AirDefense Services Platform Proximity & Analytics Configuration Guide

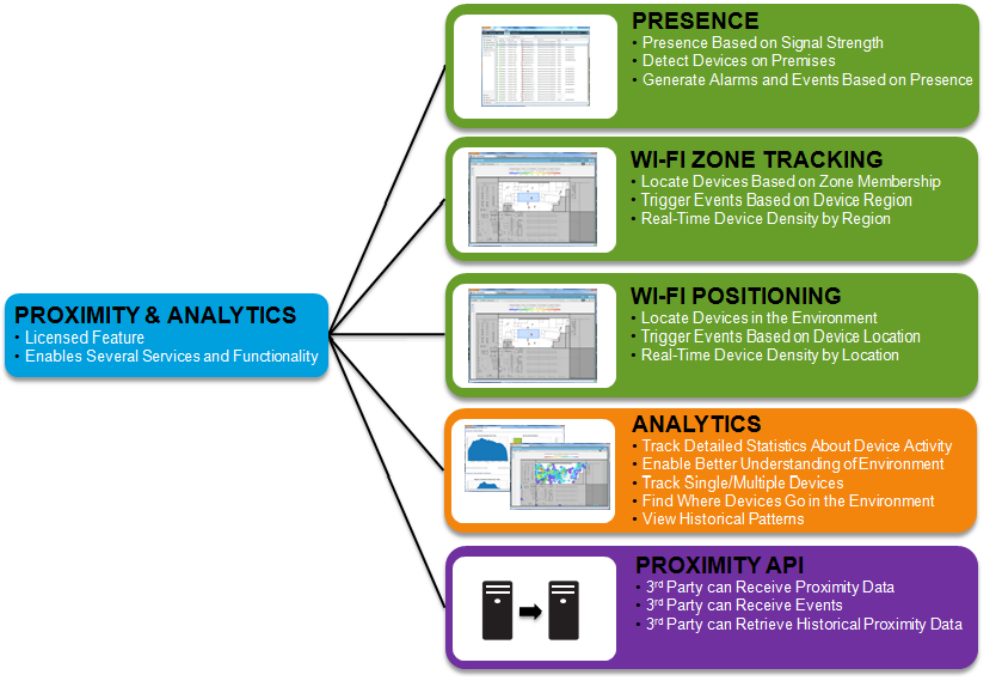
Contents

1 Overview

Proximity and Analytics is comprised of several features within the AirDefense Services Platform (ADSP). When the Proximity and Analytics licenses are applied to the system all of these features are enabled. The device tracking feature is comprised of three functional levels: Presence, Wi-Fi Zone Tracking, and Wi-Fi Position Tracking.

1.1 Feature Breakdown

The following picture depicts the key components and features of Proximity Awareness and Analytics module



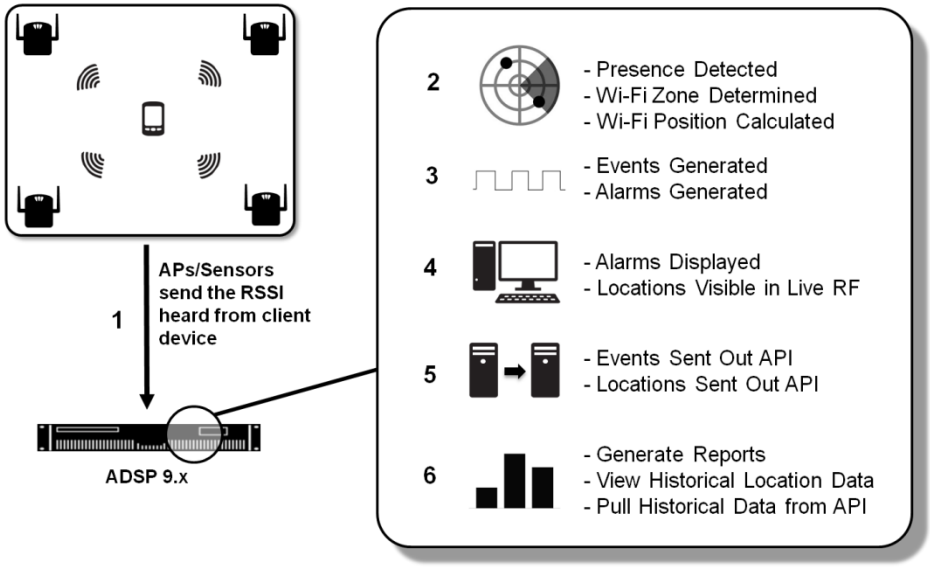
1.2 How Proximity Tracking Works

All of the Proximity functionality in ADSP is based on Wi-Fi signal strength from a client to an AP or Sensor. Each functional level is slightly different than the other in how it uses this information.

