

# Epiq™ Flying Fox™ Enterprise

RF Sensing • Mobile Device Detection



---

## USER MANUAL

V1.11.0 - SEPTEMBER 15, 2023



## CHANGELOG

Revision	Date	Description	Author
1.11.0	2023-09-15	Bundle sensor firmware with package, User initiated sensor upgrades, URL scheme for viewing specific device or detection, Bug fixes	PK
1.9.0	2022-12-20	Added SSH Test, Sensor Connection, and Sensor export to CSV Sections	LM
1.7.2	2022-08-31	Added sensor measurements section	PK
1.7.1	2022-08-05	Updated images. Zone name labels, BTCP piconet, Medical Manufacturers	PK
1.4.0-3	2021-06-28	Added note about SSL certs for v1.3.2	MJ
1.4.0-2	2021-06-25	Added firmware compatibility chart and other tweaks	MJ
1.4.0	2021-06-23	2021 Q2 Release	RZ
1.3.2	2021-04-09	2021 Q1 Release	PK
1.2.1	2020-12-07	Copy edits	GS
1.2.1	2020-12-04	Updates to images and text	PK
1.0.0	2020-08-05	Initial version	GS

# TABLE OF CONTENTS

<b>Support Forum And Contact Information</b>	<b>5</b>
Accessing the Support Forum	5
Why Visit the Support Forum?	5
How to Access the Support Forum	5
Contact	5
<b>System Setup</b>	<b>6</b>
Configuring the Hardware	6
Connecting the Sensors	6
Configuring the Appliance IP Address	7
CAC - 2FA	7
<b>Configuring Flying Fox Enterprise</b>	<b>8</b>
Logging in for the First Time	8
Using the Wizard	8
Making Changes to Sensor Placement	11
Setting Up Zones (Geo-Fences)	12
Managing Users	13
Managing Sensors	14
Testing Sensor SSH Connections	15
Sensor SSH Connection Status	15
Sensor Firmware Upgrade	16
Export Sensor Data to CSV	17
Checking Software Version	17
<b>Monitoring Detections</b>	<b>19</b>
Viewing Multiple Floors	19
Sensor Measurements	19
Grouping By Device or Event	20
Cellular Detections	21
Unknown Cellular Detections	23
Cellular Scan Events	23
Bluetooth Detections	23
Configuring Passive Bluetooth Detection	25
Bluetooth Classic Passive Piconet Connections	26
Wi-Fi Detections	27
Device Alias / Friendly Name	28
Device/Scan Details URL Sharing	28
<b>Filters</b>	<b>30</b>
By Technology	30
By Zone (Geo-Fence)	30
Excluding Possible Unreliable Location Estimates	31
Authorized Devices	33

Medical Manufacturers .....	35
<b>Historical View</b> .....	<b>39</b>
<b>Configuring Syslog</b> .....	<b>41</b>
<b>Display Preferences</b> .....	<b>42</b>
<b>Theory of Operation</b> .....	<b>44</b>
Wi-Fi Detection .....	44
Bluetooth Detection .....	44
Bluetooth Classic – Active Inquiry .....	44
Bluetooth Classic - Passive .....	44
Bluetooth Low Energy .....	45
Cellular Detection .....	45
<b>System Updates</b> .....	<b>47</b>
Appliance Software Updates .....	47
<b>Troubleshooting</b> .....	<b>49</b>
Exporting Client State .....	49
Exporting Device Data .....	49
Export Filters .....	49
Miscellaneous Troubleshooting .....	49
Can't Connect to Flying Fox Enterprise UI .....	49
Sensors are Not Populating in Sensor List .....	49
Devices From Outside the Zone are Showing Up Inside the Zone on the Floor Plan .....	49
<b>Notes</b> .....	<b>50</b>
Note 1 - 802.11ac .....	50

## SUPPORT FORUM AND CONTACT INFORMATION

### ACCESSING THE SUPPORT FORUM

We understand that staying up-to-date with the latest releases is crucial for a smooth user experience. To ensure you have access to the most recent updates, we encourage you to visit our dedicated **Support Forum**.

### WHY VISIT THE SUPPORT FORUM?

**Stay Informed:** Our Support Forum is the go-to place for announcements about new software releases, updates, and enhancements. By visiting the forum regularly, you can ensure that your system is always running the latest and greatest version.

### HOW TO ACCESS THE SUPPORT FORUM

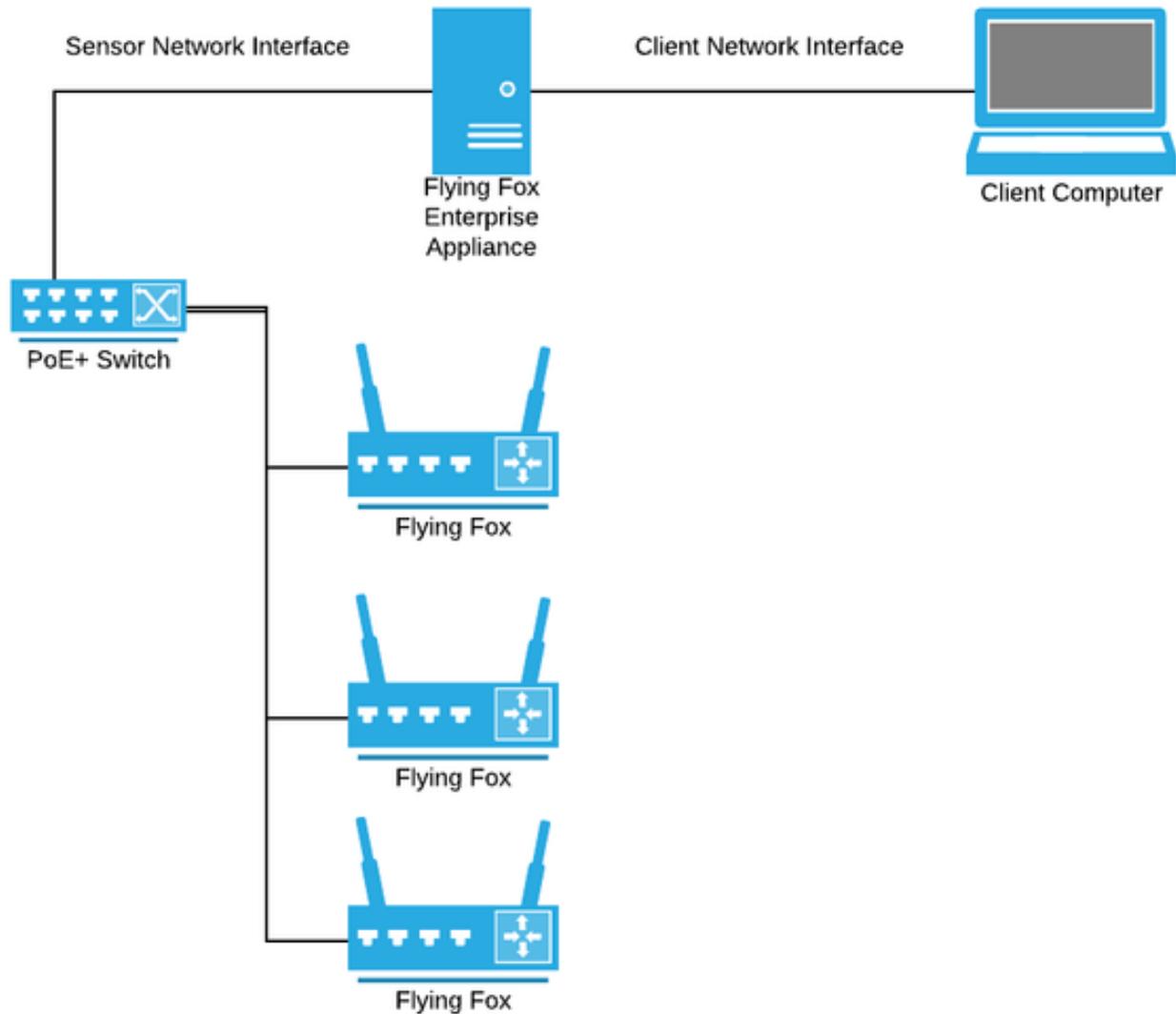
1. Open your web browser.
2. Go to our website: <https://support.epiqsolutions.com/viewforum.php?f=264>.
3. Create an account if you haven't already.
4. Browse through the various categories and threads to find the information you need.

### CONTACT

Epiq Solutions support can be reached at (847) 598-0218 or [support@epiqsolutions.com](mailto:support@epiqsolutions.com).

# SYSTEM SETUP

## CONFIGURING THE HARDWARE



**Figure 1:** Flying Fox Enterprise Network Diagram

Minimally, a Flying Fox Enterprise Deployment is made up of Flying Fox Sensors, one or more PoE+ switches and/or injectors, the Flying Fox Enterprise Appliance, and client computers. The Flying Fox Enterprise application is a web-based application that is served by the on-premise Flying Fox Enterprise Appliance and is accessed by browsers in client computers.

By default the system expects the Flying Fox Sensors to be on a private subnet that is connected to one of the interfaces on the Flying Fox Enterprise Appliance.

## CONNECTING THE SENSORS

Sensors need to be connected to a PoE+ switch or power injector that meets the 802.3at standard and can source 30W. If the switch being used is configurable, ensure that 30W is available for each

port connected to a Flying Fox Sensor.

## CONFIGURING THE APPLIANCE IP ADDRESS

The Flying Fox Enterprise Appliance is based on Red Hat Enterprise Linux. To configure the IP addresses of the network interfaces, login to the appliance from the console and configure the interfaces as desired using tools like `nmtui` or `nmccli`.

## CAC - 2FA

Flying Fox Enterprise can integrate with an RFC 4511 LDAP server and enterprise PKI for user authentication and authorization. For details of this integration, please contact [support@epiqsolutions.com](mailto:support@epiqsolutions.com)

# CONFIGURING FLYING FOX ENTERPRISE

## LOGGING IN FOR THE FIRST TIME

On a client machine, point a browser to an IP address configured in [Configuring the Appliance IP Address](#) to access the Flying Fox Enterprise web interface.

For example, if the server is configured with an IP address of `192.168.0.10`, then enter the following in the browser URL bar:

```
https://192.168.0.10
```

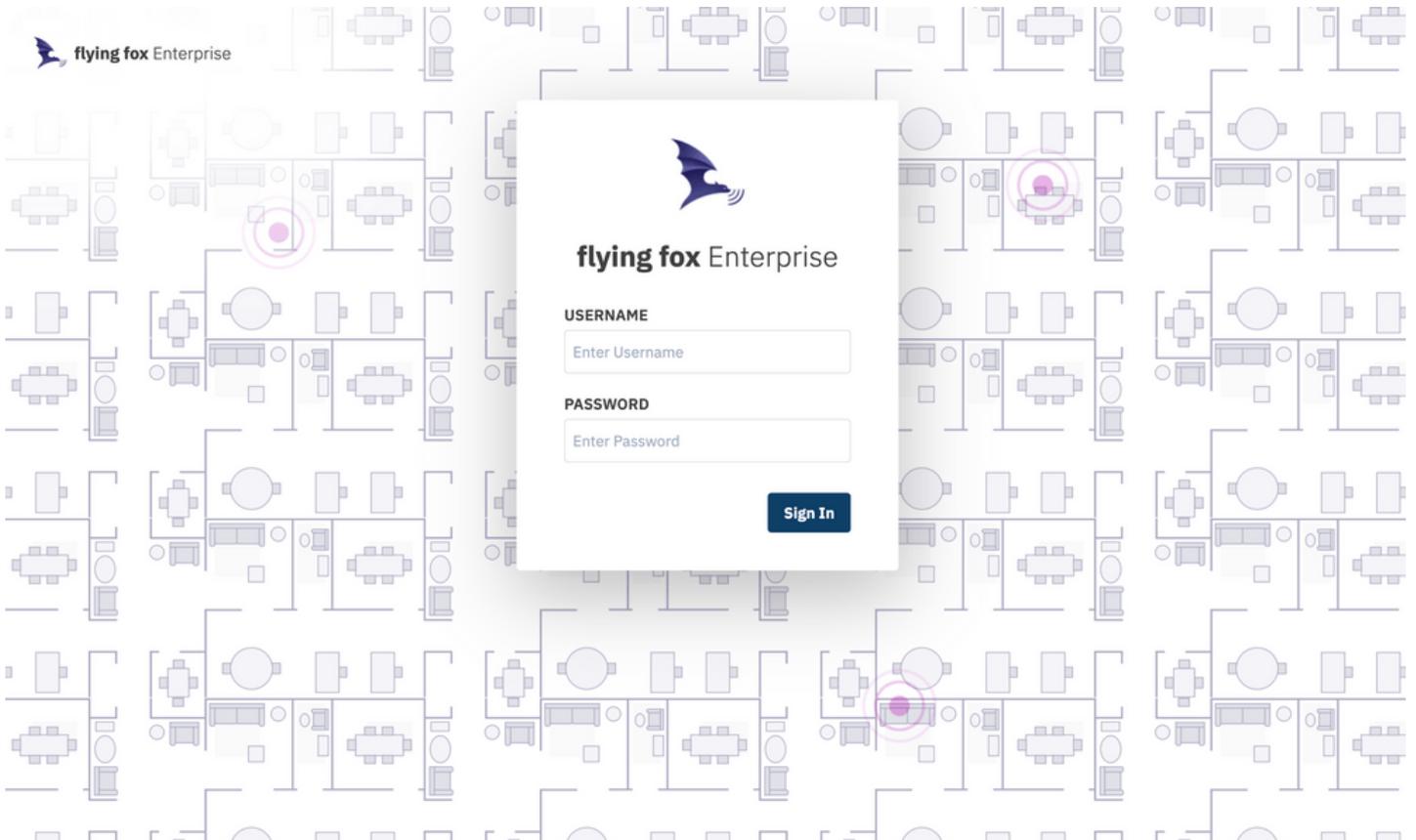
Don't forget the s in https!

The default username and password is:

```
admin:admin
```

You will be prompted to change the admin password.

**NOTE: If the system is configured for CAC - 2FA, you will not be prompted to login**



**Figure 2:** Login Page

## USING THE WIZARD

When configuring the application for the first time, or when adding buildings or floors, a setup wizard will guide the user.

Monitored areas are organized hierarchically by site, building, and floor.

To begin, create a new site.

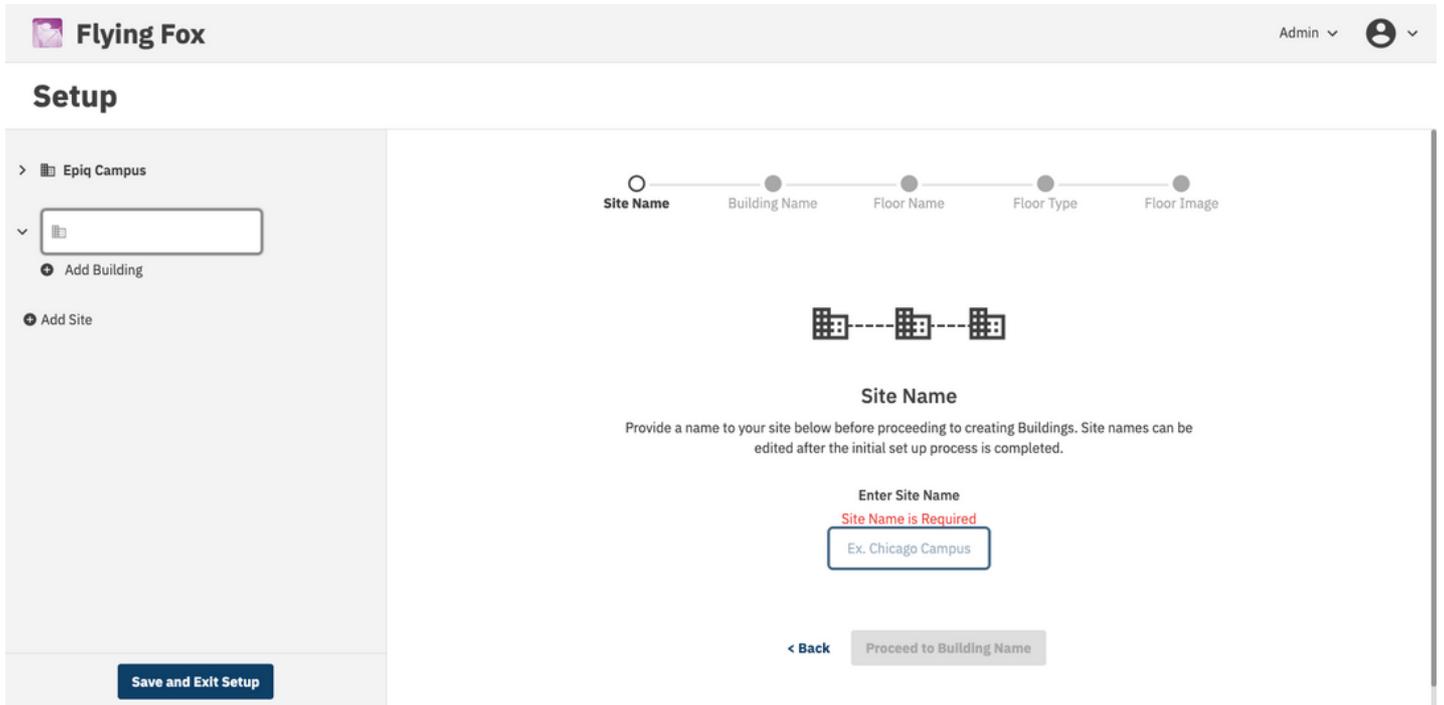


Figure 3: Creating a Site

Then create a building.

