



ExtremeLocation™ Essentials Configuration Guide

9037974-00 Rev AA
November 2023



Copyright © 2023 Extreme Networks, Inc. All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses.

End-user license agreements and open source declarations can be found at: <https://www.extremenetworks.com/support/policies/open-source-declaration/>



Table of Contents

Preface.....	4
Text Conventions.....	4
Documentation and Training.....	5
Open Source Declarations.....	6
Training.....	6
Help and Support.....	6
Subscribe to Product Announcements.....	7
Send Feedback.....	7
About this Location Essentials Configuration Guide.....	8
ExtremeLocation Essentials Prerequisites and Limitations	8
Introduction to ExtremeLocation Essentials Configuration.....	9
Configure the ExtremeLocation Essentials Network Policy.....	10
Add the Device Template.....	10
Enable Sensor Mode.....	11
Enable iBeacon Services.....	12
Enable Presence Analytics Services.....	13
Place Access Points on the Floor Plan.....	13
Location Essentials Components.....	15
Enable ExtremeLocation Essentials.....	15
Create Engagement Categories.....	16
Assign Access Points to Engagement Categories.....	17
Create Regions.....	18
Configure Device Classification Rules.....	20
Configure Device Classification Thresholds	22
Configure the Location Essentials Dashboard.....	25
Create a Dashboard.....	25
Navigating the Dashboard.....	26



Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings






Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
screen displays	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words <i>enter</i> and <i>type</i>	When you see the word <i>enter</i> in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says <i>type</i> .
Key names	Key names are written in boldface, for example Ctrl or Esc . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
<i>Words in italicized type</i>	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
<i>italic text</i>	Italic text indicates variable content.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ x y z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member [member...]</i> .
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

[Current Product Documentation](#)

[Release Notes](#)

[Hardware and Software Compatibility](#) for Extreme Networks products

[Extreme Optics Compatibility](#)

[Other Resources](#) such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the [Open Source Declaration](#) page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the [Extreme Networks Training](#) page.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to [The Hub](#).
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



About this Location Essentials Configuration Guide

This guide consists of the following major sections:

- Network Policy Configuration
- Location Essentials Configuration
- Location Essentials Dashboard Configuration.

ExtremeLocation Essentials Prerequisites and Limitations

This document provides the information you need to configure the ExtremeLocation Essentials service.

For more information, see the following product documentation:

- [ExtremeCloud IQ](#)
- [ExtremeLocation Essentials User Guide](#)
- [ExtremeLocation Essentials Setup Guide](#)

You must be familiar with accessing and performing basic functions in ExtremeCloud IQ.

Before you begin, you need the following:

- Network Policies configured in ExtremeCloud IQ
- Access points adopted and assigned to the correct Network Policies.



Introduction to ExtremeLocation Essentials Configuration

The following workflow depicts interactions between ExtremeCloud IQ, ExtremeLocation Essentials and Wi-Fi clients.


- Use the ExtremeCloud IQ user interface (UI) to enable sensor mode and the ExtremeLocation Essentials service on APs
- The sensor radio on the AP begins to scan the Wi-Fi frequency spectrum
- As a WiFi device enters the coverage area, the sensor sees and reports it to the ExtremeLocation Essentials engine
- Based on configured classification rules, the ExtremeLocation Essentials engine classifies the Wi-Fi device as one of the following:
 - Visitor
 - Staff
 - Staff Personal Device.
- Classification Threshold values determine the status of a visitor as one of the following:
 - Outside
 - Inside Bounced
 - Inside Engaged Visitor.
- ExtremeCloud IQ assigns the Wi-Fi device to the region and category where the reporting sensor is mapped. The Wi-Fi device then displays on the Floor Plan view in the ExtremeLocation Essentials UI.

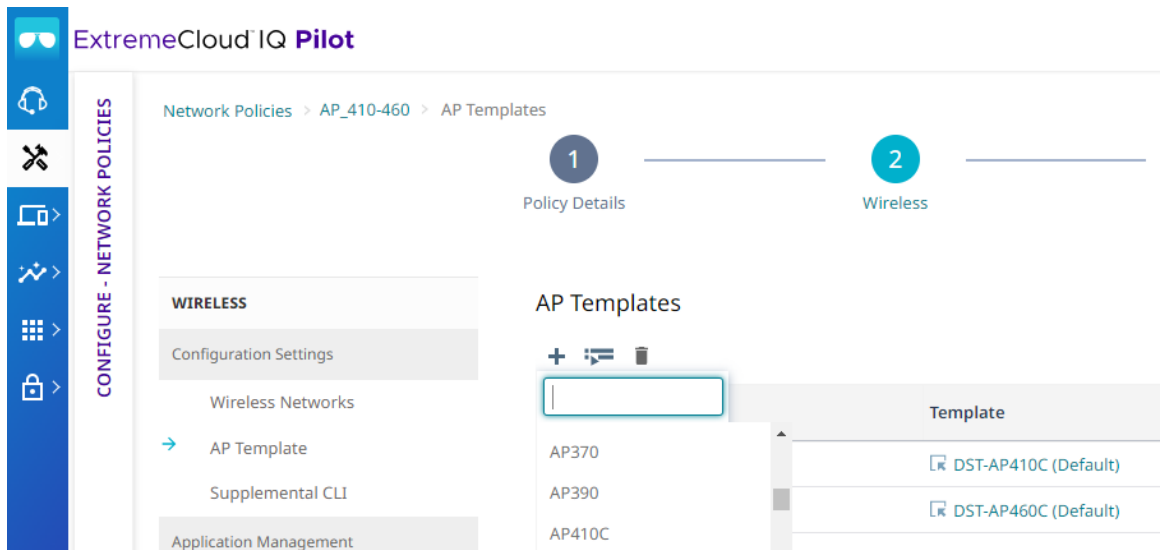
Configure the ExtremeLocation Essentials Network Policy

When configuring the ExtremeLocation Essentials network policy, you have two options. You can create a new network policy or use an existing network policy.