1.2.1 Data Acquisition

The data from the Access Points (APs) and Sensors is gathered and collected by ADSP in the same manor for all functional levels. They hear transmissions from a client and send the Received Signal Strength Indicator (RSSI) for those transmissions to ADSP. ADSP will take this information to determine where a client is located based on setup and configuration.

Wi-Fi Presence



Presence takes the RSSI information and compares it to configured RSSI thresholds to determine if a client device is outside, near, or inside the monitored environment.

Wi-Fi Zone Tracking

Wi-Fi Zone Tracking takes the RSSI information and determines the associated zone of a client device based on how close it is to a specific sensor in the monitored environment.

Wi-Fi Position Tracking

Wi-Fi Position Tracking takes the RSSI information and uses data from several APs and Sensors to calculate a location for the client device in the monitored environment.

2 Supporting Features

The Proximity and Analytics feature set utilizes functions that are inherently available within the AirDefense Services Platform (ADSP). In relation to configuring for Proximity and Analytics, a key feature in supporting setup are Client Types.

2.1 Client Types

Client Types are used to divide wireless stations with similarities into groups. These groups can be used for filtering data and views, but more importantly for Proximity and Analytics they can be used to apply unique settings.

They are assigned using the following methods.

- Manually
- Auto-Classification (from ADSP 9.1, it is part of Device Action Manager)
- Device Import Rules (from ADSP 9.1, it is part of Device Action Manager)
- File Import

3 Licensing

Licensing for Proximity and Analytics is per AP or Sensor. Every AP (Radio Share) or Sensor that will perform Proximity and Analytics functions must have the Proximity and Analytics license (AD-PROX-P-1) applied.

4 Configuring Wi-Fi Presence

The Wi-Fi Presence feature detects a device in the environment and determines if it is inside or outside the defined environment boundaries. ADSP takes this further by supporting three different boundaries to determine the progression of a device into the environment: outside environment, near environment, and inside environment.

4.1 Sensor Operation

Wi-Fi Presence detection can be performed by Dedicated and Radio Share sensors. Sensor Operation settings are used to adjust the scanning functions of dedicated sensor radios.

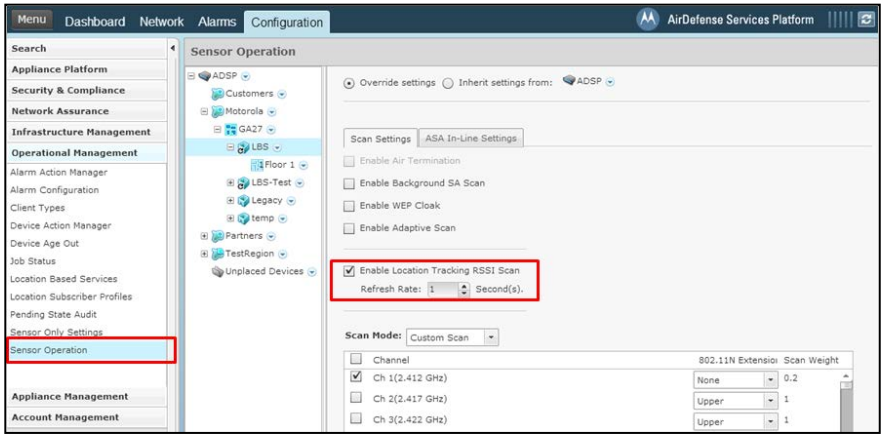
4.1.1 Location Tracking RSSI Scan

Enabling the Location Tracking RSSI Scan in the Sensor Operation settings instructs the sensors to send client RSSI data back to ADSP at the designated rate. The default value is 1 second and it is recommended to use this value.

When the Location Tracking RSSI Scan is disabled the sensor will send client RSSI data back to ADSP at 1 minute intervals. Depending on the Wi-Fi Presence detection requirements this may delay client detection for too long.

✓ ***NOTE*** This setting affects both Dedicated and Radio Share sensors.

⚠ ***CAUTION*** This setting only works with sensor APs running WiNG 5.2 or later firmware. It does not work with M400 or M5x0 sensors.