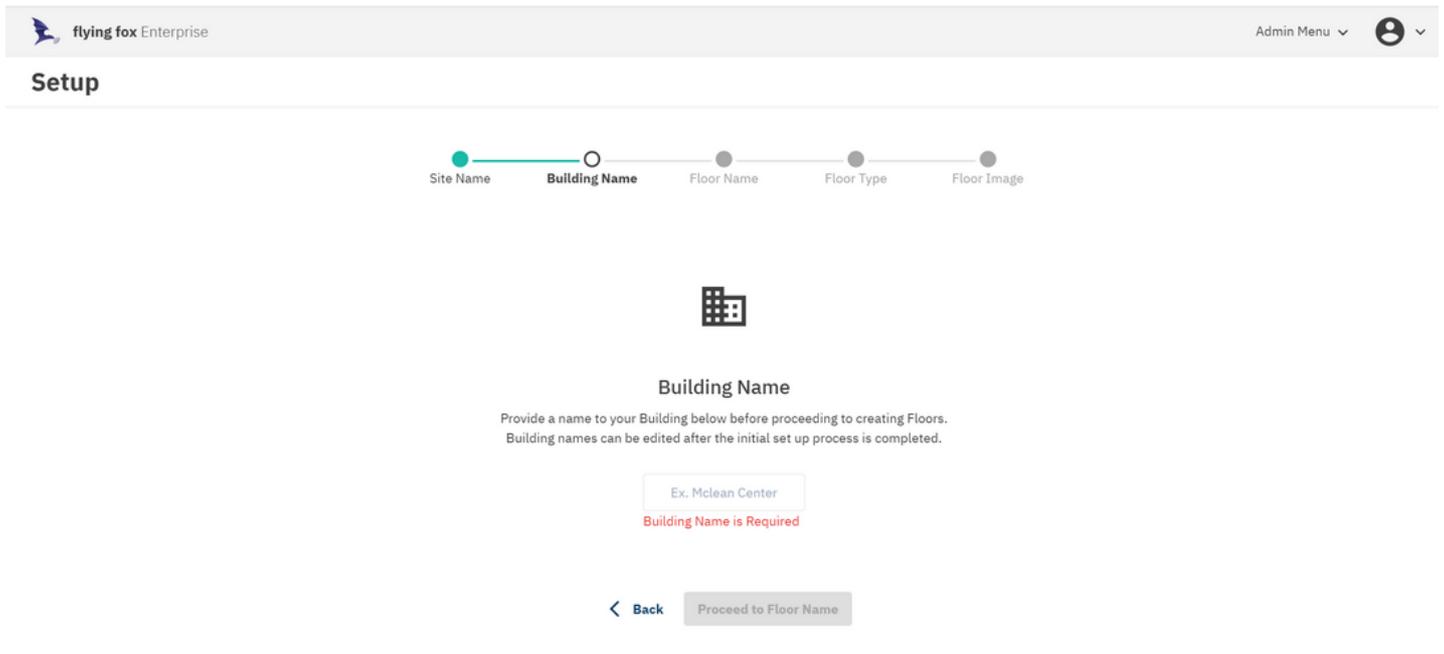
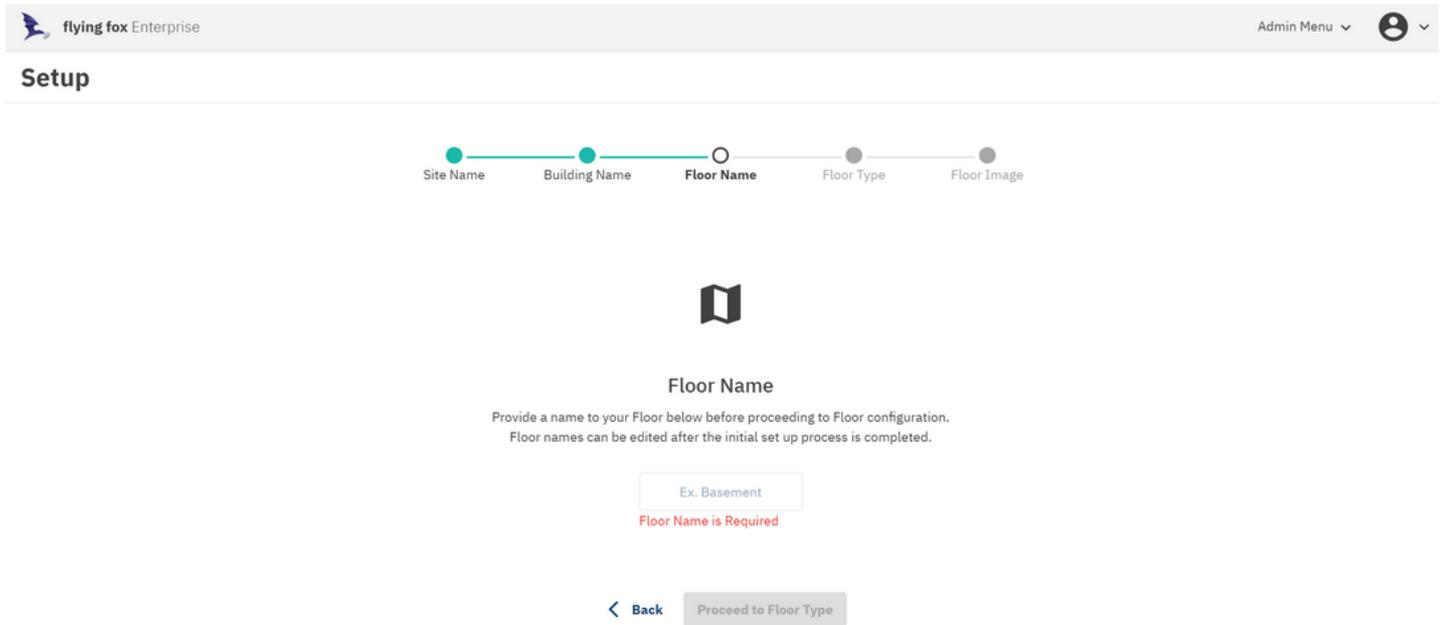


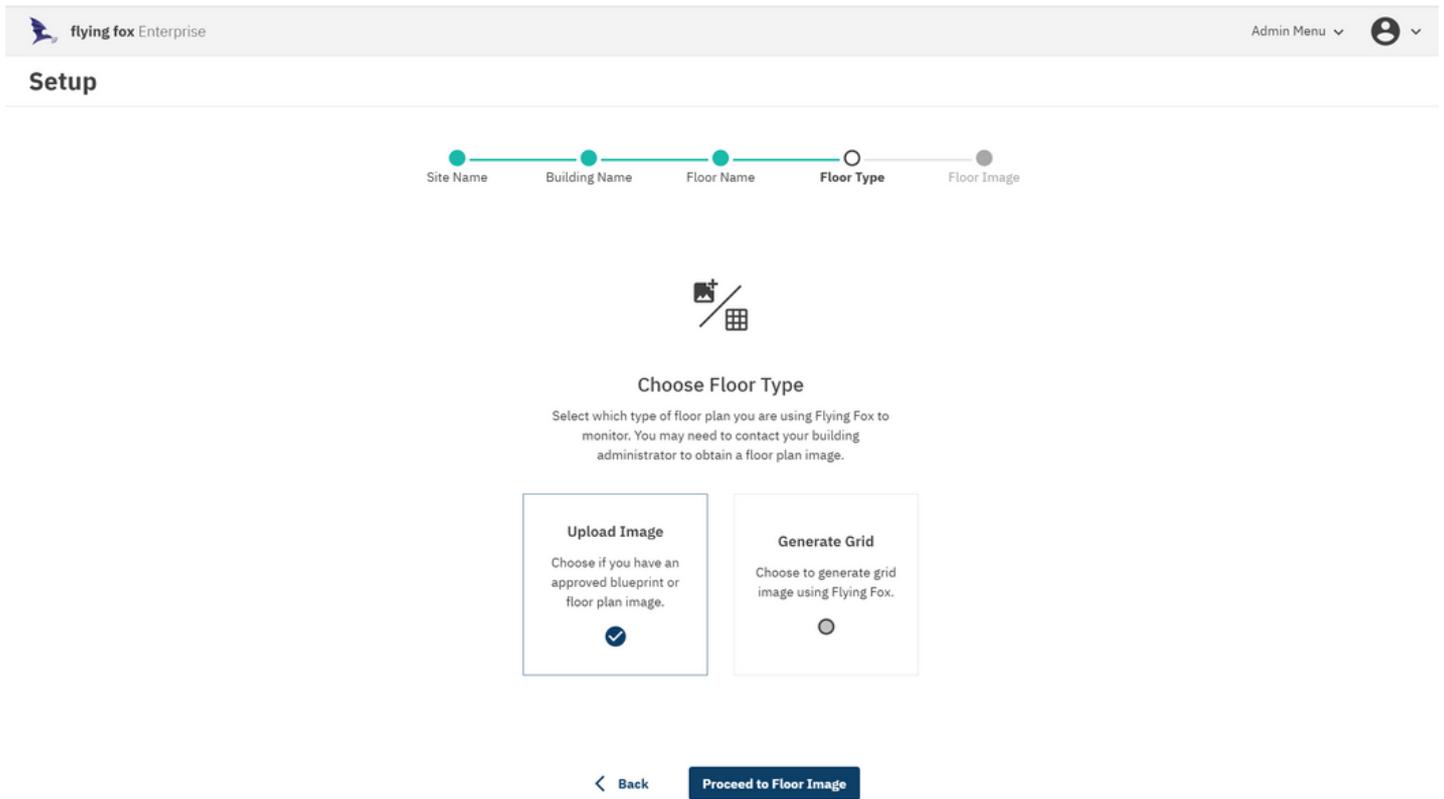
Figure 4: Creating a Building

Finally create a floor.



**Figure 5: Creating a Floor**

The floor will be used to map detections. The system will ask to upload a floor plan image. If an image is not available, the system will generate a rectangular grid.



**Figure 6: Choosing a Floor Type**

After uploading a floor plan image, configure the application with the GPS coordinates of the top left, bottom left, and bottom right corners. These coordinates will ensure that all detections will be tagged with their accurate geo-location.

The screenshot shows the 'Setup' window in the Flying Fox Enterprise application. On the left is a sidebar with a tree view containing 'Epiq Campus', 'East Lansing Camp...', 'FRIB', and 'Main Floor'. The 'Main Floor' is selected. Below the sidebar are buttons for 'Add Floor', 'Add Building', and 'Add Site'. At the bottom of the sidebar is a 'Save and Exit Setup' button.

The main area has three tabs: 'Floor Properties', 'Sensor Placement', and 'Zones'. The 'Floor Properties' tab is active, showing a map of the floor plan with four corner markers labeled 'TOP LEFT', 'BOTTOM LEFT', and 'BOTTOM RIGHT'. The map also shows an 'ENTRANCE' and 'Handicap Parking' area. Below the map is a form for 'Floor Coordinates' with the following fields:

HEIGHT (meters)	Calculated Dimensions	
<input type="text" value="3"/>	215.16 meters x 255.52 meters	
TOP LEFT	BOTTOM LEFT	BOTTOM RIGHT
<input type="text" value="42.096351, -88.028308"/>	<input type="text" value="42.095918, -88.028319"/>	<input type="text" value="42.095919, -88.027768"/>

*Figure 7: Configuring Floor Properties*

## MAKING CHANGES TO SENSOR PLACEMENT

Once the floor is configured, sensors need to be placed.

Click on the Sensor Placement header in the Setup window.

The system will present the user with a list of sensors. Those that have not been added to a floor will be available to add to a floor.

Click on the "Add to Floor" link and the sensor will be placed on the floor plan. Drag the sensor to its actual location on the floor plan.

When complete be sure to click "Save and Exit Setup." Note that the server will restart after this operation, so allow about a minute for the restart before attempting to login again.

The screenshot shows the 'Setup' interface for Flying Fox Enterprise. On the left is a sidebar with a tree view of locations: Epiq Campus, HQ, Main (selected), Add Floor, Add Building, East Lansing Camp..., FRIB, and Main Floor. A 'Save and Exit Setup' button is at the bottom of the sidebar. The main area has three tabs: 'Floor Properties', 'Sensor Placement' (active), and 'Zones'. The 'Sensor Placement' tab shows a floor plan with several sensor icons. Below the floor plan is a table for sensor placement:

SENSOR ID	SENSOR NAME	
7602	flyingfox-7602	+ Add to Floor
7613	flyingfox-7613	- Remove from Floor

Below the table is a 'Default Sensor height above floor in meters' input field with the value 2.74.

