *Monitor*

The Monitor *Clients* screen displays live data about the clients associated with the access point in the Tenant's networks. By default, a system-wide summary of all the Tenant's clients is displayed. Use this screen to monitor the performance of the Tenant's member clients. To view site-specific client details, select the site from the menu tree on the left of the screen. Client information for the selected site is then displayed.

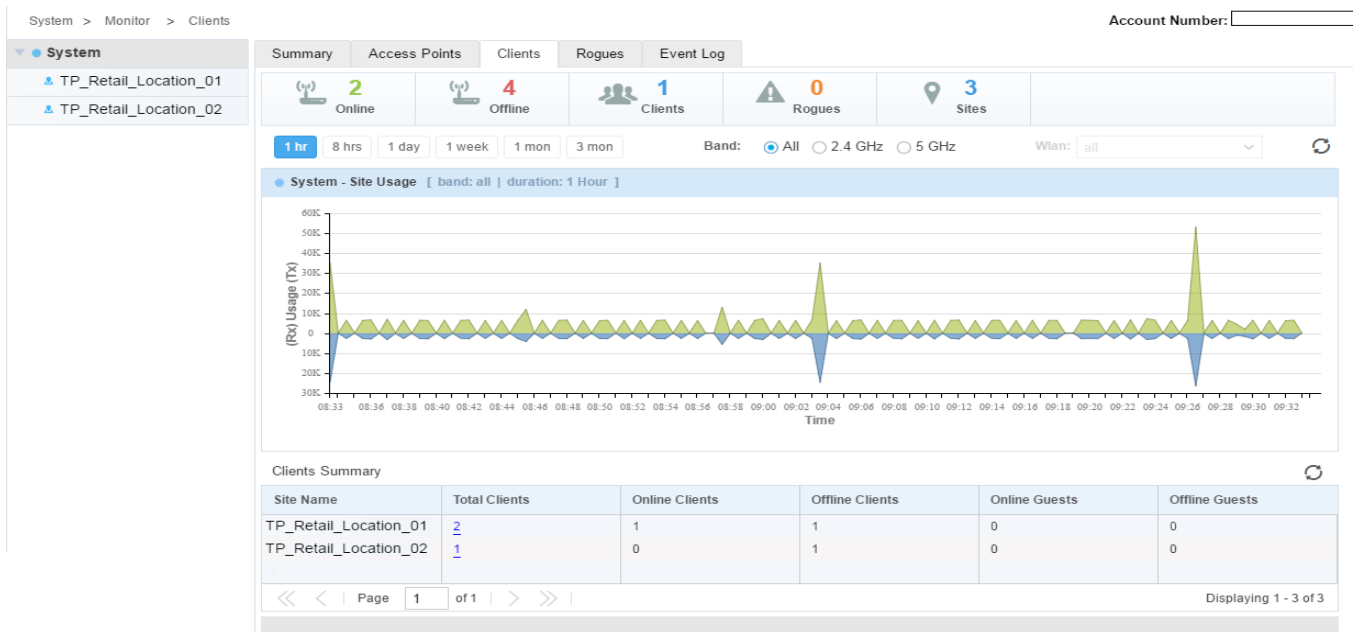




Figure 1-29 Tenant Monitor View - Monitor Clients



NOTE: All the graphs on this screen can be filtered based on the available WLAN, the band of operation (2.4 GHz/5 GHz/all) and time duration (last 1 Hour/8 Hours/1 Day/1 Week/1 Month/3 Months). These filters are independent of each other and can be used together for fine grained control over the data being displayed. These filtering criteria are hidden by default. Use the  icon located to the top left of the graph title to display the filtering criteria.






The **Clients Summary** table displays the Tenant's system-wide, clients by default. The following information is displayed.

Site Name	Displays the name of the Tenant's site.
Total Clients	Displays the total number of clients in the Tenant's site. This is the sum of all the online clients, offline clients, online guests and offline guests. Select this link to view more details on the clients at this site.
Online Clients	Displays the total number of online clients in the Tenant's site
offline Clients	Displays the total number of offline clients in the Tenant's site

When a site is selected from the tree view on the left, this table lists the client details. Client details for **Online Clients** and **Offline Clients** can be viewed. Select the appropriate button to view the details. Use the  icon to refresh the information displayed. The table displays the following information for each client type.

Status	Displays the client's status. If a client is online, a green icon along with the word "Associated" is displayed. If a client is offline, a red icon along with the word "Disassociated" is displayed.
MAC Address	Displays the client's factory-assigned <i>Media Access Control</i> (MAC) address. The MAC address represents the client's unique hardware network identifier. To view detailed client information, click on the client's MAC address, which displays as a link.
Name	Displays the client's unique administrator-assigned name provided upon initial adoption.
Vendor	Displays the manufacturer of the client as a means of assessing its support capabilities with the existing wireless infrastructure.
IP Address	Displays the IPv4 address the client is currently using as a network identifier.
User Name	Displays the assigned client username associated with each wireless client on the network.
BSSID	Displays the <i>Broadcast Service Set ID</i> (BSSID) of the access point (the radio's MAC address) to which the client is currently associated.
WLAN	Displays the WLAN's <i>Service Set ID</i> (SSID) of the administrator-defined WLAN the client is utilizing within the network.
Channel	Displays the client's channel of operation.
OS Type	Displays the client's <i>Operating System</i> (OS) type identity (Android, Windows, etc.)
IPv6 Address	Displays the IPv6 address, if assigned, that the wireless client is currently using for a network identifier.
Authentication	Displays the Authentication scheme (captive portal, PSK, etc.) applied to the client for inter-operation with its connected access point radio.
Encryption	Displays the encryption scheme (TKIP-CCMP, WEP 128, WEP 64, etc.) applied to the client for inter-operation with its connected access point radio.
Client Availability Capability	Displays the channels (2.5 GHz, 5 GHz, etc.) in which the client can operate.

Client Connected Capability	Displays the 802.11x IEEE WLAN standards supported by the client (11a, 11an, etc.).
------------------------------------	---

The group of icons  located to the top right of the **Device List** table are used to perform specific actions on the data displayed in this table. Use the  icon to refresh the data displayed in this table. Use the  to reset the table columns to default order if their order was changed. Use the  icon to print the information displayed in this table and is displayed in a new tab. Use the  icon to export the data displayed in the table.

1.3.3.1 Client Details

▶ Monitor Clients

When the **MAC Address** link in the **Current Client** table is selected, the following screen displays:

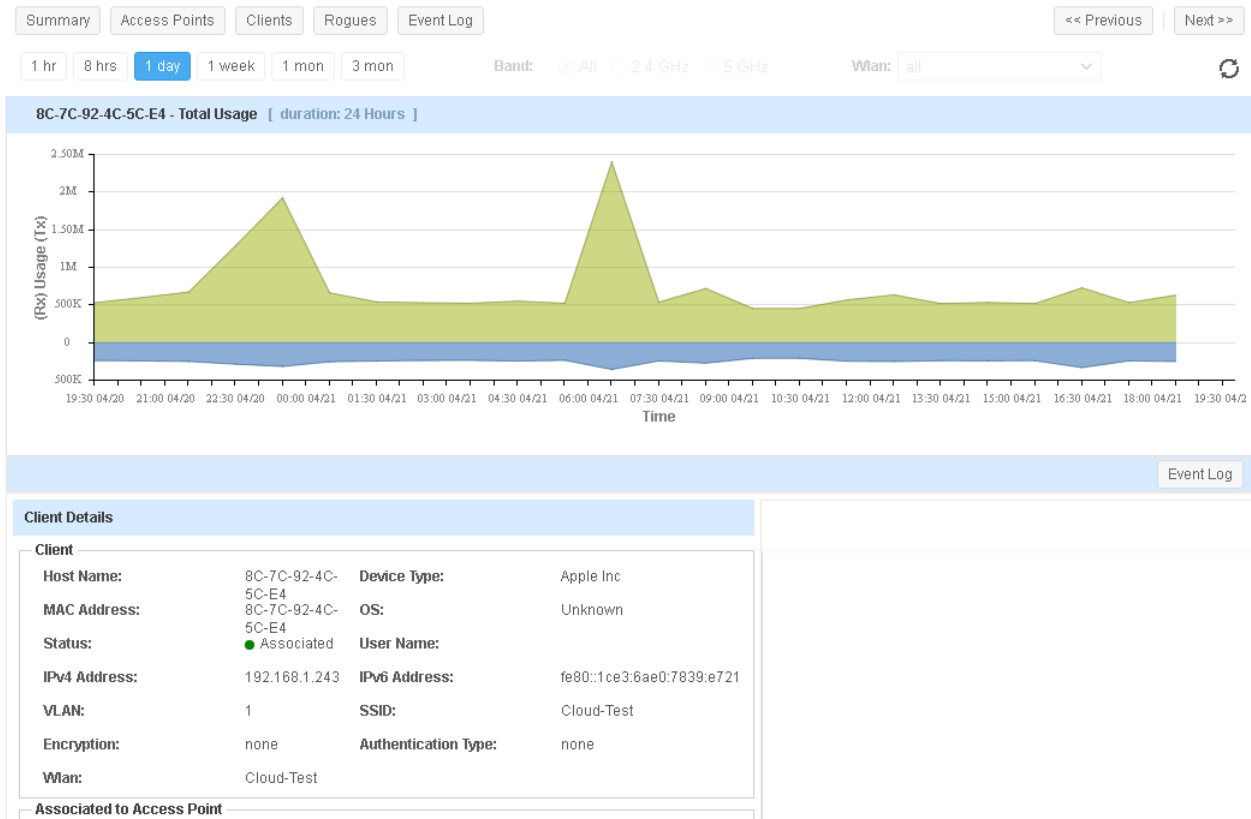


Figure 1-30 Tenant Monitor View - Monitor Access Points - Client Details screen

This screen displays a large amount of detailed information about the selected client. The **Total Usage** graph displays the client usage (Tx and Rx) over time.

- The **Client Details** area displays detailed client information. For each client, the following information is displayed:

Host Name	Displays the user assigned name for this client. If no name is assigned, then this field displays the MAC address of the client.
MAC Address	Displays the client's factory-assigned <i>Media Access Control</i> (MAC) address. The MAC address represents the client's unique hardware network identifier.
Status	Displays the associated status of the client.
IP Address	Displays the IPv4 address assigned to this client.

VLAN	Displays the VLAN assigned to this client.
Encryption	Displays the encryption scheme used on the WLAN used by the client.
WLAN	Displays the WLAN which this client uses.
Device Type	Displays the type of device. If a mobile device, displays the vendor name.
OS	If available, displays the Operating System installed on the client.
User Name	If available, displays the username on this client.
IPv6 Address	If assigned, displays the IPv6 address assigned to the client.
SSID	Displays the SSID used by the client.
Authentication Type	Displays the authentication type used on the WLAN used by the client.

- The **Associated to Access Point** area displays detailed information about the access point the client is associated with. The following information is displayed:

Name	Displays the user assigned name for this access point. If no name is assigned, then this field displays the MAC address of the access point.
MAC Address	Displays the access point's factory-assigned <i>Media Access Control</i> (MAC) address. The MAC address represents the access point's unique hardware network identifier.
Radio Mode	Displays the radio used by this client.
BSSID	Displays the BSSID that uniquely identifies the network this client is connected to. A BSS is a set of stations that can communicate with one another.
Channel	Displays the current radio channel that the client uses.

- The **RF** area displays detailed information about the radio in use. The following information is displayed:

Client Available Capability	Displays a list of supported wireless protocols (802.11an, 802.11bgn, 802.11ac etc.) that the client can use to connect to an access point.
Client Connected Capability	Displays the wireless protocol (802.11an, 802.11bgn, 802.11ac etc.) that the client is using to connect to the access point.
Last Transmit Rate	Displays the last transmit rate for this client.
Last Receive Rate	Displays the last receive rate for this client.
Error Rate	Displays the error rate for this client. This is the rate of Tx and Rx error
Average Retry	Displays the average retry rate for this client.
Signal (RSSI)	Displays the RSSI information on this client. This information is displayed as a graph as well as in dBm value.
Noise	Displays the signal noise as recorded by the client. This information is displayed as a graph as well as in dBm value.
SNR	Displays the signal to noise ratio as recorded by the client. This information is displayed as a graph as well as in dBm value.

- The **Utilization** area displays the Tx and Rx utilization volume for this client. The following information is displayed:

TX	Displays the Tx traffic volume in KB/MB/GB.
RX	Displays the Rx traffic volume in KB/MB/GB.

- The **Floor Map** area displays a graphical floor map of the site with a overlay of the client's location. This is only displayed if a floor map for the site is available and the client's can be located on the floor map.
- The **Top 10 Application by Usage** graph displays a graph of the top 10 applications by bandwidth usage.

1.3.4 Monitor Rogues

▶ Monitor

Rogue devices are those devices detected in a sanctioned radio coverage area but have not been deployed by the network administrator as a known device. Authorized devices and clients are generally known to the administrators and conform with the organization's security policies. Unauthorized devices are those detected as inter-operating within the network, but are not approved. These devices should be filtered to avoid jeopardizing the data within a managed network. Use this screen to monitor the number of rogue access points detected within the Tenant managed networks

The *Rogues Summary* screen displays a summary of rogue access points detected by the access points in the Tenant managed network.

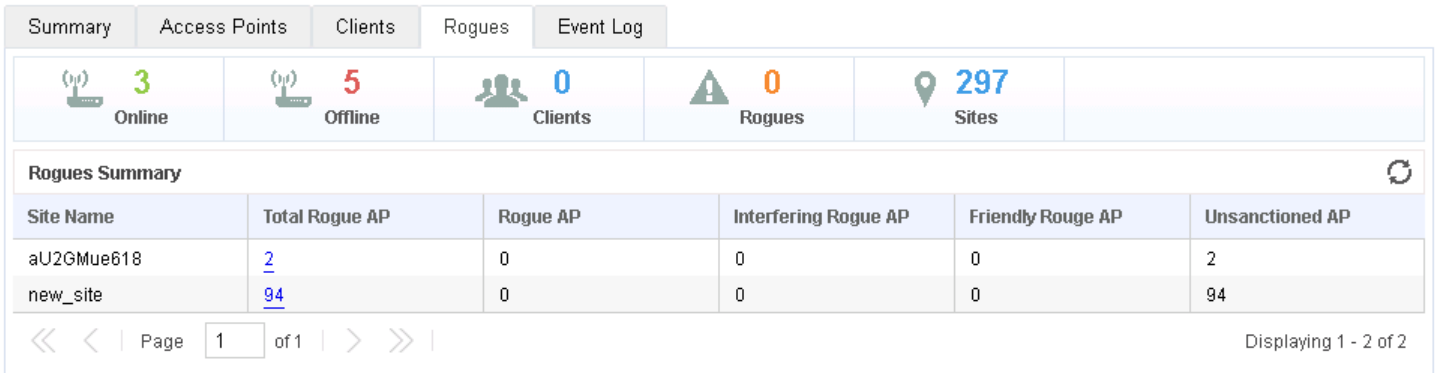


Figure 1-31 Tenant Monitor View - Monitor Rogues

The *Rogues Summary* screen displays a summary of all rogue access points discovered in the Tenant managed network. The following information is displayed:

Site Name	Displays the Tenant managed site where the rogue access points are discovered.
Total Rogue AP	Displays the total number of discovered rogue access points for this site. Use this link to get a detailed description about the discovered rogue access points.
Rogue AP	Displays the total number of access points classified as rogues. Rogue access points are unsanctioned access points that carry traffic.
Interfering Rogue AP	Displays the total number of access points classified as Interfering Rogue access points. These access points run in the same channels used by sanctioned access points.

Friendly Rogue AP	Displays the total number of access points classified as Friendly Rogue access points. These access points are ones that are known and are known not to have any threat associated with them. For example, an access point running in a nearby establishment.
Unsanctioned AP	Displays the total number of access points classified as Unsanctioned access points.

1.3.4.1 Rogue Access Point List

► *Monitor Rogues*

When the link in the **Total Rogue AP** field is selected, the following screen displays:

The screenshot shows a dashboard with tabs for Summary, Access Points, Clients, Rogues, and Event Log. The Rogues tab is active, displaying a summary of 2 Online and 0 Offline access points, 0 Clients, and 0 Rogues. Below the summary is a table titled "List of Rogues and Unsanctioned APs" with the following data:






Status	BSS ID	Vendor	SSID	Signal Stren...	First Seen	Top Reporter	Site Name	Reason
Un...	FE-0A-81-BB...	*Zebra Tech	test_ap7502	-80	4/6/2016, 12:...	ap1-84-24-8...	new_site	Unsanctione...
Un...	FC-0A-81-BC...	Zebra Tech	wx9_sanity_si...	-77	4/4/2016, 6:2...	ap1-84-24-8...	new_site	Unsanctione...
Un...	FC-0A-81-AD...	Zebra Tech	testwlanbanu	-79	4/5/2016, 10:...	ap1-84-24-8...	new_site	Unsanctione...
Un...	FC-0A-81-8D...	Zebra Tech	falcon	-73	4/4/2016, 6:1...	ap1-84-24-8...	new_site	Unsanctione...
Un...	FC-0A-81-8A...	Zebra Tech	wx9_sanity_si...	-57	4/4/2016, 6:1...	ap1-84-24-8...	new_site	Unsanctione...
Un...	FC-0A-81-50...	Zebra Tech	M-Wireless	-78	4/6/2016, 3:1...	ap1-84-24-8...	new_site	Unsanctione...
Un...	FC-0A-81-14...	Zebra Tech	stability_apt...	-63	4/5/2016, 9:5...	ap1-84-24-8...	new_site	Unsanctione...
Un...	B4-C7-99-F3...	Zebra Tech	M-Guest	-83	4/6/2016, 2:5...	ap1-84-24-8...	new_site	Unsanctione...
Un...	B4-C7-99-F3...	Zebra Tech	M-Guest	-72	4/4/2016, 6:1...	ap1-84-24-8...	new_site	Unsanctione...
Un...	B4-C7-99-F3...	Zebra Tech	M-Wireless	-72	4/4/2016, 6:2...	ap1-84-24-8...	new_site	Unsanctione...
Un...	B4-C7-99-CF...	Zebra Tech	N/A	-77	4/5/2016, 11:...	ap1-84-24-8...	new_site	Unsanctione...
Un...	B4-C7-99-95...	Zebra Tech	test_bug	-91	4/6/2016, 2:0...	ap1-84-24-8...	new_site	Unsanctione...
Un...	74-67-F7-0B...	Zebra Tech	tenantseven	-71	4/6/2016, 3:3...	ap1-84-24-8...	new_site	Unsanctione...
Un...	B4-C7-99-8B...	Zebra Tech	alpstest1	-73	4/4/2016, 6:1...	ap1-84-24-8...	new_site	Unsanctione...
Un...	B4-C7-99-67...	Zebra Tech	OPEN_AUTH	-67	4/6/2016, 3:2...	ap1-84-24-8...	new_site	Unsanctione...
Un...	B4-C7-99-66...	Zebra Tech	NEUw	-75	4/6/2016, 2:0...	ap1-84-24-8...	new_site	Unsanctione...
Un...	B4-C7-99-53...	Zebra Tech	adsp-system...	-87	4/6/2016, 2:5...	84-24-8d-83-...	new_site	Unsanctione...

Figure 1-32 Monitor Rogue - Rogue Access Points List

The following information is displayed for each Rogue access point.

Status	Displays the status for this access point. This is the classification of the access point as a rogue device.
BSS ID	Displays the <i>Basic Service Set</i> (BSS) the rogue access point belongs to. A BSS is a set of stations that can communicate with one another. Select this link to view further details for this rogue access point.
Vendor	Displays the manufacturer name for the rogue access point.
SSID	Displays the <i>Service Set ID</i> (SSID) of the network to which the detected rogue access point belongs.
Signal Strength	Displays the signal strength of the detected rogue access point.

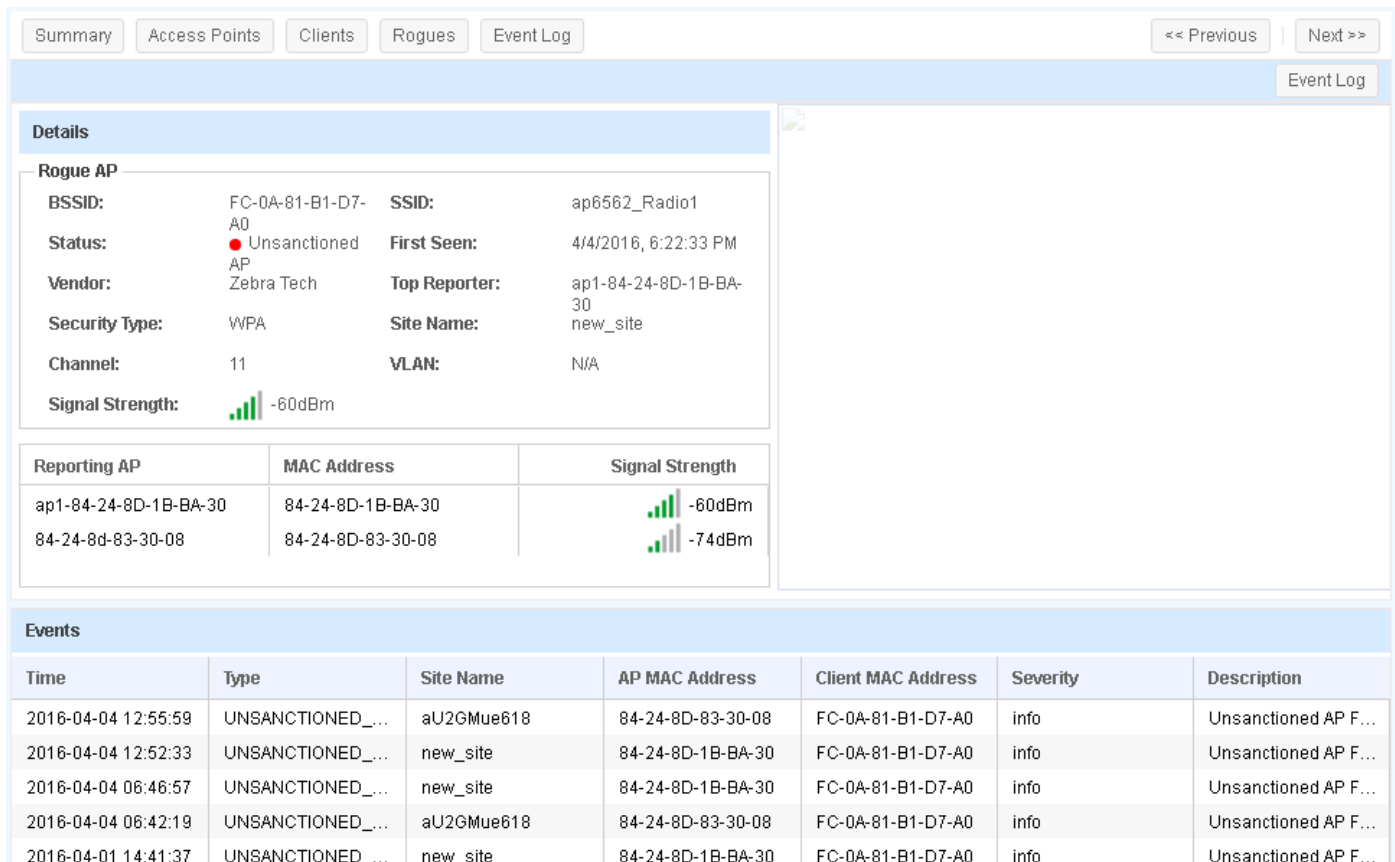
First Seen	Displays the timestamp when this rogue access point was first detected.
Top Reporter	Displays the user assigned name of the access point that reported this rogue access point.
Site Name	Displays the Tenant managed site where this rogue access point was discovered.
Reason	Displays the system assigned reason the access point is marked as rogue.

The group of icons  located to the top right of the **List of Rogue and Unsanctioned APs** table are used to perform specific actions on the data displayed in this table. Use the  icon to refresh the data displayed in this table. Use the  to reset the table columns to default order if their order was changed. Use the  icon to print the information displayed in this table and is displayed in a new tab. Use the  icon to export the data displayed in the table.

1.3.4.2 Rogue Access Point Details

► Monitor Rogues

When the **BSS ID** of a Rogue access point is selected in the list of rogue access points, the following screen displays:






Summary Access Points Clients Rogues Event Log << Previous | Next >>

Event Log

Details

Rogue AP

BSSID:	FC-0A-81-B1-D7-A0	SSID:	ap6562_Radio1
Status:	● Unsanctioned AP	First Seen:	4/4/2016, 6:22:33 PM
Vendor:	Zebra Tech	Top Reporter:	ap1-84-24-8D-1B-BA-30
Security Type:	WPA	Site Name:	new_site
Channel:	11	VLAN:	N/A
Signal Strength:	 -60dBm		

Reporting AP	MAC Address	Signal Strength
ap1-84-24-8D-1B-BA-30	84-24-8D-1B-BA-30	 -60dBm
84-24-8d-83-30-08	84-24-8D-83-30-08	 -74dBm

Events

Time	Type	Site Name	AP MAC Address	Client MAC Address	Severity	Description
2016-04-04 12:55:59	UNSANCTIONED_...	aU2GMue618	84-24-8D-83-30-08	FC-0A-81-B1-D7-A0	info	Unsanctioned AP F...
2016-04-04 12:52:33	UNSANCTIONED_...	new_site	84-24-8D-1B-BA-30	FC-0A-81-B1-D7-A0	info	Unsanctioned AP F...
2016-04-04 06:46:57	UNSANCTIONED_...	new_site	84-24-8D-1B-BA-30	FC-0A-81-B1-D7-A0	info	Unsanctioned AP F...
2016-04-04 06:42:19	UNSANCTIONED_...	aU2GMue618	84-24-8D-83-30-08	FC-0A-81-B1-D7-A0	info	Unsanctioned AP F...
2016-04-01 14:41:37	UNSANCTIONED ...	new site	84-24-8D-1B-BA-30	FC-0A-81-B1-D7-A0	info	Unsanctioned AP F...

Figure 1-33 Monitor Rogues - Rogue Access Point Details

The Rogue AP **Details** table displays the following information.

BSSID	Displays the <i>Basic Service Set</i> (BSS) the rogue access point belongs to. A BSS is a set of stations that can communicate with one another.
Status	Displays the status for this access point. This is the classification of the access point as a rogue device.
Vendor	Displays the manufacturer name for the rogue access point.
Security Type	Displays the security type in use on the rogue access point.
Channel	Displays the channel on which the rogue access point was found.
Signal Strength	Displays the signal strength of the detected rogue access point.
SSID	Displays the <i>Service Set ID</i> (SSID) of the network to which the detected rogue access point belongs.
First Seen	Displays the timestamp when this rogue access point was first detected.
Top Reporter	Displays the user assigned name of the access point that reported this rogue access point.
Site Name	Displays the Tenant managed site where this rogue access point was discovered.
VLAN	If available, displays the VLAN on which the rogue access point was discovered.

The **Reporting AP** table displays the following information.

Reporting AP	Displays the user assigned name of the access point that reported this rogue access point.
MAC Address	displays the MAC address of the access point that reported this rogue access point.
Signal Strength	Displays the signal strength of the rogue access point as seen by the reporting access point.

The **Events** table displays the following information.

Time	Displays the date and time stamp for this event.
Type	Displays the type of event.
Site Name	Displays the site on which this event was reported.
AP MAC Address	Displays the MAC address of the access point that reported this rogue access point.
Client MAC Address	Displays the MAC address of the rogue access point.
Severity	Displays the event severity information.
Description	Displays a detailed information on this event.

1.3.5 Monitoring Event Logs

► *Monitor*

Use the **Event Log** tab to view a list of events for this Tenant. Event logs enables the Tenant to view the current state of a network and provides a detailed insight into any incident/error that occurs on a particular network.

The *Event Log* screen provides customizable access to network events and other log information which can then be used to troubleshoot issues with the network. Events and logs can be filtered on various criteria to enable the Tenant administrator have a deep look at the network's state.

To view event log for a Tenant:

1. Select the **Monitor** tab from the menu on the top of the screen. The **Monitor > Summary** screen displays.
2. Select **Event Log** from the list of tabs. By default, the event log screen displays the event logs for all the networks for this Tenant. To filter events for a particular network, select the network from the menu tree on the left of the screen.

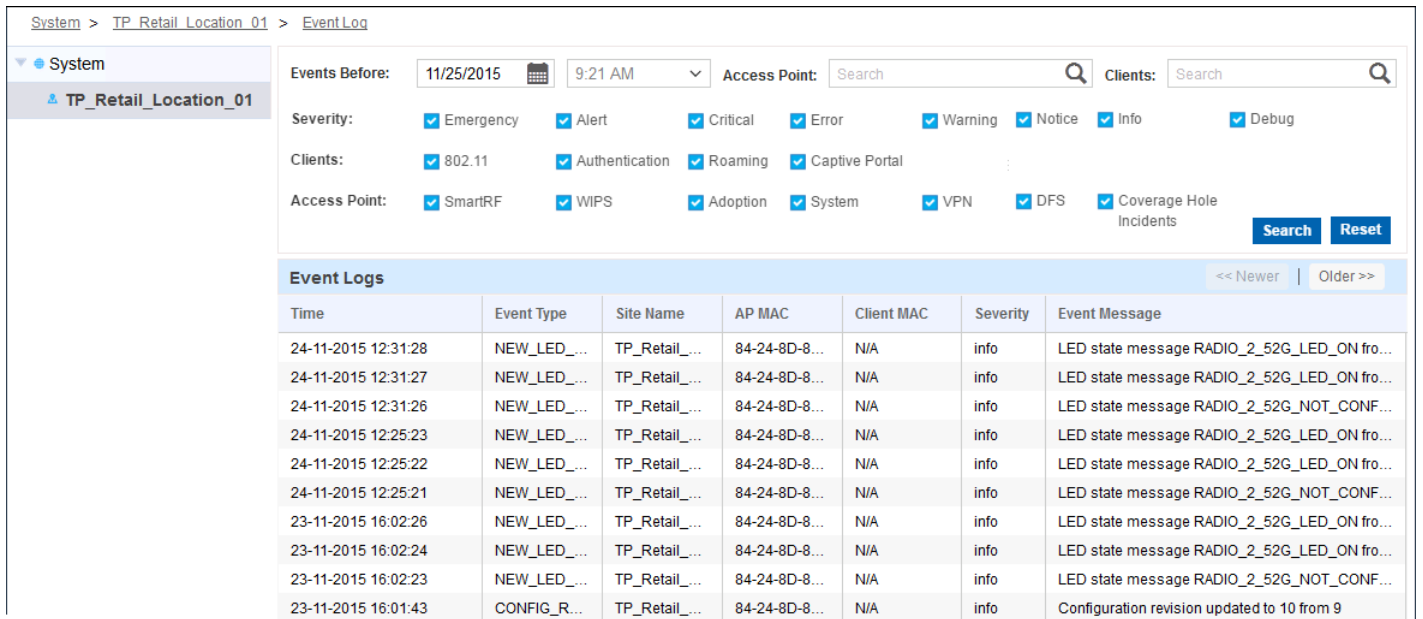


Figure 1-34 Tenant Monitor View - Monitor Logs

The *Event Log* screen is divided into a configuration section at the top of the page and a log section on the lower half of the page. Use the configuration section to filter events based on different criteria.