Add the Device Template

Perform these steps to log in to ExtremeCloud IQ and add a device template to the network policy.

1. Log into ExtremeCloud IQ.
2. In the main navigation bar, select .
3. Select **Network Policies**.
4. Select a network policy in use by a managed AP.
5. Select **Add Device Template**.
6. From the **Add Device Template** drop-down menu, select **Add AP Template**.
7. Select **+** to add an AP template to the network policy.
8. In the **Template Name** field, type a unique name.



ExtremeCloud IQ Pilot

Network Policies > AP_410-460 > AP Templates

1 Policy Details

2 Wireless

CONFIGURE - NETWORK POLICIES

WIRELESS

Configuration Settings

- Wireless Networks
- AP Template
- Supplemental CLI

Application Management

AP Templates

+ [wrench icon] [trash icon]

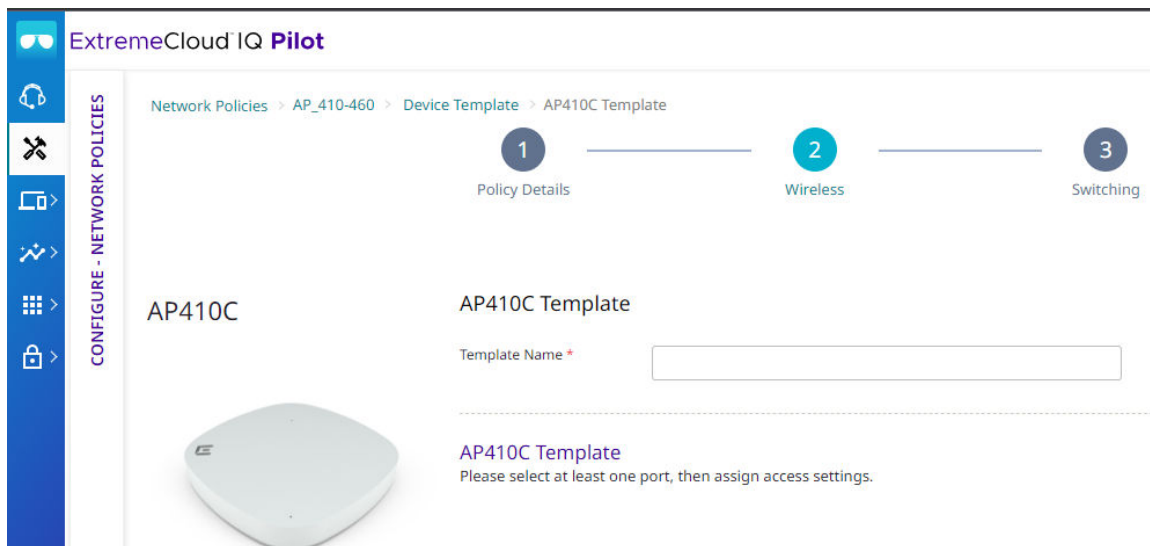
AP370

AP390

AP410

Template

- ☑ DST-AP410C (Default)
- ☑ DST-AP460C (Default)



9. Select **Save Template**.

Enable Sensor Mode

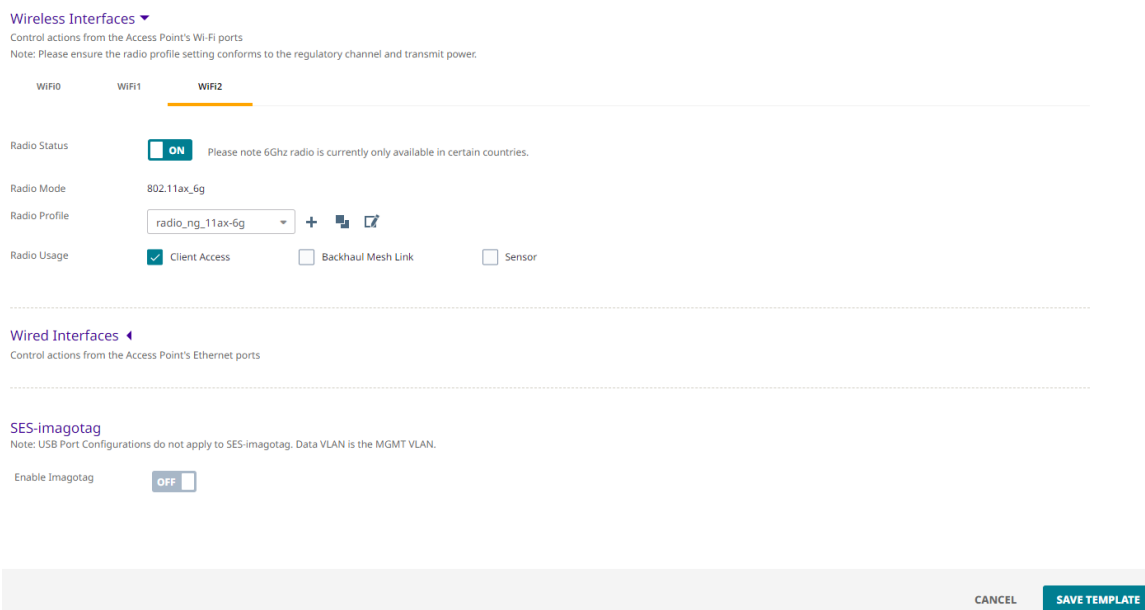


Note

Dedicated sensors provide functionality for various ExtremeCloud IQ applications such as ExtremeLocation Essentials and Extreme AirDefense Essentials.

Perform the following steps to enable sensor mode.