*Figure 8: Placing Sensors*

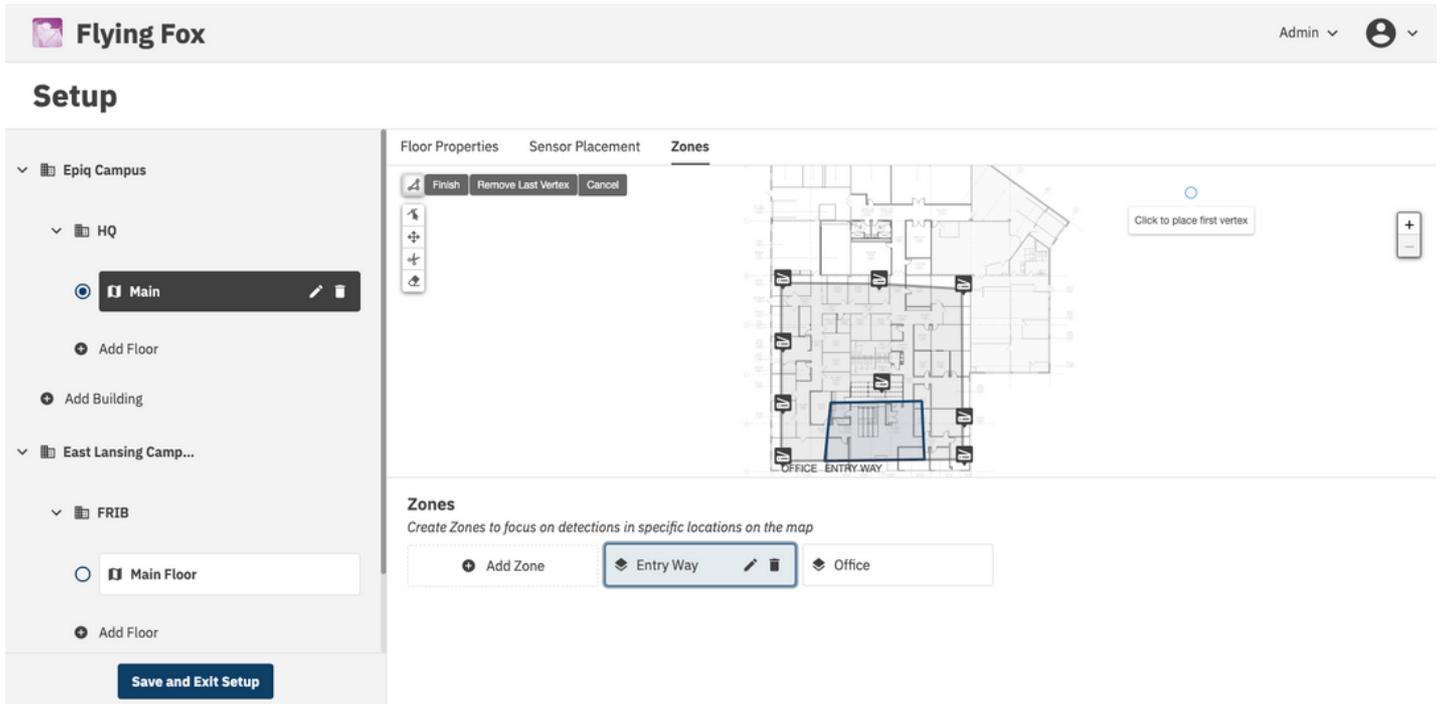
## SETTING UP ZONES (GEO-FENCES)

Zones or geo-fences can be used to filter unwanted detections or to highlight detections in specific areas. A user can create multiple zones, and zones can overlap.

To create a zone, click "Zones" in the Setup menu. Click "Add Zone" and click the pencil icon to give the zone a name. Click the vertex tool in the upper left corner and draw the zone geometry on the floor plan. After finishing the polygon, click the disk icon to link the zone geometry with the new zone.

The zone name will automatically be added to the floor plan near the bottom left corner of the zone geometry. The name label can be placed in any location on the floor plan by clicking and dragging the label.

When complete be sure to click "Save and Exit Setup." Note that the server will restart after this operation, so allow about a minute for the restart before attempting to login again.



*Figure 9: Setting up Zones*

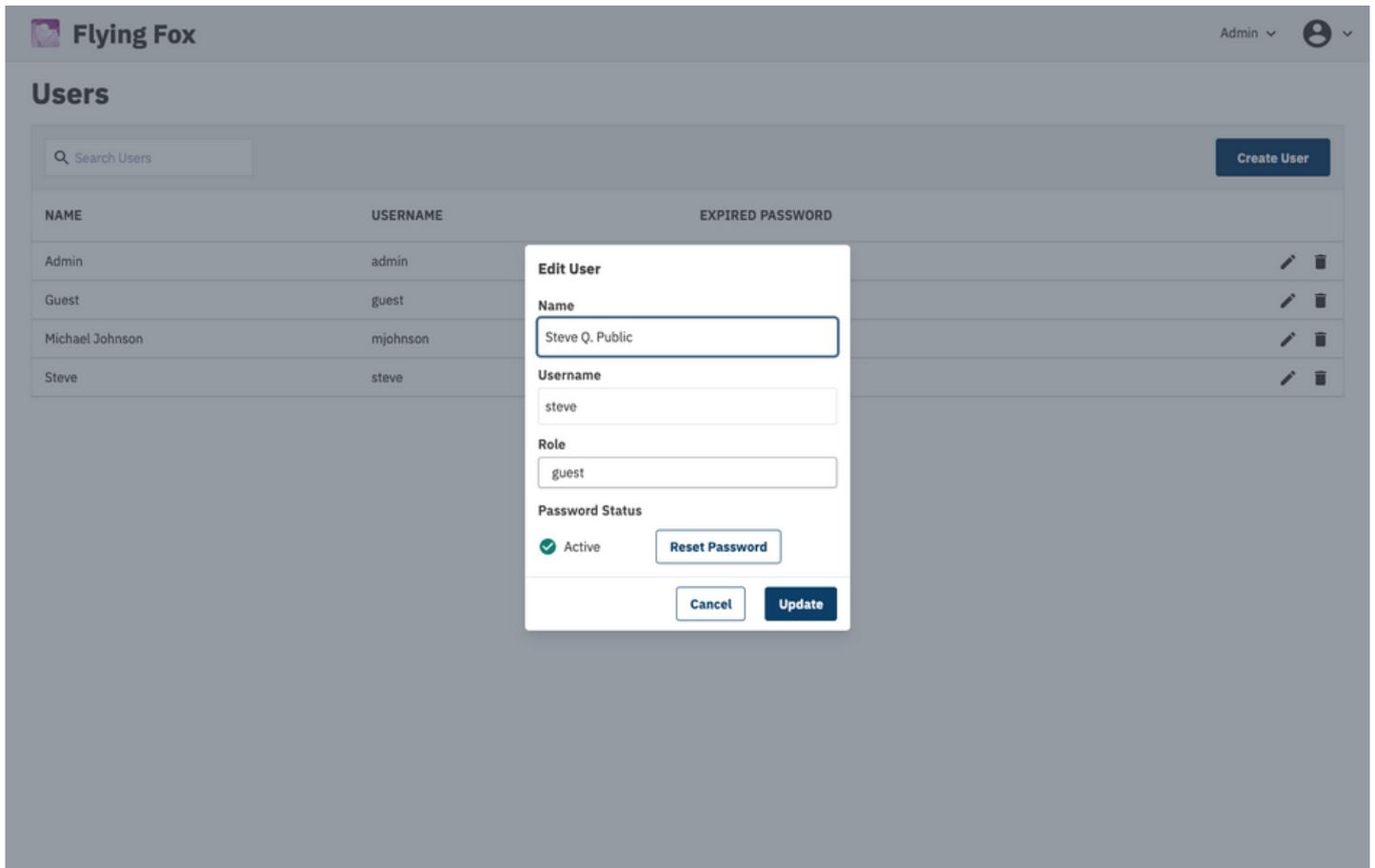
## MANAGING USERS

Flying Fox Enterprise is a multi-user, multi-role application. An administrator can create new users by selecting "Users" in the "Admin" menu.

Create a user with a name, a username, a password, and a role. The role can be admin or guest, the latter of which will not have access to the admin menu.

Once a user is created, the user will be prompted to change their password the first time they log in.

Admin users can edit users and reset their passwords.



*Figure 10: Managing Users*

## MANAGING SENSORS

Sensor health is displayed in the "Sensor" menu either at the top level or in the "Admin" menu.

Sensors with a green check status are operating normally.

## Sensors

[Sensor List](#) [Cellular Channels](#)

Search Sensors									
	STATUS	SENSOR ID	SITE	BUILDING	FLOOR	CONNECTED	SOFTWARE	CARDS	GROUP
ICD Mismatch	<span style="color: red;">●</span>	760K	Epiq Campus	EPIQ Hawaii	Maui	No	6.7.1	4	Default
	<span style="color: red;">●</span>	760E	N/A	N/A	N/A	No	6.11.3	4	Default
>	<span style="color: green;">●</span>	761H	Epiq Campus	HQ	Main	Yes	6.11.6	4	Default
	<span style="color: red;">●</span>	7602	N/A	N/A	N/A	No	6.11.6	4	Default
>	<span style="color: green;">●</span>	7613	Epiq Campus	HQ	Main	Yes	6.11.6	4	Default
∨	<span style="color: green;">●</span>	7612	Epiq Campus	HQ	Main	Yes	6.11.6	4	Default

Sensor Details		Sensor Health	
<b>CARD STATUS</b>		<b>SENSOR TIMESTAMP</b>	
Card 0 66811 DL	Card 1 66811 UL	<span style="color: green;">●</span> Synchronized	<b>CPU TEMPERATURE</b> <span style="color: green;">●</span> 56.9 °C
Card 2 4384 UL	Card 3 Scan	<b>INPUT VOLTAGE</b> <span style="color: green;">●</span> 48.20 V	<b>MEMORY AVAILABLE</b> <span style="color: red;">●</span> 20.3% Free

Figure 11: Managing Sensors

## TESTING SENSOR SSH CONNECTIONS

The "Test SSH Connection" button can be used to test the SSH connection to a sensor. This is useful for troubleshooting sensor connectivity issues and is required before updating sensor firmware. Once the SSH test is successful, connection and firmware version data will be updated in the sensors table.

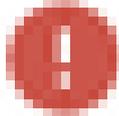
Figure 12: Testing SSH Connections

## SENSOR SSH CONNECTION STATUS

Once a SSH connection test is ran, statuses can either be failed with a red exclamation point icon or pass with a green checkbox icon.

---

Yes

SSH Test: 

---

Yes

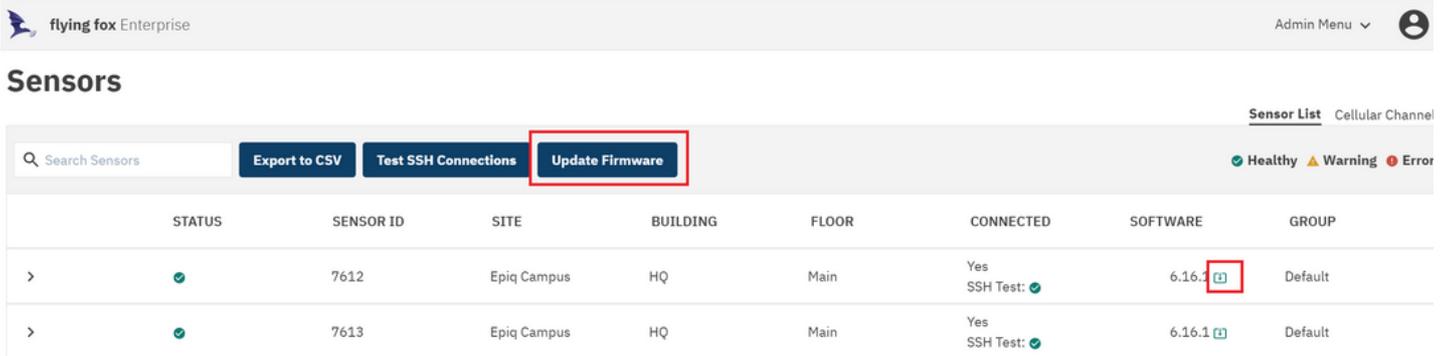
SSH Test: 

---

*Figure 13: Testing SSH Connections*

### **SENSOR FIRMWARE UPGRADE**

In order to update the sensor firmware, an SSH test must be conducted first to verify the sensor connection status and get firmware information. Once an SSH test has been run and at least one sensor has a firmware update available, the firmware update buttons are enabled. You can update the firmware for a single sensor by clicking the update icon next to the firmware version number in the sensor table or update all sensors by clicking the "Update Firmware" button above the sensors table.



**Sensors**

Search Sensors | Export to CSV | Test SSH Connections | **Update Firmware**

Healthy Warning Error

	STATUS	SENSOR ID	SITE	BUILDING	FLOOR	CONNECTED	SOFTWARE	GROUP
>	✓	7612	Epiq Campus	HQ	Main	Yes SSH Test: ✓	6.16.1 	Default
>	✓	7613	Epiq Campus	HQ	Main	Yes SSH Test: ✓	6.16.1 	Default

*Figure 14: Update Sensor Firmware*

## EXPORT SENSOR DATA TO CSV

Click "Export to CSV" to download a CSV file containing the sensor data. If an SSH connection test has been performed, the CSV will contain the connection status and firmware version data.



*Figure 15: Export Sensor Data*

## CHECKING SOFTWARE VERSION

The current Flying Fox Enterprise software version can be seen on the user profile page. This is accessed by selecting the user icon on the top right and clicking "Profile"

Admin Menu 

## User Profile

[Download Client State](#)

### User Information

**NAME**  
Admin

**USERNAME**  
admin

**ROLE**  
admin

**PASSWORD EXPIRED**  
No

### Reset Password

**CURRENT PASSWORD**

**NEW PASSWORD**

**CONFIRM NEW PASSWORD**

[Change Password](#)

### Software Version

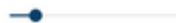
1.7.1

### Display Preferences

Play Detection Alerts

Enable Hashed IDs

Enable Active Bluetooth Scanning

**MINIMUM PARK TIME**  
27 

**SYSLOG SERVER ADDRESS**  
Enter an IP address or a hostname reachable on this network

[Change Address](#)

Figure 16: Checking Software Version

# MONITORING DETECTIONS

## VIEWING MULTIPLE FLOORS

The screenshot displays the monitoring interface for 'HQ'. At the top right, there is an 'Admin Menu' and a user profile icon. Below these, a dropdown menu is set to '1 Floor', which is highlighted with a red box. The main area shows a floor plan map with several detection icons (Wi-Fi and Cellular) and their associated sensor locations. A blue line connects a detection icon to its sensor locations. The left sidebar contains a 'Detections' section with a 'Time Filter' set to 'LIVE' and a 'Reset Time' button. Below this, there is a search bar and a list of detections categorized by device type: Wi-Fi Device (Cisco SPVTG), Cellular Device (Verizon Wireless / LTE), and Wi-Fi Device (Nest Labs Inc.). The bottom right corner of the map area has a 'Main' label.

**Figure 17:** Visible Floors Dropdown

The map view can be configured to display up to four floors by using the dropdown selector above the map which is highlighted with a red box in the image above.

## SENSOR MEASUREMENTS

In live view mode, sensor measurements for a detection can be viewed directly on the map by clicking a detection icon on the map. A line and RSSI measurement label will be drawn between the detection and each sensor involved in the detection. Click the detection again to remove the lines and labels.