Events can be filtered on the following criteria:

Events Before	Use the calendar control and the time drop-down list to filter events before a particular date and time of interest. When set, events before the set date and time are displayed.
Access Point	Use this drop-down list to select the access point of interest to view the events for. This is a dynamic field and filters out those content that do not match the current entry in this field. Use any value such as the MAC address or device name in this field to narrow down your search for the access point of interest.
Client	Use this drop-down list to select the client of interest to view the events for. This is a dynamic field and filters out those content that do not match the current entry in this field. Use any value such as the MAC address or device name in this field to narrow down your search for the client of interest.

Severity	Use the check-boxes to include a category of events in the filter. When selected, events for that particular severity category are included in the displayed events. To exclude a particular category of events, clear the check-box for that category.
Clients	Use the check-boxes to include different client types. When selected, clients of the particular type are included in the displayed events. To exclude a particular category of clients, clear the check-box for that category.
Access Point	Use the check-box to include different events specific to access points. When selected, events for a particular category are included in the displayed events. To exclude a particular category of access point events, clear the check-box for that category.

3. After setting the filter criteria, select **Search** to filter. Use the **Reset** button to reset the filter criteria to default values.

1.4 Reports

► [Tenant Management](#)

Use the Tenant's *Reports* screen to view the reports for this Tenant. Tenants add reports through the **Manage Reports** tab. Reports can be created with any combination of type, scope and period parameters. Reports can be scheduled to have periodic data for further analysis.

Use the reports to have a record of the performance of the networks managed by the Tenant and use them to tune the network for better performance or for troubleshooting.

Detailed reports enable Tenant network administrators to view attempted intrusions into their networks and to have a detailed insight into the activities of their clients.

1.4.1 Generated Reports

► [Reports](#)

The *Generated Reports* screen displays the reports generated for a Tenant. These reports can be filtered for each configured network for the Tenant.

By default, there are no existing reports for a Tenant. The Tenant must create, configure and schedule reports of interest for the Tenant.

To view reports for a Tenant:





1. Select **Reports** from the menu at the top of the screen. The **Generated Report** tab displays a list of generated reports.

Report	Category	User	Start Date	End Date	Run on	Actions
schedule_test	Device Summary	zebra@zebra.com	2016-04-07	2016-04-29	2016-04-11 01:30 AM	[Print] [Email] [Delete]
schedule_test	Device Summary	zebra@zebra.com	2016-04-07	2016-04-29	2016-04-07 04:42 PM	[Print] [Email] [Delete]
schedule_test	Device Summary	zebra@zebra.com	2016-04-07	2016-04-29	2016-04-07 04:39 PM	[Print] [Email] [Delete]
test	Device Type/Firmwa...	zebra@zebra.com	N/A	N/A	2016-04-07 01:27 PM	[Print] [Email] [Delete]

Figure 1-35 Tenant Reports View - Generated Reports

2. Generated Reports display the following information:

Report	Displays the name of the report as a link. Select the link to view the report in greater detail within a separate window.
Category	Displays the report category as a brief description of the report's content type.
User	Displays the e-mail address of the user who created the report as an indication of its originator.
Start Date	If configured, this field displays the start date for generating the report. The report is only generated on or after this start date. Displays N/A if not configured.
End Date	If configured, this field displays the end date for generating the report. The report is not generated after this date. Displays N/A if not configured.
Run On	Displays the date and time when this report was run last. Use this an indicator of this report's current relevance.

Action	Use the  icon to save and view the report as a PDF. Similarly, use the  icon to save and view the report as a <i>comma separated value</i> (CSV) file. Use the  icon to delete the report. Use the  icon to refresh this screen with the latest report values.
---------------	--

1.4.2 Manage Reports

▶ Reports

Use the *Manage Reports* screen to create, edit or delete custom reports for the Tenant. The Tenant can customize reports to suit specific report data capture requirements. Reports can be scheduled or run as required.

To manage Tenant reports:

1. Select **Reports** from the menu at the top of the screen. The **Generated Reports** tab displays by default. Select **Manage Reports**.

The *Manage Reports* screen displays a list of existing Tenant reports. To refine this list, select the network from the menu tree on the left-hand of the screen.

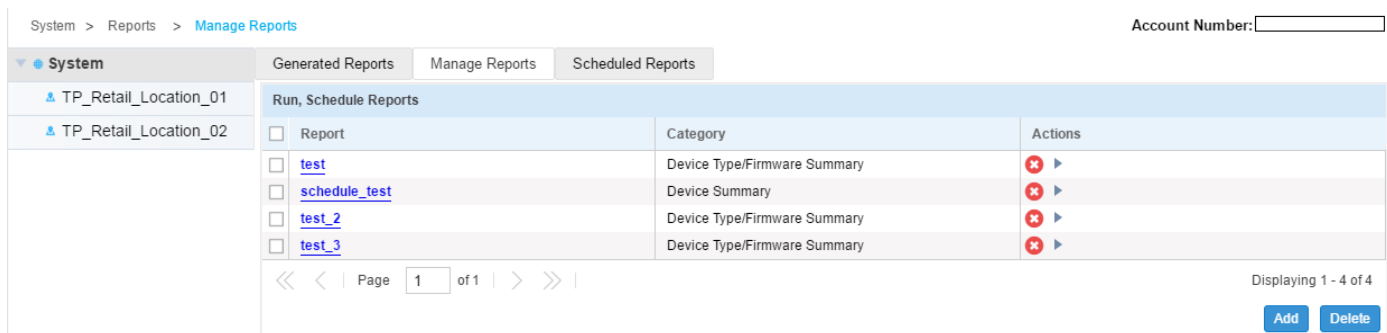




Figure 1-36 Tenant Reports View - Manage Reports

2. The following report data displays:

Report	Displays the name of the report as a link. Select the link to edit report content in a separate window.
Category	Displays the report type. A report is classified based on the contents of the report and the part of the system that it reports on.
Action	Use the  icon to delete a report. Use the  icon to run the report immediately irrespective its scheduled time.

3. Select the **Add** button located at the bottom right of the screen to create a new report. The following screen displays.

Figure 1-37 Tenant Reports View - Manage Reports - Add/Edit Reports

4. Create or edit the following report parameters:

Title	Provide a title for this report to better apply significance to the data you hope to capture during the report's trending period.
Type	<p>Use the drop-down menu to select the type of report. Report type can be one of:</p> <ul style="list-style-type: none"> • <i>Device Type/Firmware Summary</i> - This report type provides a summary of the devices for the Tenant and lists the firmware installed on the Tenant's networks. • <i>Device Summary</i> - This report type provides a summary of device usage for the Tenant. • <i>Client Inventory</i> - This report type provides a summary of the clients using the Tenant's networks. • <i>PCI Compliance Report (3.1)</i> - This report type creates reports that lists compliance to the <i>Payment Card Industry (PCI) Data Security Standard</i> parameters. • <i>Network Usage</i> - This report type creates a report on the network usage of a Tenant's network. • <i>RF Health</i> - This report type creates a report on the radio frequency usage and health of the Tenant's network.
Scope	Use the drop-down list to select the scope of the report. Use <i>System</i> to generate a report for the whole system including each configured network. Select a network from the drop-down list to restrict the report to the selected Tenant network.

Period	<p>Use the drop-down list to select the reporting period for this report. Period can be one of:</p> <ul style="list-style-type: none"> • <i>Last Hour</i> - Creates a report of status in the last hour. • <i>Last Day</i> - Creates a report of status in the last day. • <i>Last Week</i> - Creates a report of status in the last week. • <i>Last Month</i> - Creates a report of status in the last month. • <i>Custom</i> - Creates a report of status for a customized duration. Use the <i>Start/End</i> fields to configure the period for generating the report.
Schedule	<p>Set a start date and end date for report duration. The report will only run on or after the date set in the <i>Start Date</i> field. The report will not run after the date set in the <i>End Date</i>, so ensure this values adequately captures the required data trending period.</p>
Recurrence	<p>Schedule the time this report is run. Reports can be run either:</p> <ul style="list-style-type: none"> • <i>Daily</i> - Use the <i>Time</i> drop-down menu to select the time at which to run the daily report. • <i>Weekly</i> - Select this option to run the report on a particular day of the week. Use the <i>Day of Week</i> field to select the weekday to run the report on. Use the <i>Time</i> drop-down menu to select the time the weekly report is generated. • <i>Monthly</i> - Run this report on a particular date of the month each month. Use the <i>Day of Month</i> field to set the date. Use the <i>Time</i> drop-down menu to select the time begin the historical report data gathering process.
Format	<p>Select the output format for this report.</p> <ul style="list-style-type: none"> • <i>PDF</i> - The report is saved in PDF format. • <i>CSV</i> - The report is saved as a <i>comma separated value</i> (CSV) format file.
Destination	<p>Use the following destination options to set how a generated report is stored.</p> <ul style="list-style-type: none"> • <i>Store on Server</i> - Stores and archives a generated report on the server. Generated reports are listed in the Generated Reports tab. • <i>Store and Email</i> - Stores and archives a generated report on the server and sends the report to the e-mail address entered in the adjoining text box.
Run	<p>Select <i>Run</i> to immediately start the report's data gathering process despite its scheduled start time. The report is not saved however.</p>
Save	<p>Select <i>Save</i> to save the report for running later. The report is not run (started) when saved.</p>
Save & Run	<p>Use the <i>Save & Run</i> option to save the report and queue the report to begin running.</p>
Cancel	<p>Select <i>Cancel</i> to stop an in progress report creation or report save operation.</p>

5. These options are applicable when report **Type** is set to *PCI Compliance Report (3.1)*.

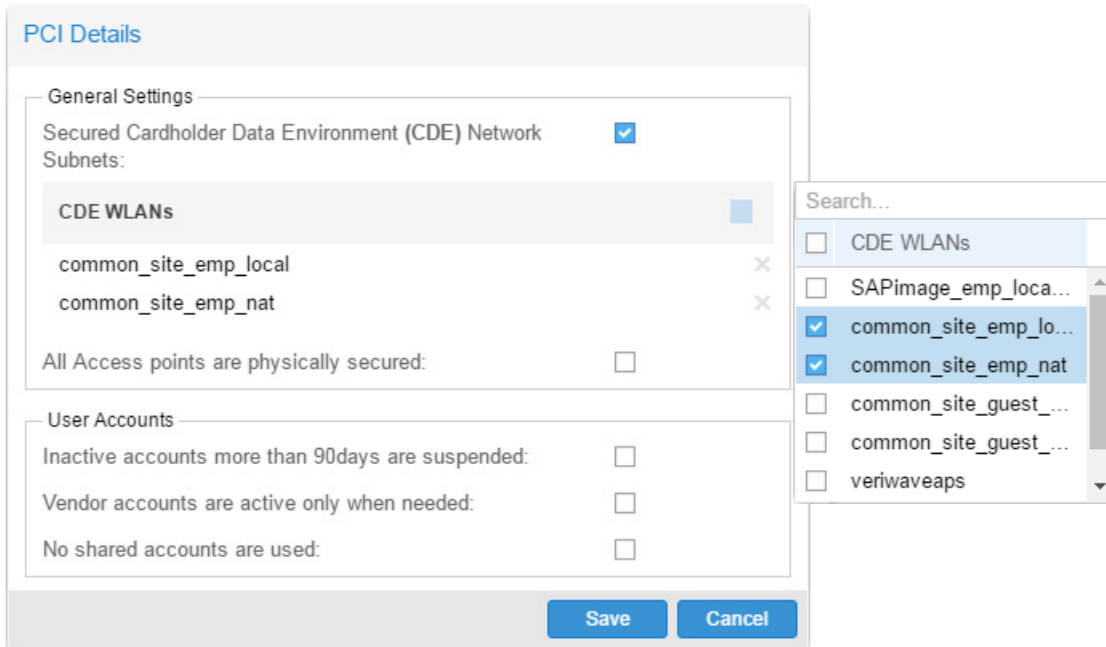


Figure 1-38 Tenant Reports View - Manage Reports - PCI Compliance Report Configuration

Secured Cardholder Data Environment (CDE) Network	Select this option to include the <i>Cardholder Data Environment (CDE)</i> networks when creating the report. When this option is selected, the CDC WLANs field is enabled. Click the blue box on the right to display a list of available CDC WLANs. From this list, select the WLANs to include when generating the report. When selected, the WLAN is listed in the main window.
All Access points are physically secured	Select this option to indicate that all access points are physically secured. When enabled, the report indicates that all access points are verified as being physically secured.
Inactive accounts more than 90 days are suspended	Select this option to indicate that the PCI compliance report checks and reports if user accounts that are inactive for more than 90 days are suspended.
Vendor accounts are active only when needed	Select this option to indicate that the PCI compliance report checks and reports if the vendor accounts are only activated when it is required.
No shared accounts are used	Select this option to indicate that the PCI compliance report checks and reports if there are any shared accounts in use in the system.

Select **Save** to save the PCI compliance report configuration. Select **Cancel** at any time to exit without configuring this report.

1.4.3 Scheduled Reports

The *Scheduled Reports* screen displays reports scheduled to run for a Tenant. Reports are added from the *Manage Reports* screen and are configured to run at a schedule at create time. This screen lists those reports that are scheduled to run at a future point of time for this Tenant.

To view the scheduled reports for this Tenant:

1. Select **Reports** from the menu at the top of the screen. The **Generated Reports** tab displays.

2. Select the **Scheduled Reports** tab.

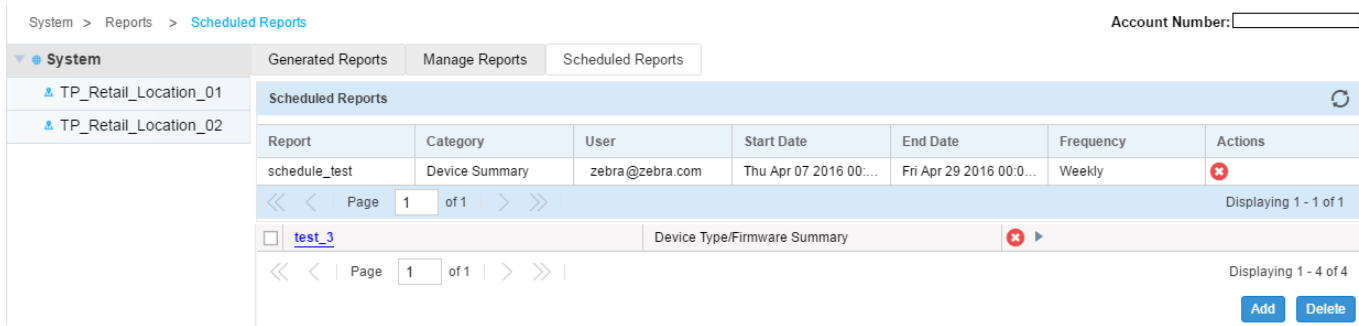



Figure 1-39 Tenant Reports View - Scheduled Reports

3. Scheduled Reports screen displays the following information:

Report	Displays the name of the report.
Category	Displays the report category as a brief description of the report's content type.
User	Displays the e-mail address of the user who created the report as an indication of its originator.
Start Date	If configured, this field displays the start date for generating the report. The report is only generated on or after this start date. Displays N/A if not configured.
End Date	If configured, this field displays the end date for generating the report. The report will not be generated after this date. Displays N/A if not configured. Ensure the end data provides an adequate window for data capture and reporting significance.
Frequency	If configured, this field displays the frequency of report run. Displays NA if not configured.
Action	Use the  icon to delete a scheduled report. When deleted, the report is removed from the run queue but not removed from the list of configured reports.

1.5 Tools

▶ [Tenant Management](#)

The **Tools** screen provides network troubleshooting tools to help diagnose connectivity and quality issues on the Tenant managed network.

The following tools are available:

- [Packet Capture](#)
- [Wireless Debug Log](#)
- [Ping/Traceroute](#)

1.5.1 Packet Capture

▶ [Tools](#)

The Azara dashboard interface provides tools to capture the network traffic. Packet capture is an important tool in the administrator's toolkit providing an insight into the traffic flow across the network and is primarily used as a forensics and troubleshooting tool. Packet capture is used to analyze network problems, to detect misuse of the network by internal or external users, monitor utilization of network resources among other things.

To capture packets

1. Select **Tools** from the menu at the top of the screen.
2. Select **Packet Capture**. From the menu tree on the left-hand side of the screen, select the target site.

Packet Capture | Wireless Debug Log | Ping/Traceroute

Site Name: test_bug Include All Devices Search Send Packets To: Screen

Capture Locations

All Wired Packets

Dropped

Wired Packet Direction: Any

Wireless Packet Direction: Any

Note: The max packet capture data limit is 15MB.

Filter

Filter By MAC Address: XX-XX-XX-XX-XX-XX

Filter By IP:

IP Protocol: TCP

Port: 1

Settings

Maximum Packet Count: 200

#	Time	Captured On	Inte...	Sou...	Sport	Des...	DPort	VLAN	Ext...	Pro...	Info
Details											

Figure 1-40 Tenant Tools View - Packet Capture Tool

3. Refer to the following for more information:

<p>Site Name</p>	<p>Enter the first few characters of the site name into the text field and select the search icon to search for the site. From the resulting drop-down list, select the site of interest. Packets from other sites will be ignored.</p>
<p>Include All Devices</p>	<p>Select the option to include all devices in a site when capturing packets for the site. This option is enabled by default.</p> <p>To capture packets for a particular device in a site, un-select this option and use the enabled Devices search box to search for the device of interest. Enter the first few characters of the device's MAC address into the text field and select the search icon. From the resulting drop-down list, select the device of interest.</p>
<p>Send Packets To</p>	<p>Use the drop-down list to select the destination for the captured packets. This is a list of various options available for displaying or saving the captured packets. The default option is an output to the local PC's screen.</p>
<p>Capture Locations</p>	<p>Use this field to define the packets types to capture.</p> <ul style="list-style-type: none"> • <i>All Wired Packets</i> – Select this option to capture all packets from the different wired ports. Packets in both directions are captured. • <i>Dropped</i> – Select this option to capture all packets dropped due to various reasons such as ACLs and timeouts. • <i>Wired</i> – Select this option to capture packets from a particular wired interface. The interface is selected from the drop-down listing the interface type and the interface number. Use the Packet Direction drop-down to select the packet flow direction. Select <i>Any</i> to capture packets traversing the interface in any direction. Select <i>Inbound</i> or <i>Outbound</i> to capture packets traversing the interface in that direction. • <i>Wireless</i> – Select this option to capture packets from a particular wireless radio interface. The interface is selected from the drop-down listing the available radios for the access point. Use the Packet Direction drop-down to select the packet flow direction. Select <i>Any</i> to capture packets traversing the interface in any direction. Select <i>Inbound</i> or <i>Outbound</i> to capture packets traversing the interface in that direction.
<p>Filter</p>	<p>Use this field to define the filtering criteria when capturing packets. Packet capture captures all packets defined by the Capture Locations criteria. This capture will contain a large amount of packets that will not be of interest in a particular situation. Use the following criteria to filter out the packets that do not interest you.</p> <ul style="list-style-type: none"> • <i>Filter by MAC Address</i> – Select this option to filter out all packets that are not from/to the device with the MAC address specified in the box. Provide the MAC address of the device of interest in the text box. • <i>Filter by IP</i> – Select this option to filter out all packets that are not from/to the device with the IP address specified in the box. Provide the IP address of the device of interest in the text box. • <i>Filter by Protocol</i> – Select the protocol of interest from the drop-down. All protocols except the one selected are filtered out from display. • <i>Port</i> – Set the port of interest using the spinner control. Packets from all other ports are filtered out from display. <p>Note: The above filters can be combined for finer control over the packet capture.</p>

Maximum Packet Count

Use the spinner control to set the maximum number of packets to be captured. Packet capture is stopped once these many packets are captured. Set a value in the range of 0 - 4000. The default value is 200 packets.

- Use the **Start** button to start the packet capture. If the **Send Packets To** is set to *Screen*, the captured packets are displayed in the area below. To know more information about a captured packet, select the packet in the list to display its details in the **Details** area.

Use the **Stop** button to stop packet capture.

Start
Stop
Hide Capture Options

#	Time	Captured On	Inte...	Sou...	Sport	Des...	DPort	VLAN	Ext...	Pro...	Info
1	0.00...	7532-80-BF-E8	ge1	84:2...	N/A	84:2...	N/A	N/A	N/A	MINT	MINT 64547
2	0.00...	7532-80-BF-E8	ge1	84:2...	N/A	84:2...	N/A	N/A	N/A	MINT	MINT 67
198	1.95...	AP7522-1	radio...	fc:0a...	N/A	ff.ff.f...	N/A	N/A	N/A	802...	Beacon, SSID:...
199	1.95...	AP7522-2	radio...	86:2...	N/A	ff.ff.f...	N/A	N/A	N/A	802...	Beacon, SSID:...
200	1.95...	AP7522-1	radio...	84:2...	N/A	ff.ff.f...	N/A	N/A	N/A	802...	Beacon, SSID:...

Details

- [-] Frame 200: 304 bytes transmitted, 304 bytes captured
 - [+] Frame Number: 200
 - [+] Frame Length: 304
 - [+] Captured Length: 304
- [-] TZSP: Radio
 - [+] Captured On: AP7522-1
 - [+] Capture Location: radio 1
 - [+] RSSI: -39
 - [+] Data Rate: 1MB/s
 - [+] Channel: 11

```

00000 01 00 00 12 50 08 41 50          37 35 32 32 2D 31 51 07  ....P.AP7522-1Q.
00010 72 61 64 69 6F 20 31 0A          01 09 0C 01 02 12 01 08  radio 1.....
00020 28 04 00 00 00 62 29 02          01 05 01 80 00 00 00 FF  (.b).....
00030 FF FF FF FF FF 84 24 8D          92 53 B0 84 24 8D 92 53  ....$.S$.S
00040 B0 10 9A 63 8A 9E 14 A3          01 00 00 64 00 01 04 00  ...c.....d...
00050 0C 61 75 74 6F 5F 73 73          69 64 5F 75 73 01 08 82  .auto_ssid_us...
00060 84 88 96 24 30 48 6C 03          01 08 05 04 01 02 01 01  ..$0Hl.....
00070 07 06 55 53 20 01 0B 1E          2A 01 00 32 04 0C 12 18  ..US ...*.2....
00080 60 08 05 01 00 C4 12 7A          2D 1A AD 19 17 FF FF 00  ^.....z-.....
00090 00 00 00 00 00 00 00 00          00 00 00 00 00 00 00 00  .....
000a0 00 00 00 00 3D 16 0B 08          15 00 00 00 00 00 00 00  ....=.....
000b0 00 00 00 00 00 00 00 00          00 00 00 00 4A 0E 14 00  .....J...
000c0 0A 00 2C 01 C8 00 14 00          05 00 19 00 7F 08 05 00  ,.....
000d0 08 00 00 00 00 40 AD 0F          00 A0 F8 01 00 31 00 FC  ...@.....1..
000e0 00 00 00 E2 61 90 57 DD          1E 00 A0 F8 03 00 01 00  ....a.W.....
000f0 00 00 00 00 00 4D 82 94          DC 00 01 00 01 84 24 8D  ....M.....$.
00100 82 94 DC 00 01 11 0B DD          07 00 50 F2 02 00 01 80  .....P.....
00110 DD 1E 00 90 4C 04 08 BF          0C 92 59 81 0F FA FF 00  ...L....Y....
00120 00 FA FF 00 00 C0 05 00          0B 00 00 00 C3 02 00 02  .....
    
```

Figure 1-41 Tenant Tools View - Packet Capture - Output

- Use the **Hide Capture Options** button to hide the packet capture configuration section of this screen. Similarly, use the **Show Capture Options** button to show the hidden configuration section.

1.5.2 Wireless Debug Log

► [Tools](#)

Wireless Debug Log is a diagnostic tool that enables live wireless debugging event log capture on one or more access points deployed by the tenant. Use this tool to get a real-time look into the state of the access points and their associated wireless clients. Wireless debug information obtained through the debug logs is retained by each access point and discloses the 802.11 protocol level errors that may be occurring but that are yet not reported at other levels in the system debug log.

A thorough analysis of debug logs helps you understand how the access points are performing and troubleshoot performance related issues. Consequently, it is a useful tool for preempting potential threats to the smooth functioning of the network.

To view wireless debug logs:

1. Select **Tools** from the menu at the top of the screen.
2. Select the **Wireless Debug Log** tab. The following screen displays:

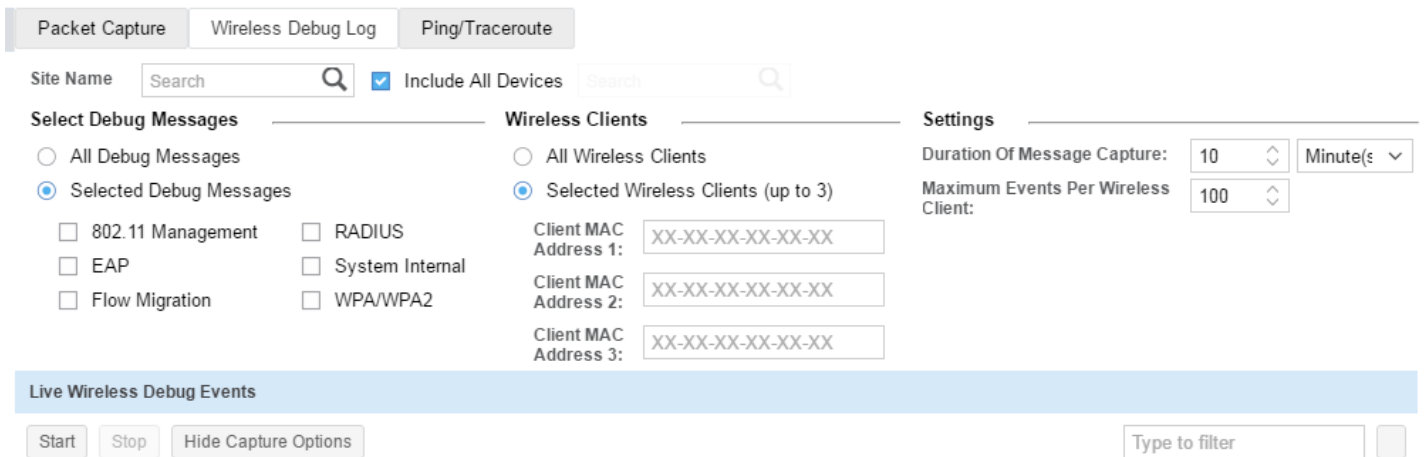


Figure 1-42 Tenant Tools View - Wireless Debug Log

3. Use the options available on this screen to enter details based on which the system captures and displays debug logs.

<p>Site Name</p>	<p>Enter the first few characters of the site name into the text field and select the search icon to search for the site. From the resulting drop-down list, select the site of interest. Wireless debug log packets from other sites will be ignored.</p>
<p>Include All Devices</p>	<p>Select the option to include all devices in a site when capturing wireless debug log for the site. This option provides full visibility into remote wireless clients as they associate, authenticate, re-authenticate and roam throughout the site across all deployed access points. This option is enabled by default.</p> <p>To capture wireless debug logs for a particular device in a site, un-select this option and use the enabled Devices search box to search for the device of interest. Enter the first few characters of the device’s MAC address into the text field and select the search icon. From the resulting drop-down list, select the device of interest.</p>

4. In the **Select Debug Messages** section, use the options available to specify the events for which messages are to be captured.

All Debug Messages	Use this option to capture all wireless debug messages.
Selected Debug Messages	<p>Use this option to select the message types to capture:</p> <ul style="list-style-type: none"> • <i>802.11 Management</i> – Logs WLAN IEEE 802.11 connection (log in/log out) event messages. This event filter helps troubleshoot mobility and SMART client load-balancing issues. • <i>EAP</i> – Logs EAP authentication related event messages. This event filter helps troubleshoot events relating to client unable to authenticate or re-authenticate during roaming issues. • <i>Flow Migration</i> – Logs migrating flows of wireless clients migrating from one AP to another AP within the specified site. This event filter helps troubleshoot roaming related issues. • <i>RADIUS</i> – Logs RADIUS authentication related event messages. This event filter helps troubleshoot connectivity issues between the APs and RADIUS authentication servers. • <i>System Internal</i> – Logs system internal debug messages. This event filter helps troubleshoot system related issues. • <i>WPA/WPA2</i> – Logs WPA/WPA2 authentication/encryption related event messages. This event filter helps troubleshoot 4-way handshake issues during initial association, re-authentications, or roaming. <p>Note: The above debug message capture type filters can be combined for finer control over the debug log contents.</p>

5. In the **Wireless Clients** section, use the options available to specify the wireless clients for whom logs are to be captured.

All Wireless Clients	Use this option to capture wireless debug messages for all wireless clients for the selected site.
Selected Wireless Clients (up to 3)	<p>Use this option to configure up to 3 individual client MAC address to display debug information for. Enter the MAC address in the XX-XX-XX-XX-XX-XX format.</p> <ul style="list-style-type: none"> • <i>Client MAC Address 1:</i> – Enter MAC address of wireless client 1 • <i>Client MAC Address 2:</i> – Enter MAC address of wireless client 2 • <i>Client MAC Address 3:</i> – Enter MAC address of wireless client 3 <p>Note: The system captures and displays debug information only from these wireless clients.</p>

6. In the **Settings** section, specify the capture duration and the maximum number of events to capture per wireless client.

Duration of Message Capture:	Use the spinner control to specify the message capture duration. For example, if the value is set to 10 minutes, the system captures debug information for a period of 10 minutes. Specify the duration either in hours, minutes, or seconds. The default value is 10 minute.
Maximum Events Per Wireless Client:	Use the spinner control to specify the maximum number of debug messages to capture per wireless client. Specify a value from 1 - 10000 messages. The default value is 100 messages.

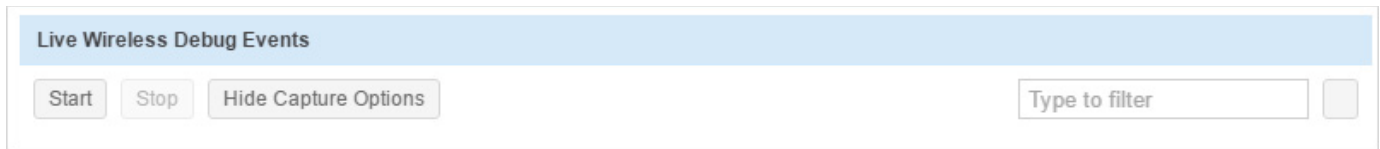


Figure 1-43 *Tenant Tools View - Wireless Debug Log - Live Wireless Debug Events*

7. Use the **Start** button to start viewing the wireless debug log capture. Use the **Stop** button to stop. Click the **Save to Disk** link to save the captured wireless debug log to the local PC's hard disk.
8. Use the **Hide Capture Options** button to hide the wireless debug log capture configuration section of this screen. Similarly, use the **Show Capture Options** button to show the hidden configuration section.
Use the **Type to filter** text area to filter logs from the list displayed to filter only those logs of interest.