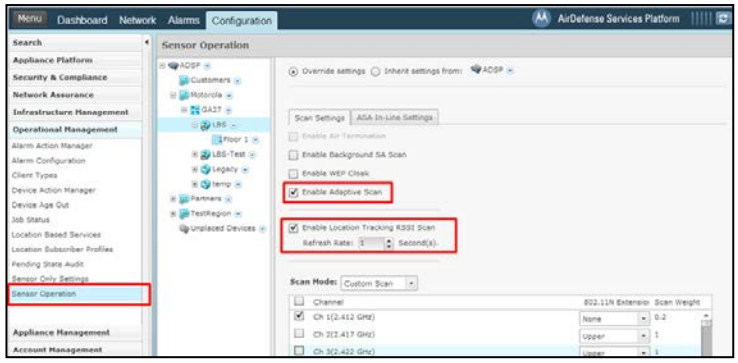
4.1.2 Adaptive Scan

Adaptive Scan is a feature that is enabled in the Sensor Operation. When this is enabled ADSP uses information that it has sensed in the environment and critical issues that it has found to determine how much time it should spend monitoring each channel.

In ADSP 9.1 Adaptive Scan is updated with support for Proximity and Analytics. When Adaptive Scan is enabled along with Location Tracking RSSI Scan, ADSP will assume that any channels configured on Sanctioned BSSs are Proximity channels. It will then adjust the sensor scanning pattern to better support the Proximity and Analytics requirements on those channels.

✓ ***NOTE*** This setting only affects Dedicated sensor radios not Radio Share sensor radios.

⚠ ***CAUTION*** The Adaptive Scan updates for Proximity and Analytics are only available in ADSP 9.1 or later.

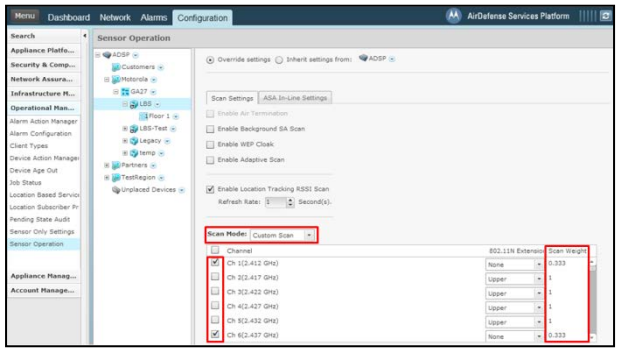


4.1.3 Channel Settings

To meet the Presence Detection deployment requirements it maybe necessary to limit the channels monitored by dedicated sensors. As mentioned before Adaptive Scan in ADSP 9.1 is updated to automatically adjust channel settings for Proximity and Analytics. In ADSP 9.0.x it may be required to limit the number of channels scanned by a dedicated sensor. For Wi-Fi Presence the fewer channels that are required to be scanned and the lower the dwell the faster ADSP will be able to detect a station's presence.

This configuration is also made in the Sensor Operation settings. First change the Scan Mode to Custom Scan. Then use the enable check boxes to select the channels that should be scanned by the dedicated sensors.

The Scan Weight can be adjusted to change the dwell time for a channel. A Scan Weight of '1' is approximately 1 second, so reducing the weight below one will reduce the dwell time. The lowest value is '0.1'.



✓ ***NOTE*** The channel setting only affect Dedicated sensors radios not Radio Share sensor radios.

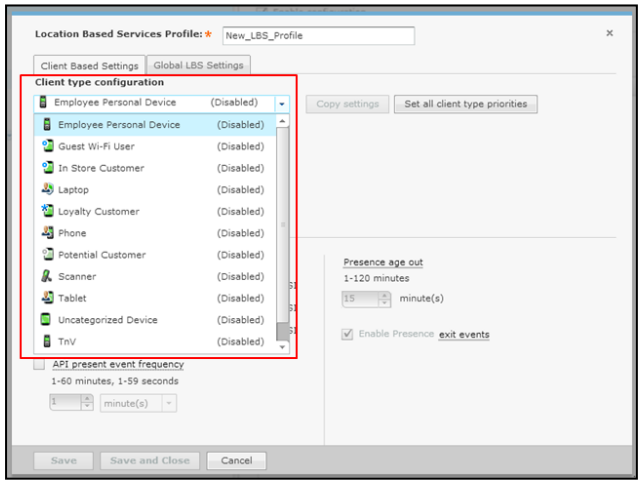
⚠ ***CAUTION*** Enabling Adaptive Scan is the preferred method of dedicated sensor scanning adjustment in ADSP 9.1.