1. From the Device Template **Wireless Interfaces** section, select the drop-down menu.



2. Select **WIF2**.
3. Select the **Radio Status** and toggle it **ON**.
4. Select **Save Template**.

Enable iBeacon Services

The iBeacon service allows access points with embedded iBeacon transmitters to broadcast numerical advertisements that trigger an action on blue tooth-enabled devices that are within range.

For example, an app running on a mobile device might react to an iBeacon signal by displaying welcome messages, sale announcements, or coupons.

For this exercise, only the iBeacon monitoring mode is in scope.

Perform the following steps to enable iBeacon Services.

1. From the **WIRELESS** → **Configuration Settings** navigation list, select **Application Management** → **iBeacon Services**.

The screenshot shows the ExtremeCloud IQ Pilot configuration interface. The top navigation bar includes the ExtremeCloud IQ Pilot logo and a breadcrumb trail: Network Policies > AP_410-460 > iBeacon Service. Below the breadcrumb, there are two numbered steps: 1 Policy Details and 2 Wireless. The main content area is divided into two sections: WIRELESS and Network Services. Under WIRELESS, there are links for Configuration Settings, Application Management, Device Data Collection And Monitoring, iBeacon Service (highlighted with a blue arrow), Presence Analytics, WIPS, and Location Server. Under Network Services, there are links for Network Services and QoS Options. The iBeacon Services configuration panel is visible, showing a toggle switch set to ON. Below the toggle, there are input fields for Service Name, Description, and iBeacon UUID. The iBeacon UUID field has a tooltip that reads: "UUID format: 32 hexadecimal (base 16) digits, displayed in five groups separated by hyphens, in the form 8-4-4-4-12 for a total of 36 characters (32 alphanumeric and four hyphens). For example: 123e4567-e89b-12d3-a456-426655440000". There is a checked checkbox for "Enable iBeacon Monitoring" and an input field for "iBeacon Interval" set to 60. Below the input field, it says "(Default 60; Range: 10 - 1200) Seconds".

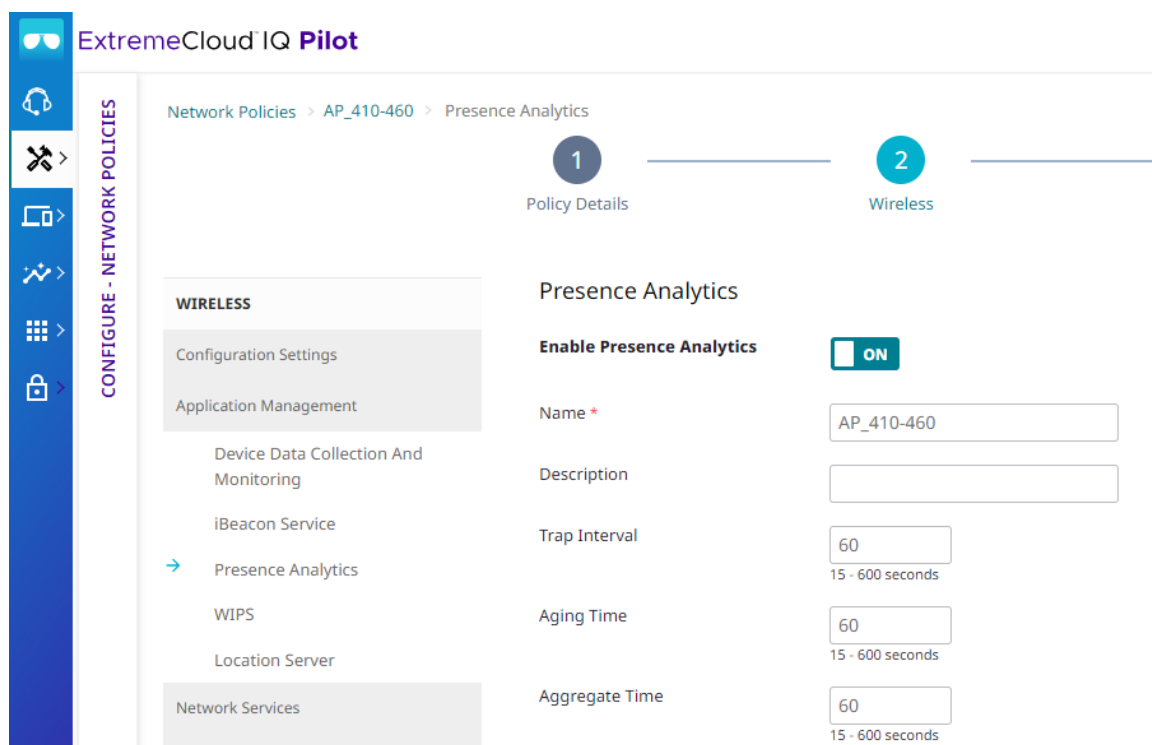
2. Toggle **iBeacon Service ON**.
3. In the **Service Name** field, type a service name, for example, BLE-Location.
4. Select the **Enable iBeacon Monitoring** check box.
5. In the **iBeacon Interval** field, type **60**.
6. Select **Save** to complete the configuration.

Enable Presence Analytics Services

Presence Analytics allows a WIFI sensor to collect the Media Access Control (MAC) addresses of WIFI devices within the coverage area and send these MAC addresses to the ExtremeLocation Essentials engine for processing.

Perform the following steps to enable Presence Analytics Services.

1. From the **WIRELESS** → **Configuration Settings** navigation list, select **Application Management**.



2. Select **Presence Analytics** and toggle it **ON**.
The **Name** field populates automatically with the name of the Network Policy.
3. Select **Save** to complete the configuration.