1.5.3 Ping/Traceroute

► Tools


The Azara dashboard interface provides tools to troubleshoot network connection issues. Use *ping* to test if a host can be reached on an IP network and measure the round trip time from originating host to its destination and back again. *Traceroute* is a diagnostic tool for displaying a route (path) and measuring the delays for packets traversing the network. The history of the route is recorded as the round-trip times of packets received at each successive host in the route. The sum of the mean times to each hop is the total time required to establish the connection to the remote host.

The traceroute and ping operations can only be performed for online devices.

To troubleshoot network issues on a connected access point:

1. Select **Tools** from the menu at the top of the screen.
2. Select **Ping/Traceroute**. From the menu tree on the left-hand side of the screen, select the target network.

Figure 1-44 Tenant Tools View - Ping/Traceroute Tool

3. Use the **Device** field to search for devices to troubleshoot. Use the  icon to search for devices within the Tenant network. A drop-down menu displays a list of online access points. Select the appropriate access point from the list.
4. Use the **IP Address** field to enter a target IP address to ping or trace. Only IPv4 formatted addresses are supported.
5. Select **Ping** to ping to the selected IP address. Similarly, click **Trace Route** to trace the packet path to the defined IP address. Use the **Stop** button to abort an in progress ping or trace. Use the **Clear** button to clear the contents in the **Results** area.

System > Tools > Ping/Traceroute Account Number:

System	Ping/Traceroute
TP_Retail_Location_01	Device <input type="text" value="cloudap-2-ap7522"/>
TP_Retail_Location_02	IP Address or DNS Name <input type="text" value="8.8.8.8"/>