4.2 Location Based Services Profile

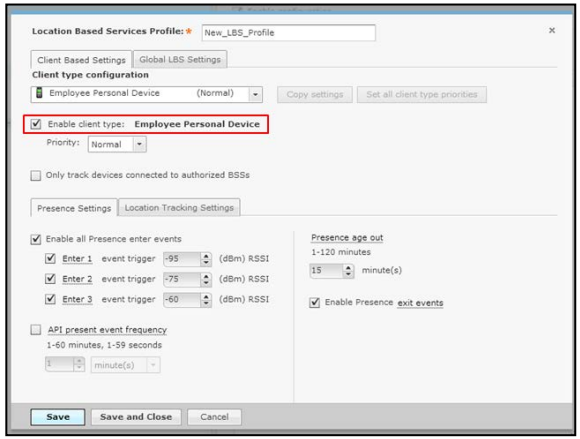
To enable Wi-Fi Presence detection it must be configured in the Location Based Services (LBS) profile located in the Configuration tab in the Operational Management settings. LBS profiles contain all the Proximity settings and unique profiles can be assigned at any scope level.

Most of the Proximity settings are applied per Client Type to allow unique tracking for different groups of devices.

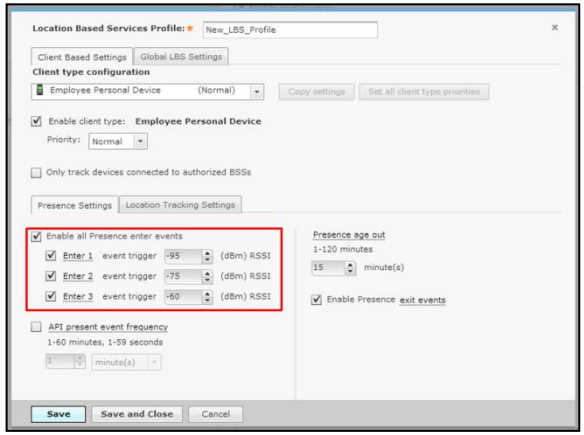
First a Client Type must be selected to configure its settings.



The Client Type should then be enabled.

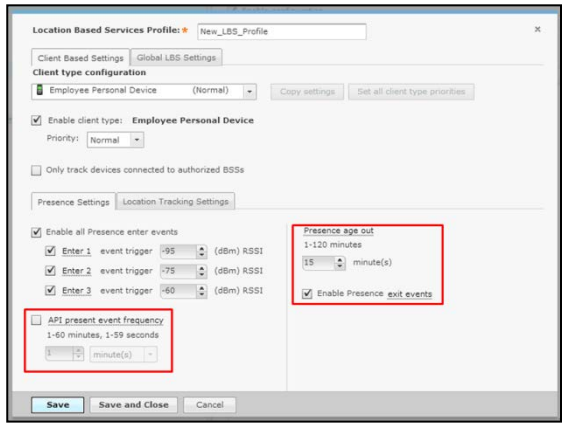


Once the Client Type is enabled the Presence Settings tab should be selected to access the Wi-Fi Presence detection configuration. The first parameters are for the Presence Enter events that are triggered when a device is detected in the environment. There are three Presence Enter events that can be triggered when the signal strength from the wireless station goes above its corresponding RSSI trigger.



The next setting is the Presence Age Out, which controls the time that must past before a device is considered not present any more. When a device crosses the lowest Presence Enter RSSI trigger level, the Presence Age Out timer starts. If the defined amount of time expires before the device cross one of the Presence Enter RSSI triggers it is considered not present. If the device crosses back above one of the Presence Enter triggers before the Presence Age Out time expires the device is still considered in the environment (visit has not ended). In this case the Presence Age Out will be reset.

Once a Presence Enter event is triggered for a device it will not be retriggered until the Presence Age Out expires and the device cross one of the Presence Enter triggers again.