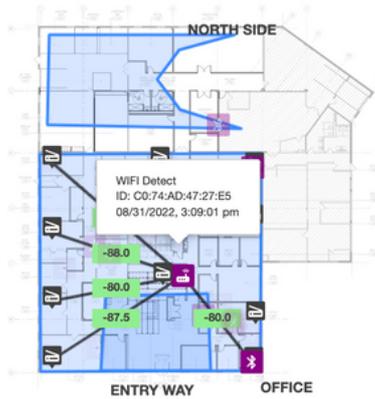


Figure 18: Sensor Measurements

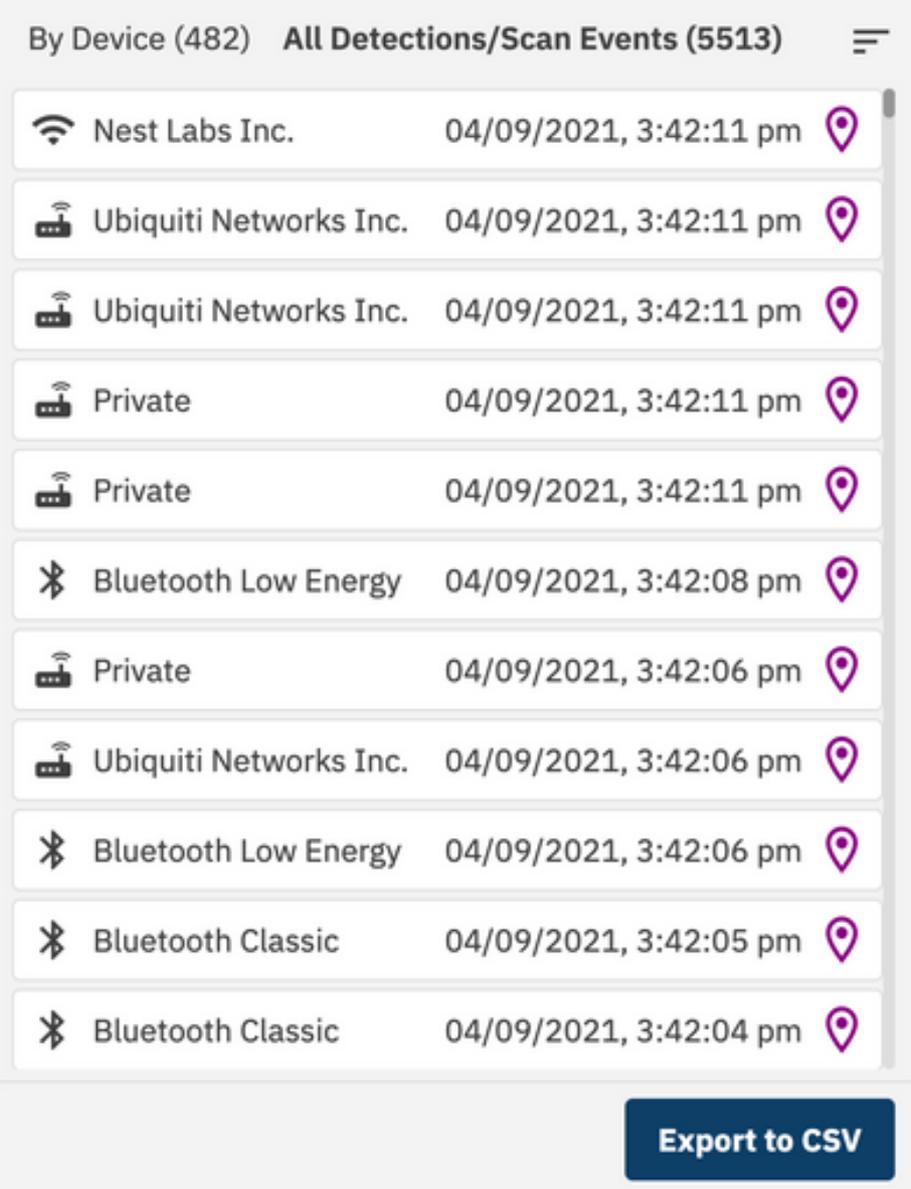
### GROUPING BY DEVICE OR EVENT

Device	Detections
Wi-Fi Device (NETGEAR)	34
Wi-Fi Device (Private)	57
Wi-Fi Device (Ubiquiti Networks Inc.)	64

Figure 19: Group or List View

The list of detections can be viewed in two modes: **By Device** or **All Detections**. When viewing By Device, the list will show cards for each detected device and will list the number of recent detections for that device. This view is shown above. When viewing All Detections, the list will show individual

detection events which is shown below. When returning to the list view from a details view, the list view will automatically scroll to the previously opened device/scan.



By Device (482)		All Detections/Scan Events (5513)	
	Nest Labs Inc.	04/09/2021, 3:42:11 pm	
	Ubiquiti Networks Inc.	04/09/2021, 3:42:11 pm	
	Ubiquiti Networks Inc.	04/09/2021, 3:42:11 pm	
	Private	04/09/2021, 3:42:11 pm	
	Private	04/09/2021, 3:42:11 pm	
	Bluetooth Low Energy	04/09/2021, 3:42:08 pm	
	Private	04/09/2021, 3:42:06 pm	
	Ubiquiti Networks Inc.	04/09/2021, 3:42:06 pm	
	Bluetooth Low Energy	04/09/2021, 3:42:06 pm	
	Bluetooth Classic	04/09/2021, 3:42:05 pm	
	Bluetooth Classic	04/09/2021, 3:42:04 pm	

[Export to CSV](#)

*Figure 20: All Detections List*

## CELLULAR DETECTIONS

Detections of cellular devices are shown as smartphone icons on the floor plan and the detections and devices pane. Cellular devices that have been detected through an RRC Connect Procedure (See Theory of Operation) will have an ID value located in the device summary card. In the example below, a device was identified as a T-Mobile device with the s-TMSI listed.

Clicking on one of the detections, further expands the data available to the user.

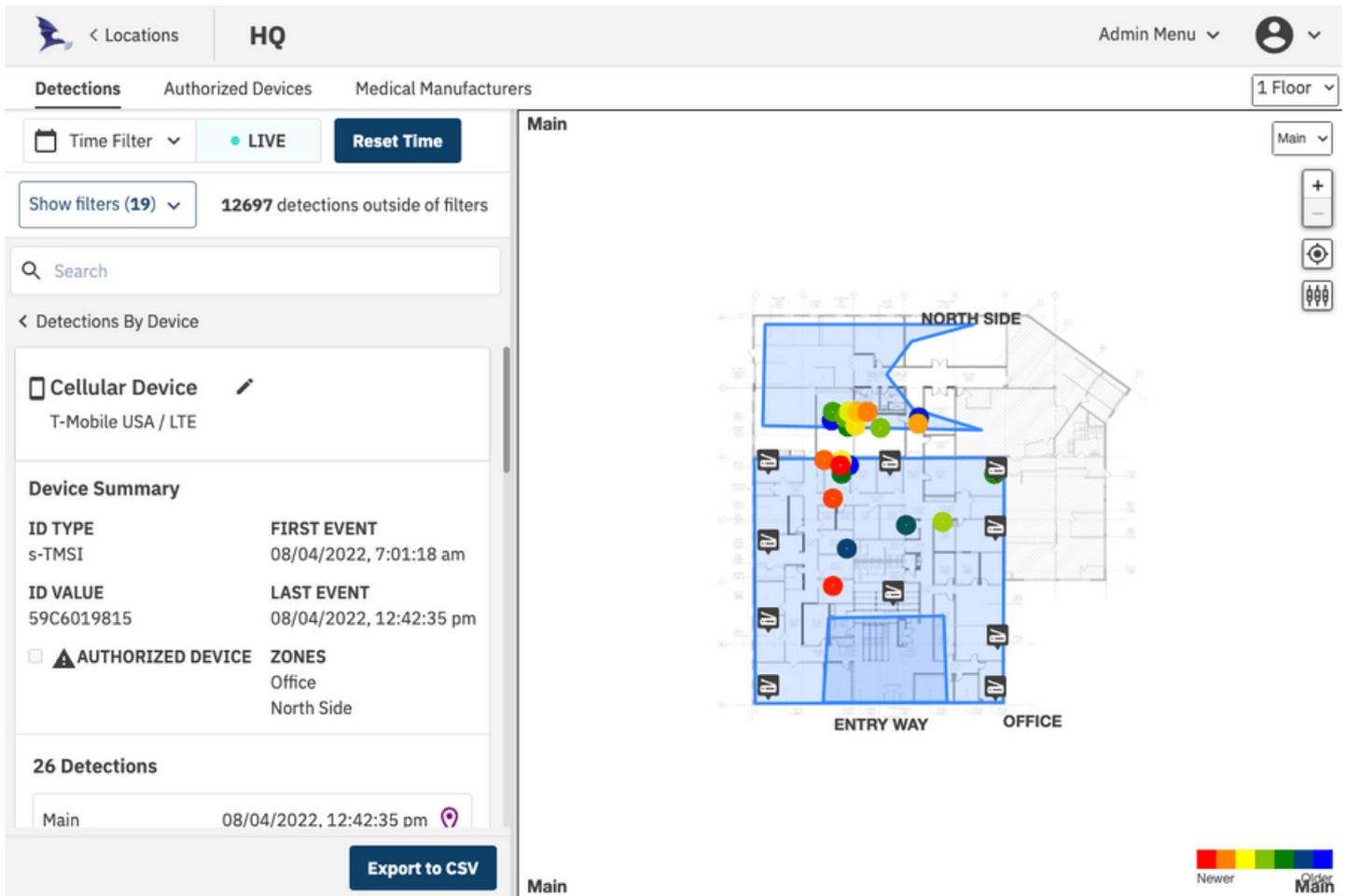


Figure 21: Cellular Detection Example

For each detection event associated with this device, band and channel information as well as sensors involved and power levels are presented. All of this data can be exported to a CSV file by using the "Export" button at the bottom of the pane.

Sensors that are involved in the estimate of detections will be highlighted.

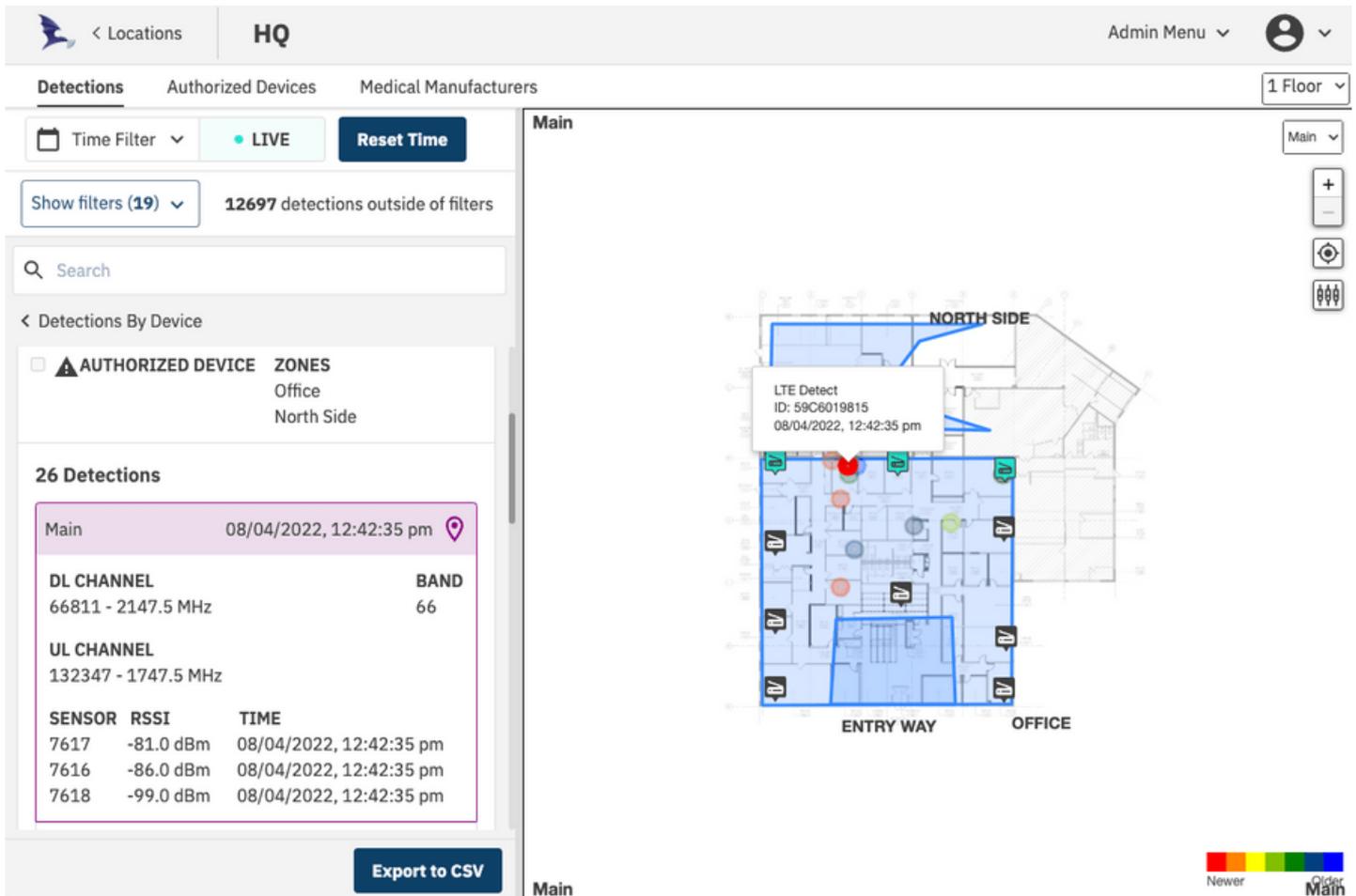


Figure 22: Cellular Detection Example

## Unknown Cellular Detections

Cellular detections with "ID TYPE" listed as "UNKNOWN" are groups of detections where the complete RRC Connect Procedure was not fully decoded, and therefore the device's temporary identifier was not captured. Without the identifier, the system is unable to uniquely identify each transmission. In these cases, different devices may be transmitting at the same time and therefore location data may be unreliable.

## Cellular Scan Events

As part of the detection procedure described in the Theory of Operation section, the system will look for any cellular activity in known cellular bands. These scan events indicate the likely presence of a cellular device, but because they cannot uniquely identify the device or properly synchronize the sensors to these events, location data from scan events is unreliable, and these events are filtered by default. To see these events in the detection pane and floor plan, check the "Include Scan Events" option in the filters list.

## BLUETOOTH DETECTIONS

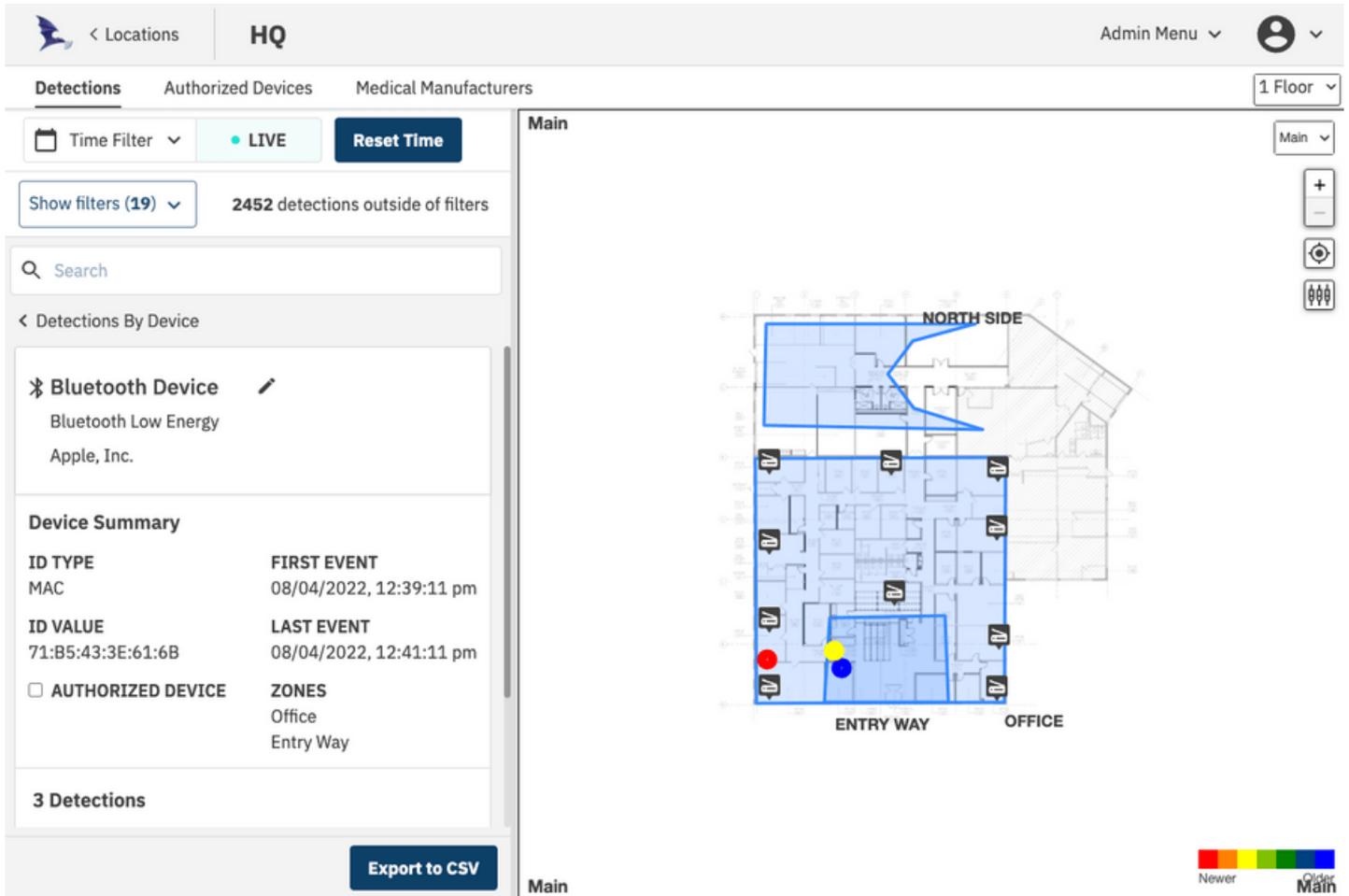


Figure 23: Bluetooth Detection Example

Detections of Bluetooth Classic and Bluetooth Low Energy (LE) devices will be shown on the floorpan as well as the detection and devices pane. Detected Bluetooth devices will have their MAC address in the device card, and additional information about each detection is available by clicking the detections list.