Results

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=48 time=48.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=48 time=49.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=48 time=47.8 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=48 time=49.7 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=48 time=47.3 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4064ms
rtt min/avg/max/mdev = 47.375/48.548/49.759/1.017 ms
TRACE_END
```

Figure 1-45 Tenant Tools View - Tools - Ping Results

1.6 Configuration

▶ [Tenant Management](#)

Use the *Configuration* screens to setup Tenants and their networks. Tenant configuration involves setting the Tenant's networks and sites, adding devices, creating users and configuring automatic firmware update settings. Use the *Licenses* screen to apply licenses to this Tenant's account.

Refer to the following sections:

- [Configuring Tenant Networks](#)
- [Configuring Sites](#)
- [Managing Inventory/Devices](#)
- [Configuring Tenant Users](#)
- [Configuring Tenant Preferences](#)
- [Licensing](#)
- [Captive Portal](#)

1.6.1 Configuring Tenant Networks

▶ [Configuration](#)

Use the *Network* screen to manage networks for this Tenant. Networks can be added, removed or modified using this screen. Multiple networks can be created to better define the Tenant's requirements.

To view the list of networks configured for this Tenant:

1. From the **Configuration** menu item, select **Network**.

The list of networks for this Tenant displays.



Figure 1-46 Tenant Configuration View - View Existing Networks

The screen displays the following:

Name	Displays the name of networks already created within this Tenant.
SSIDs	Displays the SSIDs associated with each network.
Status	Displays the status of the network. The icon indicates the network is active. The icon indicates the network is inactive.
Actions	Displays the actions that can be performed on configured networks. A network can either be edited or deleted. To edit a network's settings, select the icon. To delete a network, select the icon.

2. To add a new network, select the icon from the top right-hand corner of the **Network Details** bar.

Network Name * Clone From Network

Figure 1-47 Tenant Configuration View - Add a Network

3. Enter the following information for the new network:

Network Name	Enter a name for this new network. Network name cannot be longer than 32 characters. Name cannot contain any special characters except the “-” (hyphen) and “_” (underscore) characters. Name can contain spaces and numbers.
Clone From	If cloning the new network from an existing network, use the drop-down menu to select the network from which to clone. When a network is cloned, the network configuration is copied from the network selected in this field. Once created, edit only those configurations that differ (from that of the cloned network) in the new network.

4. Select the **Create Network** button. The network is created and the following screen displays:

System > Configuration Account Number:

Network | Sites | Captive Portal | Inventory / Devices | Users | Preferences | License Info

Network Name *

SSID(s) | Network Wide Settings

Enter SSID

Service Type *

Name *

SSID *

Status

Security [Open](#)

Band Dual (2.4 & 5 Ghz) 2.4 Ghz 5 Ghz

Advanced Settings

Client IP Assignment

WLAN Settings

Firewall Settings

Application Visibility and Control

Figure 1-48 Tenant Configuration View - Create a Network

5. Select the **Service Type**. The options are *Guest* and *Employee*. A *Guest* network is basically a captive portal configured to provide guest users temporary access to the network. Ensure appropriate **Service Type** is selected, as it impacts other parameters of the network. This is a mandatory field.
6. Enter a **Name** for this SSID. Enter a name that describes the purpose of this network and differentiates it from other networks. For ease of use, the **SSID** field is also populated with this value.

7. Enter the network's SSID. This is a mandatory field.

Each network can have a maximum of 16 SSIDs associated with it. To add an SSID select the + button below the **SSID(s)** tab, provide the **Service Type** and proceed with defining the parameters along the lines documented in the following steps.

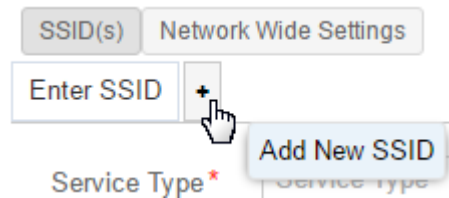


Figure 1-49 Tenant Configuration View - Create a Network - Add SSID



NOTE: The **Network Wide Settings** tab is applicable for AP7502 only.

8. Select the **Status** drop-down list to expand it. The options are *Enabled* and *Disabled*. By default the *Enabled* option is selected. When enabled, this network is available for use.
9. Use the **Security** field to configure the network's security parameters. Select the [Open](#) link and configure the encryption and authentication modes to provide some measure of security. The options are: **Open**, **Secure-PSK**, or **Secure-802.1x**.

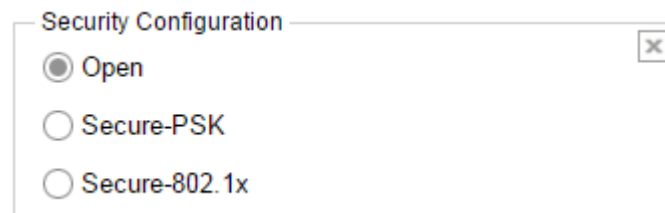


Figure 1-50 Tenant Configuration View - Create a Network - Configure Security

10. Select **Open** for no encryption and authentication. This is the default setting. However, this option is not recommended as it provides no data protection.
11. Select **Secure-PSK** for password protected encryption. If selecting **Secure-PSK**, define the following parameters:

Security Configuration

Open Encryption Key must have min of 8 & max of 63 chars for ASCII encoding

Secure-PSK Key Show

Secure-802.1x ASCII HEX

Figure 1-51 Tenant Configuration View - Create a Network - Configure Secure-PSK Security

Encryption	<p>Specify the mode of encryption as <i>WPA2-CCMP</i>, <i>TKIP-CCMP</i>, <i>WEP-128</i> or <i>WEP-64</i>.</p> <p><i>WPA2-CCMP</i> - WPA2 is a newer 802.11i standard that provides stronger and more reliable wireless security than <i>Wi-Fi Protected Access (WPA)</i> and <i>Wired Equivalent Privacy (WEP)</i>. WPA2/CCMP is based on the concept of a <i>Robust Security Network (RSN)</i>, which defines a hierarchy of keys with a limited lifetime (similar to TKIP). Like TKIP, the keys the administrator provides are used to derive other keys. Messages are encrypted using a 128-bit secret key and a 128-bit block of data. The end result is an encryption scheme as secure as any an access point provides for its connected clients. This is the default setting.</p> <p><i>TKIP-CCMP - Temporal Key Integrity Protocol (TKIP)</i> encryption addresses WEP's weaknesses with a re-keying mechanism, a per-packet mixing function, a message integrity check and an extended initialization vector. However, TKIP also has vulnerabilities.</p> <p>Note: CCMP, common to both the above options, is a security standard used by the <i>Advanced Encryption Standard (AES)</i>. AES serves the same function TKIP does for WPA-TKIP. CCMP computes a <i>Message Integrity Check (MIC)</i> using the proven <i>Cipher Block Chaining (CBC)</i> technique. Changing just one bit in a message produces a totally different result.</p> <p><i>WEP-64</i> - WEP 64 uses a 40 bit key concatenated with a 24-bit initialization vector (IV) to form the RC4 traffic key. WEP 64 is a less robust encryption scheme than WEP 128 (containing a shorter WEP algorithm for a hacker to potentially duplicate), but networks that require more security are at risk from a WEP flaw.</p> <p><i>WEP-128</i> - WEP 128 uses a 104 bit key which is concatenated with a 24-bit <i>initialization vector (IV)</i> to form the RC4 traffic key. WEP may be all a small-business user needs for the simple encryption of wireless data. WEP 128 provides a more robust encryption algorithm than WEP 64 by requiring a longer key length and pass key. Thus, making it harder to hack through the replication of WEP keys.</p> <p>Note: Networks requiring more security are at risk from a WEP flaw. WEP is only recommended for networks having client devices incapable of using higher forms of security. The existing 802.11 standard alone offers administrators no effective method to update keys.</p>
Key	<p>Enter the key. If the format selected is <i>ASCII</i>, enter an alphanumeric string of 8 to 63 ASCII characters. The alphanumeric string allows character spaces. The string is converted into a numeric value. If the format selected is <i>HEX</i>, enter 64 HEX characters as the key.</p> <p>The key configured here is the primary string both transmitting and receiving authenticators must share. In other words, this is the key shared between the wireless client and the access point. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.</p>

ASCII/HEX	Select the ASCII or HEX radio button to specify the pre-shared key format.
------------------	--

- Select **Secure-802.1x** to enable RADIUS authentication. If selecting Secure-802.1x, define the following parameters:

Figure 1-52 Tenant Configuration View - Create a Network - Configure Secure-802.1x Security

- Use the **RADIUS** option to configure external RADIUS servers. Provide a Primary and an optional Secondary RADIUS server for user authentication requests.

RADIUS	Configures the external RADIUS server authenticating 802.1X EAP users. The server resides externally to the access point. When configured, EAP authentication requests are forwarded to the specified external RADIUS server. Note: The On Board RADIUS server capability (RADIUS server hosted locally on the access point) will be enabled in future releases. As of now it is disabled.
IP Address/Hostname	Select the IP Address or Hostname radio button to specify the format used to identify the RADIUS server.
Primary/Secondary Server	Enter the RADIUS server's numeric IP address or text string hostname (depending on the option selected). The server should be configured and running.
Shared Secret	Enter the secret string (password) required for authentication requests on the specified RADIUS server. It should be 8 to 127 characters in length. This is the secret string shared between the RADIUS server and the access point. By default, the secret is hidden. To show the secret in plain text, select the Show check box.
Check connectivity	Select to confirm connectivity with the specified RADIUS server.

- Select the network's **Band** of operation. The options are: **Dual (2.4 & 5 Ghz)**, **2.5 Ghz** and **5 Ghz**. When **Dual** is selected, the radios operate in both 2.4 GHz and 5 GHz bands.
- Configure the network's **Advanced Settings**. The Advanced Settings configuration varies depending on the service type selected.

The following Advanced Settings configurations are common to both *Guest* and *Employee* networks:

- Client IP Assignment** - Specify the networking mode.

Client IP Assignment

Client IP Assignment Bridge Mode (Clients get DHCP from the local LAN)
 NAT Mode (Clients get IP Address from the AP and NATed)

Figure 1-53 Tenant Configuration View - Create a Network - Configure Client IP assignment Mode

Client IP Assignment	<p>Use one of the following options:</p> <ul style="list-style-type: none"> • <i>Bridge Mode (Clients get DHCP from the local LAN)</i> - In this mode, wireless clients obtain their IP address from a DHCP server on the LAN to which the client joins. • <i>NAT Mode (Clients get IP Address from AP and NATed)</i> - In this mode, the access point acts as a DHCP server and provides an IP address to the clients connecting to it. The access point in turn, NATs the traffic between the external network and the wireless clients.
-----------------------------	--

- **WLAN Settings** - Specify the following WLAN Settings:

WLAN Settings

SSID broadcast	<input checked="" type="checkbox"/>	
Enforce Client Load Balancing	<input type="checkbox"/>	
Per Client WLAN Rate Limit	<input type="checkbox"/>	5000 50 - 1000, 000 Kbps
Aggregate WLAN Rate Limit	<input type="checkbox"/>	5000 50 - 1000, 000 Kbps
Voice VLAN	<input type="checkbox"/>	
Client Roam Assist	<input type="checkbox"/>	
Client To Client Communication	<input checked="" type="checkbox"/>	
Fast BSS Transition	<input type="checkbox"/>	
Radio Resource Measurement	<input type="checkbox"/>	
Content Filtering Using Open DNS	None	Register Open DNS Network End Devices

Vlan 2500 is reserved for NAT.
 ⚠ Ensure that the VLANs are mapped to the appropriate LAN ports and configured on wired networks

VLAN(s) +		
Vlan	Number Of Clients	Actions
1	Unlimited	


Figure 1-54 Tenant Configuration View - Create a Network - Configure WLAN Settings

Refer to the following for more information:

SSID Broadcast	Select to enable or disable SSID broadcast. This option is enabled by default. When enabled, SSID is broadcast for devices to connect.
Enforce Client Load Balancing	Select to enable load balancing of wireless clients. This option is disabled by default. When enabled, wireless client traffic is load balanced.
Per Client WLAN Rate Limit	Select to enable or disable per-client rate limiting. This option is disabled by default. If enabling per-client rate limiting, specify the rate limit between 50 - 1,000,000 Kbps. When enabled, specified rate limits are applied to traffic ingressing or egressing the network. Traffic exceeding the specified rate limit is dropped.
Aggregate WLAN Rate Limit	Select to enable or disable aggregate WLAN rate limiting. This option is disabled by default. Use this option to specify a limit for the aggregate WLAN traffic on a per radio basis. It is a means of ensuring guest WLAN users do not use more air time allowed by the WLAN rate limit. It can be used in conjunction with <i>Per Client WLAN Rate Limiting</i> to provide more refined control. By default, aggregate rate limiting is disabled. If enabling this option, specify the aggregate rate limit from 50 - 1,000,000 Kbps.
Voice VLAN	Select to enable or disable voice VLAN. This option is disabled by default.
Client Roam Assist	Select to enable or disable client roam assist. This option is specifically designed for legacy clients that do not roam, even when signal strength is weak. In such scenarios access points, with the <i>Client Roam Assist</i> option enabled, can de-authenticate the client forcing it to associate with another access point. This option is disabled by default. For clients that support 802.11v, the access point sends a transition packet instead of a de-authentication packet. It is up to the client to decide whether to roam away from the access point.
Client to Client Communication	Select to enable or disable client-to-client communication within the WLAN. When enabled, clients within a WLAN are allowed to exchange packets with each other. The disabled state only prevents clients within the WLAN from inter operating. It does not prevent clients on other WLANs from sending packets to this WLAN.
Fast BSS Transition	Select to enable fast BSS transition. Fast BSS transition is used to permit wireless clients to move quickly between access points when in transit. When disabled, the wireless clients have to re-authenticate with each access point when moving between them.
Radio Resource Measurement	Select to enable Radio Resource Measurement. When enabled, this feature is used to dynamically measure the radio usage for the access point and the wireless clients and then use this information to manage the radio parameters for optimal radio resource management.

Content Filtering Using Open DNS	<p>Select to enable content filtering using Open DNS filters. Open DNS is a service provided by CISCO to resolve domain names and IP addresses and other services. To use the Open DNS provided content filtering service, use the drop-down and select the appropriate filter from the list. To create a filter, select the Register Open DNS Network End Device link. You should have the following information:</p> <ul style="list-style-type: none"> • <i>Open DNS API Token</i> – This is the API key provided by Open DNS • <i>Label</i> – Enter an appropriate name for this filter. <p>To view a list of registered Open DNS filters, see Preferences on page 1-125.</p>
---	--

16. To create a VLAN use the  icon located on the top right of the VLANs table.

Vlan	Use the spinner control to set a numeric (virtual) VLAN ID from 1-4094.
Number of Clients	Use the spinner control to configure the maximum number of clients supported by this VLAN. Set a number from 1- 8192. Use Unlimited to allow any number of clients (up to a maximum of 8192 clients).
Action	Select the  icon to delete and permanently remove a configured VLAN.

17. Specify the following **Firewall Settings**:

Firewall Settings ⌵


Reduce unneeded Broadcast/Multicast Traffic





WLAN ACL Rules +							
Description	Enabled	Operation	Source IP	Destination IP	Protocol	Direction	Actio...
WLAN Client Association ACL Rules +							
Operation			Start MAC	End MAC	Actions		

Figure 1-55 Tenant Configuration View - Create a Network - Configure Firewall Settings




Use the **Reduce unneeded Broadcast/Multicast Traffic** slider to reduce the amount of broadcast and multicast traffic from the access point to the wireless clients. Use this option to increase the available bandwidth for normal traffic between the access point and the clients.


Select the  icon from the WLAN ACL Rules bar and define the following:

Description	Enter an appropriate description for this ACL rule to help differentiate it from other ACL filter rules with similar configurations.
Enabled	Set the status of this ACL rule. The status could be either <i>Enabled</i> or <i>Disabled</i> . By default, the ACL rule is enabled. To disable the rule, double-click on the  icon and select <i>Disable</i> from the list.

Operation	<p>Configures the action taken when a packet matches the criteria specified in this ACL rule. The action could be either <i>Allow</i> or <i>Deny</i>. The default is <i>Allow</i>.</p> <ul style="list-style-type: none"> • <i>Allow</i> - In case of a match, instructs the firewall to allow the packet to be forwarded to its intended destination. This is the default setting. • <i>Deny</i> - In case of a match, instructs the firewall to stop the packet from being forwarded. By default, the value of <i>Operation</i> is set to <i>Allow</i>. To change the value to <i>Deny</i>, double-click  <i>Allow</i> and clear the <i>Allow</i> check box. The <i>Operation</i> field displays  <i>Deny</i>.
Source IP	<p>Configures a source(s) as the match criteria. The options are <i>Any</i>, <i>Host</i> or <i>Network</i>.</p> <ul style="list-style-type: none"> • <i>Any</i> - Configures the source as any device. Traffic from any source is forwarded or dropped (depending on the filter operation specified). This is the default setting. • <i>Host</i> - Configures the source as a specific device. If selecting this option, specify the device's IP address. Traffic from this host is forwarded or dropped (depending on the filter operation specified). • <i>Network</i> - Configures a network as the source. If selecting this option, specify the network address and mask in A.B.C.D/M format. Traffic from this network is forwarded or dropped (depending on the filter operation specified).
Destination IP	<p>Configures the destination(s) as the match criteria. The options are <i>Any</i>, <i>Host</i> or <i>Network</i>.</p> <ul style="list-style-type: none"> • <i>Any</i> - Configures the destination as any device. Traffic to any destination is forwarded or dropped (depending on the filter operation specified). This is the default setting. • <i>Host</i> - Configures the destination as a specific device. If selecting this option, specify the device's IP address. Traffic to this host is forwarded or dropped (depending on the filter operation specified). • <i>Network</i> - Configures a network as the destination. If selecting this option, specify the network address and mask in the A.B.C.D/M format. Traffic is forwarded or dropped (depending on the filter operation specified).
Protocol	<p>Configures the traffic's protocol as the match criteria. The options are <i>ip</i>, <i>icmp</i>, <i>igmp</i>, <i>tcp</i>, <i>udp</i>, <i>eigrp</i>, <i>gre</i>, <i>igp</i>, <i>ospf</i>, <i>vrrp</i> and <i>other</i>.</p> <p>If selecting <i>ICMP</i> as the protocol to match, optionally specify the ICMP type and ICMP code.</p> <p>If selecting <i>TCP</i> or <i>UDP</i> as the protocol to match, specify the Source and Destination ports.</p> <p>If selecting <i>Other</i> to identify protocols not included in the drop-down menu, specify the protocol's Internet Assigned Numbers Authority (IANA) number.</p> <p>All traffic matching the specified protocol is forwarded or dropped (depending on the filter operation specified).</p>
Directions	<p>Configures the traffic direction as either incoming or outgoing (To Client or From Client). To change the direction, double-click Direction .</p>
Actions	<p>Select the  icon to delete and permanently remove a configured WLAN ACL rule.</p>

18. Select the  icon on the **WLAN Client Association ACL Rules** bar and define the following:

Operation	Configures the action taken when the traffic originates from or is destined for a specific client or clients. The action could be either <i>Allow</i> or <i>Deny</i> . <i>Allow</i> - In case of a match, instructs the firewall to allow the packet to proceed to its destination. This is the default setting. <i>Deny</i> - In case of a match, instructs the firewall to stop the packet from being forwarded. By default, the Operation is set to Allow. To change the Operation to Deny, double-click  Allow and clear the Allow check box. The Operation displays as  Deny .
Start MAC	Configures a specific client or a range of clients as the source or destination to match. Specify the client's MAC address in the AA-BB-CC-11-22-33 format. If specifying a client range, enter the first MAC address in the range.
End MAC	If specifying a client range, enter the last MAC address (in AA-BB-CC-11-22-33 format) in the range.
Actions	Select the  icon to delete and permanently remove a configured WLAN Client Association ACL rule.

19. Use the  icon to expand the **Application Visibility and Control (AVC)** area. AVC enables application recognition and control using *Deep Packet Inspection (DPI)*. DPI is used to identify, classify, route or block packets based on the contents of the packet. Use this section to configure DPI on this network. On *Guest* networks, use this option to configure AVC rules defining actions to apply on recognized applications/ application categories.

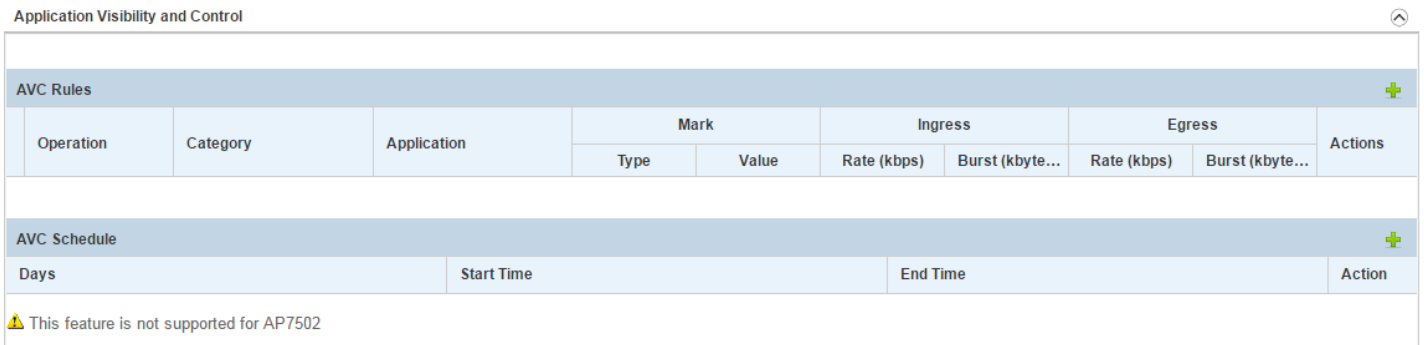



Figure 1-56 Tenant Configuration View - Create a Network - Application Visibility and Control

20. Select the  icon on the **AVC Rules** bar and define the following:

Operation	Configures the action taken on the applications (within an application category) specified in this AVC rule. The action could be either Allow, Deny, Mark or Rate. <ul style="list-style-type: none"> <i>Allow</i> - Packets matching the specified applications are allowed. <i>Deny</i> - Packets matching the specified applications are denied. <i>Mark</i> - Packets matching the specified applications are marked with DSCP/8021p values used for QoS. Use this option to identify packets for rate limiting. If selecting this option, use the Mark field to configure related parameters. <i>Rate</i> - Packets matching the specified applications are rate limited. If selecting this option, use the Ingress and Egress fields to configure rate limits applied to incoming and outgoing packets respectively. <p>Note: <i>Mark</i> and <i>Rate</i> are the only two actions that can be combined for an application and category. All other combinations are invalid.</p>
------------------	---

Category	Configures the application category. Double-click within the <i>Category</i> field to access the category menu. Select the category to which this AVC rule applies. The default is set to <i>streaming</i> .
Application	Configures the applications to monitor within the specified category. Double-click within the <i>Application</i> field to access the list of applications available within the selected application category. Select <i>All</i> to apply the rule to all applications within the selected application category. If this AVC rule applies to a specific application (within the selected category), select that application from the displayed menu.
Mark	Configures the <i>Operation Mark</i> related parameters. If the <i>Operation</i> is set to <i>Mark</i> , use this field to define the following: <ul style="list-style-type: none"> • <i>Type</i> - Specify the Mark Type as DSCP or 8021p. The default setting is 8021p. To change the value to DSCP, double-click within the Type field and select DSCP. • <i>Value</i> - Double-click in the Value field and specify the DSCP/8021p value. Note: These fields are enabled only if the <i>Operation</i> selected is <i>Mark</i> .
Ingress	Configures the <i>Operation Rate</i> related parameters. If the <i>Operation</i> is set to <i>Rate</i> , use this field to define the rate limits applied to incoming traffic. <ul style="list-style-type: none"> • <i>Rate (kbps)</i> - Define a rate limit from 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum number of packets received. Traffic exceeding the defined rate is dropped. The default setting is 50 kbps. • <i>Burst (kbytes)</i> - Define the burst size from 2 - 1024 kbytes. The smaller the burst, the less likely an upstream packet transmission results in congestion for the WLAN's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should add a 10% margin (minimally) to allow for traffic bursts. The default value is 2 kbytes. Note: This field is enabled only if the <i>Operation</i> selected is <i>Rate</i> .
Egress	Configures the <i>Operation Rate</i> related parameters. If the <i>Operation</i> is set to <i>Rate</i> , use this field to define the rate limits applied to outgoing traffic. <ul style="list-style-type: none"> • <i>Rate (kbps)</i> - Define a rate limit from 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets received. Traffic exceeding the defined rate is dropped. The default setting is 50 kbps. • <i>Burst (kbytes)</i> - Define the burst size from 2 - 1024 kbytes. The smaller the burst, the less likely an upstream packet transmission results in congestion for the WLAN's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should add a 10% margin (minimally) to allow for traffic bursts. The default is 2 kbytes. Note: This field is enabled only if the <i>Operation</i> selected is <i>Rate</i> .
Actions	Select the  icon to delete and permanently remove an AVC rule.

AVC Schedule +			
Days	Start Time	End Time	Action
All	12:00 AM	12:00 AM	

This feature is not supported for AP7502

Figure 1-57 Tenant Configuration View - Create a Network - Configure AVC Schedule

21. Select the icon on the **AVC Schedule** bar and schedule the day and time when the configured AVC rule is enforced. This feature is not supported for the AP7502 access points.

Days	Configures the day of the week on which this AVC rule is enforced. Double-click in the <i>Days</i> field and select the day as <i>Monday, Tuesday</i> , etc. Select <i>All</i> to apply the rule to all days of the week.
Start Time	Configures the enforcement start time. Double-click in the <i>Start Time</i> field and select the start time. This is the time at which this AVC rule enforcement begins.
End Time	Configures the enforcement end time. Double-click in the <i>End Time</i> field and select the end time. This is the time at which this AVC rule enforcement ends.
Actions	Select the icon to delete the AVC schedule.

22. Expand **Access Control Settings**. Select one of the following guest authentication modes. This option is only available when the **Service Type** is *Guest Access* and **Captive Portal Type** is set to *AP Local*.
 Select to enable or disable the **Bypass Captive Portal** option. Enable this option to allow Apple iOS® devices to successfully authenticate when using social media authentication such as Google account or Facebook account validation.

Access Control Settings ⌵

Bypass Captive Portal

Guest Authentication No Authentication External Radius Server Registration Email Mobile Other

Registration Type

Connection Mode Http Https

Google App ID Provide App ID to enable respective social media authentications in the Captive Portal's login page.

Facebook App ID

Captive Server

Logout FQDN

List of DNS +		
DNS Entry	Match Suffix	Actions

Figure 1-58 Tenant Configuration View - Create a Network - Guest Network - Configure Access Control Settings

<p>Guest Authentication</p>	<p>Configures the guest user (captive portal) authentication mode. The options are:</p> <ul style="list-style-type: none"> • <i>No Authentication</i> – Guest users are provided network access without authentication. This is the default setting. This option is not recommended, as it provides no security. See section No Authentication on page 1-70. • <i>External Radius Server</i> – Uses an external RADIUS server to verify guest user credentials before providing network access. If selecting this option, define a Primary RADIUS server and an optional secondary RADIUS server. See section External Radius Server on page 1-70. • <i>Registration</i> – Uses an external RADIUS/registration server to capture user information when the user visits the network for the first time. When the user visits the captive portal the next time, this stored information is used to verify the user and enable quicker access to the captive portal resources. See section Registration on page 1-70. • <i>Email</i> – Uses the e-mail ID provided by the user as a form of user registration and authentication. See section Email on page 1-71. • <i>Mobile</i> – Uses the mobile number provided by the user as a form of user registration and authentication. See section Mobile on page 1-71. • <i>Other</i> – Uses custom information captured from the user as a form of user registration and authentication. See section Other on page 1-71.
------------------------------------	--

No Authentication

When **Guest Authentication** type is *No Authentication*, the user is not authenticated before being granted access to the network through the Captive Portal. When the **Registration Type** field is set to *None*, no information is captured for the user. When the **Registration Type** field is set to *Device*, the user's device's MAC address is captured and stored in the configured RADIUS/registration servers. The next time the user tries to access the network with a registered device, the user is automatically authenticated and granted access.

External Radius Server