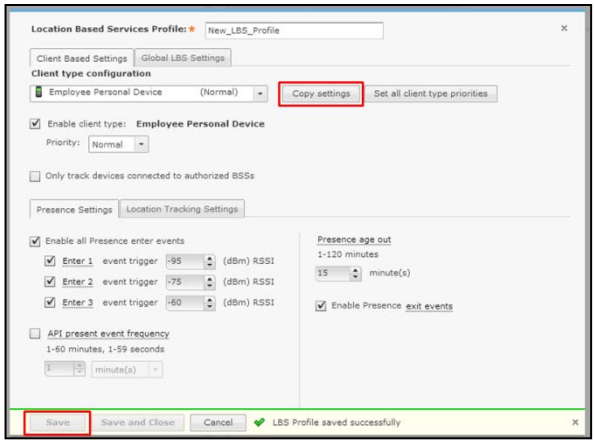


If the Presence Exit event is enabled it will be triggered when the Presence Age Out expires for that device.

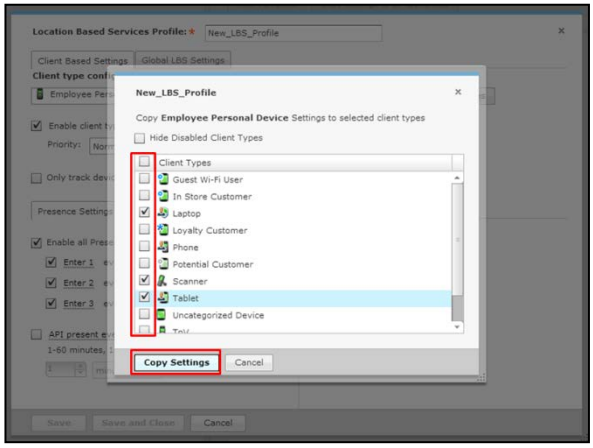
There is one more Wi-Fi Presence detection trigger called the Presence Present event. There is not an alarm triggered for this event and is only seen on the API. When enabled the Presence Present event will be repeated at the defined interval as long as the device's Presence Age Out has not expired.

Once the Client Type is configured others can be selected and configured as well. If there are several Client Types which will have the same settings then the settings from one can be copied to the others. First save the settings by pressing the Save button.

Then verify that the Client Type you want to copy is selected, and press the Copy Settings button to open the selection window.



In the selection window select all the Client Types that the settings should be copied to and then press the Copy Settings button. Then in the main LBS profile window press the Save button.

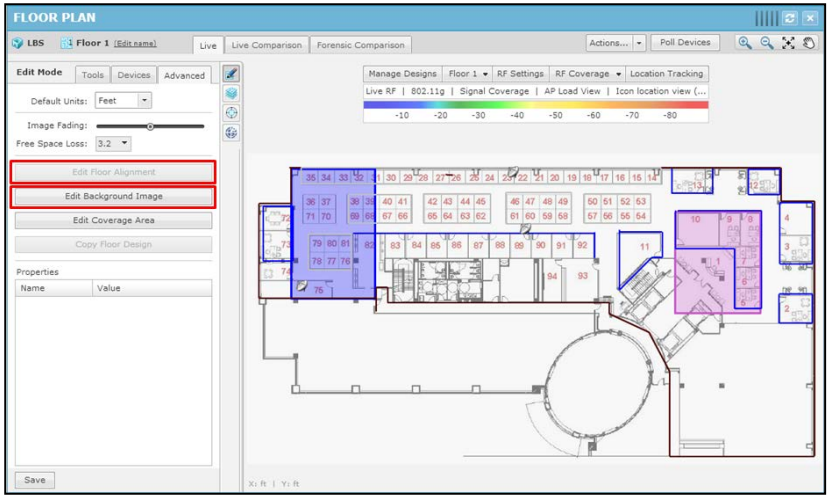


5 Configuring Zone Tracking

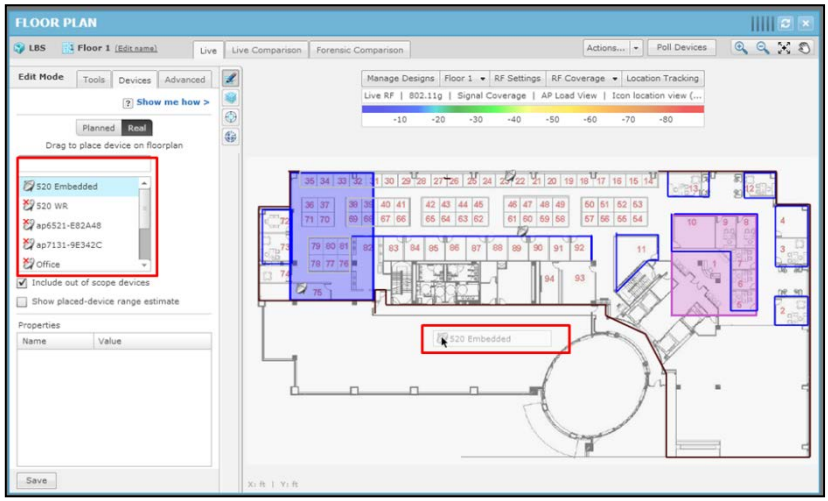
Wi-Fi Zone Tracking is the detection of a device within a sensor's zone based on a configured RSSI threshold. This can be used to simply detect if a device is present in particular areas of the environment or can be used as course location tracking.