Place Access Points on the Floor Plan



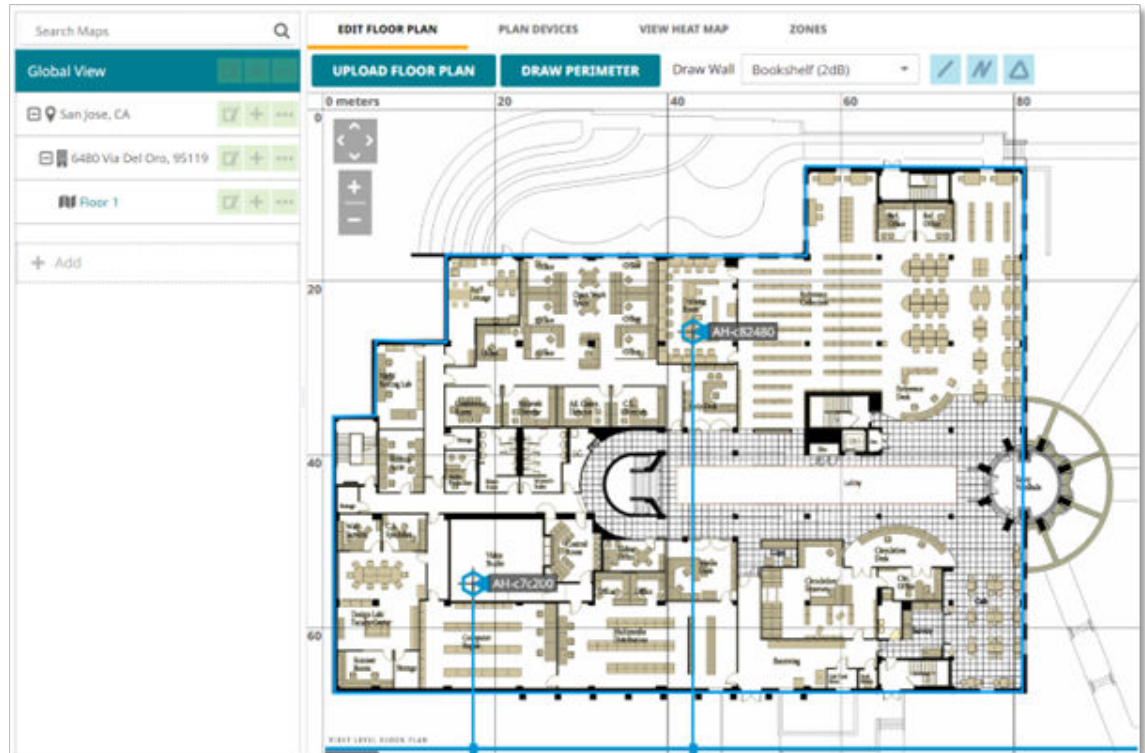
Note

To receive accurate location analytics and statistics, you must correctly map access points onto the floor plans.

Perform the following steps to place access points on the floor plan.

1. In the main navigation bar, select .
2. Select **Planning**.

3. Do one of the following:
 - Create a new location
 - Use an existing location
4. Drag and drop access points to their correct locations on the floor plan.



Note

Floor plans under the **Planning** menu are the only place where you can change and configure access point placements at a later time, if needed. The ExtremeLocation Essentials floor plan screen does not provide an option to change access point placements.



Location Essentials Components

The ExtremeLocation Essentials service is included with the Pilot subscription at no additional cost.

When enabled, you can only disable the ExtremeLocation Essentials service by resetting the ExtremeCloud IQ instance to factory default.

Enable ExtremeLocation Essentials

Perform the following steps to enable ExtremeLocation Essentials

1. Log into ExtremeCloud IQ.
2. In the main navigation bar, ☰.
3. Select ExtremeLocation.
4. Select **Enable**.

ExtremeLocation Essentials
Location and Analytics

Cloud-managed
Location services & Analytics

- Indoor location services for Wi-Fi and BLE devices
- Presence, Zone tracking, Asset tracking
- ExtremeLocation Essentials brings out the true value of location-based services by delivering powerful analytics and trends to provide business insights

Want to know more about ExtremeLocation Essentials?

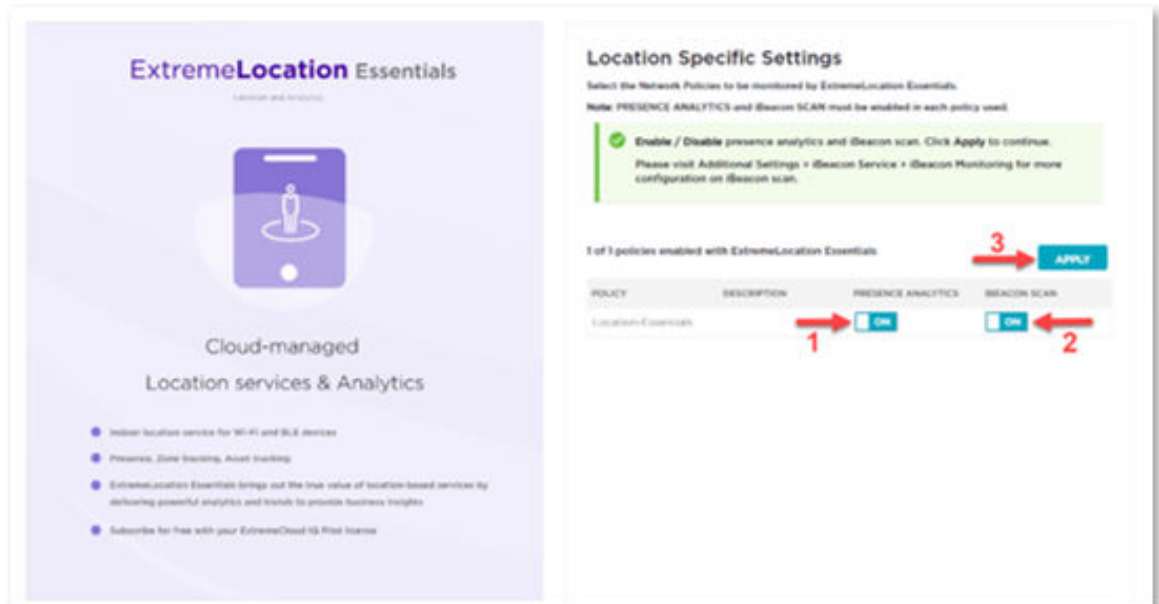
Enable

Enable to explore Location Services
Included with Pilot subscription - no additional cost