When **Guest Authentication** type is *External Radius Server*, user information is stored in the configured RADIUS servers and the information provided by the user is verified with the RADIUS server before the user is granted access. Provide the RADIUS server **IP Address/Host Name** for the Primary Server. Also provide the **Shared Secret** when authenticating with the RADIUS server. If available, provide the **IP Address/Host Name** for the Secondary Server and its **Shared Secret**.

Registration

When **Guest Authentication** type is *Registration*, user information is stored in the configured RADIUS servers and the information provided by the user is verified with the RADIUS server before the user is granted access. Provide the RADIUS server **IP Address/Host Name** for the Primary Server. Also provide the **Shared Secret** when authenticating with the RADIUS server. If available, provide the **IP Address/Host Name** for the Secondary Server and its **Shared Secret**.

- When the **Registration Type** is *Device*, the user device's MAC address is captured and stored in the configured RADIUS/registration servers. The next time the user accesses the network with a registered device, the user is automatically authenticated and granted access.
- When **Registration Type** is *User*, user information is captured and stored in the configured RADIUS/registration servers. The user can then use a combination of user name and password to access the network from any device.
- When **Registration Type** is *Device OTP*, the first time a user access the network, an *One Time Password* (OTP) is sent to the registered device provided by the user at registered time. The user uses this OTP to register the device with the captive portal for the first time. The next time the user accesses the network with the registered device, the user is automatically authenticated and granted access. For more information on configuring a SMS gateway for sending the Device OTP, see [SMS Gateway on page 1-122](#).

Email

When **Guest Authentication** type is *Email*, the user provides an e-mail address when registering for the captive portal service. If the **Registration Type** field is set to *None*, no information is captured for the user. The user has to provide a valid e-mail address every time network access is required. If the **Registration Type** field is set to *Device*, the user’s device’s MAC address is captured and stored in the configured RADIUS/registration servers. The next time the user accesses the network with the registered device, the user is automatically authenticated and granted access.


Mobile

When **Guest Authentication** type is *Mobile*, the user provides a Mobile number when registering for the captive portal service. If the **Registration Type** field is set to *None*, no information is captured for the user. The user has to provide a valid mobile number every time network access is required. If the **Registration Type** field is set to *Device*, the user’s device’s MAC address is captured and stored in the configured RADIUS/registration servers. The next time the user accesses the network with the registered device, the user is automatically authenticated and granted access.

Other

When **Guest Authentication** type is *Other*, any field from those in the *Reg Page Settings* screen can be used when registering for the captive portal service. If the **Registration Type** field is set to *None*, no information is captured for the user. The user has to provide valid information for the field every time network access is required. If the **Registration Type** field is set to *Device*, the user’s device’s MAC address is captured and stored in the configured RADIUS/registration servers. The next time the user accesses the network with the registered device, the user is automatically authenticated and granted access.

Provide the following common information:

Google App ID	Provide the application ID received from Google™ to be used for authenticating with Google™ credentials.
Facebook App ID	Provide the application ID received from Facebook™ to be used for authenticating with Facebook™ credentials.
Captive Server	Provide a hostname for the local access point. When using social authentication apps for login, user information is redirected to the social app’s page for validation. When the page is redirected, this hostname is used instead of the access point’s IP address. Social authentication providers such as Facebook™ and Google™ require that authentication request URLs contain hostnames instead of IP addresses. If an authentication request is sent from an IP address, it is generally rejected. Note: For social authentication to work, the server hostname configured here must also be configured on Facebook™ and Google™ when registering your captive portal. Note: You can use this field to prevent the display of the access point’s IP address under normal use too.
Logout FQDN	Use this field to provide the FQDN to the logout screen for this Captive Portal.
List of DNS	Use this table to add a list of valid Domain Name Servers for this Captive Portal. Use the + icon to the right to add a row to this table. <ul style="list-style-type: none"> • <i>DNS Entry</i> – Enter the IP address or the host name of the DNS server. • <i>Match Suffix</i> – Select to enable matching the domain name suffice when doing DNS query. • <i>Action</i> – Use the  icon to delete this entry.

23. Use the **Edit Splash Settings** option to define the appearance and flow of the Web pages wireless clients encounter when accessing the guest network. Specify whether the Web pages are default files (hosted locally on the access point) or hosted externally. If using default files, specify the following page display elements:

1-72 Azara User's Guide

Edit Splash Page ⌵

Show Terms and Conditions Page

Use Default Files User External Pages

Organization's Name:

Title Text:

Header Text:

Message:

Footer Text:

Main Logo URL: Use as banner

Small Logo URL:

Signature:

Org Name/Signature Background color
 Org Name/Signature Text color
 Body Background color
 Body Text color

Figure 1-59 Tenant Configuration View - Create a Network - Guest Network - Captive Portal Splash Page Settings

Show Terms and Conditions Page	Select this option to include terms that must be adhered to for clients requesting captive portal access.
Use Default Files	Select this option to use default Web pages. When selected, locally hosted (on the access point) Web pages are displayed to requesting clients.
Login/ Terms and Conditions/ Welcome/ Login Fail/ No Service/ Registration	If using default files, select the Web page, whose attributes are to be configured, and specify the <i>Organization's Name</i> , <i>Title Text</i> , <i>Header Text</i> , <i>Message</i> , <i>Footer Text</i> , <i>Main Logo Url</i> , <i>Small Logo Url</i> and <i>Signature</i> for each screen.
Organization's Name	Specify the organizational specific name or identifier which clients see during login.
Title Text	Specify the title text displayed on the page when clients access the network. The text should be in the form of a page title describing the respective function of each page and should be unique to each function.
Header Text	Specify the header text unique to the function of each page.
Message	Specify a message containing unique instructions or information for the clients accessing the <i>Login</i> , <i>Agreement</i> , <i>Welcome</i> or <i>Fail</i> pages. In the case of the <i>Agreement</i> page, the message can be the conditions requiring agreement before captive portal access is permitted.
Footer Text	Specify a footer message displayed on the bottom of each page. The footer text should be any concluding message unique to each page before accessing the next page in the succession of the Web pages.
Main Logo Url	Specify the Main Logo URL. This is the URL for the main logo image displayed on the <i>Login</i> , <i>Agreement</i> , <i>Welcome</i> and <i>Fail</i> pages.
Small Logo Url	Specify the Small Logo URL. This is the URL for the small logo image displayed on the <i>Login</i> , <i>Agreement</i> , <i>Welcome</i> and <i>Fail</i> pages.

Signature	Specify the copyright and legal information associated with the usage of the network and the usage of the organization name provided.
Org Name/Signature Background Color	Specify the background color of the bar/field displaying the Organization's Name and Signature. Select the icon on the left of this item to launch a color palette where screen colors can be defined uniquely.
Org Name/Signature Text Color	Specify the color of the text displaying the Organization's Name and Signature. Select the icon on the left of this item to launch a color palette where text colors can be specified for the Organization's Name and Signature fields.
Body Background Color	Specify the background color of the main body of the Web page. Select the icon on the left of this item to launch color palette where the background color can be specified for the text in the body of the page.
Body Text Color	Specify the color of the text displayed in the main body of the Web page. Select the icon on the left of this item to launch a color palette where the color can be specified for the text displayed on the page.
Preview Page	Select Preview Page to review the screen's color selections before implementing them.

24. If using user registration, select the **Registration Page Settings** tab. The following screen displays:

Edit Splash Page ⌵

Show Terms and Conditions Page

Use Default Files User External Pages

Field ID	Field Type	Enabled?	Mandatory?	Display Label	Placeholder Text
Name	text	true	false	Full Name	Enter First Name, Last Name
Age-range	dropdown-menu	true	false	Age Range	Age Range
Dob	date	true	false	Date of Birth	MM/DD/YYYY
Gender	dropdown-menu	true	false	Gender	Gender
Member	text	true	false	Loyalty/Member Card Number	Enter Loyalty/Member Card Num...
Street	text	true	false	Address	123 Any street
City	text	true	false	City	Enter City
Zip	number	true	false	Zip	Zip
Country	dropdown-menu	true	false	Country	Enter Country
Mobile	number	true	false	Mobile	Mobile Number with Country code
Via-sms	checkbox	true	false		SMS Preferred
Email	e-address	true	true	Email	you@domain.com
Via-email	checkbox	true	false		Email Preferred
Optout	checkbox	true	false		Do not remember and use my det...
Disclaimer	checkbox	true	false		Use of this information is subject...

Figure 1-60 Tenant Configuration View - Create a Network - Guest Network - Captive Portal Registration Page Settings

This screen displays a table to configure registration page display and behavior. The fields are fixed and are listed in the table rows. The table's columns control the field display and behavior.



Configure the following settings:

Field ID	This fixed field identifies the field name. This field cannot be modified.
-----------------	--

Field Type	This fixed field identifies the control type displayed on the registration screen. This field cannot be modified.
Enabled?	This field controls enabled/disabled status. When enabled, users can update field values. When disabled, the field is grayed out and cannot be modified.
Mandatory?	When enabled, the field is considered mandatory and the user cannot complete registration without providing a valid value. When disabled, the user can skip this field.
Display Label	This field sets the label displayed for each field. Some of the fields have their default labels already provided.
Placeholder Text	This field sets the text displayed when no data is entered for a field. For example, when no text is entered in the <i>Name</i> field, and the <i>Placeholder Text</i> is set to <i>Enter First Name, Last Name</i> , then this text is displayed in the <i>Name</i> field. Review and change if required.

25. If using the **User External Pages** option, provide URLs for the *Welcome*, *Login Failure*, *Login*, *Agreement*, *Registration* and *No Service*. It is mandatory to provide the *Welcome*, *Login Failure*, *Login* and *Agreement* page URLs, but the other pages are optional. Captive portal users are served the *Welcome* page on successful authentication.

Figure 1-61 Tenant Configuration View - Create a Network - Guest Network - Captive Portal External Web Page URLs

26. Select **Save Changes** to save and exit the network configuration screen.
27. To edit an existing Tenant network's details, navigate to **Configuration** and select **Network**. The list of networks configured for this Tenant is displayed.
28. Select the required network from amongst those displayed, and select the  icon. The selected network's details are displayed. Make the necessary edits and select **Save Changes** to save the changes made.
29. To remove an existing network, select the network from amongst those displayed and select the  icon. The selected network is removed from the list of networks configured for this Tenant.

1.6.1.1 Configuring Network Wide Settings

► [Configuring Tenant Networks](#)

The settings on this screen is applicable to all the networks configured for this Tenant.

Figure 1-62 Tenant Configuration View - Network Wide Settings screen

Use the **Deep Packet Inspection** slider to enable or disable in depth analysis of each packet traversing this network. The information from the deep packet inspection is used by the Tenant administrator to decide on how to control application’s access to the network. The Application Visibility and Control feature on Azara Cloud provides in-depth control on each application’s access to any resource and service provided by Azara Cloud service.

Use the **Lan Port Settings** area to configure AP7502 specific settings. AP7502 provides three (3) fast ethernet ports fe1, fe2, fe3 of which one (fe3) also provides *Power Over Ethernet* (PoE) to connected devices.

Port	Displays the available ports on the AP7502. The available ports are <i>fe1</i> , <i>fe2</i> and <i>fe3</i> . This is a display only field.
Status	Displays the current status of this port. Select this field and set this field to <i>Disabled</i> to disable this port. The default value is <i>Enabled</i> .
Allowed VLANs	Displays the VLANs allowed on this port. Select this field and enter the VLANs that are allowed on this FE port.
Untagged VLAN	Displays the native VLAN for this network. This is a display only field.
POE Out	Note: This feature is available only on the <i>fe3</i> port. Displays the status of PoE on the port. Select this field and set this field to <i>Enabled</i> to supply power over ethernet to connected devices. The default value is <i>Disabled</i> .

1-76 Azara User's Guide

Use the **Client Management** area to configure the following parameters for each of the bands (2.4GHz and 5.0 GHz):

Band Ratio	Use the sliders to configure the band ratio for the bands. Set a value in the range 0 - 10. These values set the ratio of devices in each band. For example, if the sliders are set to 3, 2 respectively, the access point tries to maintain a ratio of 3:2 devices between the 2.4 GHz and 5.0 GHz bands. When this ratio is not maintained, the access point tries to steer the client, if it is capable, to the other band of operation to enable it to maintain the set ratio.
Probe Response Threshold	Use the sliders to set the probe response threshold for each band. Probe request below this threshold will not be acknowledged by the access point.

Use the **Radio Rates** area to manually configure the data transmission rates to use for each of the two supported frequencies. Data transmission rates for each frequency can be selected using the **Select** button next to the rate. The following screen displays.

Radio Setting 2.4 Ghz [Close]

Radio Transmission Data Rates

b-only rates
 bg-only rates
 bgn-only rates
 Default

g-only rates
 gn-only rates
 Custom Rates

802.11b Rates

1Mbps 2Mbps 5.5Mbps 11Mbps

Basic

Supported

802.11g Rates

6Mbps 9Mbps 12Mbps 18Mbps 24Mbps 36Mbps 48Mbps 54Mbps

Basic

Supported

802.11n Rates

MCS-1 Streams MCS-2 Streams MCS-3 Streams

Basic

Supported

OK

Figure 1-63 Tenant Configuration View - Radio Rates for 2.4 GHz screen

Use the options to configure the **Radio Transmission Data Rates** for the selected band. When an available option is selected, the appropriate rates are automatically selected. Select **Custom Rates** option to manually select the different rates to configure for this radio frequency. Select **OK** to save the changes made to the Radio Settings.

Select **Save** to save changes made to this screen. To exit without saving any changes made to this screen, click on any tab on the screen, and on the confirmation window that displays, select **Yes**.

1.6.2 Configuring Sites

► Configuration

Use the *Sites* screen to manage sites for this Tenant. Sites can be added, removed or modified.

To view the networks configured for this site:

1. From the **Configuration** menu item, select **Sites**. The following screen displays.

System > Configuration Account Number:

Network	Sites	Captive Portal	Inventory / Devices	Users	Preferences	License Info
Site Details +						
Name	Site Manager Name	Email	Contact Phone	Actions		
TP_Retail_Location_01	StoreManager	storemanager_fairbanks@corporate.com	1122334455			
TP_Retail_Location_02	Storemanager	storemanager_suisun@corporate.com	1122334455			

Figure 1-64 Tenant Configuration View - Sites Management

2. Review the following information to assess whether a new site requires creation or an existing site needs modification or removal:

Name	Displays the names of existing sites created within this Tenant.
Site Manager Name	Displays the name of the administrative point of contact assigned for managing the site, if configured.
Email	Displays the e-mail address of the network administrator managing the site, if configured.
Contact Phone	Displays the contact number of the network administrator managing the site, if configured. This information can be used when troubleshooting network issues (for example, when the site is unreachable).
Actions	Displays actions that can be performed on configured sites. A site can either be edited or deleted. To edit a site's settings, select the icon. To delete a site select the icon.

3. To add a new site, from the top right-hand corner of the **Site Details** bar, select the icon. The following screen displays.

Site Name* Clone From Site

Figure 1-65 Tenant Configuration View - Site Management - Create New Site

4. Enter the following information for the new site:

Site Name	Enter a name for this new Site. Site name cannot be longer than 32 characters. Name cannot contain any special characters except the “-” (hyphen) and “_” (underscore) characters. Name can contain spaces and numbers.
Clone From Site	If cloning the new site from an existing site, use the drop-down menu to select the site from which to clone. When a site is cloned, the site configuration is copied from the site selected in this field. Once created, edit only those configurations that differ (from that of the cloned site) in the new site.

5. Select the **Create Site** button. The site is created and the following screen displays:

System > Configuration Account Number:

Site Name*

Country Code*

Time Zone

Site Manager's Name

Email

Contact Phone

Country

Region

City

Campus

Geo Latitude

Geo Longitude

Click on Map to choose a location

Advanced Settings

Smart RF

Floor MAP

Wireless IPS

Management Policy

Location Based Services

Figure 1-66 Tenant Configuration View - Site Management - Add New Site

6. Enter the following information for the site:

Country Code	<p>Use the drop-down menu to select the site's country code (code of the country where the site is deployed). Selecting the correct country is central to legal operations, because regulatory restrictions concerning electromagnetic emissions and the maximum RF signal strength that can be transmitted vary from country to country. This is a mandatory field.</p> <p>Note: Use the map provided to auto-populate location related information, such as Time Zone, Country Code, City etc. Enter the city name in the Search field and select Search. The location-related fields auto-populate with the relevant information.</p>
Time Zone	<p>Use the drop-down menu to configure the site's time zone. The setting should be complimentary with the selected country of deployment.</p> <p>Note: Use the map provided to auto-populate location related information, such as Time Zone, Country Code, City etc. Enter the city name in the Search field and select Search. The location-related fields auto-populate with the relevant information.</p>
Site Manager Name	<p>Enter the name of the network administrator managing the site. This is the point of contact responsible for troubleshooting site issues.</p>
Email	<p>Enter the e-mail address of the network administrator managing the site.</p>
Contact Phone	<p>Enter the contact number of the network administrator managing the site. The credentials provided should accurately reflect the individual responding to service queries.</p>

- On the map view, locate the site and click to select. When a location is selected, the following fields are auto populated based on the location selected on the map. Otherwise, manually configure the following parameters to display the exact location of the site in the Map view.

Country	Configures the site's country of deployment. If a location is selected on the map, this field populates with the country.
Region	Configures the site's region of deployment. If a location is selected on the map, this field populates with the region.
City	Configures the site's city of deployment. If a location is selected on the map, this field populates with the city.
Campus	Configures the site's campus of deployment. If a location is selected on the map, this field populates with the campus if available.
Geo Latitude	Configures the exact geographical location of the site in terms of the latitude. Latitude is the angular distance north or south from the equator of a point on the earth's surface. If a location is selected on the map, this field populates with the Latitude.
Geo Longitude	Configures the exact geographical location of the site in terms of the longitude. Longitude is the angular distance east or west on the earth's surface. If a location is selected on the map, this field populates with the Longitude.

When editing a site, select the **View Stats** button - located to the top right of the screen - to view the statistics of the site being edited. When selected, the **System > Monitor > Summary** screen for that particular site is displayed.

- Expand the **Smart-RF** settings.

Self Monitoring At Run Time RF Management (Smart RF) is designed to simplify RF configuration for new deployments, while (over time) providing on-going deployment optimization radio performance improvements. It is an efficient means of reducing deployment costs by scanning the RF environment to determine the best channel and transmit power for each radio.

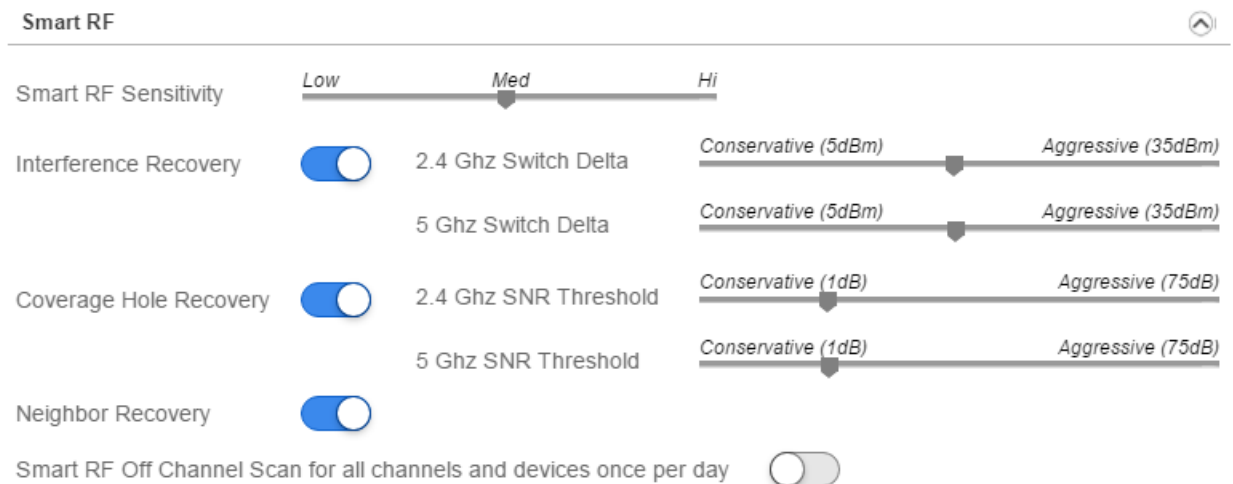


Figure 1-67 Tenant Configuration View - Site Management - Smart-RF Settings

Configure the following parameters to set the Smart-RF parameters:

<p>Smart RF Sensitivity</p>	<p>Use this slider to configure the Smart-RF sensitivity.</p> <ul style="list-style-type: none"> • <i>Low</i> – Sets Smart-RF sensitivity to low. When low, the <i>Interference Recovery</i> value is set to <i>Aggressive</i>. Smart-RF will only enable compensation from neighboring radios if the signal to noise ratio for a wireless client, as seen by the access point, exceeds the value set for <i>Interference Recovery</i>. If a client's signal to noise value is above the threshold, the transmit power is increased until the signal to noise rate falls below this threshold. • <i>Med</i> – Sets Smart-RF sensitivity to medium. When medium, <i>Interference Recovery</i> value is set to a value between <i>Conservative</i> and <i>Aggressive</i>. This is the default value. • <i>Hi</i> – Sets Smart-RF sensitivity to high. When high, <i>Interference Recovery</i> value is set to <i>Conservative</i>.
<p>Interference Recovery</p>	<p>Use this slider to enable compensations from neighboring radios when radio interference is detected. When interference is detected, Smart-RF first determines the power increase needed based on the signal to noise ratio for a client (as seen by the access point radio). If a client's signal to noise value is above the threshold, the transmit power is increased until the signal to noise rate falls below the threshold. This option is enabled by default.</p>
<p>Coverage Hole Recovery</p>	<p>Use this slider to enable coverage compensation from neighboring radios when a radio coverage hole is detected within the Smart-RF supported radio coverage area. When coverage hole is detected, Smart-RF first determines the power increase needed based on the signal to noise ratio for a client as seen by the access point radio. If a client's signal to noise value is above the threshold, the transmit power is increased until the signal to noise rate falls below the threshold. This option is enabled by default.</p>
<p>Neighbor Recovery</p>	<p>Use this slider to enable automatic recovery by instructing neighboring access points to increase their transmit power to compensate for the coverage loss. This option is enabled by default.</p>

Use the **Smart RF Off Channel Scan for all channels and devices once per day** slider to force Smart-RF to scan all channels once per day during off peak hours.

Smart RF ⌵

Allowed Channel List

Disable DFS Channels

Radio 2.4 Ghz

Channels All

Default

1

2

3

4

5

6

7

8

9

10

11

12

13

14

Channel Width 20MHz 40MHz auto

Power Settings Min Max (1-20) dBm

Scanning

Client Aware Scanning (1-255)

Voice Aware Scanning (dynamic)

Radio 5 Ghz

Channels All

Default

21

25

34

36

38

40

42

44

46

48

52

56

60

64

74

100

104

108

112

116

Channel Width 20MHz 40MHz 80MHz auto

Power Settings Min Max (1-20) dBm

Scanning

Client Aware Scanning (1-255)

Voice Aware Scanning (dynamic)

Figure 1-68 Tenant Configuration View - Site Management - Smart-RF Settings

Configure the following **Smart-RF** settings to calibrate your network to correctly and dynamically respond to changing RF conditions.

Disable DFS Channels is only applicable to radios operating in the 5 GHz band. To avoid interference with government weather radar systems, the *Federal Communication Commission (FCC)* has identified certain 5 GHz channels for radar use. Devices operating on these channels have to be DFS-enabled. A DFS-enabled 5 GHz radio can detect and avoid channels with radar signals. On detection of radar, the radio automatically switches to a radar-free channel. However, the channels used for radar activities differ for different countries and regions. Select to remove *Dynamic Frequency Selection (DFS)* channels from the list of 5 GHz channels available for Smart RF assignment.

The following channel and power related settings are common to both 2.4 GHz and 5 GHz radios. When configured, these parameters determine the channel and power assigned to each of the Smart RF managed radio.

Channels All	<p>Select to assign all available channels for Smart RF operation. When selected, all channels are marked with a red bar on top.</p> <p>Note: To assign a select set of channel(s) for Smart RF, click on the desired channel(s). The selected channel(s) will be marked with a red bar on top.</p> <p>Note: If the <i>Disable DFS Channels</i> check box is selected, for 5 GHz radios, DFS channels are excluded form the list of channels available.</p>
Default	<p>Select to assign only the default channels for Smart RF operation. The default channels are the ones with a red bar on top. The default channels vary for the 2.4 GHz and 5 GHz bands.</p> <p>Note: To assign a select set of channel(s) for Smart RF, click on the desired channel(s). The selected channel(s) will be marked with a red bar on top.</p>

<p>Channel Width</p>	<p>Select the channel width for the access point radio. The options are:</p> <ul style="list-style-type: none"> • <i>20 MHz and 40 MHz</i> - Available for both 2.4 GHz and 5 GHz radios. This mode is supported for 11n users on both the 2.4 GHz and 5 GHz radios. When 20/40 is selected, clients can take advantage of wider channels. 802.11n clients experience improved throughput using 40 MHz while legacy clients (either 802.11a or 802.11b/g depending on the radio selected) can still be serviced without interruption using 20 MHz. The default is 20 MHz and 40 MHz for the 2.4 GHz and 5 GHz radios respectively. • <i>80 MHz</i> - Available only for 5 GHz radios. Use this option if deploying an 802.11ac supported access point. • <i>auto</i> - Available for both 2.4 GHz and 5 GHz radios. The auto option enables automatic channel assignments to working radios. When selected, the overlapping of channels and interference from external RF sources is avoided.
<p>Power Settings</p>	<p>Configure the Smart RF recovery settings for the selected 5 GHz (802.11a) or 2.4 GHz (802.11bg) radio.</p> <ul style="list-style-type: none"> • <i>Min</i> - Use the spinner control to select a 1 - 20 dBm minimum power level Smart RF can assign to a radio. The default for both 2.4 GHz and 5 GHz bands is 4 dBm. • <i>Max</i> - Use the spinner control to select a 1 - 20 dBm maximum power level Smart RF can assign a radio. The default for both 2.4 GHz and 5 GHz bands is 17 dBm.

The following **Scanning** configurations are common to both 2.4 GHz and 5 GHz radios. Smart RF relies on *Off-Channel Scanning* (OCS) to monitor the RF environment in real-time to allow Smart RF managed radios to adapt to changes in the RF environment. Smart RF managed radios that go off-channel can impact certain devices. Therefore, Smart RF is adaptive since by default it prevents OCS on a Smart RF managed radio if it detects an active voice call or packets are queued for *Power Save Polling* (PSP) clients.

<p>Client Aware Scanning</p>	<p>Enables or disables client aware scanning. If enabling this option, define a <i>Client Aware Scanning</i> threshold for 2.4 GHz and 5 GHz radios to determine the number of associated wireless clients on a given Smart RF managed radio to prevent OCS. The range is from 1 - 255. Channel scanning is avoided when the number of clients associated with the access point's radio equals the value configured here. This option is disabled by default on both 2.4 GHz and 5 GHz bands.</p>
<p>Voice Aware Scanning</p>	<p>Enables or disables dynamic voice aware scanning. When enabled, Smart RF monitoring is disabled as long as there is data buffered for a voice client on the Smart RF managed radio. This option is enabled by default on both 2.4 GHz and 5 GHz bands.</p>