Sensors that are involved in the estimate of detections will be highlighted.

The screenshot displays the 'Monitoring Detections' interface for the 'HQ' location. The top navigation bar includes 'Locations', 'HQ', 'Admin Menu', and a user profile icon. Below this, there are tabs for 'Detections', 'Authorized Devices', and 'Medical Manufacturers', with a '1 Floor' dropdown menu. The interface is divided into a left sidebar and a main content area.

**Left Sidebar:**

- Time Filter:** Set to 'LIVE' with a 'Reset Time' button.
- Show filters (19):** 2498 detections outside of filters.
- Search:** A search bar for finding devices.
- Detections By Device:** A section for filtering by device, currently showing 'AUTHORIZED DEVICE' with zones 'Office' and 'Entry Way'.
- 3 Detections:** A list of recent detections:
 

SENSOR	RSSI	TIME
7612	-83.8 dBm	08/04/2022, 12:40:11 pm
76J1	-84.1 dBm	08/04/2022, 12:40:11 pm
76J2	-97.0 dBm	08/04/2022, 12:40:21 pm
- Export to CSV:** A button to export the detection data.

**Main Content Area:**

- Map:** A floor plan of the 'Main' floor showing 'NORTH SIDE', 'ENTRY WAY', and 'OFFICE'. A yellow dot indicates a Bluetooth detection at 08/04/2022, 12:40:11 pm. A tooltip provides details: 'BLUETOOTH Detect ID: 71:B5:43:3E:61:6B 08/04/2022, 12:40:11 pm'.
- Map Controls:** Includes a 'Main' dropdown, zoom in (+) and zoom out (-) buttons, a location pin icon, and a legend for 'Newer' (red) and 'Older' (blue) detections.

Figure 24: Bluetooth Detection Example

The device can be given an alias / friendly name by clicking the pencil icon beside the device name in the device card. Additionally, a user can search for devices by entering the friendly name, MAC address, carrier, technology, or manufacturer in the search bar.

### Configuring Passive Bluetooth Detection

As noted in the Theory of Operation section, Bluetooth Classic detection can be done through active inquiry or passive monitoring. Bluetooth LE detection is always passive.

To enable active inquiry of Bluetooth Classic devices select the "Enable Active Bluetooth Scanning" option in the user profile page. Note that when this option is clear, the system will be completely passive.

**User Profile**

[Download Client State](#)

**User Information**

**NAME**  
Admin

**USERNAME**  
admin

**ROLE**  
admin

**PASSWORD EXPIRED**  
No

**Reset Password**

**CURRENT PASSWORD**

**NEW PASSWORD**

**CONFIRM NEW PASSWORD**

[Change Password](#)

**Software Version**  
1.7.1

**Display Preferences**

Play Detection Alerts

Enable Hashed IDs

Enable Active Bluetooth Scanning

**MINIMUM PARK TIME**  
27

**SYSLOG SERVER ADDRESS**  
Enter an IP address or a hostname reachable on this network

127.0.0.1

[Change Address](#)

*Figure 25: Configuring Passive Bluetooth Detection*

## Bluetooth Classic Passive Piconet Connections

Bluetooth devices in a piconet will share the same lower address part (LAP) and be grouped together as a single device. For devices in a piconet, that is the LAP of the master. The "Show Piconet Connections" map display preference will draw connecting lines between bluetooth classic passive detections that have the same LAP as long as the LAP is not a reserved value

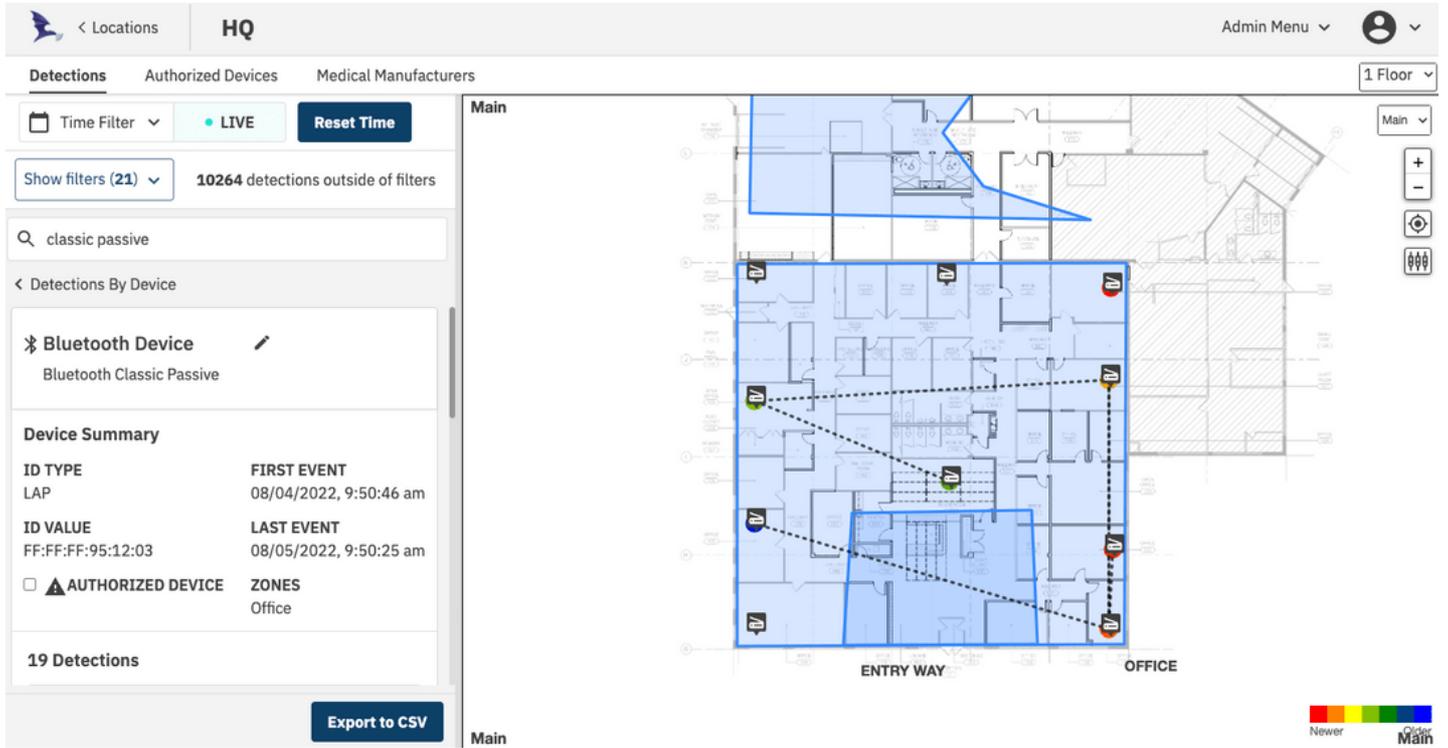


Figure 26: Piconet Connections

### WI-FI DETECTIONS

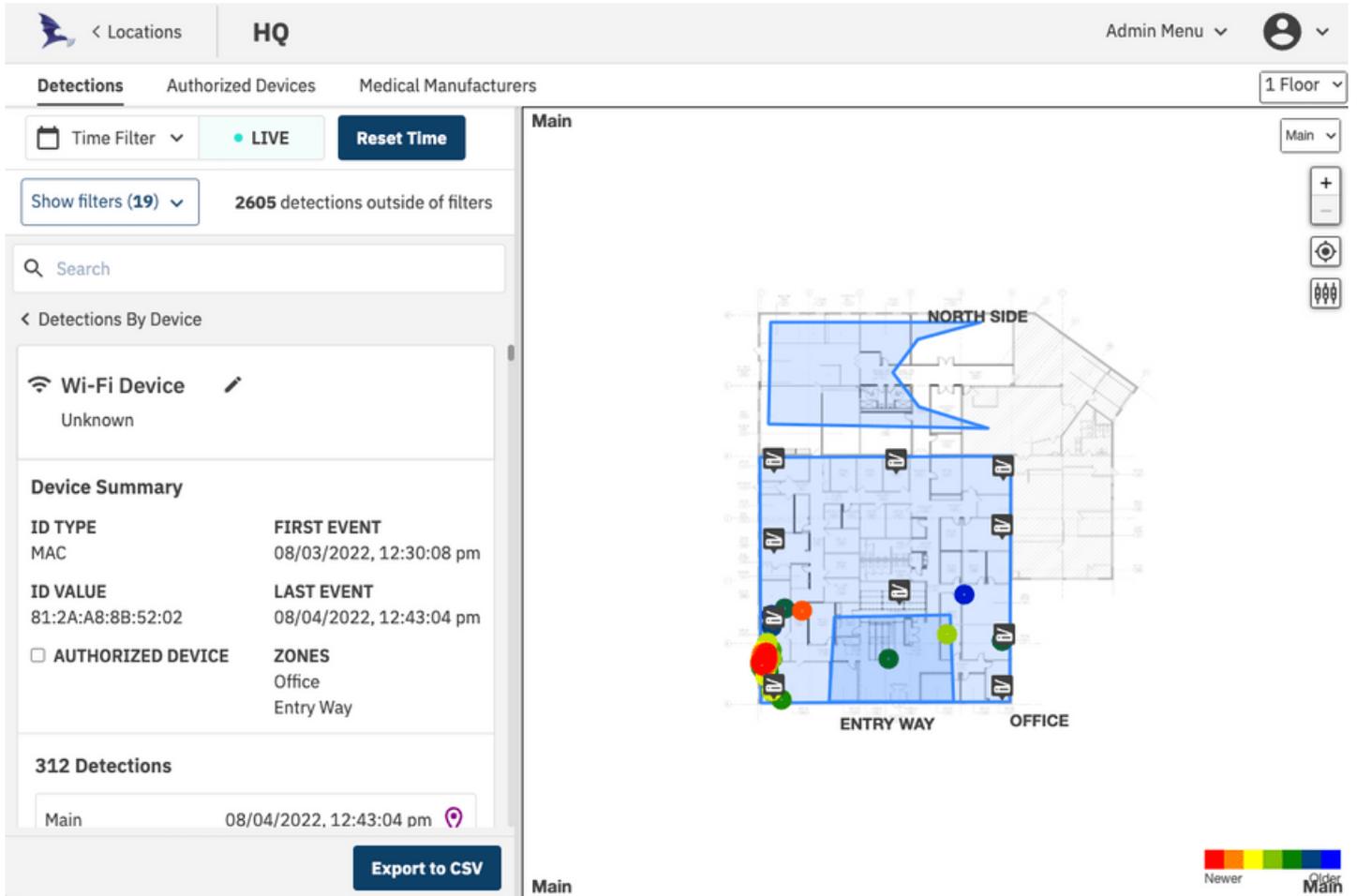


Figure 27: technology selector

Detections of Wi-Fi devices will be shown on the floor plan as well as the detection and devices pane. Detected devices will have their MAC address in the device card, and additional information about each detection is available by clicking the detections list.

Sensors that are involved in the estimate of detections will be highlighted.

### DEVICE ALIAS / FRIENDLY NAME

Devices can be given an alias / friendly name by clicking the pencil icon beside the device name in the device card.

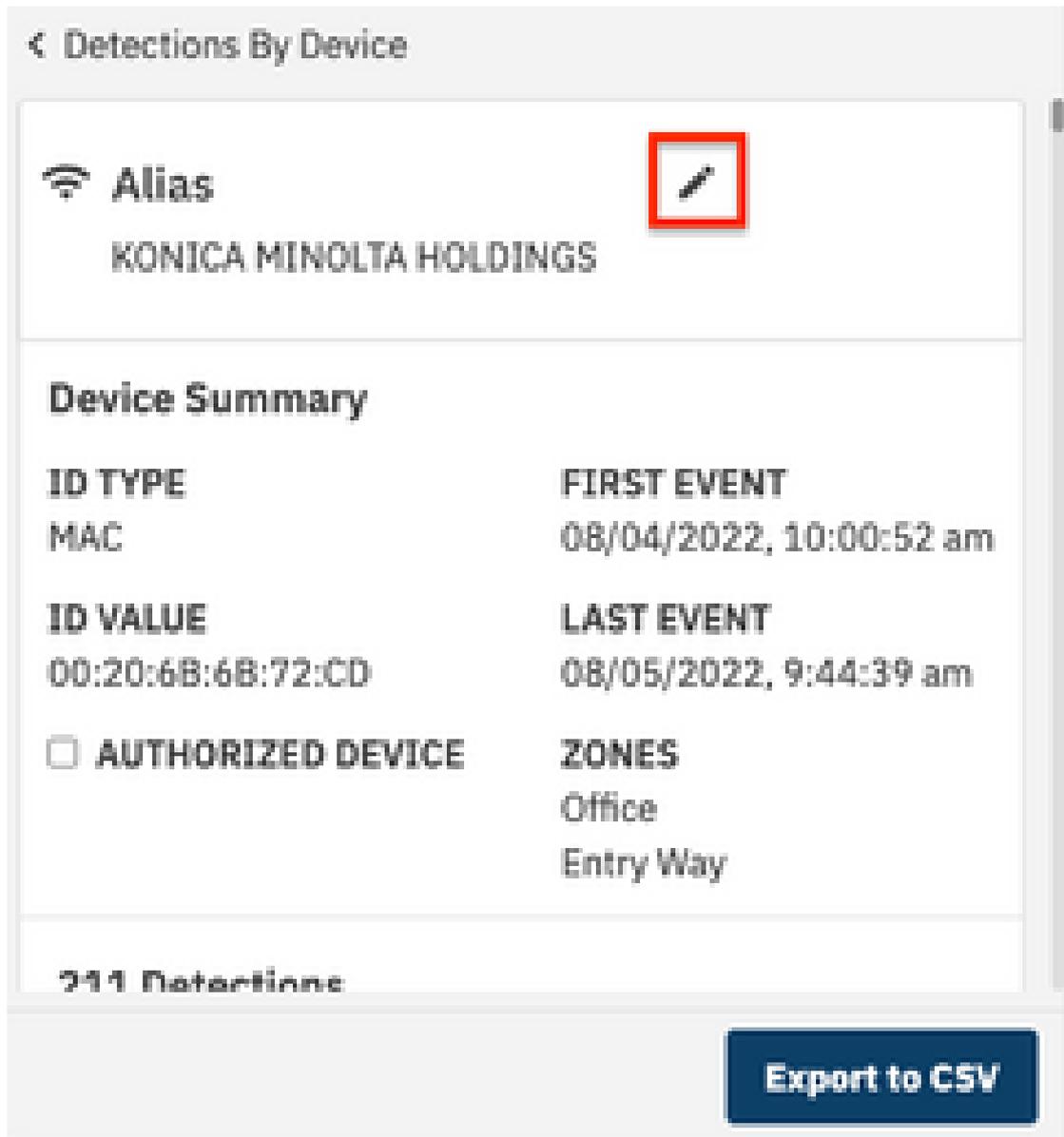


Figure 28: device alias

### DEVICE/SCAN DETAILS URL SHARING

When clicking into a device/scan details, the URL will be updated with information related to the selected element. This is useful for sharing information about a specific device or scan with other users. The URL can be as specific as a device detail, a device detail's detection, or even the sensor

for a detection. You can also click on a detection on the map to show the pop up details and click "View Details" to go to that detection's details page with the updated URL.