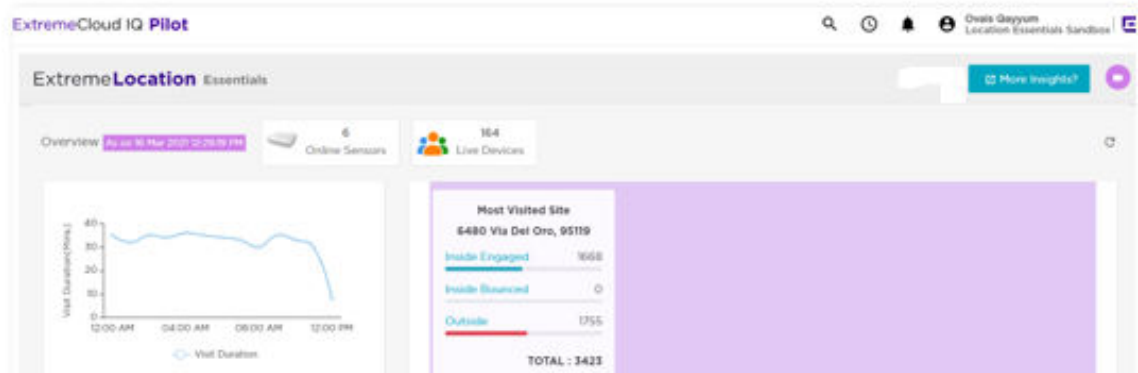
ENABLE

ExtremeLocation Essentials Supported Devices
AP302W, AP305C/CX, AP410C, AP460C, AP460S,
AP510C, AP4000, AP4000U, AP650, AP650X, AP3000,
AP3000X, AP5010, AP5010U, AP5050U, AP5050D

- Toggle **ON** the **Presence Analytics** and **iBeacon Scan**.



- Select **Apply**.
The ExtremeLocation Essentials **Overview** screen presents an overview of the ExtremeLocation Essentials Insights and Analytics.
- Select **More Insights** to access the ExtremeLocation Essentials configuration screen.



Note

The system requires at least 30-60 minutes to process and display the information.

Create Engagement Categories

A Category is a logical region on a floor plan. Use categories to run analytics and user engagement activities.

Manage Engagement Categories from the **Categories** screen.

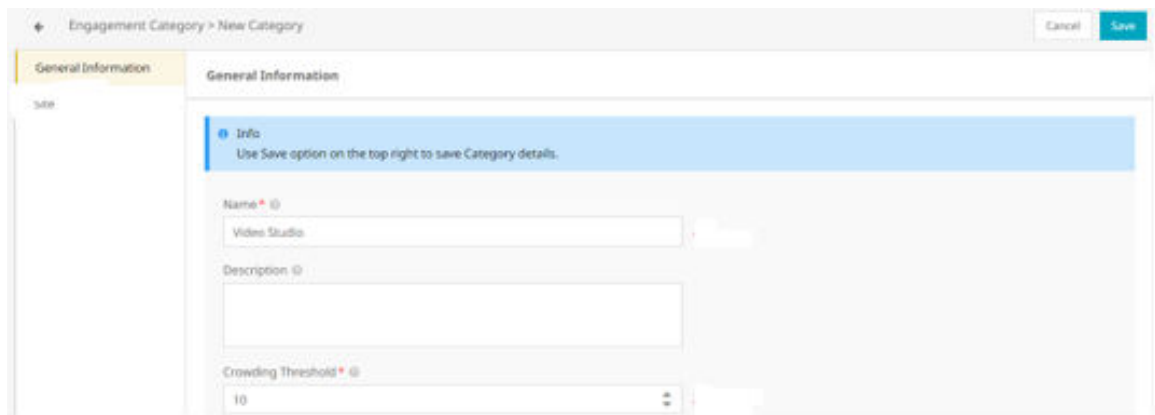
The **Categories** screen allows you to create multiple categories. You can use the same category across all sites.

Perform the following steps to create engagement categories and map them to sites.

1. In the **Categories** screen, select **Engagement Categories**.



2. To create a new engagement category, select **+**.
3. In the **Name** field, type a name for the new category.
4. Ensure the **Crowding Threshold** field contains the number **10**.
5. Select **Save**.
6. To map the category to a site, select **Site**.



7. Select the **+**.
8. Select **Map Site**.
9. Select the site from the list of available sites and drag and drop it into the **Selected** sites box.
10. Select **Map** to complete the site mapping.
11. Select **Back** to exit the screen.

Assign Access Points to Engagement Categories


There are two ways to assign an access point to an engagement category:

- Assign the access point to a region when the region contains a single category
- Manually assign the access point when a region has multiple access points and each access point is mapped to a different category or area within a region.

In the first method, when an access point is assigned to a region, it uses the same category that is mapped onto the region.

In the second method access points are manually assigned to categories individually.

Perform the following steps to assign access points to engagement categories.

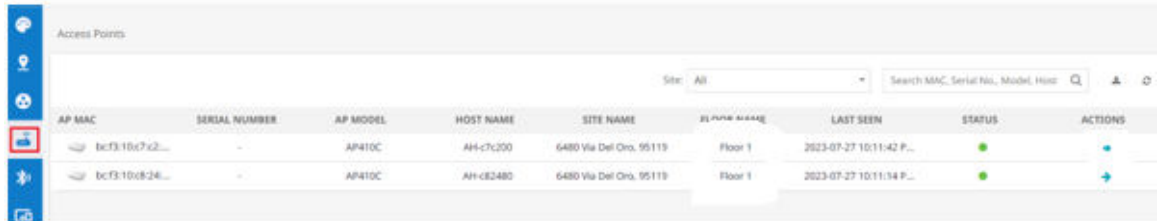
1. In the main navigation bar on the **Access Points** screen, select .
2. In the **Actions** column, select the right arrow in the access point row.