9. Expand the **Floor Map** area. Use this area to manage floor maps of the site. The Floor Map fields are enabled only for an existing site, a site that has been created and saved. Therefore, if creating a new site, save the changes and then add a floor map for the site.

Floor MAP ⌵

+		
Name	Image	Actions
fp	floorplan.jpg	

Floor Map images should be in standard JPEG (.jpg /.jpeg) format & size must be less than 10MB

Figure 1-69 Tenant Configuration View - Site Management - Floor Map Settings

10. To add a new floor map for a site, select the icon. A new row is added to the table.

Floor MAP ⌵

+		
Name	Image	Actions
FM2	16545911175_da35544ed6_o.jpg	
FM3	16294108556_85e3112e41_o.jpg	
FM4	Select a Floor Map image to upload	Browse

Floor Map images should be in standard JPEG (.jpg /.jpeg) format & size must be less than 10MB

Figure 1-70 Tenant Configuration View - Site Management - Add Floor Map

Refer the following for more information:



Name	Enter a floor map name that best represents what the map is about.
Image	Upload floor map image file. Select the Browse button, navigate to the desired location, select the floor map image file, and then select the upload icon to upload the file. Note: Images should be in standard JPEG (.jpg/.jpeg) format only and should not exceed 10 MB in size.
Actions	Displays the actions that can be performed on a floor map entry. When adding a floor map, use the icon to upload the floor map. When managing an existing floor map, either delete the floor map entry or download the image file associated with the floor map entry. To delete the floor map, select the icon. To download the floor map image, select the icon.

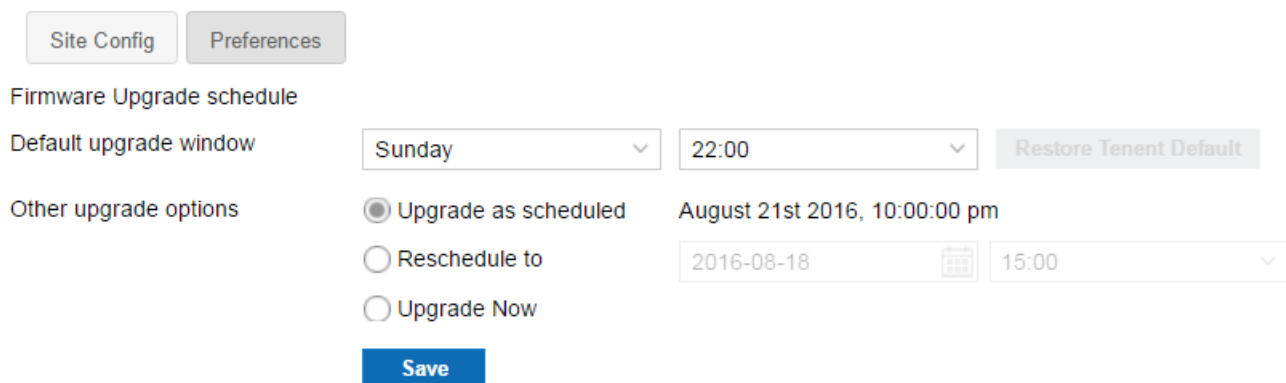
11. Use the **Wireless IPS** section to configure wireless IPS for this site.

The *Wireless Intrusion Protection System* (WIPS) protects the network, wireless clients and access point radio traffic from attacks and unauthorized access. WIPS provides tools for standards compliance and around-the-clock wireless network security in a distributed environment. WIPS allows administrators to identify and accurately locate attacks, rogue devices and network vulnerabilities in real time and permits both a wired and wireless lock-down of wireless device connections upon acknowledgment of a threat.

Select **Enable Rogue AP Detection** to enable detection of rogue access points within the configured channels. Select **Enable Off-Channel Scan** to enable the access point to scan for rouge devices on channels which is not being used by the access points for servicing clients.

12. Use the **Management Policy** section to change the password of the username “admin”. Select the **Change Password** button and then enter the current password in the **Current Password** field. Enter the new password in the **New Password** field and confirm it by entering it again in the **Confirm Password** field.

13. Use the **Location Based Services** section to manage location based services at this site. Use the **Enable** slider to enable or disable this feature at this site.
This slider is disabled by default. To use the feature at the site level, *Location Based Services* (LBS) must be enabled for all the sites for the tenant. LBS is enabled for the tenant from the **Configuration > Preferences > Management Settings > Location Based Services > Enable** slider. For more information, see [Configuring Tenant Preferences on page 1-100](#)
14. Use the **Save** button to save changes made to the configuration items on this screen. Select **Cancel** to cancel all changes made to this screen.
15. To edit an existing Tenant site's details, navigate to **Configuration** and select **Sites**. The list of sites configured for this Tenant displays. Select the required site from amongst those displayed and select the  icon. The selected site's details are displayed. Make the necessary edits and select **Save Changes** to save the changes made.
16. To remove an existing site, navigate to **Configuration** and select **Sites**. The list of sites configured for this Tenant displays. Select the site from amongst those displayed and select the  icon. The selected site is removed from the list of sites configured for this Tenant.
17. Use the **Preferences** tab to configure the firmware upgrade schedule for this particular site. The following screen displays:



The screenshot shows the 'Preferences' tab for a site configuration. At the top, there are two tabs: 'Site Config' and 'Preferences'. Below the tabs, the section is titled 'Firmware Upgrade schedule'. Under this section, there are two rows of settings. The first row is 'Default upgrade window', which has a dropdown menu set to 'Sunday', a time dropdown set to '22:00', and a 'Restore Tenant Default' button. The second row is 'Other upgrade options', which has three radio button options: 'Upgrade as scheduled' (selected), 'Reschedule to', and 'Upgrade Now'. The 'Upgrade as scheduled' option shows a date and time: 'August 21st 2016, 10:00:00 pm'. The 'Reschedule to' option has a date input field set to '2016-08-18' and a time dropdown set to '15:00'. At the bottom of the form is a blue 'Save' button.

Figure 1-71 Tenant Configuration View - Site Management - Preferences Tab

The **Default upgrade window** is set system wide and is reflected here. Use the drop-down lists to change the default upgrade window to a time suitable to the requirements of this site.

Use the **Other upgrade options** to enable the change the next scheduled firmware upgrade. The next scheduled upgrade is listed alongside the option **Upgrade as scheduled**. Use the **Upgrade Now** option to immediately upgrade the site. Select the **Reschedule to** option and use the controls to reschedule the firmware upgrade to a point of time in the future.

1.6.3 Managing Inventory/Devices

► [Configuration](#)

Use the *Inventory/Device* screen to manage all devices belonging to this Tenant. Add new access points and edit or delete existing ones as the network topology requires. Access points must be registered before they can be used. Access points can only be registered if a valid license is available for use with this Azara account.

To manage access points:

1. From the **Configuration** menu item, select **Inventory/Devices**.

A list of existing devices for this Tenant displays by default.

System > Configuration

Account Number:















Networks	Sites	Captive Portal	Inventory / Devices	Users	Preferences	License Info				
Device Details ✕    										
<input type="checkbox"/>	AP Name	MAC Address	Serial Number	Site	Network	AP Status	Config Status	Firmware Upgr...	Last Seen	Actions
<input type="checkbox"/>	HW-Blv-AP-01	11-22-33-44-55...	12345678	TP_Retail_Loc...	Shops	↑ (online)	Up-to-date	Up-to-date	04/17/2016 17...	  
<input type="checkbox"/>	Site02AP01	66-55-44-33-22...	445566778899	TP_Retail_Loc...	Shops	↑ (online)	Up-to-date	Up-to-date	04/17/2016 17...	  
<input type="checkbox"/>	bangalore	11-22-33-66-55...	40	TP_Retail_Loc...	Shops	↓ (offline)	-	-		  

Figure 1-72 Tenant Inventory/Device Management - List of Devices

2. Review the following information to assess its relevance for your network's device inventory:

AP Name	Displays the administrator name of the access point assigned when deployed. The name displays as a link that can be selected to edit the access point's parameters.
MAC Address	Displays the hardware encoded MAC address of the access point used as its network hardware identifier.
Serial Number	Displays the serial number of the access point.
Site	Displays the administrator assigned site name where this access point is located physically. The site name displays as a link that can be selected to edit the site's parameters
Network	Displays the administrator assigned network name to which the listed site belongs. Click the Network name to configure the network set on the access point.
AP Status	Displays the current access point status as either online or offline. Use this information to assess whether the access point device inventory is populated with enough online devices to support the client requirements of specific sites.
Config Status	Displays the status of the access point's configuration. Displays <i>Up-to-date</i> if the configuration has been updated and is current.
Firmware Upgrade Status	Displays the status of the access point's firmware. Displays <i>Up-to-date</i> if the access point firmware has been updated and is current.
Last Seen	Displays a datestamp when the access point was last seen by the Azara Cloud controller on the network. Use this information with the <i>AP Status</i> to assess whether the requires a troubleshooting, a reboot or other administration to ensure the site's client requirements are supported.
Actions	Displays the actions that can be performed on this access point. The access point's details can be edited or the access point can be deleted using the icons in this field. Use the edit icon to edit the access point details. To delete an access point, select the red delete icon. Use the middle blue icon to deactivate the access point. The access point is reset to factory defaults when deactivated.

3. To add a new access point, click the  icon located to the right of the Device Details bar.

System > Configuration Account Number:

Add Devices Using MAC/Serial Number ✕

Import from CSV: [Download Sample CSV file](#) + -

<input checked="" type="checkbox"/>	AP Name	MAC Address	Serial Number	Site	Network
<input checked="" type="checkbox"/>	Enter Name	Enter MAC	Enter Serial No	Select a Site	Select a Network

Figure 1-73 Tenant Inventory/Device Management - Add New Device

4. Add the following information for each new access point.

AP Name	<p>Enter a name for this access point. Use this field to identify the access point uniquely. The access point name cannot be longer than 32 characters. The following rules apply when naming access point:</p> <ul style="list-style-type: none"> • Access point names can contain [A-Z] [a-z] [0-9]. Names can contain hyphen ("-") and cannot contain other special characters. • Access point names cannot start or end with a hyphen ("-"). • Access point names cannot contain spaces between characters. <p>Provide a name that identifies each access points from others that may be deployed within the same site. Choose a unique name, for example, "Entrance-Lobby-AP", "Accounts-Department-AP", etc.</p>
MAC Address	<p>Enter the hardware encoded MAC Address for this access point. This information is generally located at the bottom of the access point and is typically used as the access point's hardware identifier.</p>
Serial Number	<p>Enter the serial number for the access point. This information is generally located at the bottom of the access point.</p>
Site	<p>Use the drop-down menu to select the site to which this access point belongs. If required, create a new site using the Create New Site link.</p>
Network	<p>Use the drop-down menu to select the network to which this access point belongs. If required, create a new site using the Create New Network link.</p>

5. Select **Activate** button to activate the access point.

You can add and activate multiple devices at a time using a pre formatted *Comma Separated Value* (CSV) file. The information to be uploaded must be formatted properly for it to be successfully used by Azara. Use the [Download Sample CSV file](#) link to download a template csv file. This file can then be used to input your device information.



CAUTION: When using the sample csv file, do not clear the contents of the first row in the file. If the first row is cleared, Azara will be unable to process the uploaded csv file. Also, create a new line for each device to be added.

Use the icon to browse your local PC for the csv file. Then, use the button to import the device information from the uploaded csv file. If the csv file is properly formatted, the devices are automatically added to the list of devices.

6. To modify the access point's configuration, select the icon. The following screen displays.

System > Configuration Account Number:

[Network](#) | [Sites](#) | [Captive Portal](#) | [Inventory / Devices](#) | [Remote Console](#) | [Users](#) | [Preferences](#) | [License Info](#)

Device Details View stats

Name *	<input type="text" value="HW-Blv-AP-01"/>	Network Name	<input type="text" value="Shops"/>
Site Name	<input type="text" value="TP_Retail_Location_01"/>	Firmware Version	5.8.3.11-244877D
Model	AP-7532-67040-WR	Uptime	8 Days 6 Hrs, 9 Mins, & 2 Secs
MAC Address	84-24-8D-80-BF-E8	Serial Number	14289522200149
IP Address	192.168.20.200	Last Seen	08/18/2016 16:01:18
Status	online	Default Gateway	<input type="text"/>

Wireless Settings

2.4 Ghz					
Channel	<input type="text" value="auto"/>	Power (dBm)	<input type="text" value="1"/>	Placement	<input type="text" value="indoor"/>
Antenna Gain (dBi) (0.0 - 15.0)	<input type="text" value="auto"/>				
5 Ghz					
Channel	<input type="text" value="auto"/>	Power (dBm)	<input type="text" value="1"/>	Placement	<input type="text" value="indoor"/>
Antenna Gain (dBi) (0.0 - 15.0)	<input type="text" value="auto"/>				

Location Based Services

Enable

LAN Port Settings <input type="button" value="+"/>					
Port	St...	Allowed VLAN (...	Un tagged ...	PO...	Ac...

IP Settings <input type="button" value="+"/>			
Interface	Description	IP Address	Actions
⚠ Ensure that the VLANs are mapped to the appropriate LAN ports and configured on wired networks			

DNS Servers <input type="button" value="+"/>	
IP Address	

Routes <input type="button" value="+"/>		
Network Address	Gateway	Actions

Figure 1-74 Tenant Inventory/Device Management - Edit Device

7. Of the information displayed on this screen, the following can be modified:


Name	<p>Enter a name for this access point. Use this field to identify the access point uniquely. The access point name cannot be longer than 32 characters. The following rules apply when naming access point:</p> <ul style="list-style-type: none"> • Access point names can contain [A-Z] [a-z] [0-9]. Names can contain hyphen ("-") and cannot contain other special characters. • Access point names cannot start or end with a hyphen ("-"). • Access point names cannot contain spaces between characters. <p>Provide a name that identifies each access points from others that may be deployed within the same site. Choose a unique name, for example, "Entrance-Lobby-AP", "Accounts-Department-AP", etc.</p>
Site Name	<p>Use the drop-down menu to select the site to which this access point belongs. If required, create a new site using the Create New Site link.</p>
Network Name	<p>Use the drop-down menu to select the network to which this access point belongs. If required, create a new site using the Create New Network link.</p>

Default Gateway	Use the field to enter the IPv4 default gateway for this access point. This is the IP address to send packets to when the route to that IP address is not known by the access point.
2.4 GHz - Channel	Use the drop-down to select the channel of operation for the 2.4 GHz radio band. To use the channel as configured as default on the device, select <i>auto</i> . To use Smart RF to select the channel, use <i>smart</i> . To use automatic channel selection to select the channel of operation, use <i>acs</i> . To manually select the channel, expand the drop-down list and select the appropriate channel,
2.4 GHz - Power (dBm)	Use the drop-down to select the Power settings for the 2.4 GHz radio band. To automatically select the correct power, select <i>auto</i> . To use Smart RF to manage the power settings, use <i>smart</i> .
2.4 GHz - Placement	Use the drop-down to select the placement for this access point radio. Placement can be either <i>Indoor</i> or <i>Outdoor</i> .
2.4 GHz - Antenna Gain (dBi)	Set the antenna gain between 0.00 - 15.00 dBi for the 2.4 GHz radio. The access point's <i>Power Management Antenna Configuration File (PMACF)</i> automatically configures the radio transmit power based on the antenna type, its antenna gain (provided here) and the deployed country's regulatory domain restrictions. Once provided, the access point calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. Only a professional installer should set the antenna gain for the 3.5 GHz radio.
5.0 GHz - Channel	Use the drop-down to select the channel of operation for the 5.0 GHz radio band. To use the channel as configured as default on the device, select <i>auto</i> . To use Smart RF to select the channel, use <i>smart</i> . To use automatic channel selection to select the channel of operation, use <i>acs</i> . To manually select the channel, expand the drop-down list and select the appropriate channel,
5.0 GHz - Power (dBm)	Use the drop-down to select the Power settings for the 2.4 GHz radio band. To automatically select the correct power, select <i>auto</i> . To use Smart RF to manage the power settings, use <i>smart</i> .
5.0 GHz - Placement	Use the drop-down to select the placement for this access point radio. Placement can be either <i>Indoor</i> or <i>Outdoor</i> .
5.0 GHz - Antenna Gain (dBi)	Set the antenna gain between 0.00 - 15.00 dBi for the 5.0 GHz radio. The access point's <i>Power Management Antenna Configuration File (PMACF)</i> automatically configures the radio transmit power based on the antenna type, its antenna gain (provided here) and the deployed country's regulatory domain restrictions. Once provided, the Access Point calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. Only a professional installer should set the antenna gain for the 5 GHz radio.


8. Use the **Location Based Services** section to manage location based services on the selected device. Use the **Enable** slider to enable or disable this feature for this device.

This slider is disabled by default. To enable or disable the feature on this device, *Location Based Services* (LBS) must be enabled for the tenant. LBS is enabled from the **Configuration > Preferences > Management Settings > Location Based Services > Enable** slider. For more information, see [Configuring Tenant Preferences on page 1-100](#)


9. Use the **Lan Port Settings** table to configure the physical ports settings. AP7502 provides three (3) fast ethernet ports fe1, fe2, fe3 of which one (fe3) also provides Power Over Ethernet (PoE) to connected devices.

Port	Displays the available ports on the access points. The available ports are <i>ge 1, fe1, fe2</i> and <i>fe3</i> . This is a display only field.
Status	Displays the current status of this port. Select this field and set this field to <i>Disabled</i> to disable this port. The default value is <i>Enabled</i> .
Allowed VLANs	Displays the VLANs allowed on this port. Select this field and enter the VLANs that are allowed on this FE or GE port.
Untagged VLAN	Displays the native VLAN for this network. This is a display only field.
POE Out	Note: This feature is available only on the <i>fe3</i> port. Displays the status of PoE on the port. Select this field and set this field to <i>Enabled</i> to supply power over ethernet to connected devices. The default value is <i>Disabled</i> .
Action	Use the  icon to delete this mapping entry.


10. Use the **IP Settings** table to configure the VLAN mappings for this access point.






Interface	Use the spinner control to set the VLAN number. Enter a numeric value in this field.
Description	Use this field to provide a brief description of this VLAN. Use this field to provide information to identify this VLAN from among the others defined on this access point.
IP Address	Use this field to provide the IP addresses that is assigned to wireless client using this VLAN. Only IPv4 addresses are supported. Leave this field blank to allow DHCP assigned IP address for this VLAN. Provide the IP address along with the subnet mask in the xxx.xxx.xxx.xxx/xx format.
Action	Use the  icon to delete this mapping entry.

11. The **DNS Servers** table displays a list of DNS servers configured on this access point. DNS servers were configured on this access point at the time of staging this device or were received from Azara along with the configuration.

Use the  icon to add additional IPv4 DNS servers to this list. Up to three (3) DNS servers can be added.

12. Use the **Routes** table to add routes to particular networks manually.

Network Address	Use this field to provide the network address along with the subnet mask in the xxx.xxx.xxx.xxx/xx format.
Gateway	Use this field to provide the gateway device to which traffic to any IP in the above Network Address field is directed to.
Action	Use the  icon to delete this routing entry.

13. Select the **Save** button to save changes made to the configuration items on this screen. Select **Cancel** to cancel all changes made to this screen.
When viewing a device's details, click the **View stats** button located at top right of the screen to display real time statistics for this access point.
14. To remove an existing device, navigate to **Configuration** and select **Inventory/Devices**. The list of devices for this Tenant displays. Select the device from amongst those displayed and select the  icon. The selected device is removed from the list of devices listed for this Tenant.
15. Periodically use the  icon to refresh the screen and to update the access point status.
16. Use the **Activate/De-Activate Multiple** icon , in the  tool bar to activate or de-activate multiple access points simultaneously. Select the check box in the first column for each access point to select it for activation or de-activation. The  icon is only enabled when multiple access points are selected. Once multiple access points are selected, select this icon to activate or deactivate them. The following message displays:

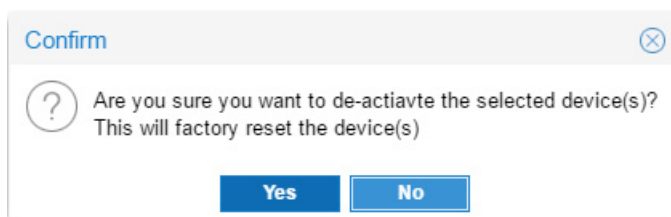





Figure 1-75 Tenant Inventory/Device Management - Manage Multiple Devices

Select **Yes** to either activate or de-activate the devices. When de-activating a device, the device is reset to its factory defaults. Select **No** to exit without performing the action.

17. Use the **Delete Multiple** icon , in the  tool bar to delete multiple access points simultaneously. Select the check box in the first column for each access point to select it for deletion. The  icon is only enabled when multiple access points are selected. Select this icon to delete the access points. The following message displays:

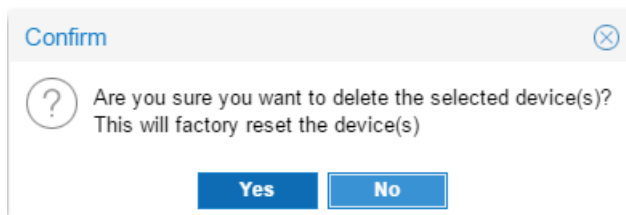


Figure 1-76 Tenant Inventory/Device Management - Manage Multiple Devices

Select **Yes** to delete the selected devices. The devices are reset to factory defaults before deletion. Select **No** to exit without performing the action.

1.6.3.1 Setting an Access Point to Factory Default

► [Managing Inventory/Devices](#)


Use the *Inventory/Devices* screen to reset one or more access points to factory default. The access point's configuration is cleared and all the data stored on the device is erased. Once the access point is set to factory default, it is rebooted. This action can be performed on more than one access point simultaneously.



NOTE: Only online access points can be reset.

The action tool bar is only enabled when at least one access point with (*online*) status is selected when selecting multiple access points. This action cannot be performed on an (*offline*) access point.

To set an access point to factory default:

1. Use the *Inventory/Devices* screen to select the access point to set to factory defaults. Select the check-box in the first column of the table for the desired access point. You can select multiple access points simultaneously.
2. Select the  icon and expand it to display its options. From the options, select **Factory-Defaults**.

System > Configuration Account Number:

Networks | Sites | Captive Portal | **Inventory / Devices** | Users | Preferences | License Info






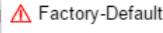

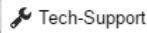






Device Details													
<input type="checkbox"/>	AP Name	MAC Address	Serial Num...	Site	Network	AP Status	Config Stat...	Firmware U...					
<input checked="" type="checkbox"/>	vallabhi	84-24-8D-8...	150795222...	Vallabhi	Wing-cloud...	↑ (online)	Up-to-date	Up-to-date	      				
<input checked="" type="checkbox"/>	Darbari	84-24-8D-8...	150795222...	Darbari	Wing-cloud...	↑ (online)	Up-to-date	Up-to-date					
<input type="checkbox"/>	Megmalhar	84-24-8D-1...	142835222...	Megmalhar	Wing-cloud...	↑ (online)	Up-to-date	Up-to-date					
<input type="checkbox"/>	Lab-AP	84-24-8D-8...	143355222...	Lab-AP	Wing-cloud...	↑ (online)	Up-to-date	Up-to-date					
<input type="checkbox"/>	Basant	84-24-8D-8...	150795222...	Basant	Wing-cloud...	↑ (online)	Up-to-date	Up-to-date					
<input type="checkbox"/>	Manjari	84-24-8D-8...	150795222...	Manjari	Wing-cloud...	↑ (online)	Up-to-date	Up-to-date					
										05/05/2016...			

Figure 1-77 Tenant Inventory/Device Management - Set To Factory Defaults

The following warning displays:

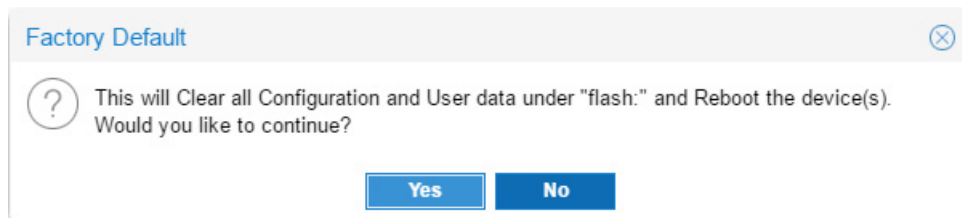



Figure 1-78 Tenant Inventory/Device Management - Set To Factory Defaults - Warning screen

3. Select **Yes** to reset the selected access points to factory defaults. Select **No** to exit the screen.

1.6.3.2 Rebooting an Access Point


► *Managing Inventory/Devices*

Use the *Inventory/Devices* screen to reboot one or more access points.

 **NOTE:** Only online access points can be rebooted.

The action tool bar is only enabled when at least one access point with (*online*) status is selected when selecting multiple access points. This action cannot be performed on an (*offline*) access point.

To reboot an access point:

1. Use the *Inventory/Devices* screen to select the access point to reboot. Select the check-box in the first column of the table of the desired access point. You can select multiple access points simultaneously.
2. Select the  icon and expand it to display its options. From the options, select **Reboot**.

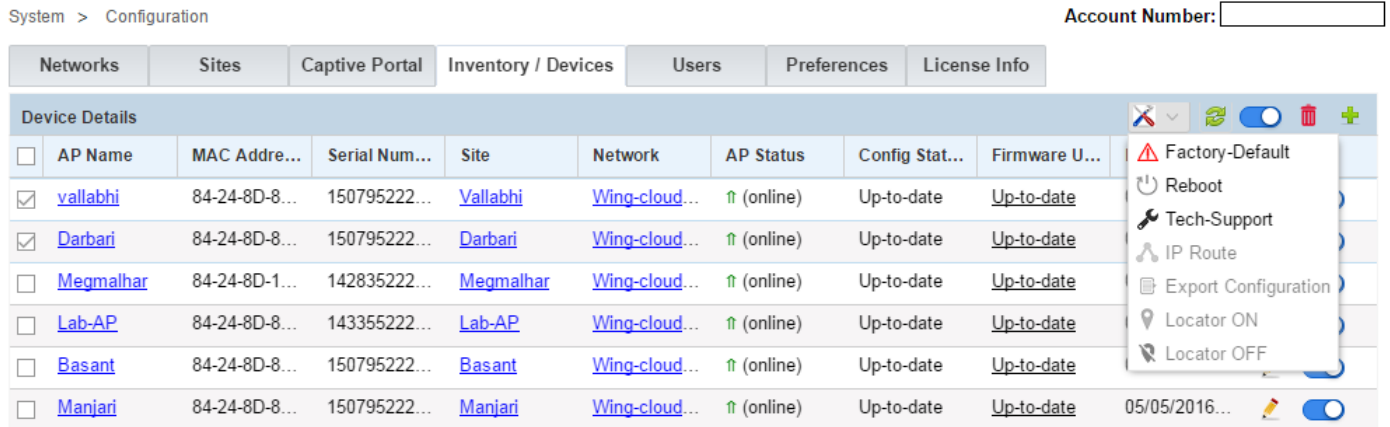


Figure 1-79 Tenant Inventory/Device Management - Reboot

The following warning displays:

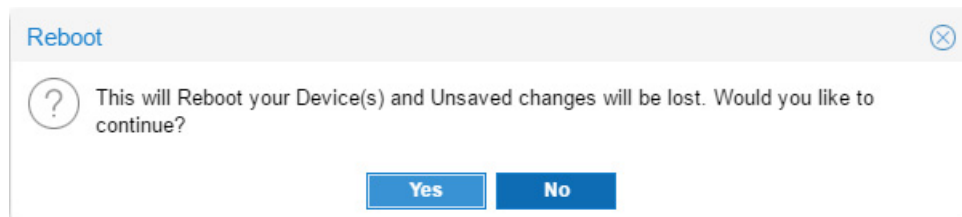


Figure 1-80 Tenant Inventory/Device Management - Set To Factory Defaults - Warning screen

3. Select **Yes** to reboot the selected access points. Select **No** to exit the screen.

1.6.3.3 Tech Support

► Managing Inventory/Devices


The Azara Support Center might require that some files be supplied to it when troubleshooting issues. The files are compressed as a single .tar.gz file. This compressed file must be sent to the Azara Support Center on request. Use the *Tech Support* screen to send the files.



NOTE: Tech Support files for online access points can only be sent.

The action tool bar is only enabled when at least one access point with (*online*) status is selected when selecting multiple access points. This action cannot be performed on an (*offline*) access point.

To send files to Azara Support Center:

1. Use the *Inventory/Devices* screen to select the access point to collect and send the Tech Support file. Select the check-box in the first column of the table of the desired access point. You can select multiple access points simultaneously.
2. Select the  icon and expand it to display its options. From the options, select **Tech Support**.

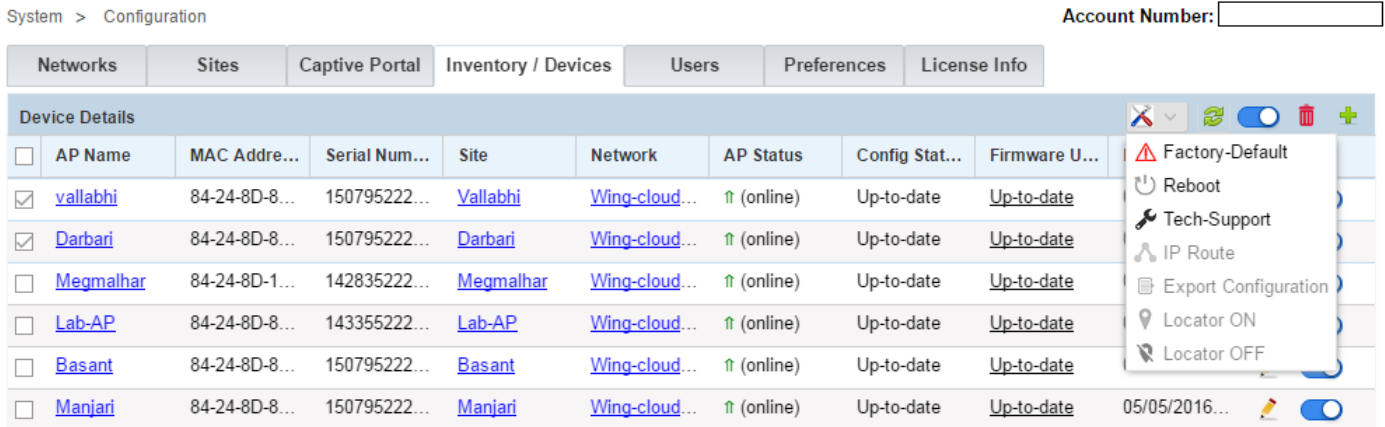


Figure 1-81 Tenant Inventory/Device Management - Reboot

The following screen displays:

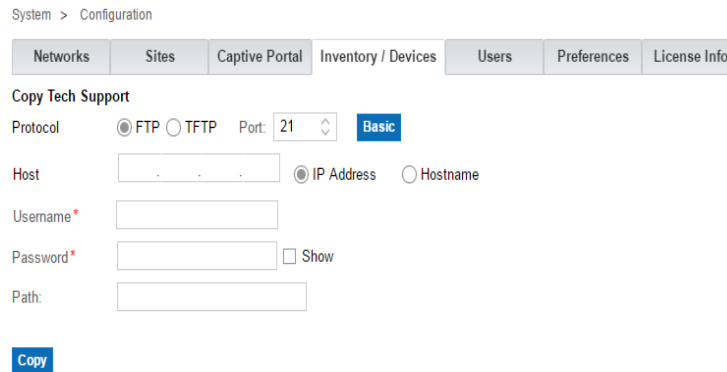


Figure 1-82 Tenant Inventory/Device Management - Send Tech Support Files

3. Select the **Basic** mode and provide the **URL** for the remote site where the Tech Support files should be placed. Select the **Advanced** mode and provide the following additional information. Tech support files can be sent using *ftp* or *tftp*.

Provide the following information when transferring files using the *ftp* protocol:

Protocol	Select the protocol used for file transfer. Select <i>ftp</i> .
Port	This is the port used by the FTP server. The default and standard port is 21. If the FTP server uses a non standard port, use the spinner to select it.
Hostname/IP Address	Enter the hostname or the IP address of the FTP server.
Username	Enter the user credentials to authenticate on the FTP server.
Password	Enter the authentication password for the user credentials provided in the <i>User</i> field.
Path (Optional)	Optionally, provide the complete path to the directory on the FTP server where the Tech Support Dump file is to be placed.

Provide the following information when transferring files using the *tftp* protocol:

Protocol	Select the protocol used for file transfer. Select <i>tftp</i> .
-----------------	--

Port	This is the port used by the TFTP server. The default and standard port is 69. If the TFTP server uses a non standard port, use the spinner to select it.
Hostname/IP Address	Enter the hostname or the IP address of the TFTP server.
Path (Optional)	Optionally, provide the complete path to the directory on the TFTP server where the Tech Support Dump file is to be placed.


4. Use the **Copy** button to begin file transfer.

1.6.3.4 IP Route

► *Managing Inventory/Devices*

Use the *IP Route* screen to view the routes configured automatically on the selected access point. Use this information to troubleshoot network issues.

To view the routes configured on this access point:

1. Use the *Inventory/Devices* screen to select the access point to view the configured IP routes. Select the checkbox in the first column of the table of the desired access point. This action is not available when multiple access points are selected.
2. Select the  icon and expand it to display its options. From the options, select **IP Route**.

System > Configuration Account Number:

Networks | Sites | Captive Portal | **Inventory / Devices** | Users | Preferences | License Info

Device Details								
<input type="checkbox"/>	AP Name	MAC Address	Serial Num...	Site	Network	AP Status	Config Stat...	Firmware U...
<input checked="" type="checkbox"/>	vallabhi	84-24-8D-8...	150795222...	Vallabhi	Wing-cloud...	↑ (online)	Up-to-date	Up-to-date
<input type="checkbox"/>	Darbari	84-24-8D-8...	150795222...	Darbari	Wing-cloud...	↑ (online)	Up-to-date	Up-to-date
<input type="checkbox"/>	Megmalhar	84-24-8D-1...	142835222...	Megmalhar	Wing-cloud...	↑ (online)	Up-to-date	Up-to-date
<input type="checkbox"/>	Lab-AP	84-24-8D-8...	143355222...	Lab-AP	Wing-cloud...	↑ (online)	Up-to-date	Up-to-date
<input type="checkbox"/>	Basant	84-24-8D-8...	150795222...	Basant	Wing-cloud...	↑ (online)	Up-to-date	Up-to-date
<input type="checkbox"/>	Manjari	84-24-8D-8...	150795222...	Manjari	Wing-cloud...	↑ (online)	Up-to-date	Up-to-date