The screenshot shows a web application interface for monitoring detections. The browser address bar contains the URL: `http://localhost:3000/buildings/1/detections?deviceId=30b59c0f-8d69-4653-beea-824d6d87e8e1&detectionId=10fb9039-adeb-48bc-9939-7ee0eb8faddc`. The interface includes a sidebar on the left with navigation options like "Locations" and "HQ", and a main content area displaying a floor plan map of the "Main" floor. A detection popup is visible on the map, showing details for a "WIFI Detect" event. The sidebar also contains a "Device Summary" section and a "1 Detections" table.

**Device Summary**

ID TYPE	FIRST EVENT
MAC	09/07/2023, 3:48:15 pm
ID VALUE	LAST EVENT
CE:CE:29:90:64:89	09/07/2023, 3:48:15 pm
<input type="checkbox"/> AUTHORIZED DEVICE	ZONES
	Office

**1 Detections**

CHANNEL	BAND	
9 - 2452 MHz	2.4	
SENSOR	RSSI	TIME
7617	-54.0 dBm	09/07/2023, 3:48:15 pm
7613	-63.0 dBm	09/07/2023, 3:48:15 pm
761F	-69.0 dBm	09/07/2023, 3:48:15 pm
7618	-70.0 dBm	09/07/2023, 3:48:15 pm
761H	-76.0 dBm	09/07/2023, 3:48:15 pm

Figure 29: Details URL

## FILTERS

In a busy building the system can capture and display a large amount of data. To simplify the system monitoring, the system provides a number of filtering options. Applied filters are saved in local storage on a per user basis and will be reapplied when redirecting back to the building detections page.

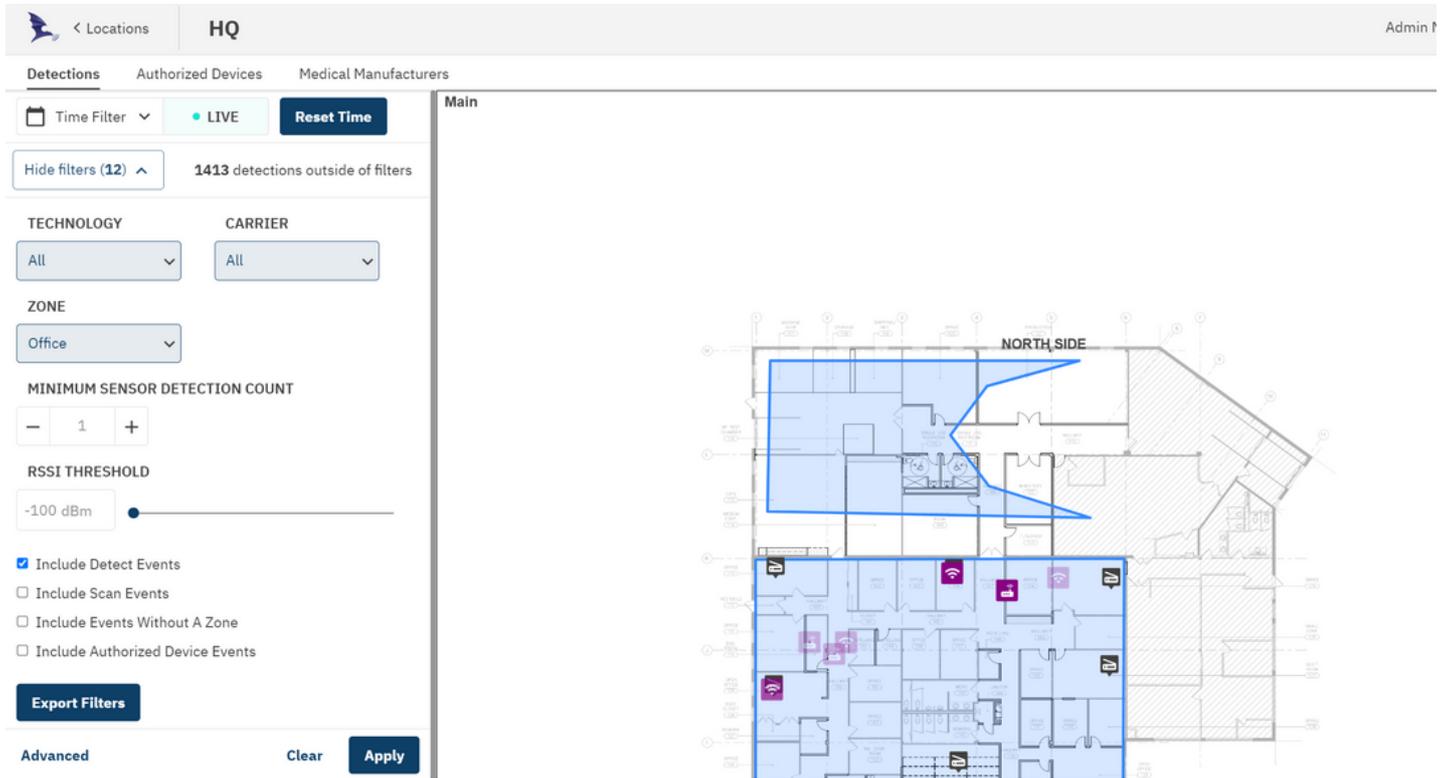
### BY TECHNOLOGY

The screenshot displays the 'HQ' location interface. On the left, the 'Detections' filter panel is active, showing 'LIVE' status and 1306 detections outside of filters. The 'TECHNOLOGY' dropdown is set to 'Cellular', and the 'CARRIER' dropdown is set to 'All'. The 'RSSI THRESHOLD' is set to -100 dBm. The 'Include Detect Events' checkbox is checked. The main view shows a floor plan with a blue shaded area labeled 'NORTH SIDE'.

**Figure 30: Technology Filter**

Detections can be filtered by technology (Cellular, Wi-Fi, and Bluetooth), and cellular detections can be filtered by carrier in the filter pane. Click "Apply" to apply the filters to the current view.

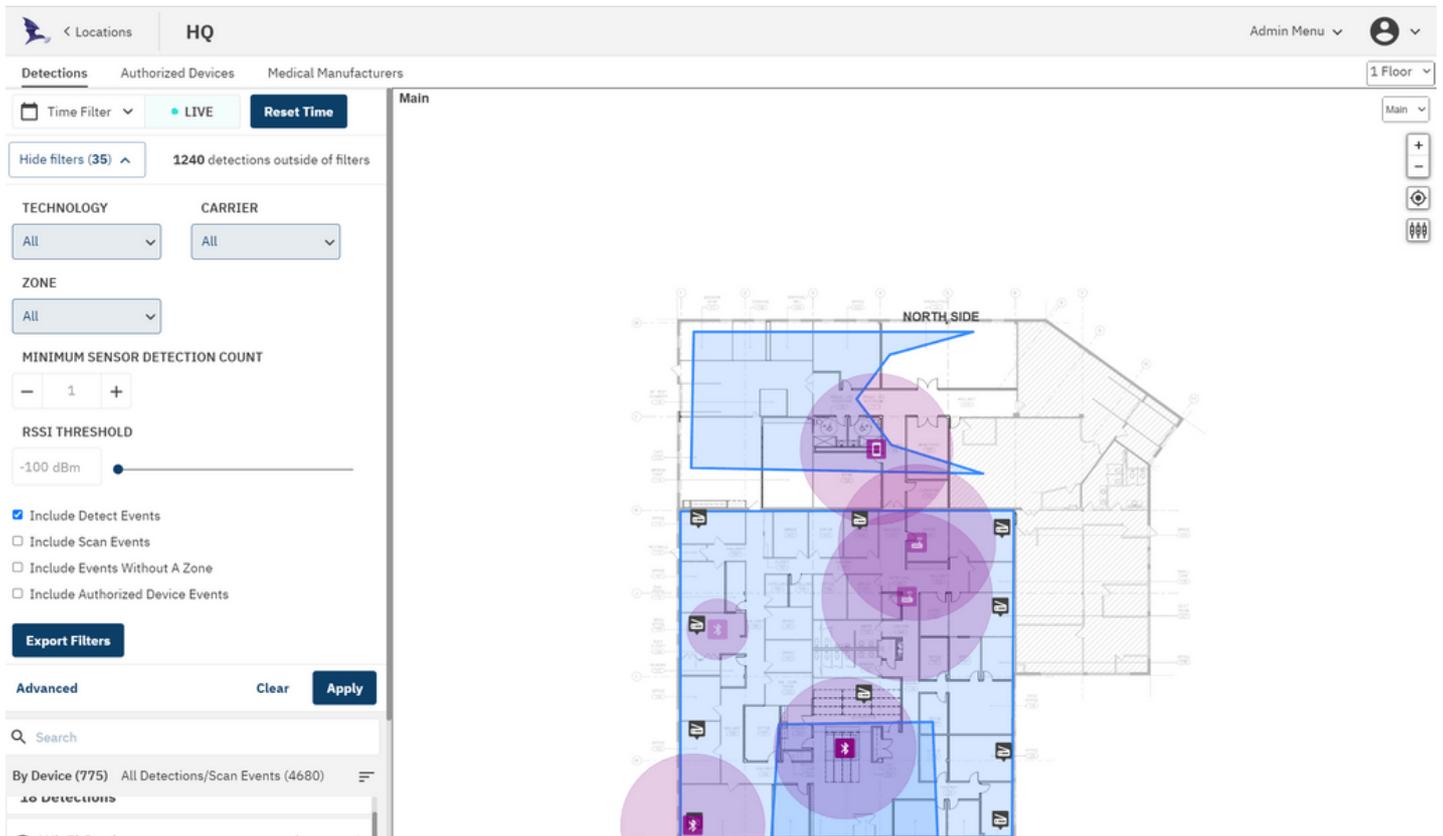
### BY ZONE (GEO-FENCE)



**Figure 31:** Zone Filter

The user can use zones to filter the detections that are displayed. The user may select one or more zones to filter in the "Zone" menu in the filter pane. Additionally to see all detections, even outside the listed zones, clear the "Include Events Without A Zone" checkbox on the detections pane. Click "Apply" to apply the filters to the current view.

## EXCLUDING POSSIBLE UNRELIABLE LOCATION ESTIMATES



**Figure 32: Improving Location Reliability**

The system uses a proprietary location estimation method to estimate the location of devices based on simultaneous detections by the sensors in the system. The system triangulates the position of the device based on the measurements made by the sensors. Location estimation accuracy is better when more sensors are involved in the calculation. Location estimates are also most accurate when their signal strength is above the noise floor.

Due to the nature of radio communication, it is possible that in some cases device transmissions will not be detected by all of the nearest sensors. This can be caused by interference, fading effects, or even covering a device with dense material.

Since devices in monitored areas are usually detected many times, it may be desirable to exclude detection events that may have unreliable location data.

Detection events that are received by fewer than 3 sensors cannot be triangulated. Detections by only two sensors will have poor location accuracy, and detections by only one sensor will have no location accuracy -- the system estimates their location at the same location of the single sensor that received them. To eliminate these unreliable estimates from the detections and device pane and the floor plan, set the "MINIMUM SENSOR DETECTION COUNT" to 3 in the filter pane.

To eliminate estimates that may be compromised by interference or noise, set the "RSSI THRESHOLD" to some figure above the local noise floor. It should be noted that setting this too high will eliminate all detections, and this setting should be changed with care.

As described in the cellular detection section, scan events indicate the likelihood of a device in the area, but because they cannot identify the device or fully decode the transmission, it may be that these detections came from devices outside the area or other interference. These events will provide unreliable location estimates.

Detection events are cellular detections where the full RRC Connect Procedure was not decoded. These events indicate a device detection, but because these do not yield a unique identifier, it is possible that more than one device in the area was transmitting at the same time. In these cases, detect event location estimates will be unreliable.

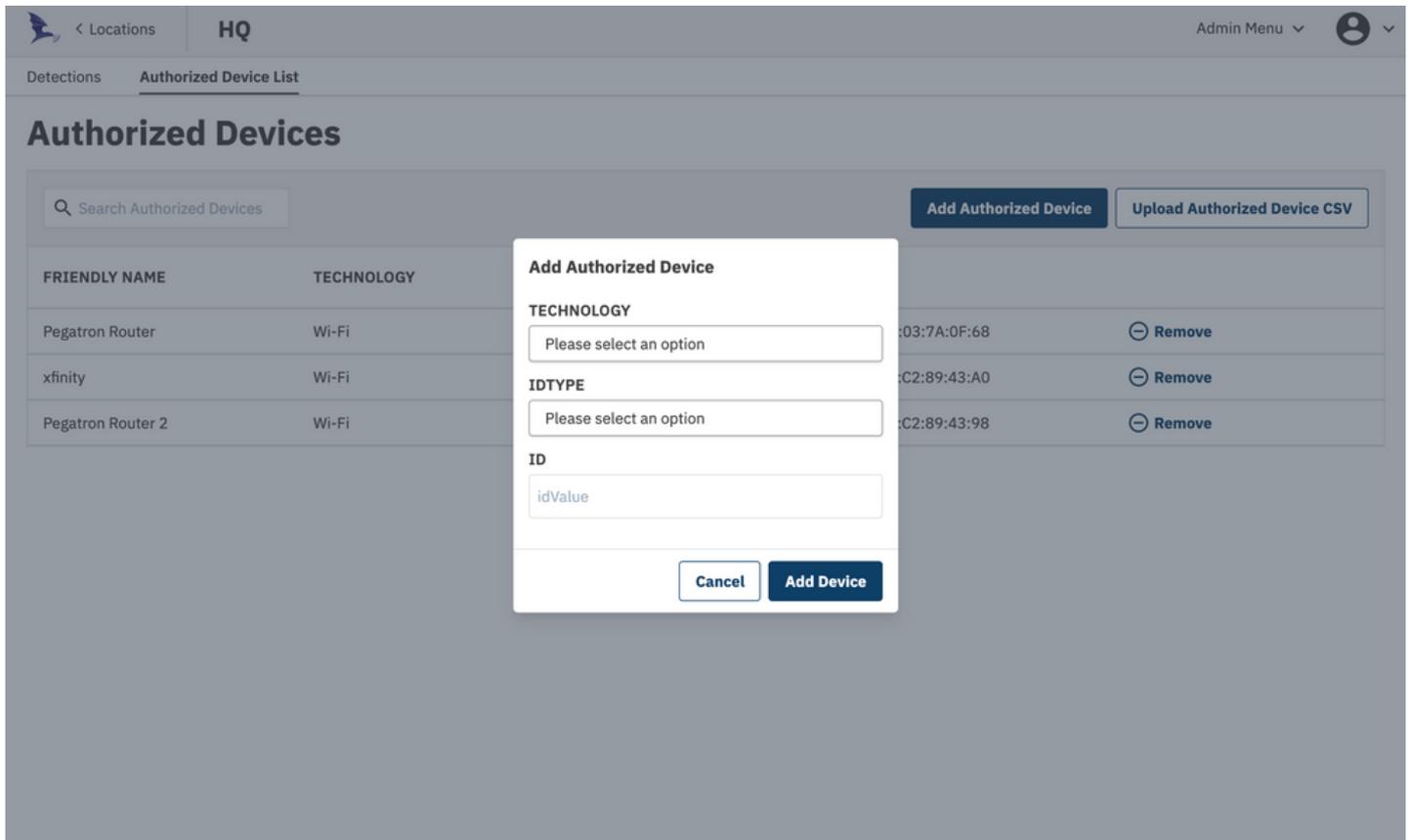
## AUTHORIZED DEVICES

The screenshot displays the 'AUTHORIZED DEVICES' section of the Epiq Flying Fox Enterprise interface. The interface includes a navigation bar with 'Locations' and 'HQ', a search bar, and a 'Detections' pane. The 'AUTHORIZED DEVICES' pane shows a list of devices, with one device highlighted: 'Wi-Fi Device' from 'Nest Labs Inc.' with MAC address '64:16:66:7A:0F:FA'. The 'AUTHORIZED DEVICE' checkbox is checked and highlighted with a red box. The main area shows a floor plan with various detection points and a color-coded legend for 'Newer' and 'Older' detections.