Note

APs are already mapped onto a pre-configured floor plan.

ExtremeLocation Essentials automatically pulls the information from the ExtremeCloud IQ floor plan configuration.



AP MAC	SERIAL NUMBER	AP MODEL	HOST NAME	SITE NAME	FLOOR NAME	LAST SEEN	STATUS	ACTIONS
bc:f3:10:c7:a2...	-	AP410C	AH-c7c200	6480 Via Del Oro, 95119	Floor 1	2023-07-27 10:11:42 P...	●	
bc:f3:10:c9:24...	-	AP410C	AH-c82480	6480 Via Del Oro, 95119	Floor 1	2023-07-27 10:11:34 P...	●	

3. Select the .
4. Assign access points to various categories.



Note

As access points are physically located in specific locations on a floor plan, assigning them to the wrong categories generate inaccurate engagements and analytical data.

5. Select **Save**.

Create Regions

Regions are locations on the floor plan that identify an area on a floor.

For example:

- In a retail store, the cosmetics aisle is marked with the region **Cosmetics**
- Similarly, in an office, the Accounts Department is marked with the region **Accounts**.

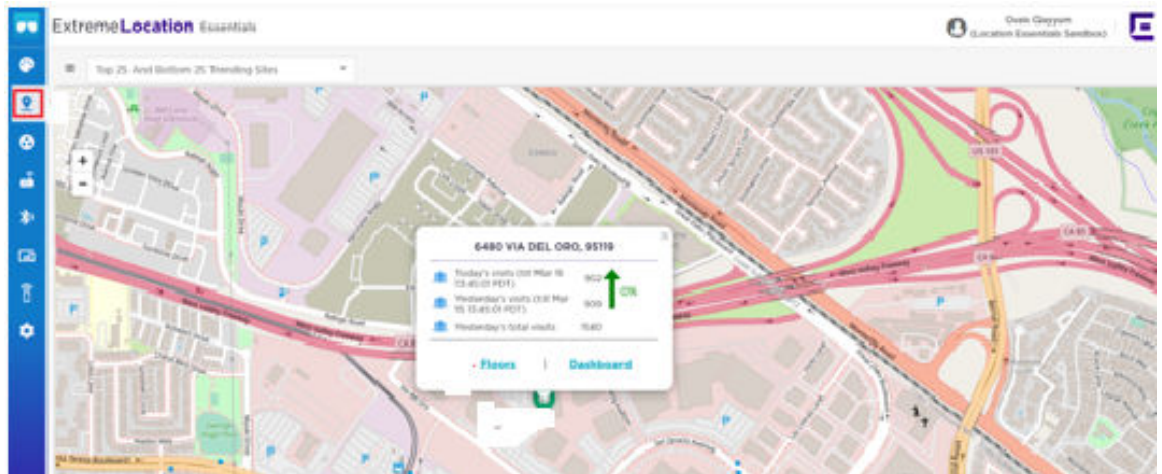
Dividing the floor into logical regions allows for the collection of data on the number of visits in that region of the floor.

Each region is assigned one or more access points. Access points are assigned to engagement categories which drives category-based insights and trends.

Perform the following steps to create regions on the floor plan.

1. In the main navigation bar on the ExtremeLocation Essentials screen, select .
2. Select the location.

3. Select **Floors** to access the site floor plans.

**Note**

Before creating a region, verify that access points are mapped on the floor plan in correct locations.

4. From the **Floor** pull down menu, select the floor.
5. Select **AP**.

**Note**

Access points are already mapped and assigned a category.

6. Select **Region**.
7. To add a new region, select **+**.
8. In the **Region Name** field, type a name for the region.
9. In the **Color** field, pick a color.
10. The cursor turns into a drawing tool, use the cursor to draw the region.

11. Select **Save**.



Note

Repeat the process to add more regions.

Site and region configurations are now complete. Sensors are detecting Wi-Fi devices which appear on the floor plan depending on proximity to the regions.

Heatmap and Crowding data are available.

View Wi-Fi Devices

To view current Wi-Fi devices, select **Device**. The **Historical** device view option is useful to search a device with MAC address or device name and to track the movement of the device between different regions.

View Heatmap

To view the Heatmap, select **Heatmap** → **Live**. The screen also provides **Historical** views, however in a newly configured environment you need to wait for heatmap displays.

You can download the Heatmap as a PDF.

View Crowding Events

When the crowding threshold exceeds the default value of 10, the ExtremeLocation Essentials generates a crowding event. ExtremeLocation Essentials generates a crowding event when the ratio of the number of visitors to the number of associates assigned to the category exceeds the threshold.

To view **Crowding** events in a category, select **Crowding** and check categories with active crowding events.

Configure Device Classification Rules

ExtremeLocation Essentials classifies devices into one of the following types:

- Visitor
- Assets
- Staff
- Staff Personal Devices.

ExtremeLocation Essentials applies classification rules when a device enters or exits a site.

When a device visits a site for the first time, ExtremeLocation Essentials classifies the device as a **Visitor** device.

When the device re-enters the site, ExtremeLocation Essentials re-classifies the device based on device classification rules.

ExtremeLocation Essentials monitors Visitor devices for re-classification. The following are a few re-classification parameters:


- The Service Set Identifier (SSID) to which the device associates
- The time duration the device is seen at a site.

The user can configure and fine tune SSID and time duration parameters for device classification. ExtremeLocation Essentials classifies personal staff devices as **Staff Personal Devices** to exclude data collection and analysis from staff personal devices.

Staff Personal Devices do not display in the **Devices View** on the floor map.