- Factory-Default
- Reboot
- Tech-Support
- IP Route**
- Export Configuration
- Locator ON
- Locator OFF

Figure 1-83 Tenant Inventory/Device Management - IP Route

The following screen displays:

System > Configuration Account Number:

Networks | Sites | Captive Portal | **Inventory / Devices** | Users | Preferences | License Info

IP Route						
Destination Address	Gateway Address	Interface	Flags	Metric	Distance	
192.168.21.0/24	0.0.0.0	vlan2100	C	0	0	
default	10.233.83.254	vlan1	CG	0	1	
10.233.83.0/24	0.0.0.0	vlan1	C	0	0	

Figure 1-84 Tenant Inventory/Device Management - IP Routes screen

Use this information to troubleshoot network issues.


3. To close this screen, use the 'x' button to the right of the IP Route bar.

1.6.3.5 Export Configuration

► *Managing Inventory/Devices*

To backup an existing configuration of an access point, the configuration file must be exported to a remote location using the *Export Configuration* action. This action can only be performed on a single access point at a time.

To export the configuration of an access point:

1. Use the *Inventory/Devices* screen to select the access point to export the configuration. Select the check-box in the first column of the table of the desired access point. This action is not available when multiple access points are selected.
2. Select the  icon and expand it to display its options. From the options, select **Export Configuration**.

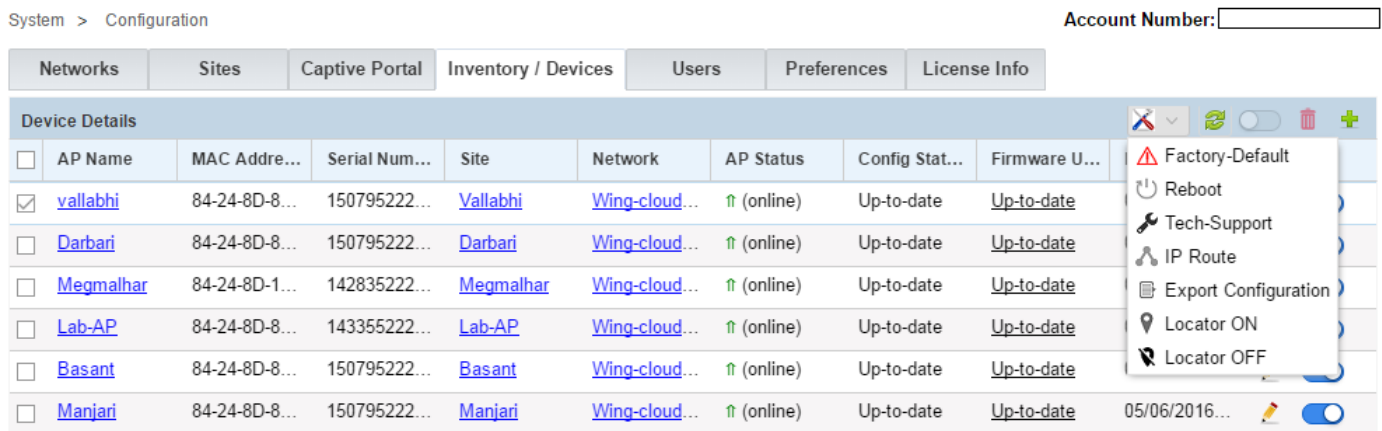


Figure 1-85 Tenant Inventory/Device Management - Export Configuration

The following screen displays:

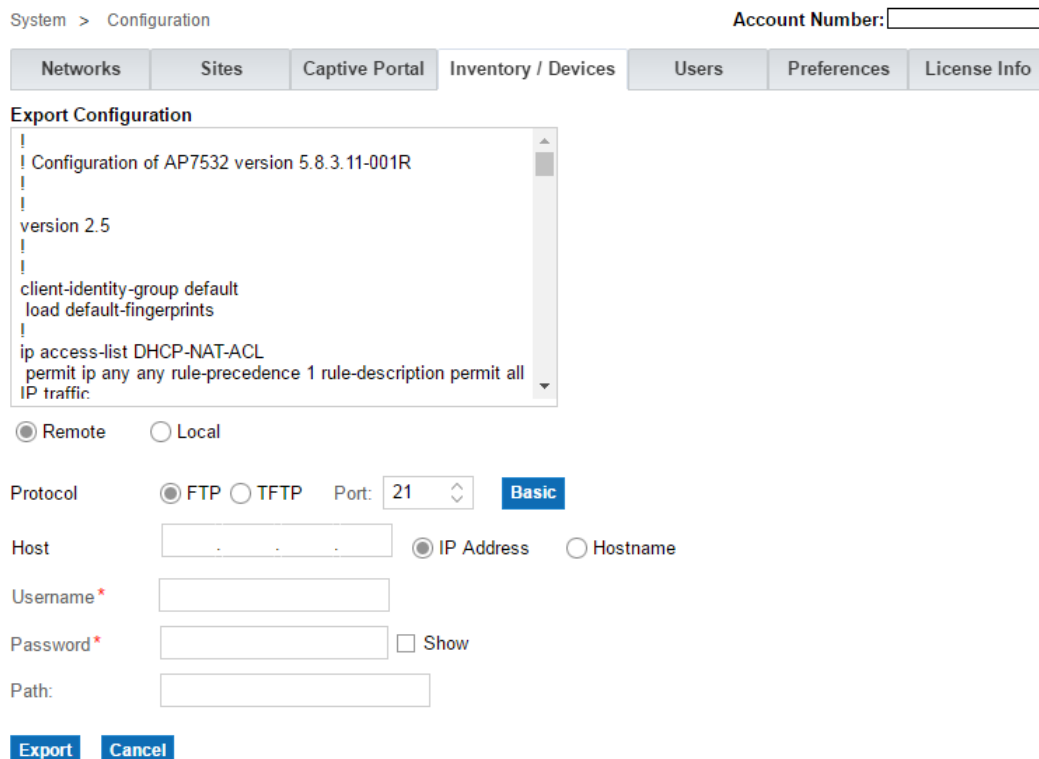


Figure 1-86 Tenant Inventory/Device Management - Export Configuration screen

- The access point's configuration is displayed in the text box. To quickly copy the configuration, click in the text box, select all the content, copy the content into the clipboard memory and paste the content to any text tool.
- Select **Remote**. Use this option to transfer the current configuration to a remote FTP or TFTP server.

Provide the following information when transferring files using the *ftp* protocol:

Protocol	Select the protocol used for file transfer. Select <i>ftp</i> .
Port	This is the port used by the FTP server. The default and standard port is 21. If the FTP server uses a non standard port, use the spinner to select it.
Hostname/IP Address	Enter the hostname or the IP address of the FTP server.
Username	Enter the user credentials to authenticate on the FTP server.
Password	Enter the authentication password for the user credentials provided in the <i>User</i> field.
Path (Optional)	Optionally, provide the complete path to the directory on the FTP server where the configuration file is to be placed.

Provide the following information when transferring files using the *tftp* protocol:

Protocol	Select the protocol used for file transfer. Select <i>tftp</i> .
Port	This is the port used by the TFTP server. The default and standard port is 69. If the TFTP server uses a non standard port, use the spinner to select it.
Hostname/IP Address	Enter the hostname or the IP address of the TFTP server.
Path (Optional)	Optionally, provide the complete path to the directory on the TFTP server where the configuration file is to be placed.

- Select **Export** to export the configuration file to the remote server. Select **Cancel** to exit this screen.
- Alternatively, select **Local** and then select **Export** to use the local browser's user interface to save the configuration file to the local PC's OS. The browser's *Save As* dialog displays. The following is an example of the *Save As* dialog of the Windows OS:

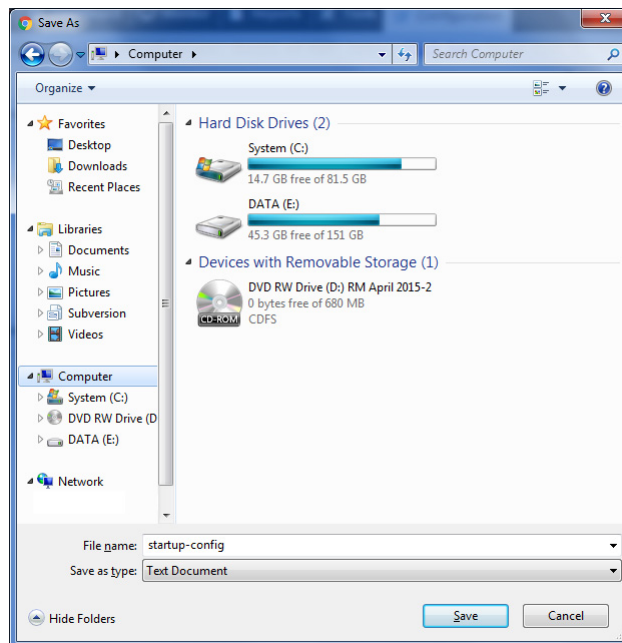



Figure 1-87 Tenant Inventory/Device Management - Export Configuration - Save As screen

1.6.3.6 Locating the Access Point

► [Managing Inventory/Devices](#)

In sites with multiple access points, it is often difficult to identify a specific access point. Use the access point's locator feature to find the device. Once configured, the access point blinks its LEDs in a specific pattern that enables it to be identified amongst all other deployed devices in the same site.

To identify an access point at a site:

1. Use the *Inventory/Devices* screen to select the access point to locate. Select the check-box in the first column of the table of the desired access point. This action is not available when multiple access points are selected.
2. Select the  icon and expand it to display its options. From the options, select **Locator ON**.

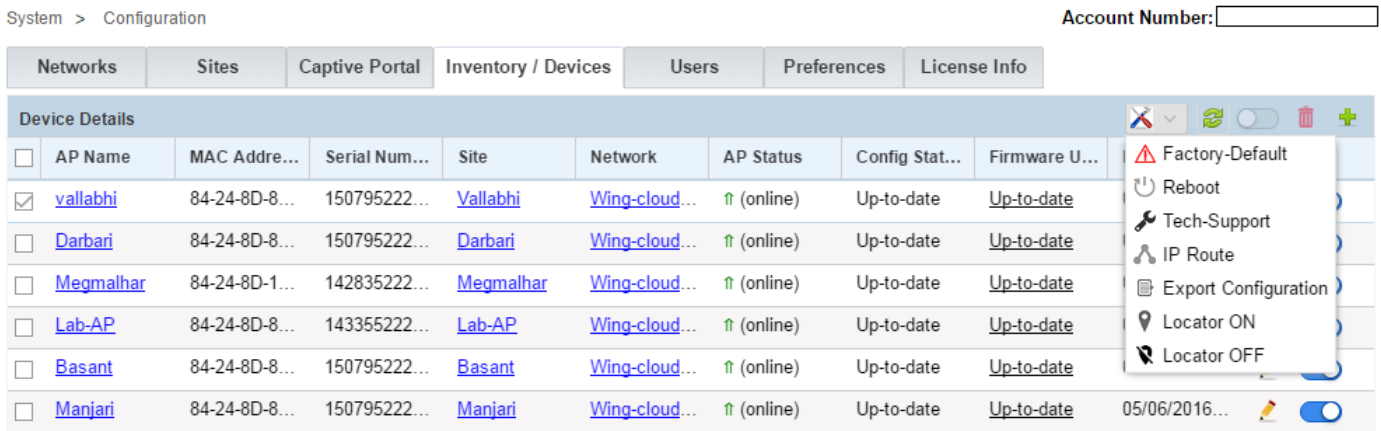


Figure 1-88 Tenant Inventory/Device Management - Locator ON

The following message displays:



Figure 1-89 Tenant Inventory/Device Management - Locator ON - Message

3. To switch off the locator LEDs on an access point, select **Locator OFF** from the action bar.



Figure 1-90 Tenant Inventory/Device Management - Locator OFF - Message

1.6.4 Configuring Tenant Users

► Configuration

The *Users* screen is the centralized location for managing Tenant users. Users can be added, removed or modified as required.

To view the list of existing users configured for this Tenant:

1. From the **Configuration** menu item, select **Users**. A list of existing users for this Tenant displays by default.

System > Configuration Account Number:

Networks Sites Captive Portal Inventory / Devices **Users** Preferences License Info










User Details ✉ 					
Name	Email	Phone Number	Account Status	Access Permission	Actions
Tenant_03	testing01@yahoo.c...		✓ Active	Super Admin	 
Testing Admin	testing03@yahoo.c...		✓ Active	Admin	 
Testing Read Write	testing04@yahoo.c...		✓ Active	Read-Write	 

Figure 1-91 Tenant Users Management - View Users

2. Refer to the following for information displayed on this screen:

Name	Displays the name of the users with management access to this Tenant. Their respective permissions vary and are listed separately in the Access Permissions column.
Email	Displays the e-mail address set by the system when each listed user was created.
Phone Number	Displays the phone number provided when this user was created.
Account Status	Displays the account status for this user. Displays <i>Active</i> when the account status is fine.
Access Permission	Displays the access permissions assigned to this user for this Tenant. Permissions include, <i>Admin</i> , <i>Read/Write</i> or <i>Read</i> .
Actions	Displays icons for the actions that can be performed on this user account. The actions are editing the user account details or deleting the user account.

3. To add a new user for this Tenant, select the  icon from the top right-hand corner of the User Details bar. To edit an existing user, select the  icon located to the extreme right of the user entry in the users list.

Add New User

Name*	<input type="text" value="Testing Admin"/>	
Email*	<input type="text" value="testing03@zebra.com"/>	
Password (Min 8 chars)*	<input type="password" value="....."/>	● Medium
Verify Password*	<input type="password" value="....."/>	
Phone	<input type="text" value="Phone"/>	
Address	<input type="text" value="Address"/>	
Access Permission*	<input type="radio"/> Admin <input checked="" type="radio"/> Read/Write <input type="radio"/> Read	
Support Phone	<input type="text" value="Support Phone"/>	
Support Email	<input type="text" value="Support Email"/>	

Figure 1-92 Tenant Users Management - Add New User

4. Enter the following information for each user.

Name	Enter the name of the new user. Once created, the user has management access to this Tenant. This field is mandatory.
Email	Enter the user's e-mail address. This field is mandatory.
Password (Min 8 chars)	Enter the password associated with this new user account. The password should be minimum 8 characters long and should contain at least 1 upper case character, 1 lower case character, 1 number and 1 symbol. This is a mandatory field.
Verify Password	Re-enter the password to confirm it. This is a mandatory field.
Phone	Enter the user's contact number.
Address	Enter the user's address as an additional contact option.
Access Permission	Select the access level for this new user. The options are <i>Admin</i> , <i>Read/Write</i> and <i>Read</i> . Some screens may not display depending on the permissions set.
Support Phone	Enter an alternate contact number for the Tenant user as an additional phone contact resource.
Support Email	Enter an alternate e-mail address for the Tenant user as an additional contact resource.

5. Select the **Save** button to save changes made to the configuration items on this screen. Select **Cancel** to cancel all changes made to this screen.
6. To delete an existing user, select the icon located to the extreme right of the user entry in the users list. The selected user is removed from the list of users configured for this Tenant.

1.6.5 Configuring Tenant Preferences

► Configuration

Use the *Preferences* screen to configure Firmware Upgrade Schedules and Security Policies for the selected Tenant. The screen enables administrators to schedule firmware updates and the security applied.

Firmware upgrades are performed automatically by the Azara system. Azara administrators configure default upgrade window for the Tenants. Tenants can adjust the upgrade window to meet unique requirements. This screen also provides the current state of the Azara system and the next upgrade window.

To configure Tenant firmware upgrade preferences:

1. From the **Configuration** menu item, select **Preferences**. The *Firmware Upgrade Schedule* configuration parameters display by default.

System > Configuration Account Number:

Network Sites Captive Portal Inventory / Devices Users **Preferences** License Info

Firmware Upgrade Schedule ⌵

Default upgrade window

Other upgrade options

Upgrade as scheduled November 6th 2016, 10:00:00 pm
 Reschedule to
 Upgrade Now

Save

Security Policy Settings ⌵

Management Settings ⌵

Location Based Services Notifications ⌵

Open DNS Network End Devices ⌵

Figure 1-93 Tenant Preferences

2. Refer the following for more information:

Default upgrade window	Use the adjacent fields to configure the default upgrade window for this Tenant. Scheduled firmware upgrades are performed once a week. Use the <i>weekday</i> drop-down to configure the day of the week for upgrade. Use the <i>hour</i> drop-down to configure the hour when the upgrade process is run every time.
Upgrade as schedule	This option is enabled or disabled based on a system-wide configuration setting. This field displays the time when the firmware upgrade is scheduled next.
Reschedule to	This option is enabled or disabled based on a system-wide configuration setting. Use this field to reschedule a missed firmware upgrade. Use the calendar control to select a specific date to reschedule the firmware upgrade. Use the hour drop-down menu to configure the hour when the upgrade is to run.

Upgrade Now	This option is enabled or disabled based on a system-wide configuration setting. When selected, the firmware upgrade is run immediately after saving the Firmware Upgrade Schedule configuration.
--------------------	---

3. Select **Save** to apply the updates to the Firmware Upgrade Schedule configuration.
4. Expand the **Security Policy Settings** area. The following fields display.

System > Configuration Account Number:

Firmware Upgrade Schedule ▼

Security Policy Settings ▲

Enable Account Lockout ⓘ Number of failed login attempts allowed
 Enable Password Expiry ⓘ Password Expiry Interval in Days
 Password Reuse ⓘ Choose passwords different from previous password(s)
 Password Min Length ⓘ Force passwords to have at least number of characters
 Login IP Ranges ⓘ Only allow access to Dashboard from IP addresses in the specified ranges
 Enter one range of IP addresses per line
 This computer is using IP address 140.101.148.1

 Two Factor Authentication ⓘ Enforce two factor authentication for the users
 Disable Partner/Support Access ⓘ Restrict account access to Partner/Support

Management Settings ▼

Location Based Services Notifications ▼

Open DNS Network End Devices ▼

Figure 1-94 Tenant Preferences - Security Policy Settings

5. The following **Security Policy Settings** can be configured. Use the blue icon next to each setting to read a brief explanation of each of these setting.

Account Lockout	Set the number of times failed logins are permitted before the account is locked. This is the number of failed attempts permitted after which the account is locked. For example, when set to 5, the account is locked after 5 consecutive failed login attempts.
Password Expiry	Select this option to enable password expiry and configure the number of days after which the password has to be reset. For example, when set to 30, the password expires after 30 days and has to be reset.
Password History	Select this option to enable password reuse restrictions and configure the number of previous passwords that cannot be reused. For example, when set to 3, the last three passwords cannot be used.
Password Min Length	Set the minimum length of the user password for this Tenant. Select this option to enable password a length check and set a value for its length. For example, when set to 8, the password cannot be shorter than 8 characters.

Login IP Ranges	Set the range of IP addresses that can access this Tenant's network. Select this option to restrict access to specific address ranges. Use the text box to provide an allowed IP address range. For example, if the range is 10.233.216.0/24, then an IP address out of this range is restricted from accessing this Tenant network.
Two Factor Authentication	Two factor authentication enhances security by requiring users to provide a second authentication value, such as a number or phrase over in addition to the account password. This second authentication value is usually sent to the user's registered phone number or e-mail.
Disable Partner/Support Access	Select this option to prevent the CSP or the MSP (the service providers) from accessing the Tenant's data. By default, Tenant's data is visible to the MSP and the CSP. When selected, the service provider can be prevented from viewing the data in the Tenant's network. The default is disabled.

6. Expand the **Management Settings** area. The following fields display:

Network	Sites	Captive Portal	Inventory / Devices	Users	Preferences	License Info	
Firmware Upgrade Schedule						⌵	
Security Policy Settings						⌵	
Management Settings						⌶	
SNMP V3 User							
Username	snmptrap	Password <input type="checkbox"/> Show	Authentication	md5	Encryption	des
SNMP Traps							
Traps Generation	<input type="checkbox"/>						
						+	
IP Address	Port	Version	Actions				
Syslog Server							
Logging	<input type="checkbox"/>						
Logging Level	Warnings						
Server IP							
Location Based Services							
Enable	<input checked="" type="checkbox"/>						
Save							
Location Based Services Notifications						⌵	
Open DNS Network End Devices						⌵	

Figure 1-95 Tenant Preferences - Management Settings

The *Management Settings* area configures the SNMP and logging functions for the tenant managed networks.

Refer to the following to configure SNMPv3 User information. The other fields in this area are not configurable.

snmptrap	Provide the password for the SNMPv3 user account. Use the Show option to view the password entered in this field.
-----------------	--

Refer to the following to configure **SNMP Traps** related parameters. Select the **Traps Generation** switch control to enable or disable SNMP trap generation. Use the table to configure SNMP trap servers. Select the green '+' button to the right to add a new SNMP trap server:


IP Address	Configure the IPv4 address for the SNMP trap server.
Port	Configure the port on which the server listens for the generated SNMP traps. Use the spinner control to set the correct port number. The default port number is <i>162</i> .
Version	Configure the version of the generated SNMP traps. Use the drop-down to select the appropriate version. The default <i>v2c</i> .
Action	Use the <i>Trash</i> icon to delete this SNMP server configuration entry.

Refer to the following to configure the **Syslog Server** related parameters. Select the **Logging** switch control to enable or disable logging to a remote server.

Logging Level	Use the drop-down to select the logging level. The default logging level is <i>Warnings</i> .
Server IP	Configure the IPv4 address for the syslog server.

- Use the **Location Based Services** section to manage location based services for this tenant. Use the **Enable** slider to enable or disable this feature.

Location Based Services (LBS) is disabled by default. Use the **Enable** slider to enable the services for the tenant. When enabled, LBS is enabled for all the sites and devices managed by the tenant. The tenant can then enable or disable LBS at the site level or at the device level. When LBS is enabled at a site, it is automatically enabled on all devices that are configured for the site.

LBS can be disabled for each device on a site from the **Configuration > Inventory/Devices >  > Location Based Services > Enable** slider. For more information, see [Managing Inventory/Devices on page 1-84](#).

- Select **Save** to apply the updates to the **Management Settings** configuration.
- Expand the **Location Based Services Notifications** area. Use this area to provide the credentials used for receiving locationing notifications from the remote server. The following fields display:

System > Configuration Account Number:

Network Sites Captive Portal Inventory / Devices Users Preferences License Info

Firmware Upgrade Schedule ⌵

Security Policy Settings ⌵

Management Settings ⌵

Location Based Services Notifications ⌵

Connection Settings

Subscriber Push URL i

Username:

Password Show

Notification Type

Device Enter -
Indicates a device entering the Wireless Infrastructures range first time or after a previous Exit from the range.

Device Exit -
Indicates a device exiting the range of the Wireless Infrastructure.

Save

Open DNS Network End Devices ⌵

Figure 1-96 Tenant Preferences - Location Based Services Notification settings

Subscriber Push URL	<p>Configure either the IP address or the fully qualified domain name (FQDN) of the remote server to which the LBS pushes device notifications. Two types of notifications are sent to the remote server:</p> <ul style="list-style-type: none"> • <i>Device Enter</i> – This notification is sent when a device enters or re-enters an area which is being monitored by the LBS system • <i>Device Exit</i> – This notification is sent when a device leaves an area which is being monitored by the LBS system
Username	Configure the user name of the account on the remote server. This account is used to send device notifications to the server.
Password	Configure the password for the account provided in the <i>Username</i> field. Use the <i>Show</i> check-box to view the password being entered in this field.

10. Select **Save** to apply the updates to the **Location Based Services Notifications** configuration.
11. Expand the **Open DNS Network End Devices** area. The following fields display:

Network Sites Captive Portal Inventory / Devices Users Preferences License Info

Firmware Upgrade Schedule ⌵

Security Policy Settings ⌵

Management Settings ⌵


Location Based Services Notifications ⌵

Open DNS Network End Devices ⌵

Device Details		
Device (Label)	Device Id	Actions

Figure 1-97 Tenant Preferences - Open DNS Network End Devices

The Open DNS Network End Devices area lists the filters registered with Open DNS's DNS service.

Device (Label)	Displays the label of the device registered with Open DNS's service.
Device ID	Displays the ID of the device registered with the Open DNS's service.
Action	Use the  icon to delete this entry.

1.6.6 Licensing

► Configuration

Azara is a subscription based service. Licenses are available for set number of devices for various durations in various combinations. Licenses must be purchased from either the MSP or from Extreme Networks directly.

The *License Information* screen displays the current license state for the Tenant. The *License Information* screen describes the active state of the license, its expiration date, number of devices that can be deployed under the terms of the license and the current number of devices deployed.

Use the *License Information* screen to apply licenses on behalf of the Tenant. When a Tenant's account is created, the Tenant is provided a demo license to apply to one hundred (100) access point for ninety (90) days. This license is made available when the first access point is added to the Tenant's account. The Tenant need not have a license to use the added access point during the demo period. However, to continue using the access point after the demo period, the Tenant must purchase a full license.

The *License Information* screen displays the following:

System > Configuration Account Number:

Network Sites Captive Portal Inventory / Devices Users Preferences License Info

License Details

Status ✔ Active

Expiration Date Dec 12 2016

License Limit 100 Devices

License Used 5 Devices
(Current Device Count)

[Apply License](#)

License History			
License Key	Category	# Devices	Date Entered
<input type="text"/>	Device	100	Tue Apr 05 2016 12:21:35 GMT+...
DEMO LICENSE	Device	1	Sun May 29 2016 11:38:39 GMT...

Figure 1-98 Tenant Management - Licenses

The following information is displayed:

Status	Displays the current status of this Tenant. Displays <i>Active</i> if the license is active and the total number of access points is less than the number of access points supported by the terms of the license. Displays <i>Expired</i> otherwise.
Expiration Date	Displays the date the current license expires. Additionally, it also displays the number of days remaining until the expiration of the license if the license is close to expiring.

License Limit	Displays the number of access points permitted by the terms of the license.
License Used	Displays the actual number of access point devices deployed by the Tenant. This is the current device count for the Tenant.

To apply a license purchased from Extreme Networks, select the **Apply License** link. Selecting the link expands it.

Apply License

Enter License Key

Apply License

Figure 1-99 Tenant Management - Licenses - Add License

Enter the license key received from Extreme Networks within the **Enter License Key** field. Click **Apply License** to add the license key. If a valid license key is supplied, the license is applied immediately and is added to the list of available licenses.

1.6.7 Captive Portal

▶ [Configuration](#)

A Captive Portal is an access policy for temporary, guest or restrictive access to an access point managed network. It is the page a user lands on when associating with a Wi-Fi SSID and opens a Web browser to access the Internet. Basically, the Captive Portal captures and re-directs user initiated Internet traffic to a login page, where the user has to provide valid credentials. On successful log in, the user is served a Success page and allowed Internet access, in case of failure a Failure message is displayed.

The Azara Captive Portal feature has three tabs: [Templates](#), [SMS Gateway](#) and [Preferences](#). These three options provide a simple and easy-to-use interface for creating and managing Captive Portal related elements, such as *Splash Pages* and *Templates*, *SMS Gateways*, and *Preferences*.

Refer to the following sections:

- [Templates](#)
- [SMS Gateway](#)
- [Preferences](#)
- [Guest Users](#)

1.6.7.1 Templates

▶ *Captive Portal*

Use Azara's Captive Portal feature to provide guest users Internet access. The Captive Portal Templates tab provides the capability to customize the Captive Portal pages such as the Login, Terms & Conditions, Welcome and other pages to match your organization's color and display schemes.

Templates provide building blocks for creating pages used for interacting with the guest users of the captive portals. Azara provides a set of templates to base your customizations on. These templates are provided for the different login/registration options available with Azara. Use these templates as a base to create your own custom pages.

Azara provides a set of templates that are set up for use for different registration and login options provided.

To access the Templates screen:

1. From the **Configuration** menu item, select **Captive Portal**.
2. Select **Templates** to display the templates screen. The **Templates** screen is differentiated into three sections: **Upload Logo**, **Splash Pages** and **Templates**.

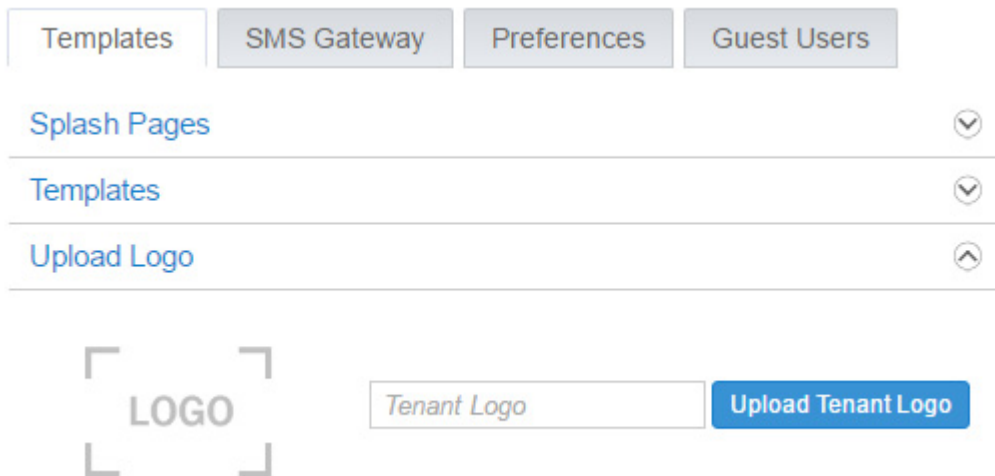


Figure 1-100 Configuration - Captive Portal - Templates

3. Use the **Upload Logo** section to upload a logo to be used across all the Captive Portal screens. Expand the **Upload Logo** area and use the **Upload Tenant Logo** button to select and upload a logo from the local PC's hard disk. The following screen shows the upload dialog for the Windows™ operating system.

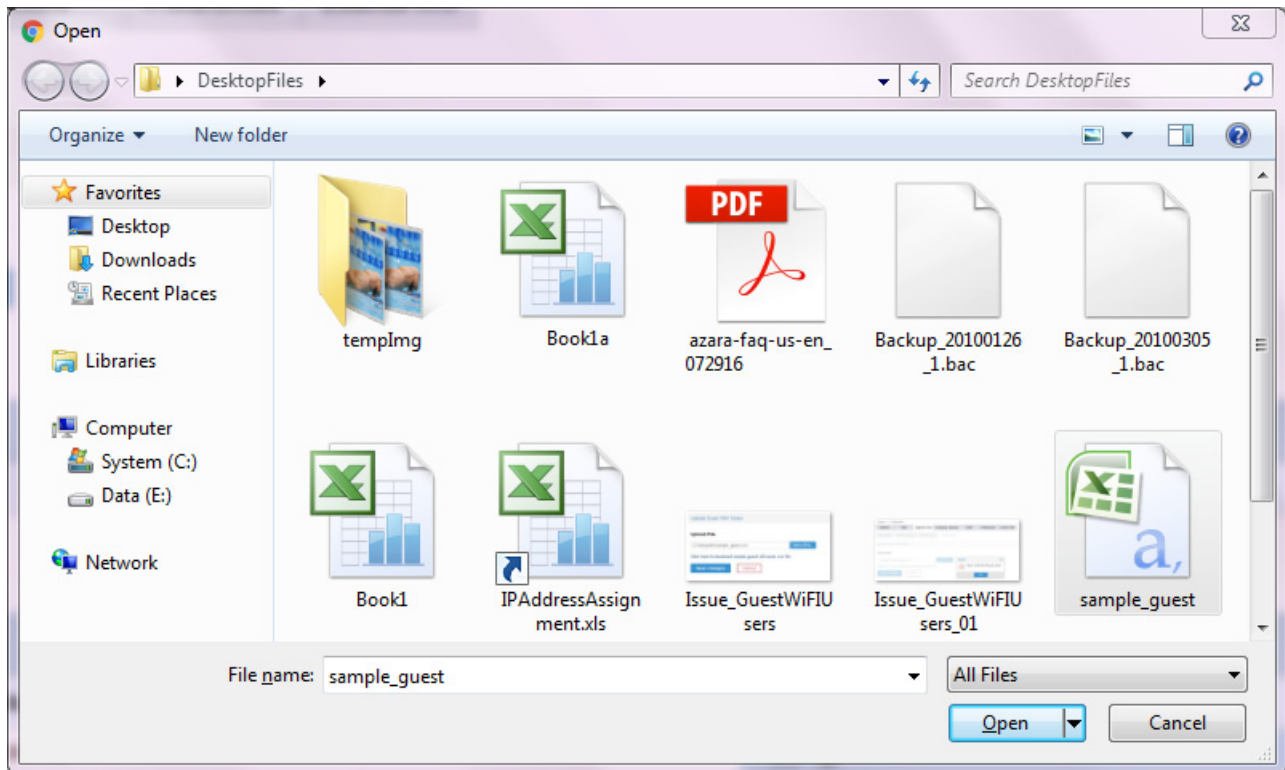


Figure 1-101 Configuration - Captive Portal - Templates - Add Logo screen

4. Review the **Splash Pages** section for an overview of existing Site to Template mappings.

<p>Name</p>	<p>Displays the name of the Splash Page configuration associating a site with a pre-defined or customized splash template.</p> <p>Since a guest user is first served a splash page when accessing a Wi-Fi site (captive portal), each site within your domain must have a splash page associated with it. By default, the system automatically maps all sites to a default built-in splash page configuration named <i>All Sites</i>. This indicates that all captive portal sites for this Tenant will use the default Azara applied template.</p>
<p>Sites</p>	<p>Displays the name of the captive portal site associated with the Splash Page configuration. If the value is <i>System</i>, it indicates all sites for this Tenant use the template defined in the <i>Template</i> field.</p>
<p>Template</p>	<p>Displays the name of the template mapped to the captive portal site.</p>
<p>Action</p>	<p>Displays icons for the actions available on this splash page configuration. The actions are <i>edit</i>, <i>delete</i> or <i>preview</i> the selected splash page configuration.</p> <p>Note: The <i>All Sites</i> splash page, being a built-in splash page configuration, cannot be deleted. However, you can edit it and replace the default template (<i>Clickthrough</i>) with another pre-defined or user defined template.</p>




5. To add a new Splash Page configuration, select the  icon located to the right of the **Splash Pages** bar. The following screen displays:


Figure 1-102 Configuration - Captive Portal - Templates - Add Splash Pages

Name	Enter an appropriate name for this new Splash Page entry. This is a mandatory field.
Site	Select a site from the drop-down menu available. The drop-down menu is populated only if the Tenant's account has sites not yet mapped to a splash template.
Splash Templates	<p>Select a template from those available in the <i>Splash Templates</i> section. Note, only those templates in the published state display. Templates in the <i>drafted</i> state cannot be associated with a site and are not listed.</p> <p>This section is divided into the following:</p> <ul style="list-style-type: none"> • <i>Tenant Designated Templates</i> – Expand this section to view a list of all templates created by the Tenant. • <i>Default Templates</i> – Expand this section to view all templates provided by Azara. You can use these templates as a base from customizing and creating your templates. <p>Splash template creation and publication is described latter in this section.</p>
Save Changes	Select to save the new splash pages configuration.
Cancel	Select to exit without saving changes.

- To edit an existing Splash Page entry, select the icon to open the splash page in the edit mode. Modify the configuration (name, site and/or the associated splash template) and select **Save Changes** to save and exit the screen, or **Cancel** to exit screen without saving changes.
- To delete an existing Splash Page entry, select the icon located to its extreme right. The selected splash page entry is removed from the list of splash pages. Default templates and the *All Sites* splash page cannot be deleted.

8. To preview an existing Splash Page entry, select the  icon. The selected the splash page opens in the preview mode.
9. To create a duplicate of an existing Splash Page entry or a default template, select the  icon.
10. Review the **Templates** section to get an overview of existing templates and their status. This section displays built-in as well as customized templates. The Azara cloud service provides the following non-editable, built-in templates: *Jumbo*, *Clickthrough*, *Email Self Registration*, *SMS Based Registration*, and *Social Logins*. Use these default templates as a base for your customized templates.

Name	Displays the name of the splash template.
Status	<p>Displays the splash template's status: <i>Drafted</i> or <i>Published</i>.</p> <ul style="list-style-type: none"> • <i>Drafted</i> – A drafted template is one that is being modified and not yet ready to be associated with a site in a splash page configuration. • <i>Published</i> – A published template is one that is complete in all respects and can be associated with a site to create a splash page configuration. <p>Azara built-in templates are in the published state and can be associated with sites. These templates are non-editable, but can be duplicated before being edited and saved under a different name.</p>
Action	<p>Displays icons for actions that can be performed on this splash template configuration. The actions are <i>edit</i>, <i>delete</i>, <i>duplicate</i> or <i>preview</i> the selected splash template.</p> <p>Note: The default templates do not have options to delete or edit them.</p>

11. To add a new splash template entry, click the  icon located to the right of the **Templates** bar. The following screen displays:

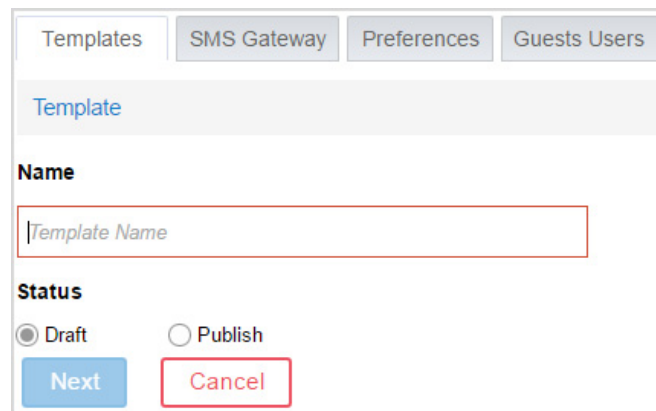


Figure 1-103 Configuration - Captive Portal - Templates - Add Splash Template

Name	Enter an appropriate name for this new template.