**Figure 33:** Authorized Devices

In some cases, devices in the environment are known and trusted, and it is desirable to exclude these devices from the devices, detections pane, and the floor plan. In those cases, the Authorized Devices feature may be used. To make a detected device an Authorized Device, check the "AUTHORIZED DEVICE" option on the device card.

Authorized Devices are tracked by their MAC address for Wi-Fi and Bluetooth devices. Note that some Wi-Fi and Bluetooth devices make use of randomized MAC addresses, which may cause their MAC addresses to change.



**Figure 34:** Add Authorized Device

Authorized devices can also be added to the list in the Authorized Devices menu at the top of the window.

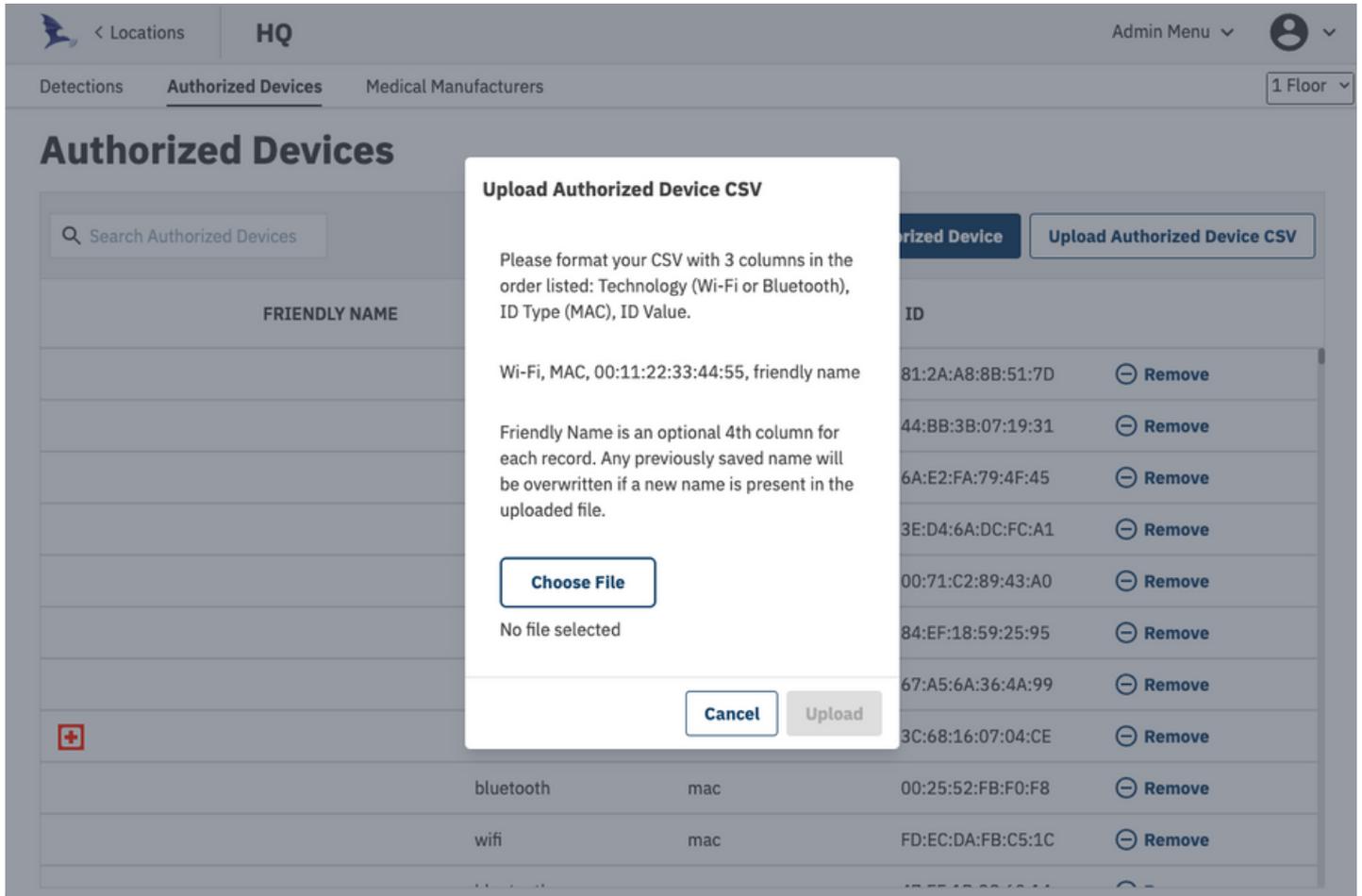


Figure 35: Authorized Device CSV

Authorized devices can also be imported from a CSV file.

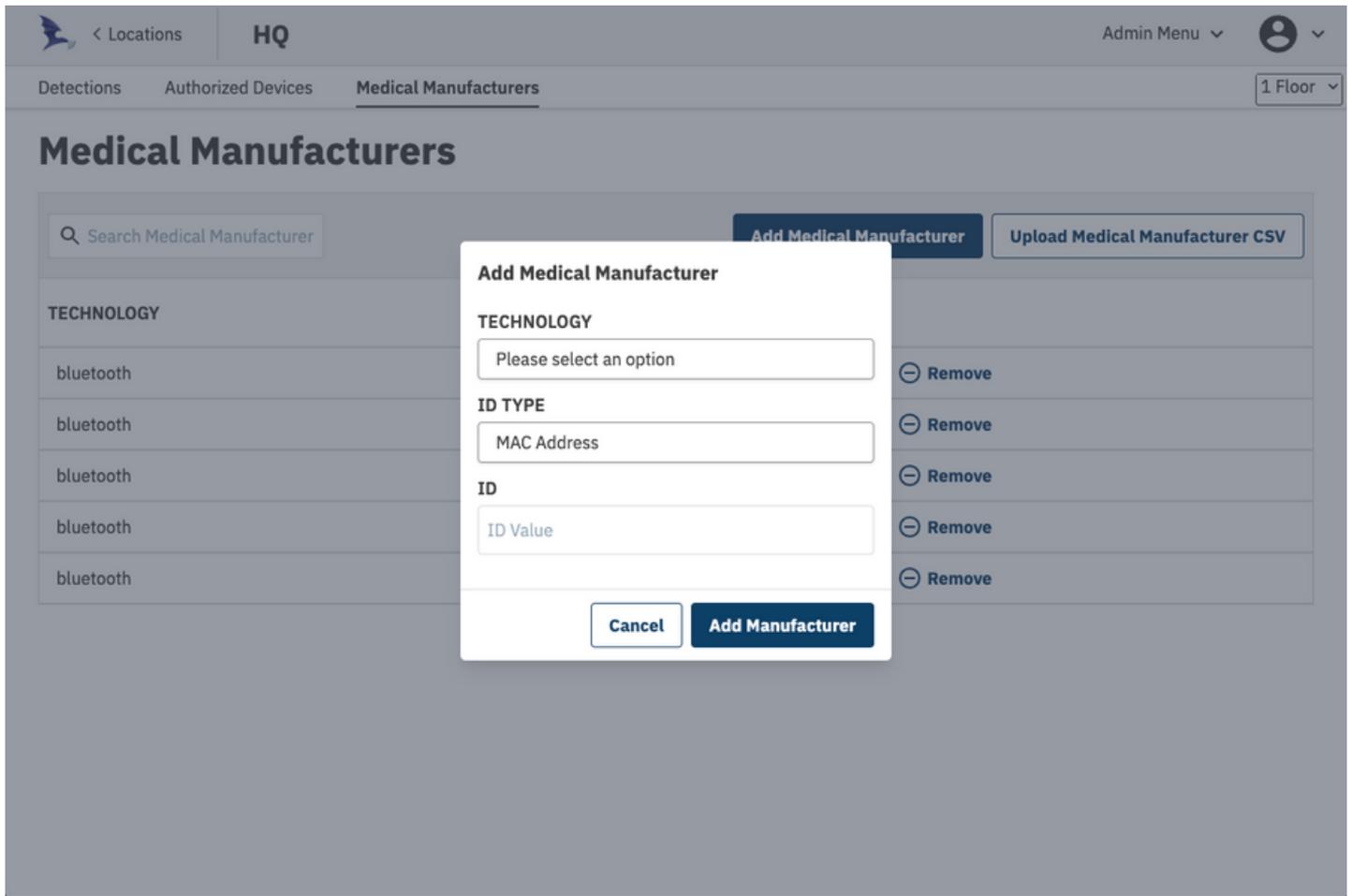
## MEDICAL MANUFACTURERS

The screenshot displays the 'Medical Manufacturers' section of the software. At the top, there is a navigation bar with a logo, '< Locations', and 'HQ'. To the right, there is an 'Admin Menu' dropdown and a user profile icon. Below this, a secondary navigation bar contains 'Detections', 'Authorized Devices', and 'Medical Manufacturers' (which is highlighted). A '1 Floor' dropdown is also present. The main content area features a search bar labeled 'Search Medical Manufacturer', a blue 'Add Medical Manufacturer' button, and a white 'Upload Medical Manufacturer CSV' button. Below these is a table with the following data:

TECHNOLOGY	ID	
bluetooth	3C:68:16	⊖ Remove
bluetooth	4D:0F:D7	⊖ Remove
bluetooth	69:FC:16	⊖ Remove
bluetooth	6A:C0:57	⊖ Remove
bluetooth	D8:14:DF	⊖ Remove

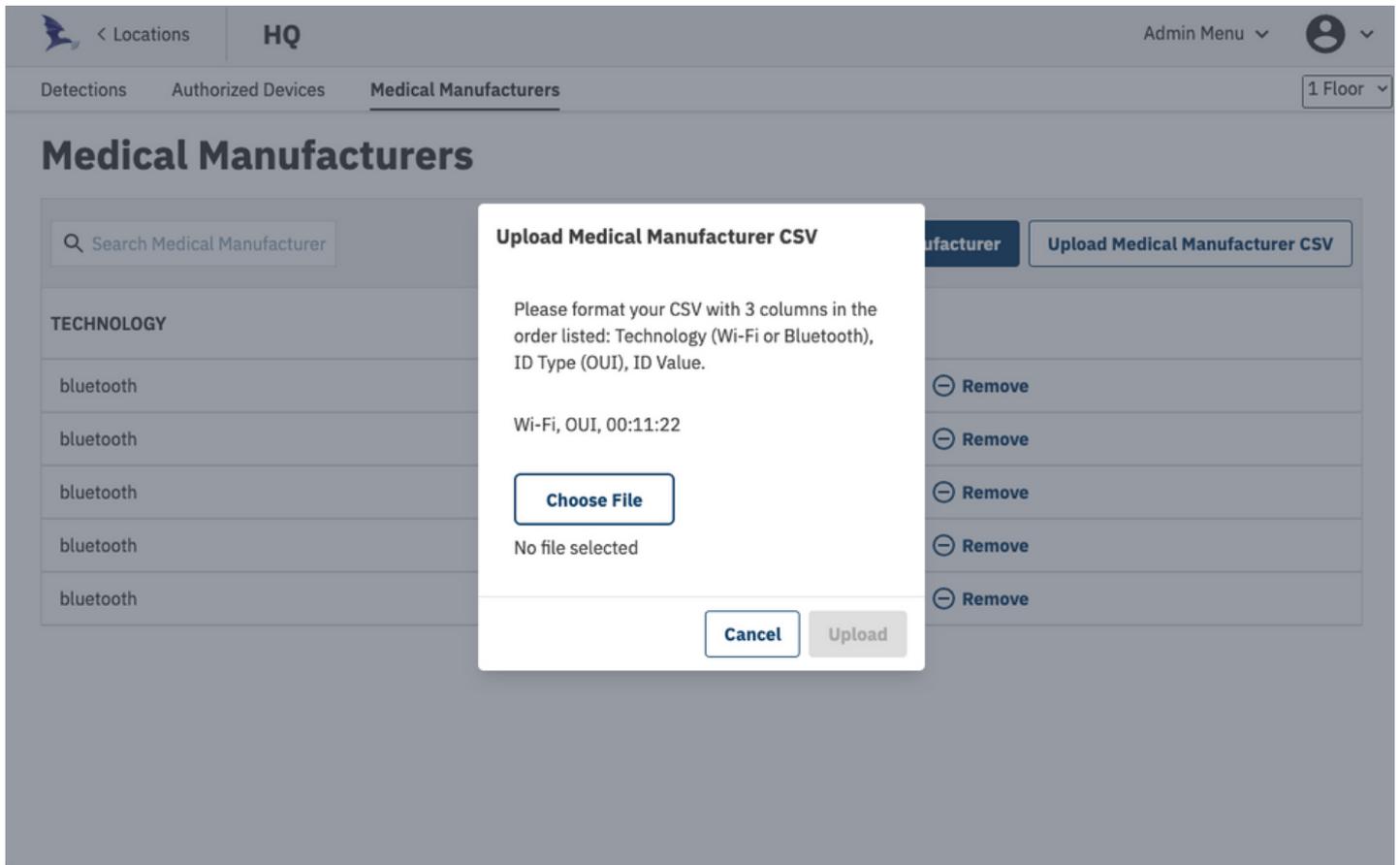
**Figure 36:** Medical Manufacturers

It may be desirable to differentiate the way medical devices appear in the detections list and on the floor plan. In this case, the Medical Manufacturers feature may be used. These devices are identified by an Organizational Unique Identifier (OUI). The OUI is the first three bytes of the six-byte field and is administered by the IEEE.



**Figure 37:** Add Medical Manufacturer

Medical Manufacturers can be added to the list in the Medical Manufacturers menu at the top of the window.



**Figure 38:** Authorized Medical Manufacturer CSV

Medical Manufacturers can also be imported from a CSV file.

# HISTORICAL VIEW

The screenshot displays the 'Historical View' interface. At the top, there's a navigation bar with 'Locations' and 'HQ', and a user profile 'Admin'. Below this, a 'Detections' section features a red warning banner: 'Sensors 7602, 760E, 760K, 7630 and 7632 are not making accurate detections. See details'. The main area is divided into a time filter section on the left and a floor plan on the right. The time filter includes a 'Time Filter' dropdown, a 'LIVE' indicator, and a 'Reset Time' button. Below this is a date range selector showing '12/06/2020 10:20 AM to 12/07/2020 11:59 PM'. Two calendar views for November and December 2020 are shown, with the 7th of December highlighted. To the right of the calendars are radio buttons for 'Last hour', 'Last 12 hours', 'Last 24 hours', 'Last 7 days', 'Last 30 days', and 'Last 90 days'. A 'Clear' button and an 'Apply' button are at the bottom of the time filter. The floor plan on the right shows a building layout with a blue path and several detection points. A purple circle highlights a specific area on the map. A 'Main' dropdown menu is visible in the top right corner. At the bottom left, a 'Wi-Fi Device' section shows 'PEGATRON CORPORATION' with an 'Export to CSV' button.

**Figure 39:** Historical View

In addition to presenting the user real-time detections in the device and detections pane and floor plan, a user can select a historical timeframe to see all devices and detections for an arbitrary time period.

Click the time selector at the top right of the detections window. The system allows for a quick select of time periods or for the user to specify start and end times and dates.

To go back to real time display, click the "Reset Time" button.

**NOTE:** Selecting a time period that is too long in a busy system will cause too much data to be fetched from the database and slow the user interface as well as truncate data. To ensure there is no data truncation, select as small a time window as practical.

When in Historical View, detections will be added to the map with a color gradient applied where red indicates the newest detections and blue indicates the oldest.