In this guide, **Assets** and **Staff** devices are classified based on Time Duration.

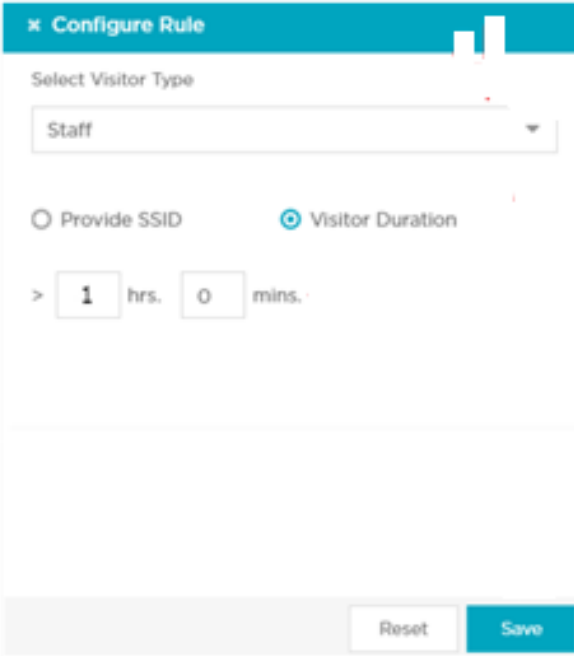
Perform the following steps to configure device classification rules.

1. In the main navigation bar on the ExtremeLocation Essentials screen, select, 
2. Select **Device Classification** .
3. Select **Device Classification and Management**.
4. To add a new device rule, select **+**



5. In the **Select Visitor Type** field, select **Staff**.
6. Select the **Visitor Duration** radio button and set the duration to **1** hour.
7. Select **Save**.

- Repeat the process to set the duration for **Asset** devices to **4** hours.



The screenshot shows a 'Configure Rule' dialog box. At the top, there is a close button (X) and the title 'Configure Rule'. Below the title, there is a section 'Select Visitor Type' with a dropdown menu currently set to 'Staff'. Underneath, there are two radio buttons: 'Provide SSID' (which is unselected) and 'Visitor Duration' (which is selected). Below the radio buttons, there are two input fields for time: '1 hrs.' and '0 mins.'. At the bottom of the dialog, there are two buttons: 'Reset' and 'Save'.

**Note**

For a newly configured environment, device classification takes some time to display.

Configure Device Classification Thresholds

To understand different visitor types and to increase analytical data accuracy, you must correctly configure device classification thresholds.

Device classification threshold values depend on many factors and varies based on the following:

- Deployment
- Location and size of the regions
- Sensor placements within a region.

ExtremeLocation Essentials classifies visitors into the following categories by calculating the Received Signal Strength Indicator (RSSI) and dwell time thresholds as follows:

Table 4: Visitor Classification

Outside Visitors	Inside Bounced Visitors	Inside Engaged Visitors
Visitors in the vicinity of the site but not entering the site. Determined by observed WIFI RSSI values.	Visitors who enter the site but leave in a short time. Determined by the observed WIFI RSSI values and the site dwell time.	Visitors who enter the site and stay for more than a specified time. Determined by the observed WIFI RSSI values and the site dwell time.

The **Threshold** window allows for the following:

- Configuring fields to classify visitors to the site
- Setting up thresholds for device categorization based on zones
- Setting up the different age outs for devices seen at the site.

Use the **Signal Strength** slider to set values for device classification as one of the following:

- Ignored Devices
- Outside Devices
- Inside Devices.

Table 5: Device Classification

Ignored Devices	Inside Devices	Outside Devices
ExtremeLocation Essentials ignores devices when the signal strength from the device is below the signal strength value set by the first slider knob.	An Inside Device has a signal strength reading that is above the signal strength value set by the second slider knob.	An Outside Device has a signal strength reading that is between the two knobs of the signal strength slider.
The red section of the signal strength slider displays the signal strength value.	The green section of the signal strength slider displays Inside Devices signal strength values.	The orange section of the signal strength slider displays Outside Devices signal strength values.
ExtremeLocation Essentials do not track Ignored Devices for analysis.		


Use the **Dwell Time** slider to set device classification values as one of the following:

- Outside
- Inside Bounce
- Inside Engaged.

Table 6: Dwell Time Device Classification

Outside Devices	Inside Bounced	Inside Engaged
Outside devices are seen in the site for a duration that is less the duration set by the first slider knob.	Inside Bounced devices are seen at the site for a duration between the times indicated by the two knobs of the Dwell Time slider.	Inside Engaged devices are seen in the site for a duration greater than the duration set by the second slider knob.
The orange section of the Dwell Time slider displays the device classification threshold.	The light green section of the Dwell Time slider displays the device classification threshold.	The dark green section of the Dwell Time slider displays the device classification threshold.

Perform the following steps to configure device classification thresholds.

1. In the main navigation bar on the ExtremeLocation Essentials screen, select, 
2. Select **Thresholds**.
3. Use the **Signal Strength** and **Dwell Time** sliders to set thresholds.
4. Select **Save**.



Note
Threshold changes are not updated in real-time.



Configure the Location Essentials Dashboard


After the ExtremeLocation Essentials service is configured, the next step is to use the customizable ExtremeLocation Essentials Dashboard to display data for sites that ExtremeLocation Essentials manages.