Status	<p>Select the status. The options are:</p> <ul style="list-style-type: none"> • <i>Drafted</i> – A drafted template is one that is being modified and not ready to be associated with a site in a splash page configuration. • <i>Published</i> – A published template is one that is complete in all respects and can be associated with a site to create a splash page configuration. When creating a new splash page configuration (Step 4), only published templates are listed in the Splash Templates section.

Next	Select to save the new splash template configuration and move to the next step in creating the template. On selecting <i>Next</i> the newly created template opens in the edit mode. Customize the template as per your requirement using the options provided. For more information on customizing the splash template, see Customizing Splash Templates on page 1-112 .
Cancel	Select to exit without saving the new template.

Customizing Splash Templates

Page Settings

Before inserting the splash page elements (text, images, login forms, buttons, etc.) you can modify the splash template's page settings by changing the background color, or inserting a background image. These page settings apply to all three Captive Portal templates, namely: *Splash*, *Success* and *Failure*.

- To modify page settings, select **Page Setting** button located to the right of the *Template* name bar. The page settings edit options are displayed.

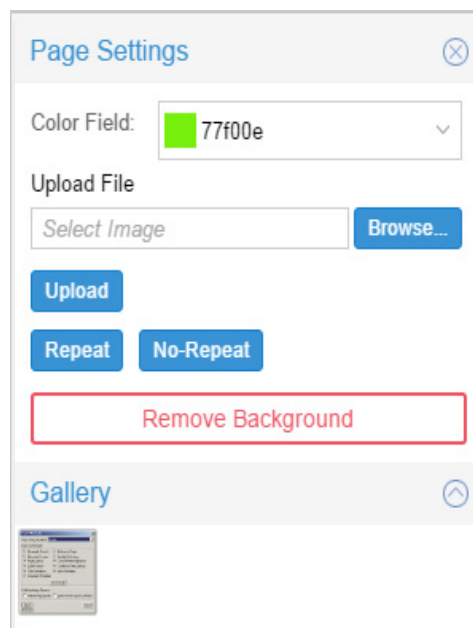


Figure 1-104 Configuration - Captive Portal - Templates - Add Splash Template - Edit Page Settings

- Use the built-in color palette to select the background color of the splash template page. This background color can be viewed only in the **Preview** mode.
- To insert a new background image, select **Browse**, navigate to the location (on your local system) of the required image file, and select the image file. The full path and file name of the background image file is displayed in the **Select Image** field. Select **Upload**. The selected image is uploaded as the background image for the site.

If the image is small and does not cover the entire page, use the **Repeat** button to force the system to repeat the image as multiple tiles in the background. Use the **No-Repeat** button to prevent the system from displaying the background image as a tile of images. This background image can only be viewed in the **Preview** mode. A thumbnail of the uploaded image is also added to the **Gallery** section. Multiple images can be uploaded to the Azara cloud service, however, only one image can be used as a background image at a time.

- To revert to default page settings, select **Remove Background**.

After modifying the template's page settings, proceed with inserting sections, text, image, buttons, etc.

- Define the template's sections (that is the general page layout) using one of the two options provided under the **Select Theme** area. These options are: **Themes** and **Modules**.

The **Themes** area provides a set of built-in themes for different page layouts. The following image shows the *Theme Column 2* option highlighted. Select the section layout appropriate for your use.

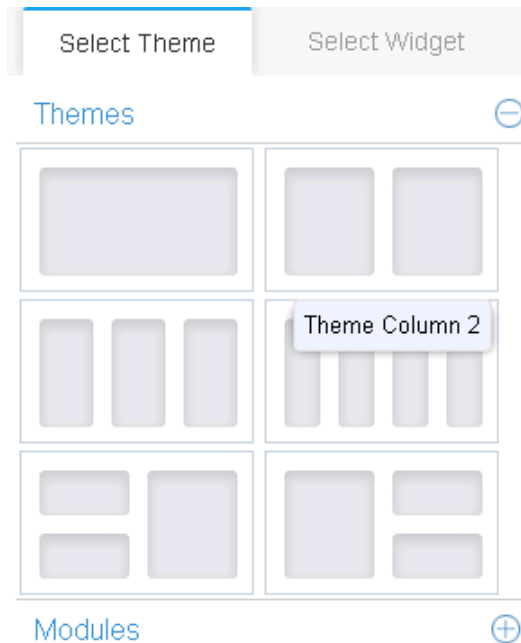


Figure 1-105 Configuration - Captive Portal - Templates - Add Splash Template - Select Themes

- To add a built-in theme, from the right-hand **Themes** pane drag and drop the desired theme on to the blank left-hand area. The following image shows the *Theme Column 2* option applied to the template.

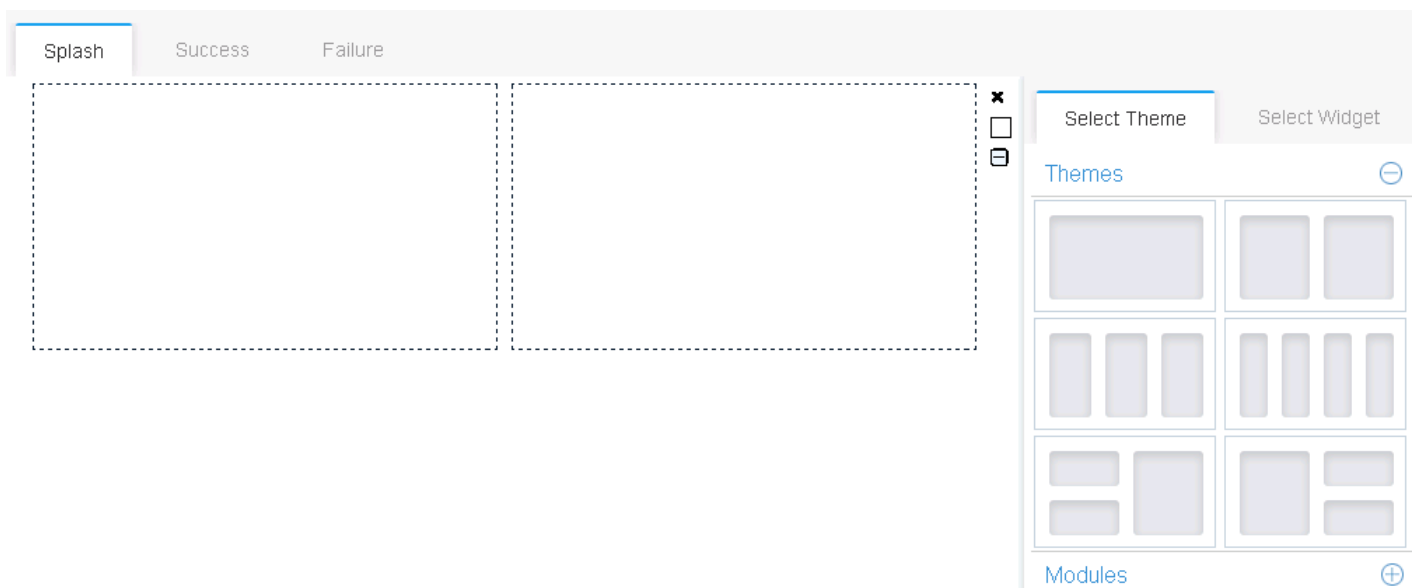




Figure 1-106 Configuration - Captive Portal - Templates - Add Splash Template - Sections - Drag-Drop Theme

Depending on the theme selected, the page is divided into sections. The height of these sections can be adjusted by clicking and dragging the top/bottom margins. The *Theme Column 2* option divides the splash page template into two sections.

- Next, click the **Select Widget** tab and drag and drop a widget in each section. Seven built-in widget types are available: *Text*, *Image*, *Button*, *Login Button*, *HTML*, *Login Form* and *Policies*.

Widgets can be only placed within a section. When dragging and dropping a widget, the  icon (on the top of the selected widget) indicates the selected location is correct, and when dropped the widget smoothly fits in to

the section. On the other hand, the  icon indicates that the selected widget location is incorrect. Further, each section can contain only one widget.

The following image shows a *Text* and an *Image* widget inserted in the two sections.

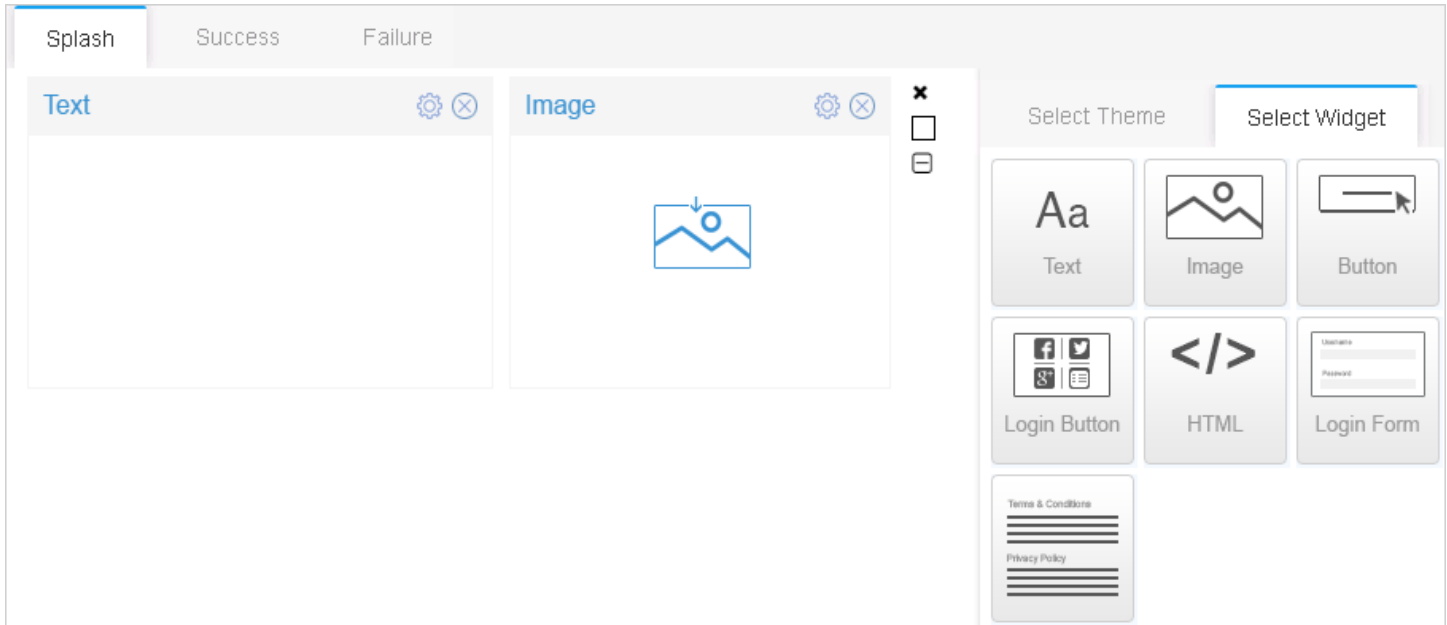



Figure 1-107 Configuration - Captive Portal - Templates - Add Splash Template - Widgets - Drag-Drop Widgets

19. Select the  icon, located to the right of each widget bar, to open the widget in the edit mode. For more information on customizing widgets, see [Customizing Widgets on page 1-115](#).
20. Azara provides a set of pre-configured modules to use as a base for customizing your pages. Expand the **Modules** area to view a list of these modules. Select an appropriate module and drag it to the template area to apply the module's layout. and widgets. You can combine templates from **Modules** and **Sections** to customize your templates.

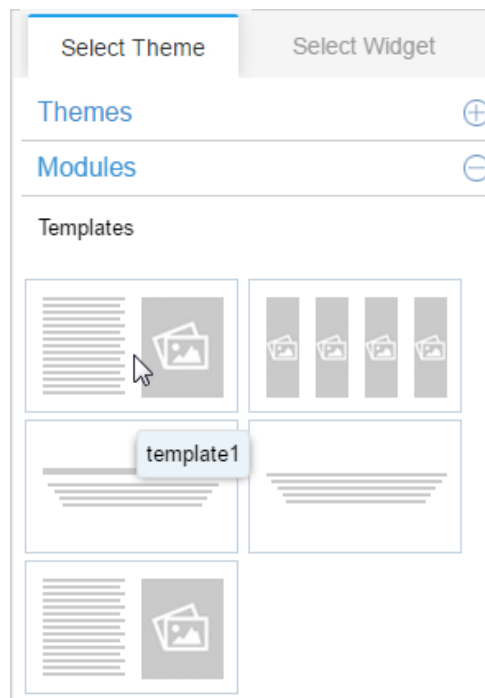


Figure 1-108 Configuration - Captive Portal - Templates - Add Splash Template - Sections - Drag-Drop Theme

Each template has a fixed layout that cannot be modified. However, you can modify the content inserted within the section. For example, *template1* divides the page into two sections, one for text and the other for images as shown in the following:

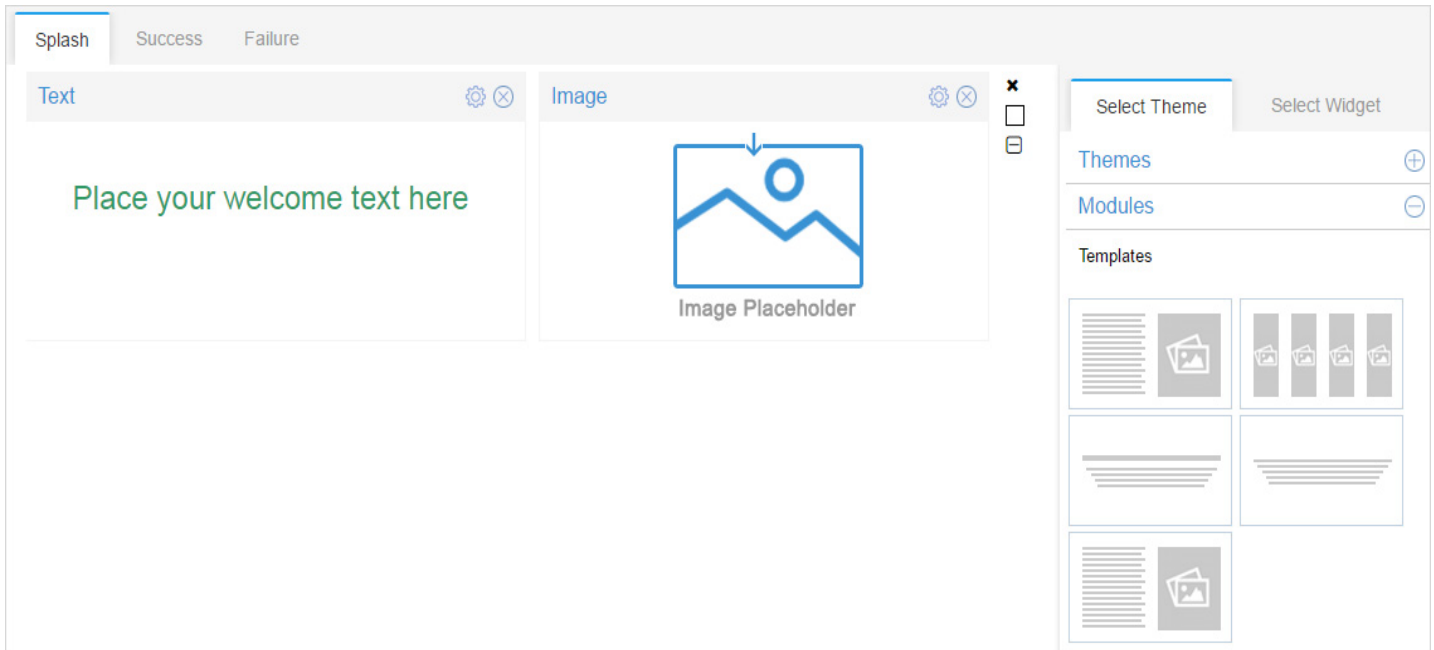





Figure 1-109 Configuration - Captive Portal - Templates - Add Splash Template - Sections - Drag-Drop Modules

21. After inserting a template, select the  icon located to the right of each section bar to open it in the edit mode. Make the necessary changes to the text and/or image. For more information on customizing widgets, see [Customizing Widgets on page 1-115](#).
22. To remove a pre-defined module template section, select the  icon located to right of the section. The pre-defined widget is removed. You can now plug-in a widget from those available in the **Select Widget** tab and customize the widget.

Customizing Widgets

Text Widget

23. To customize a *Text* widget, select the  icon, located to the right of the widget bar. The widget opens in the edit mode as shown:

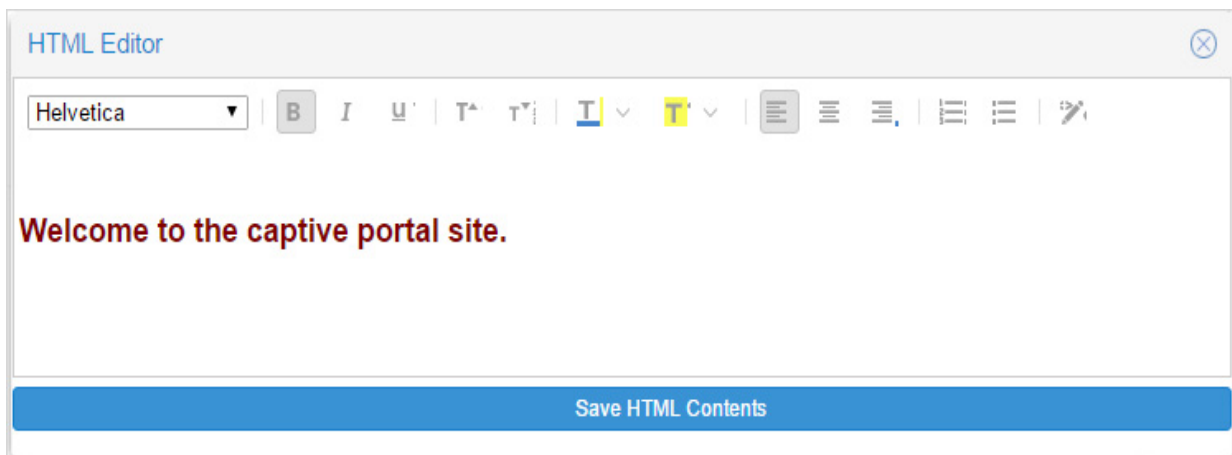



Figure 1-110 Configuration - Captive Portal - Templates - Add Splash Template - Widgets - Edit Text Widgets

24. Enter the text to display on the splash page.

25. After inserting text, customize the font type (Arial, Courier New, etc.), style (bold, underlined, or italics), size, color, alignment (Left, center or right).
26. To convert text to a hyper link, select the text and select the  icon. The following window is displayed:

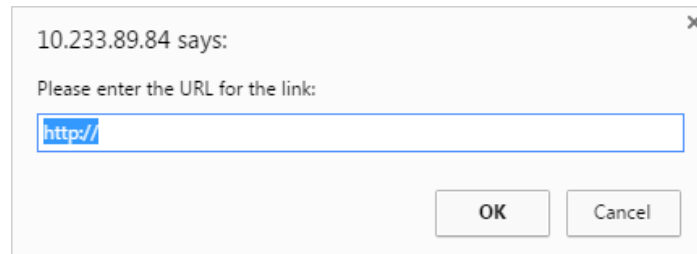



Figure 1-111 Configuration - Captive Portal - Templates - Edit Text Widgets - Convert to Hyper link

27. Enter the URL to which the hyper link points. Select **OK** to save and exit or select **Cancel** to exit without saving the URL details.
28. To save changes and exit the text widget edit mode, select **Save HTML Contents**.

Image Widget

29. To customize an *Image* widget, select the  icon to open the widget in the edit mode as shown in the following:

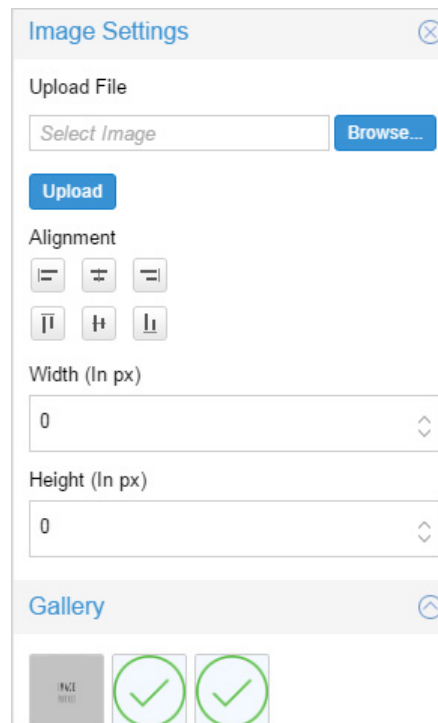


Figure 1-112 Configuration - Captive Portal - Templates - Edit Image Widgets

30. To insert a new image, select **Browse** and navigate to the location (on your local system) of the required image file. The image path and file name populates the **Select Image** field. Select **Upload**. The selected image is uploaded to the image widget area, and is added to the **Gallery** below.
31. To insert an image from the *Gallery*, drag and drop it into the blank image widget section.
32. After inserting the image, customize the image placement (within the image widget section) and size using the *Alignment*, *Width* and *Height* controls.

Terms and Conditions Widget

The following shows the default *Terms & Conditions* widget:

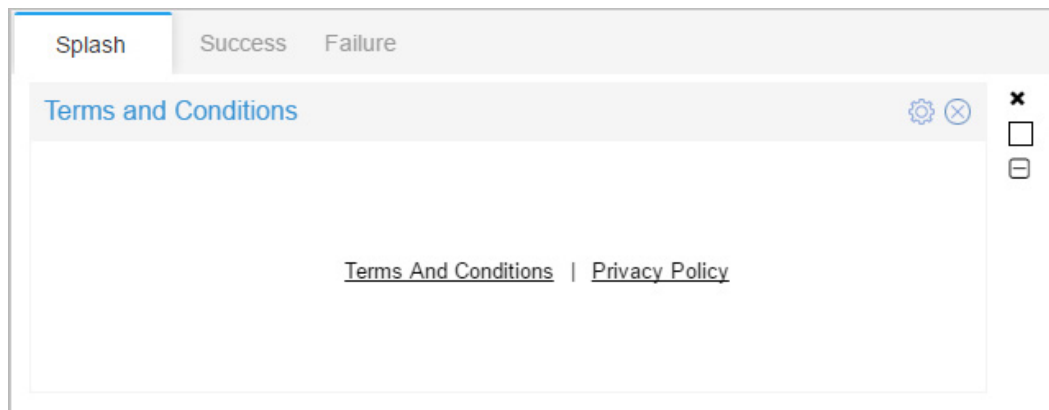



Figure 1-113 Configuration - Captive Portal - Templates - Default Terms & Conditions text

33. To customize the *Terms & Conditions* widget, select the  icon to open it in the edit mode.
34. In the **Policy Text Settings** pane modify the default *Terms And Conditions* text, *Privacy Policy* text, and/or the *Separator* text as shown in the following:

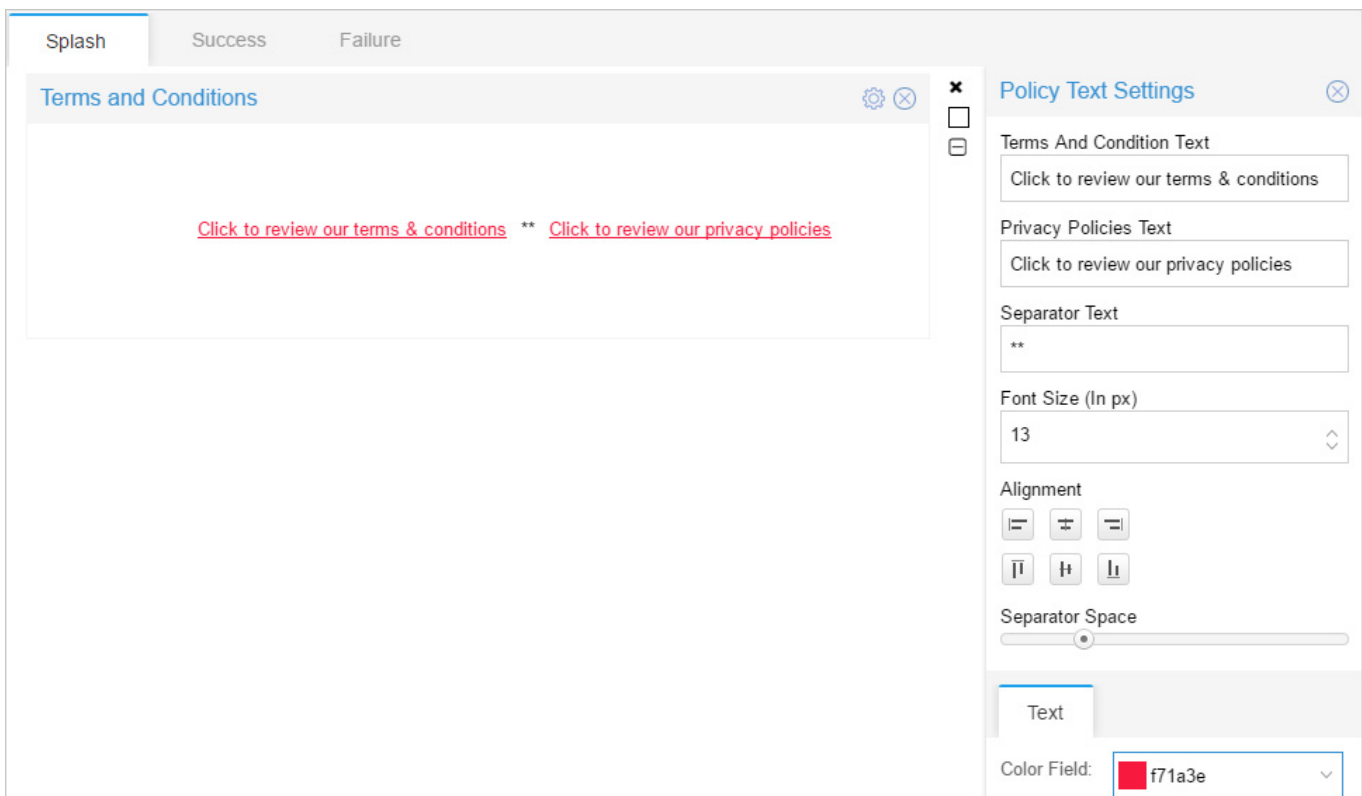



Figure 1-114 Configuration - Captive Portal - Templates - Edit Terms & Conditions Widgets

35. After modifying the text, customize the font type (Arial, Courier New, etc.), style (bold, underlined, or italics), size, color, alignment (Left, center or right), etc.

HTML Widget

The HTML widget allows you to design your Web page from scratch, without using any of the built-in, system provided sections, templates, or widgets.

36. To customize an *HTML* widget, select the  icon, located to the right of the widget bar. The widget opens in the edit mode as shown in the following:

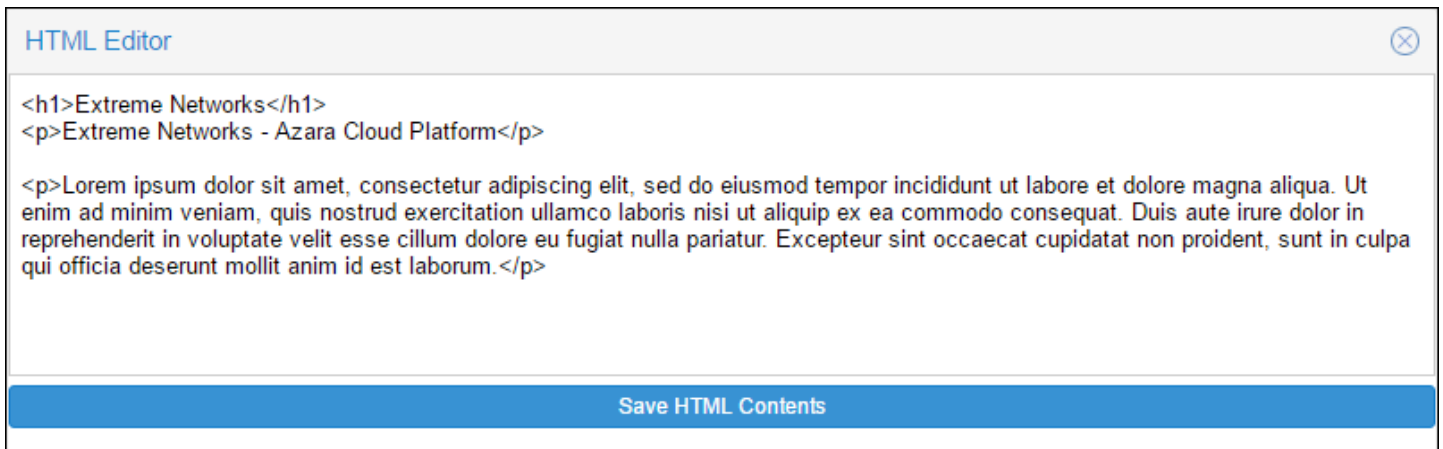


Figure 1-115 Configuration - Captive Portal - Templates - Edit HTML Widget

37. Enter the HTML code and select **Save HTML Contents**.


Button Widget

The Button widget allows a clickable Button, which when clicked navigates to pre-assigned URL.

The following screen shot shows the default *Button* widget:



Figure 1-116 Configuration - Captive Portal - Templates - Default Button Text

38. To customize a *Button* widget, select the  icon, located to the right of the widget bar. The widget opens in the edit mode as shown in the following:

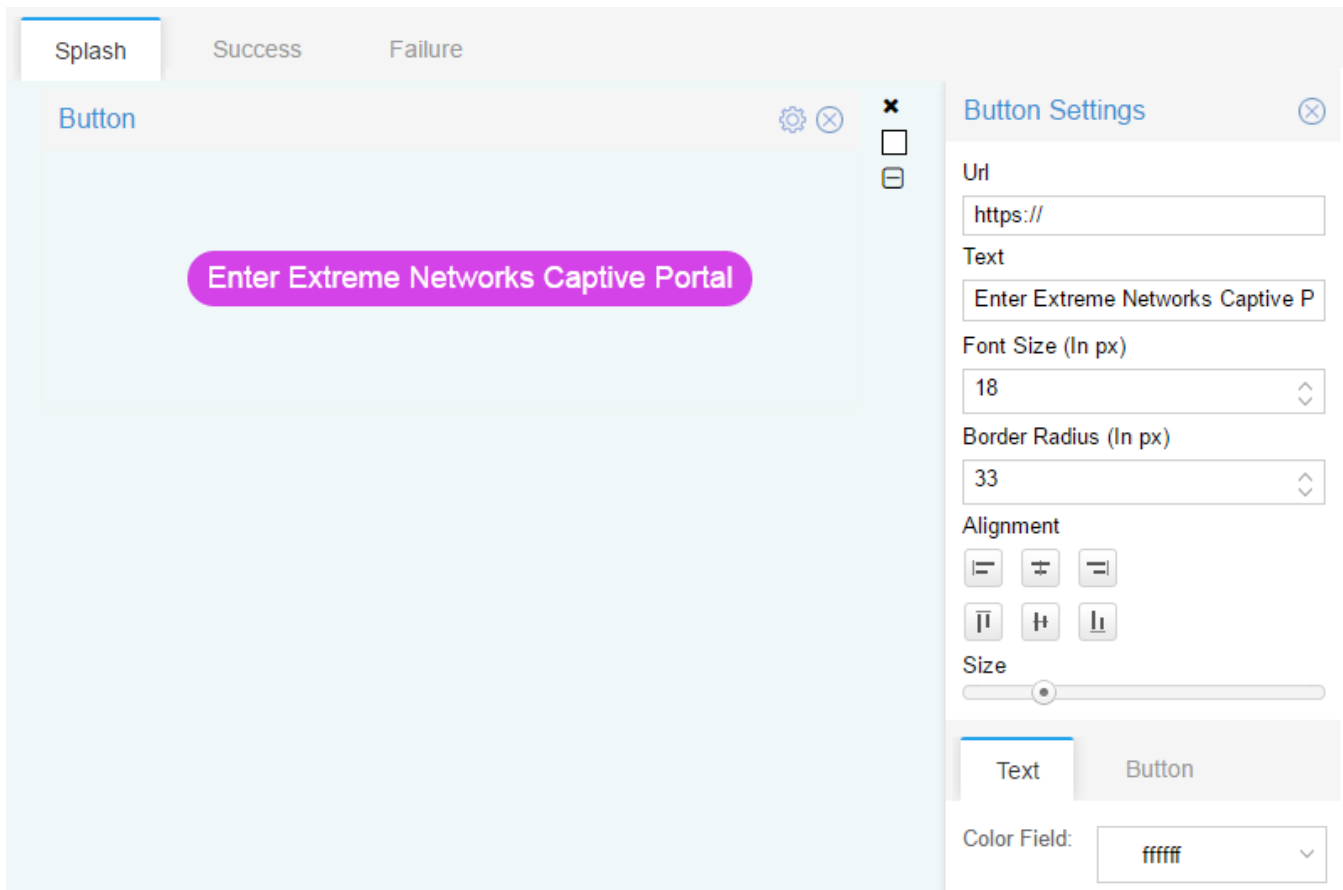


Figure 1-117 Configuration - Captive Portal - Templates - Edit Button Widget

39. In the **Button Settings** window, enter the destination site address in the **URL** field.
40. Modify the button text, if required, in the Text field.
41. Customize the button's text size, text color, border radius, alignment, size, and the background color.
42. To view the final Web page as it will appear to the user, select **Preview** located to the right of the Splash Page name bar.

Preview Option

The **Preview** option opens the template in the Preview mode, allowing you to preview how the page appears when viewed in a browser.

43. While customizing the splash template, use the **Preview** option located to the right of the Splash Page name bar to preview the final Web page.

The following image shows a text widget in the Preview mode.

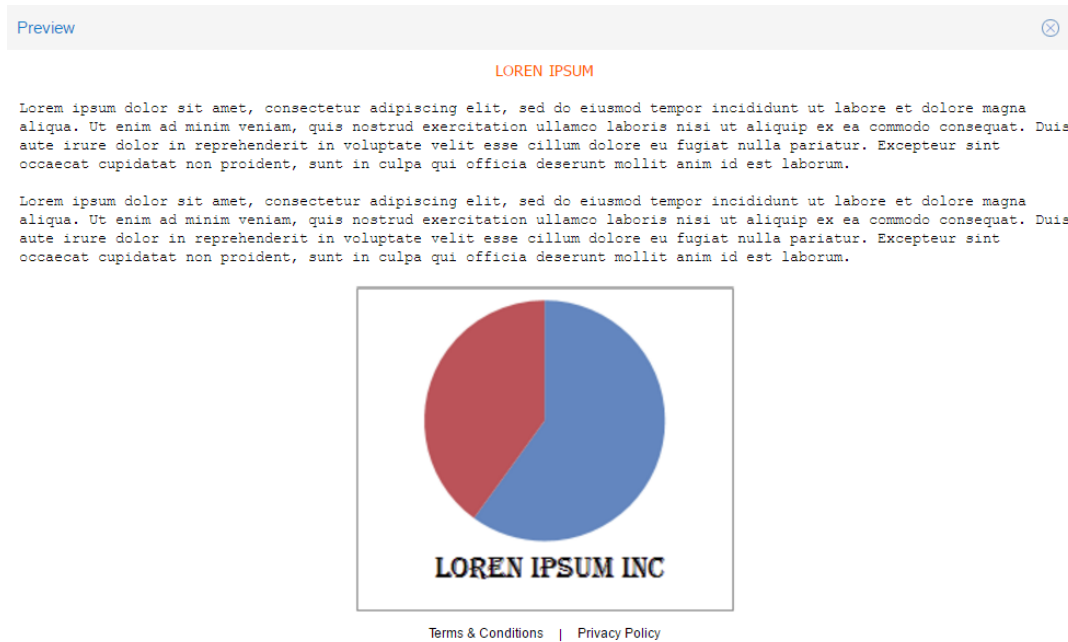






Figure 1-118 Configuration - Captive Portal - Templates - Preview - Text Widget

The following is a preview of a splash template showing a background image repeated (tiled) to cover the entire page:



Figure 1-119 Configuration - Captive Portal - Templates - Preview - Tiled Background Image

44. In preview mode, use the     icons to preview the created page as seen on different devices and orientation. The following viewing options are available:

- On large screen devices like laptops (960 px wide)
- On tablets and other wide screen devices (768 px wide)
- On mobiles with landscape orientation (568 px wide)
- On mobiles with portrait orientation (320 px wide)

The following is a preview of the above splash template as viewed on a mobile device in portrait mode:



Figure 1-120 Configuration - Captive Portal - Templates - Preview - Layout Changed

1.6.7.2 SMS Gateway

▶ Captive Portal

Azara uses *Short Message Service* (SMS) to send a registration code to guest users registering and agreeing to receive a *one time passcode* (OTP). OTP is only sent to the device used for accessing the Captive Portal. Azara sends the OTP to the device and the user uses this OTP to authenticate.

To review how to configure your network for device authentication using OPT, see [Registration on page 1-70](#).

Azara uses third-party SMS gateway service providers to provide the SMS OTP services. Once configured, these gateways allow Tenants to send SMSs to their guest users when registering. The Tenant must register the captive portals with these third-party service providers before using OTP based device registration.

1. From the **Configuration** menu, select **Captive Portal**.
2. Select the **SMS Gateway** tab. The following screen displays:

SMS Gateway +			
Name	Type	Status ↑	Action
Cdyne_Gateway_Active	cdyne	inactive	
Cdyne_Gateway_Backup	cdyne	active	

Figure 1-121 Configuration - Captive Portal - SMS Gateway

3. Review the existing **SMS Gateway** configurations to determine whether new configuration requires creation or an existing configuration requires modification or deletion.

Name	Displays the Gateway name. This is a user defined name to identify the SMS gateway service provider.
Type	Displays the gateway service provider for this SMS gateway.
Status	Displays the gateway's status. Only one SMS gateway can be active at a time.
Action	Displays icons for the actions that can be performed on this SMS gateway configuration. The options are <i>edit</i> and <i>delete</i> .

4. To add a new SMS Gateway configuration, select the icon located to the right of the **SMS Gateway** bar. The following screen displays:

Add New SMS Gateway

Name

Gateway Type

Status
 Active

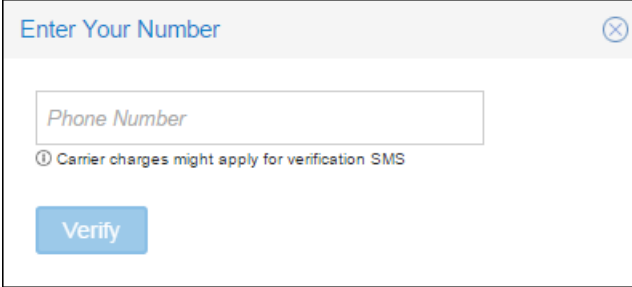
Account Details
[How to get the API details for My Clickatell Account?](#)

Figure 1-122 Configuration - Captive Portal - SMS Gateway - Add SMS Gateway

5. Enter the following information as required:

Name	Provide a unique name for the new SMS gateway configuration. This name is used to distinguish the SMS gateway service provider.
Gateway Type	Select the SMS gateway provider. Azara uses third-party SMS gateway service providers to provide the SMS OTP services. Select from one of the service providers in this drop-down list.
Status	Select the Active checkbox to enable the gateway. Only one SMS gateway can be set as <i>Active</i> at any time. OTP SMSs are only sent through an active SMS gateway.
Account Details	Provide configuration information received from the third-party SMS gateway service provider. Each service provider has a different registration process for their service. The fields in this area change according to the information required by the SMS gateway service provider selected in the <i>Gateway Type</i> field. <ul style="list-style-type: none"> • How to get the API details for My <SMS Gateway Service Provider> Account? – Select to navigate to the selected SMS Gateway service provider’s web site. Use the instructions provided on the web site to create an account or to obtain the information required to provide the SMS OTP service to guest users.

6. Once you have configured the SMS gateway information, select the **Verify** button. The following screen displays.



The screenshot shows a dialog box titled "Enter Your Number" with a close button in the top right corner. Inside the dialog, there is a text input field with the placeholder text "Phone Number". Below the input field, there is a warning icon (a circle with an exclamation mark) followed by the text "Carrier charges might apply for verification SMS". At the bottom of the dialog, there is a blue button labeled "Verify".

Figure 1-123 Configuration - Captive Portal - SMS Gateway - Verify SMS Gateway

7. Verify the configuration by entering a valid phone number and selecting **Verify**. If configured properly, depending on the service provider, you will either receive a test SMS from the service provider or a message is displayed about the validity of the supplied credentials.
8. Select **Save Changes** to save the new SMS gateway configuration details and exit. Select **Cancel** to exit without saving the changes.

1.6.7.3 Preferences

▶ *Captive Portal*

Use the *Preferences* tab to configure Captive Portal preferences such as the content to display for the Terms and Conditions & Privacy pages and to globally configure the application IDs and secrets for use for authenticating with Social Apps such as Google Plus™, Twitter™ and Facebook™.

To configure Captive Portal preferences:

1. From the **Configuration** menu item, select **Captive Portal**.
2. Select **Preferences** to display the preferences screen. The **Preferences** screen displays the **Terms And Conditions** section by default.

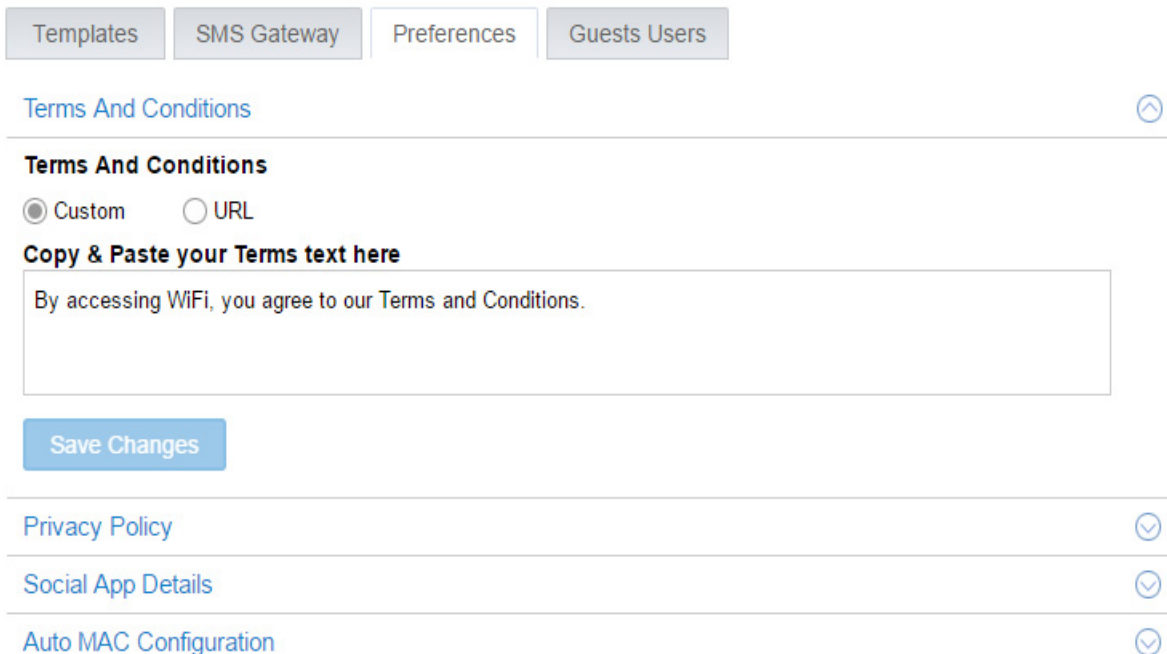



Figure 1-124 Configuration - Captive Portal - Preferences tab

Use the **Terms And Conditions** fields to either configure the custom message to be displayed or the external link to be displayed when the user logs on to the Captive Portal. These messages are displayed when the user selects the **Terms and Conditions** link on the Splash screen, the Success screen or the Failure screen.

Refer to the following for more information:


<p>Custom</p>	<p>Select this option to provide a custom Terms and Conditions message that is displayed when the user logs on to the captive portal. This option is selected by default.</p>
<p>Copy & Paste your terms text here</p>	<p>Use this area to configure the Terms and Conditions message to be displayed to the user after successfully logging into the Captive Portal. A Terms and Conditions message for Azara is provided by default. Change the content of this field to match your requirement.</p> <p>This message is displayed when the user selects the Terms and Conditions link on the Splash screen, the Success screen or the Failure screen.</p>


URL	Select this option to provide an external URL which will be displayed when the user successfully logs on to the Captive Portal. The contents of the URL is displayed when the user selects the Terms and Conditions link on the Splash screen, the Success screen or the Failure screen.
External URL	This field is only displayed when <i>URL</i> is selected. Enter the complete path to the page that contains the Terms and Conditions to be displayed when the user successfully logs on to the Captive portal. The contents of the external URL is displayed when the user selects the Terms and Conditions link on the Splash screen, the Success screen or the Failure screen.
Save Changes	Select this button to save changes made to this section of Captive Portal Preferences.

3. Select the  icon to the right of the **Privacy Policy** field to expand it.

Use the **Privacy Policy** fields to either configure the custom message to be displayed or the external link to be displayed when the user logs on to the Captive Portal to inform the user about the Captive Portal's Privacy Policy.

Templates
SMS Gateway
Preferences
Guests Users

[Terms And Conditions](#) 

[Privacy Policy](#) 


Privacy Policy

Custom URL

Copy & Paste your Privacy Policy text here

By accessing WiFi, you agree to our Privacy Policy.

Save Changes

[Social App Details](#) 



[Auto MAC Configuration](#) 

Figure 1-125 Configuration - Captive Portal - Preferences tab - Privacy Policy

Refer to the following for more information:

Custom	Select this option to provide a custom Privacy Policy message that is displayed when the user logs on to the captive portal. This option is selected by default.
Copy & Paste your Privacy Policy text here	Use this area to configure the Privacy Policy message to be displayed to the user after successfully logging into the Captive Portal. A Privacy Policy message for Azara is provided by default. Change the content of this field to match your requirement.


URL	Select this option to provide an external URL which will be displayed for the Privacy Policy when the user successfully logs on to the Captive Portal.
External URL	This field is only displayed when <i>URL</i> is selected. Enter the complete path to the page that contains the Privacy Policy to be displayed when the user successfully logs on to the Captive portal.
Save Changes	Select this button to save changes made to this section of Captive Portal Preferences.


4. Select the  icon to the right of the **Social App Details** field to expand it.


Use the **Social App Details** fields to provide application IDs and secrets for using Social Apps like Twitter™, Facebook™ and Google Plus™ in the Captive Portal for authenticating the captive portal user.

You must have the application ID and the application secret that you received from these service providers before you can enable this feature in the Captive Portal.

Templates
SMS Gateway
Preferences
Guests Users

Terms And Conditions


Privacy Policy


Social App Details


Facebook
[How to get the My Facebook App details?](#)

APP ID

APP Secret

Twitter
[How to get My Twitter App details?](#)

APP ID

APP Secret

Google Plus
[How to get My Google Plus App details?](#)

APP ID

APP Secret

Save Changes


MAC Auth Configuration


Figure 1-126 Configuration - Captive Portal - Preferences - Social App Details

Refer to the following for more information:

<p>Facebook</p>	<p>Facebook Social App integration enables your users to use their Facebook™ credentials to login to the captive portal.</p> <ul style="list-style-type: none"> • <i>APP ID</i> – The application ID received when registering the Captive Portal as an authentication user with Facebook™. • <i>APP Secret</i> – The secret received from Facebook™ to be used when a user tries to login to the Captive Portal using Facebook™ credentials. <p>Note: Use the <i>How to get the My Facebook App details?</i> link to learn how to get more information about using Facebook™ credentials for authenticating captive portal users.</p>
<p>Twitter</p>	<p>Twitter Social App integration enables your users to use their Twitter™ credentials to login to the captive portal.</p> <ul style="list-style-type: none"> • <i>APP ID</i> – The application ID received when registering the Captive Portal as an authentication user with Twitter™. • <i>APP Secret</i> – The secret received from Twitter™ to be used when a user tries to login to the Captive Portal using Twitter™ credentials. <p>Note: Use the <i>How to get My Twitter App details?</i> link to learn how to get more information about using Twitter™ credentials for authenticating captive portal users.</p>
<p>Google Plus</p>	<p>Google Plus Social App integration enables your users to use their Google Plus™ credentials to login to the captive portal.</p> <ul style="list-style-type: none"> • <i>APP ID</i> – The application ID received when registering the Captive Portal as an authentication user with Google™. • <i>APP Secret</i> – The secret received from Google™ to be used when a user tries to login to the Captive Portal using Google Plus™ credentials. <p>Note: Use the <i>How to get My Google Plus App details?</i> link to learn how to get more information about using Google Plus™ credentials for authenticating captive portal users.</p>
<p>Save Changes</p>	<p>Select this button to save changes made to this section of Captive Portal Preferences.</p>

5. Select the  icon to the right of the **MAC Auth Configuration** field to expand it.

Use the **MAC Auth Configuration** fields to set the number of days the MAC address of a device – used by a captive portal user and authenticated using any of the Social Apps – is retained in the Azara database.

When a user accesses the captive portal using a device, the MAC address of which is available in the Azara database, the user is automatically authenticated and is immediately granted access without further authentication processes.

Templates
SMS Gateway
Preferences
Guests Users

Terms And Conditions ⌵

Privacy Policy ⌵

Social App Details ⌵

MAC Auth Configuration ⌴

MAC Auth Configuration

Enable Disable

MAC Auth Duration(days)

30 ⌵

Save Changes

Figure 1-127 Configuration - Captive Portal - Preferences - MAC Auth Configurations

Refer to the following for more information:

MAC Auth Configuration	Use this option to control storing of Captive Portal user device MAC address in the Azara database for quicker authentication. <ul style="list-style-type: none"> • <i>Enable</i> – Select to enable this feature. • <i>Disable</i> – Select to disable this feature. This is the default.
MAC Auth Duration (days)	Set the number of days a Captive Portal user device’s MAC address is stored and retained in Azara database to enable a returning device faster access. Use the spinner control to set the number of days. The default value is 30 days. At the end of 30 days of the device’s MAC address being added to the Azara database, the entry is removed and the device is forced to re-authenticate.

6. Select **Save Changes** to save the Captive Portal preferences and exit.

1.6.7.4 Guest Users

▶ *Captive Portal*

Use the *Guest Users* tab to pre-configure a list of guest user accounts authorised to use the Captive Portal. User accounts can be created for repeated use in scenarios where the tenant administrators prefer the traditional user based authentication instead over social app integrated authentication.

1. From the **Configuration** menu item, select **Captive Portal**.
2. Select **Guest Users** to display the *Guest WiFi Users* screen. The screen displays a list of users already configured for this Captive Portal.

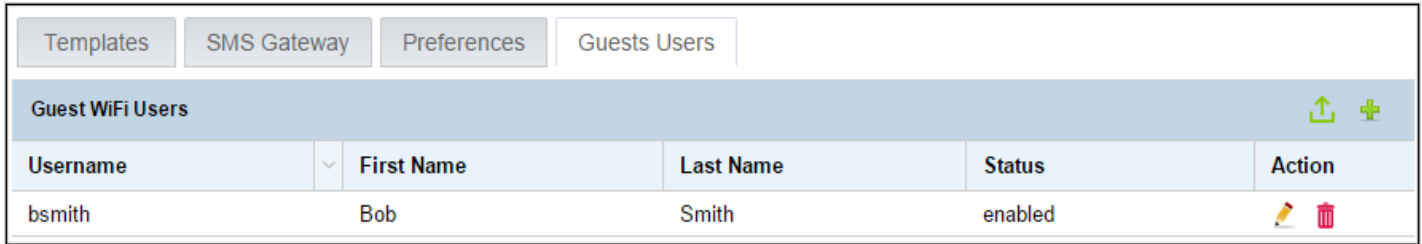


Figure 1-128 Configuration - Captive Portal - Guest Users - Guest WiFi Users

The Guest Users screen enables you to create a list of pre-approved users offline in a .csv (comma separated value) file and upload it. Use the icon to upload a file containing the list of guest user account details. The following screen displays.

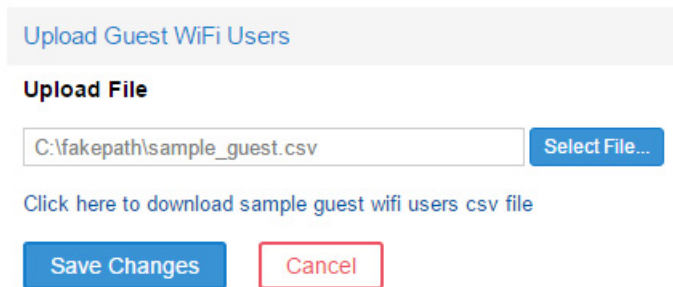


Figure 1-129 Configuration - Captive Portal - Guest Users - Upload Guest User CSV File

Use the **Select File...** button to open the operating system's file navigation window and use it to search for and locate your .csv file to upload. Select **Save Changes** button to upload and import your pre-approved guest user accounts. Use the **Click here to download sample guest wifi users csv file** link to download a sample file which can be used as a template to create your guest users file.

The Guest WiFi Users screen displays the following information:

Username	Displays the login name for this guest user account.
First Name	Displays the first name assigned to this guest user account.
Last Name	Displays the last name assigned to this guest user account.
Status	Displays the status of this account. Displays <i>Disabled</i> when the account is not available for use. Displays <i>Enabled</i> otherwise.
Action	Use the icon to delete a guest user. Use the icon to edit the guest user details.

Use the icon to the right to add a guest user to this list. The following screen displays:

Guest WiFi Users

Username

Password

Status
 Enable Disable



Additional Details 

Figure 1-130 Configuration - Captive Portal - Guest Users - Add User

Username	Enter a user name for this guest user account
Password	Enter a password for this guest user account.
Status	Select the status of this account when the account is created. Select <i>Disable</i> to create the account but not use it immediately. Select <i>Enable</i> to create the account and use it immediately.

3. Use the **Additional Details** fields to provide additional information for this guest user account. Select the  icon to expand this area. All fields in this area are optional.

Additional Details

First Name

Last Name

Email

Mobile No.

Expiry Date (GMT)

Figure 1-131 Configuration - Captive Portal - Guest Users - Add - Additional Details

First Name	Enter the first name for this guest user account.
Last Name	Enter the last name for this guest user account.
Email	Enter a contact e-mail for this guest user account
Mobile No.	Enter a valid mobile phone number for this guest user account

Expiry Date (GMT)	<p>Enter a valid date on which this account is disabled. The account is only active till this date. Select the expiry date from the following options:</p> <ul style="list-style-type: none">• <i>Today</i> – Sets the expiry date of this account to end of day today.• <i>Tomorrow</i> – Sets the expiry date of this account to end of day tomorrow.• <i>Week</i> – Sets the expiry date of this account to the end of the current week.• <i>This month</i> – Sets the expiry date of this account to the end of the current month. For example, if the account was created on 15th of the month, the account will be disable at the end of the last day of the current month.• <i>This year</i> – Sets the expiry date of this account to the end of the current month. For example, if the account was created any time during the year, the account will be disable at the end of the last day of the current year (31st December of the current year).• <i>Custom</i> – Select this option and set a date to set the expiry date of this account to a particular date.
--------------------------	--

4. Select **Save Changes** to save the new guest user details and exit. Select **Cancel** to exit without saving the changes made to this screen.

APPENDIX A

CUSTOMER SUPPORT

Customer Support

Customer support can be obtained through e-mail or through telephone within the time limits set forth in the support agreements.

When contacting customer support, please provide the following information:

- *Company Name*
- *Contact First and Last Name*
- *Contact Phone Number*
- *Contact E-mail*
- *Contact Mailing Address*
- *Azara Account Number*
- *Problem Description*

Support for Azara is available 24/7, 365 days a year only after the tenant account has been provisioned for the first time. Also, a customer must have an active Azara account for us to provide technical support via phone or e-mail.

Customer Support Through Phone

Azara customer support phone numbers are:

- Within the US: **1-800-653-5350**
- Outside the US: **011-302-444-9700**

Standard Support hours for North America are 8:00 AM to 8:00 PM Eastern. Support during Standard Support hours is available in **English** and **Spanish**.

After Support hours for North America are 8:00 PM to 8:00AM Eastern. Support during After Support hours is available in **English** only.

Extreme Networks's technical support representative will open a support request and begin steps to resolve the issue.

Customer Support Through E-mail

Azara customer support through e-mail is available through your Azara account. To obtain support via e-mail, login to your Azara web interface and click the **Contact Us** e-mail icon located in the top right corner of the user interface.

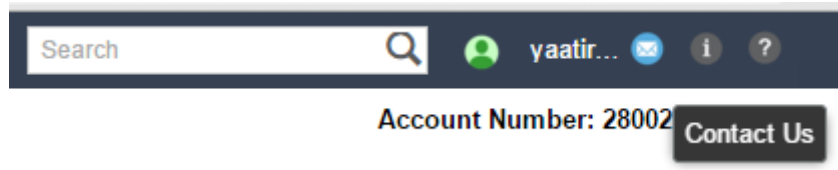


Figure A-1 *Contact Us Via Email*

Fill up the form, and if required, attach any documents and send.

Extreme Networks's technical support representative will open a support request and begin steps to resolve the issue.