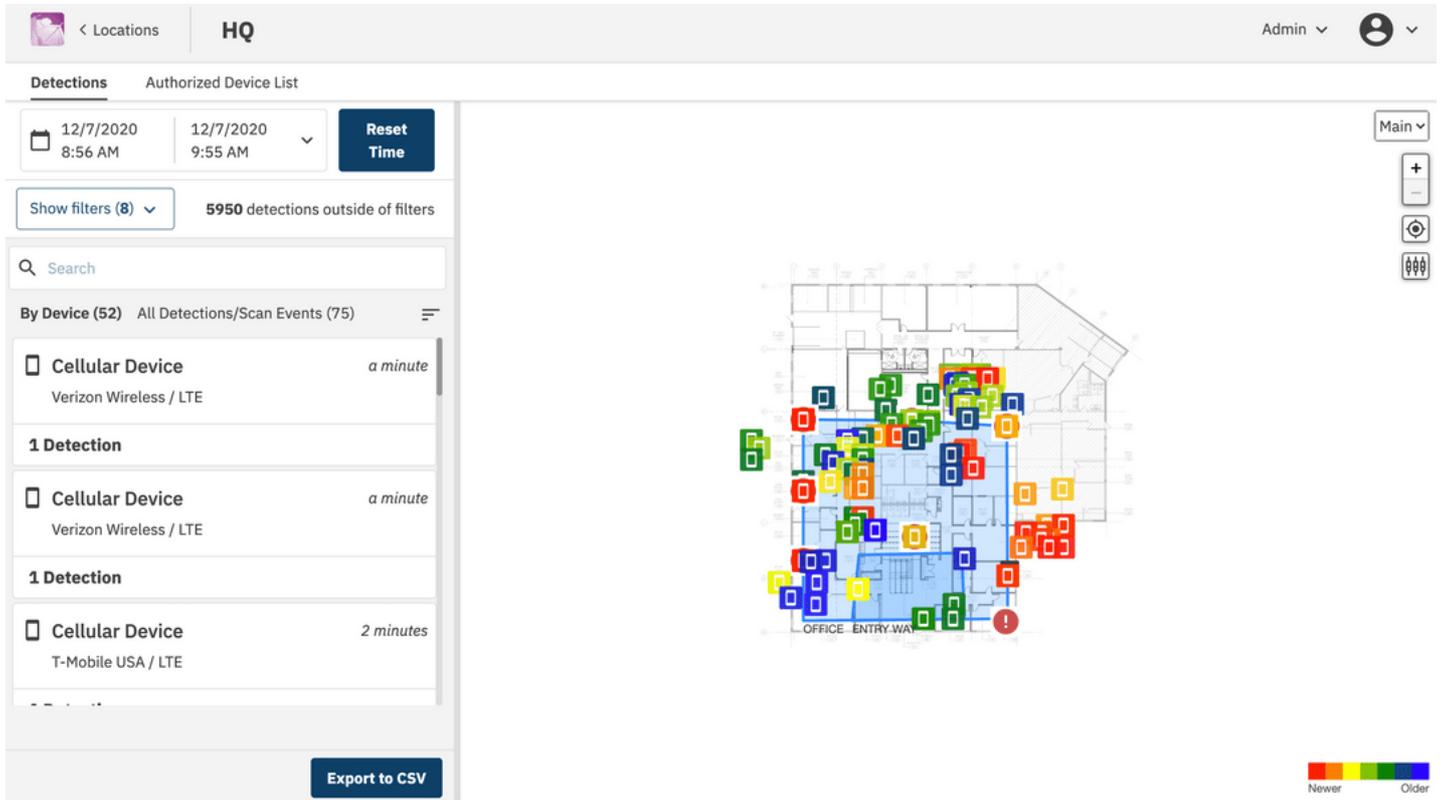


Figure 40: Historical View

# CONFIGURING SYSLOG

**Admin Menu**

## User Profile

[Download Client State](#)

### User Information

**NAME**  
Admin

**USERNAME**  
admin

**ROLE**  
admin

**PASSWORD EXPIRED**  
No

### Reset Password

**CURRENT PASSWORD**

**NEW PASSWORD**

**CONFIRM NEW PASSWORD**

[Change Password](#)

### Software Version

1.7.1

### Display Preferences

Play Detection Alerts

Enable Hashed IDs

Enable Active Bluetooth Scanning

**MINIMUM PARK TIME**  
27

### SYSLOG SERVER ADDRESS

Enter an IP address or a hostname reachable on this network

[Change Address](#)

**Figure 41:** Configuring Syslog

All geo-tagged detection and event data from the system can be configured to be sent to syslog. All of the data presented to the user on the interface will be made available to the syslog server. To configure syslog logging, set the server's IP address and configure the syslog server for UDP syslog reception on port 514.

## DISPLAY PREFERENCES

The screenshot displays the 'Display Preferences' dialog box overlaid on a floor plan visualization. The dialog box contains the following settings:

- NEW DETECTIONS FADE AFTER (MS):** A text input field containing the value '4000'.
- Show Sensors:** A checked checkbox.
- Display Estimate Confidence:** An unchecked checkbox.
- Show Piconet Connections:** An unchecked checkbox.

The floor plan visualization shows a layout with an 'ENTRY WAY' and an 'OFFICE'. The 'Main' label is visible in the top right corner of the visualization area.

**Figure 42:** Display Preferences

The user can choose how the location visualization on the floor plan works to best fit the user's needs. Press the slider bar icon at the right of the floor plan to access these preferences.

When in real time display mode, detections will be highlighted on the map and will fade after a set period of time.

Sensor icons can be hidden from view using the "Show Sensors" checkbox.

The display of variable sized circles associated with estimate uncertainty can be configured with the "Display Estimate Confidence" option.

"Show Piconet Connections" will draw connecting lines between bluetooth classic passive detections that don't have reserved LAP values.

**User Profile**

[Download Client State](#)

### User Information

**NAME**  
Admin

**USERNAME**  
admin

**ROLE**  
admin

**PASSWORD EXPIRED**  
No

### Reset Password

**CURRENT PASSWORD**

**NEW PASSWORD**

**CONFIRM NEW PASSWORD**

[Change Password](#)

### Software Version

1.7.1

### Display Preferences

Play Detection Alerts

Enable Hashed IDs

Enable Active Bluetooth Scanning

**MINIMUM PARK TIME**  
27

**SYSLOG SERVER ADDRESS**  
Enter an IP address or a hostname reachable on this network

127.0.0.1

[Change Address](#)

**Figure 43:** Configuring Hashed IDs

In some cases it may be desirable to obfuscate actual MAC addresses in the application window. To use hashed values instead select the "Enable hashed IDs" option in the user profile window.

# THEORY OF OPERATION

## WI-FI DETECTION

The Wi-Fi detection engine in the Flying Fox Sensor detects 802.11a/b/g/n/ac<sup>1</sup> access points and device transmissions. These technologies use 56 (mostly overlapping) channels between the 2.4G and 5G bands. In order to decode the necessary information for identification and location each channel must be decoded individually.

The system presently iterates through the Wi-Fi channels, dwelling on each for approximately 1 second and completing a scan in approximately 90 seconds.

This means that the probability of detection of a short, single burst is approximately 1%. However, a connected Wi-Fi device in practice produces a large amount of traffic spread over time. Even a seemingly idle Wi-Fi device takes part in physical layer management messaging, MAC layer management messaging, and network protocol items such as TCP acks and keep-alives. This is in addition to background messaging for applications on the PED. If a device is connected and transmits at least one packet every second in the course of 90 seconds, the probability it will be detected in that time period is nearly 100%.

## BLUETOOTH DETECTION

### Bluetooth Classic – Active Inquiry

The Flying Fox sensor supports Bluetooth 4.0 and 5.0 as well as backwards compatibility for prior versions. Bluetooth 4.0 introduced Bluetooth Low Energy which works slightly differently from the Bluetooth Classic devices. At present, most common Bluetooth devices are Bluetooth Classic.

For customer who desire it, the Flying Fox Enterprise system can transmit inquiry packets to surrounding devices to detect and locate them. This is an optional and configurable feature and can be disabled if a fully passive solution is desired. This can be configured in the User Profile screen.

Bluetooth Classic devices that wish to pair are constantly listening for the transmission of an Inquiry Packet.

Where inquiry is used, inquiry packets are transmitted about once every 10 seconds. Bluetooth Classic device in the monitored area that are not connected to another device (not in a piconet) will respond to the inquiry with identifying information. This is used by Flying Fox to detect, identify, and locate the device.

### Bluetooth Classic - Passive

Bluetooth Classic devices that are already connected to another device (in a piconet) will not respond to Inquiry Packets. This makes it impossible to discover these devices the normal way. Instead, passive detection of these devices' transmissions is performed by an SDR. Passive detection can be done in parallel to active detection, or as mentioned above, can be done without active detection enabled.

The Bluetooth Classic passive scanner uses one SDR. The Bluetooth scanner captures 100 milliseconds of data on a single Bluetooth Classic channel once every 5 seconds. Bluetooth is a frequency hopping protocol and hops between its 80 channels every 125 microseconds. This means a Bluetooth transmitter active for more than 5 seconds will very likely be detected during this 100-millisecond window.

### **Bluetooth Low Energy**

Bluetooth LE devices that wish to pair periodically transmit an advertising packet.

The Flying Fox detector is collecting advertising packets nearly continuously, meaning the probability of detecting an advertising packet in the monitored area is nearly 100%.

Bluetooth Low Energy devices transmit an advertising packet as frequently as every 20 milliseconds or as rarely as every 10 seconds. Bluetooth Low Energy devices, as the name implies, are designed to minimize power consumption and can cease or dramatically slow the advertising rate based on conditions it chooses.

### **CELLULAR DETECTION**

The cellular detection algorithm takes place in two phases on the sensor. One SDR resource is continuously scanning the LTE bands for uplink activity. Devices in the monitored area that are active on an LTE data channel will be detected by this scan. Due to the breadth of the spectrum scanned, the sensor rotates through the LTE bands and completes a scan approximately every 2 seconds. Therefore, a device that is active for more than 2 seconds will have nearly a 100% chance of being detected by the scan.

Uplink activity detected by a scan does not provide identity information and its measurements are of limited utility for location because they may arise from multiple devices in the monitored area and their measurements cannot be differentiated. Scan events alone provide unreliable location information, as they cannot be traced to a single device. Scan events are available in the UI but filtered out by default (See Filter Section).

In order to provide the device's temporary identifier as well as a reliable location, the system must capture an LTE RRC Connection procedure. In order to do this Flying Fox sensor enters the second phase of detection and monitors both the the uplink (cell phone to tower) and downlink (tower to cell phone) frequencies of a cell. The cells with recent uplink activity that were found in the scan are

used to inform the cells to be monitored by this second phase of detection. When a device requests cell resources through RRC connection procedure, this signaling handshake is captured, a device is uniquely identified, and a unique location estimate can be confidently made.

In a very quiet environment, like a SCIF, scan detection of uplink activity on a particular cell will ensure that the tasked SDRs are tuned to the proper frequencies for a subsequent RRC connection. When activity is found only on a single cell, the tasked SDRs will have a 100% duty cycle and the probability of detecting and decoding the full RRC connection procedure will be between 70-100%.

In an environment where there are a number of different PEDs associated with a number of different cells, the tasked SDRs will split time between the cells active in the area, and the probability of detection of any single RRC connection procedure will diminish in turn.

RRC connection procedures are commonly seen when devices wakeup from sleep, send or receive background data, text messages, originate or terminate phone calls, or start a data session like web browsing or streaming. LTE data use, and therefore RRC connection procedures, can be very sparse if a PED is connected to a Wi-Fi network (which it prefers to LTE) or if it is idle and in sleep mode.

In the case of when a PED is connected to a Wi-Fi network, detecting its Wi-Fi activity is a more reliable way to detect, identify, and locate the device.

Flying Fox supports UMTS in addition to LTE and its detection works similarly.

# SYSTEM UPDATES

## APPLIANCE SOFTWARE UPDATES

The Flying Fox Enterprise application is distributed as a Red Hat RPM package. Updating the appliance's application software involves downloading the latest RPM and transferring it to the appliance to install.

**NOTE** that the upgrade procedure for some versions of the Flying Fox Enterprise package require extra care or support from Epiq Solutions. Specifically, FFE version 1.3.2 or greater requires an SSL certificate to be installed in the Apache webserver. If this is the case, please contact Epiq Solutions for support.

**Also NOTE** that the IP address of the appliance may differ from the examples if it was changed from the default during configuration.

1. Download the latest software RPM with your account from [Epiq Solutions Support](#).
2. Using a [Secure Copy Protocol \(SCP\)](#) client, transfer the RPM to the appliance.

On a macOS or Linux-based computer:

```
scp ~/Downloads/flying-fox-enterprise_MAJOR.MINOR.PATCH.rpm flyingfox@192.168.0.10:~/
```

On Windows, using [PuTTY's](#) SCP client:

```
pscp.exe C:\Users\%USERNAME%\Downloads\flying-fox-enterprise_MAJOR.MINOR.PATCH.rpm  
flyingfox@192.168.0.10:~/
```

Note the default password for the *flyingfox* user on the FFE server is *EpiqEpiqEpiq123!*

3. Using an SSH client, connect to the appliance to execute commands in the Red Hat OS.

On a macOS or Linux-based computer:

```
ssh flyingfox@192.168.0.10
```

On Windows, using [PuTTY's](#) SSH client:

```
putty.exe -ssh flyingfox@192.168.0.10
```

4. Using `sudo rpm -e flying-fox-enterprise`, uninstall the existing version of the application.

```
sudo rpm -e flying-fox-enterprise  
[sudo] password for flyingfox:  
Stopping the service...  
Disabling the service...  
Removed symlink /etc/systemd/system/multi-user.target.wants/flyingfox.service.  
Cleaning up...  
Reloading services...
```

5. Using `sudo rpm -i ~/flying-fox-enterprise_MAJOR.MINOR.PATCH.rpm`, install the new version.

```

sudo rpm -i flying-fox-enterprise_MAJOR.MINOR.PATCH.rpm
Configuring permissions for user 'flyingfox'...
Reloading services...
Enabling the service...
Created symlink from /etc/systemd/system/multi-user.target.wants/flyingfox.service to
/etc/systemd/system/flyingfox.service.
Starting the service...

```

## SENSOR FIRMWARE UPDATES

Note: User controlled sensor firmware updates will be supported in a future version of Flying Fox Enterprise. Included here is a compatibility table for sensor firmware versions and Flying Fox Enterprise releases. Please contact your Epiq Solutions representative if your sensors are running and incompatible firmware version.

FFE version	Sensor Firmware version
1.0.0	6.7.0
1.1.0	6.10.0
1.1.1, 1.1.2, 1.1.3, 1.1.4, 1.2.1, 1.2.2, 1.3.2, 1.4.0, 1.4.2, 1.5.1, 1.5.2	6.11.1, 6.11.6, 6.11.8, 6.11.9
1.6.1, 1.7.0, 1.7.1, 1.8.0, 1.9.0	6.15.0
1.10.0, 1.11.0	6.16.1

**Table 1:** Sensor Firmware Compatibility Table

## TROUBLESHOOTING

### EXPORTING CLIENT STATE

There are times when it is useful to export the client state to a file. This can be done by clicking the "Download Client State" button in the user profile page. This downloads authorized and medical device settings, zones, sensors data, and user preferences.

### EXPORTING DEVICE DATA

You can export the device or scan list data by viewing the "By Device" or "All Detections/Scan Events" lists and clicking "Export All to CSV" at the bottom of the list. You can also export a single device/scan data by clicking into a device or scan details and clicking "Export Device" or "Export Scan" at the bottom of the details pane.

### EXPORT FILTERS

You can export the current filter settings by clicking the "Export Filters" button in the filter pane.

### MISCELLANEOUS TROUBLESHOOTING

#### Can't Connect to Flying Fox Enterprise UI

Verify the client has connectivity to the Flying Fox Enterprise Appliance.

Verify the Flying Fox Enterprise service is running.

#### Sensors are Not Populating in Sensor List

Verify connectivity to the sensors.

Verify the sensors are in the same subnet / multicast domain as the appliance.

#### Devices From Outside the Zone are Showing Up Inside the Zone on the Floor Plan

This is usually caused by an inaccurate location estimate. To hide these estimates see the [Excluding Possible Unreliable Location Estimates](#) section.

---

## NOTES

### NOTE 1 - 802.11AC

802.11ac device detection is based on management frames and 802.11n backward-compatibility traffic.