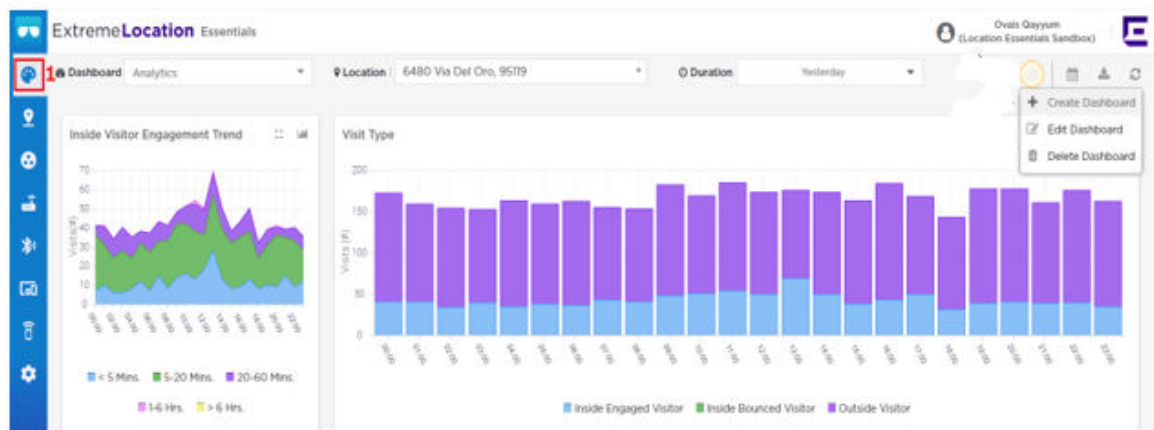
The ExtremeLocation Essentials dashboard provides many widgets to filter site data. You can create many custom dashboards that meet analytics and trend monitoring requirements.

ExtremeLocation Essentials filters and displays data on the dashboard by location and time period. You can apply **Location** and **Time** filter options independent of each other.

Create a Dashboard

Perform the following steps to create a new Category Analytics dashboard.

1. In the main navigation bar, on the ExtremeLocation Essentials screen, select .
2. Select **Manage Dashboard**.
3. Select **Create dashboard**.





4. Select **Category Analytics** to use widgets to display category or region analytics data.
5. Select as many widgets as you wish but you must select **Category Path Analysis** and **Category Crowding** widgets.



Note

A green check mark displays on the top right of selected widgets.

6. Select **Next**.
7. Use  to adjust the look and feel of the newly created dashboard.
8. Select **Save**.
9. In the **Dashboard Name** field, type a name for the dashboard.
10. Select **Save**.
11. To delete unwanted widgets, select .

Navigating the Dashboard

Perform the following steps to navigate the dashboard.

1. In the main navigation bar, on the ExtremeLocation Essentials screen, select .



Note

The dashboard marked with  automatically loads and is the default.

2. To make the Category Analytics dashboard the default, select **Category Analytics**.

Location

3. When multiple sites are available under the ExtremeLocation Essentials account, to display data for a selected site, in the **Location** field, select the drop-down arrow and select the site.
4. To configure the time range and apply time-based filters, in the **Duration** field, select the drop-down menu.





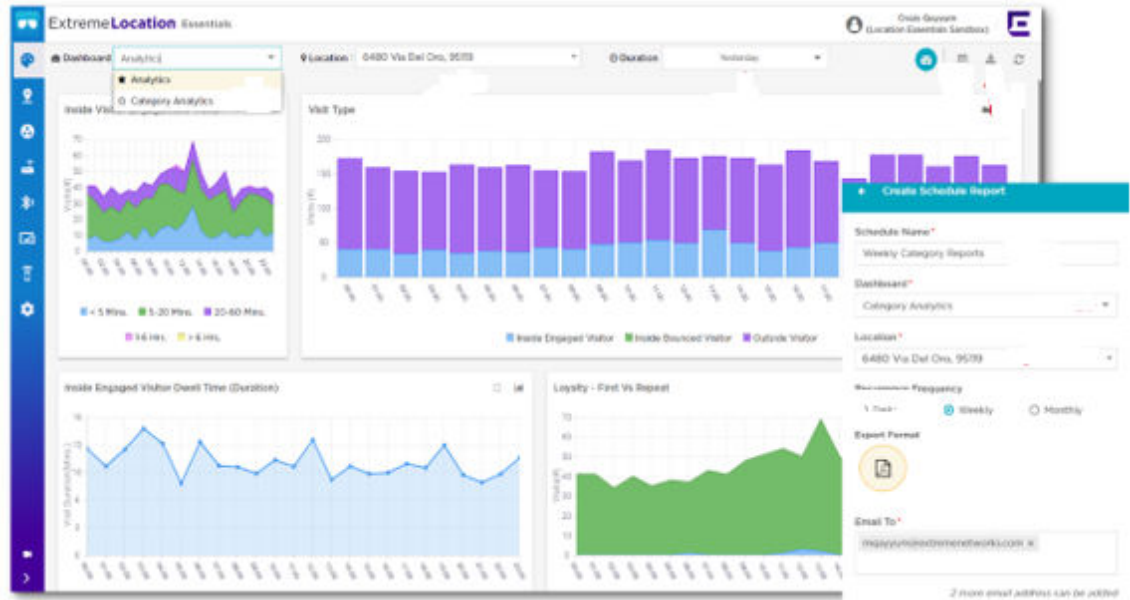
Note

The **Duration** field drop-down menu provides a set of pre-configured and custom time range options for filtering data.

Scheduled Reports

The **Scheduled Reports** option provides the workflow to create reports that run periodically.

5. To configure the report schedule, create a new schedule and use the **Dashboard** and **Location** drop-down arrow to select the data of interest.
6. Select .
7. Use the **Recurrence Frequency** field to configure the recurrence frequency.
8. In the **Email To** field, type the email address of the report recipient.
9. Select **Create** to finish the Scheduled Reports setup.
10. To save the dashboard as a PDF or CSV file, select  and choose PDF or CSV.



Crowding Events

Select Crowding Events for each category to use data to avoid crowding by allocating enough associates to an area or category within a region.

Category Path Analysis

The **Category Path Analysis** widget maps the movement of devices between different categories.

Category Path Analysis data estimates a category's footfall and traffic flow between various categories. For example, in a retail store or an exhibition hall, use category path analysis to plan and utilize floor space more efficiently.