5.1 Floor Plan Setup

Floor plans are used for several functions in ADSP, but Wi-Fi Position Tracking requires that the AP/Sensors be placed on the building floor plan, otherwise device locations will not be tracked. The floor plan for the building should be as accurate as possible and scaled properly. The Edit Background Image tool under the Advanced tab in the Edit menu can be used to adjust the scale. The floor alignment also needs to be as accurate as possible as well. In the same menu the Edit Floor Alignment tool can be used for adjustment.



When placing the AP/Sensors on the floor plan they need to be placed as accurately as possible.



To place the AP/Sensor select it from the device list in the editor menu and drag it to the correct location.

5.2 Sensor Operation

Wi-Fi Zone Tracking can be performed by Dedicated and Radio Share sensors. Sensor Operation settings are used to adjust the scanning functions of dedicated sensor radios.

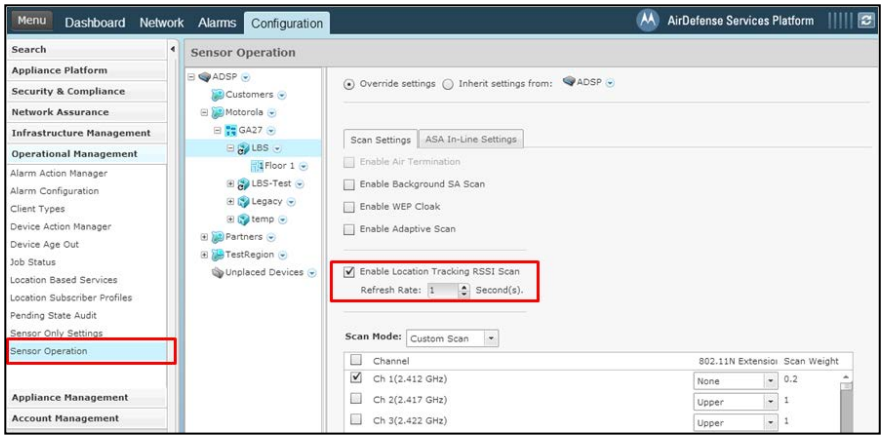
5.2.1 Location Tracking RSSI Scan

Enabling the Location Tracking RSSI Scan in the Sensor Operation settings instructs the sensors to send client RSSI data back to ADSP at the designated rate. The default value is 1 second and it is recommended to use this value.

When the Location Tracking RSSI Scan is disabled the sensor will send client RSSI data back to ADSP at 1 minute intervals. Depending on the Wi-Fi Zone Tracking requirements this may delay client detection for too long.

✓ ***NOTE*** This setting affects both Dedicated and Radio Share sensors.

⚠ ***CAUTION*** This setting only works with sensor APs running WiNG 5.2 or later firmware. It does not work with M400 or M5x0 sensors.



5.2.2 Adaptive Scan

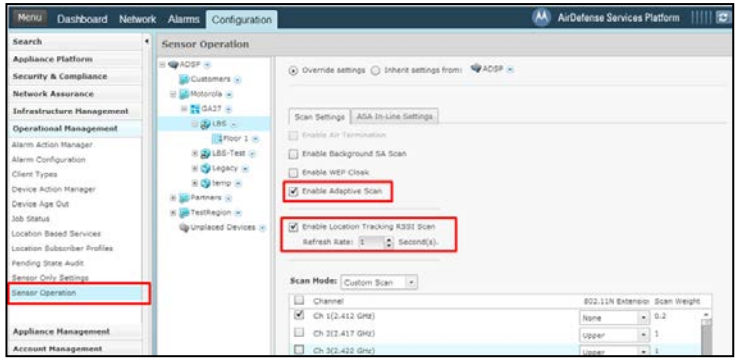
Adaptive Scan is a feature that is enabled in the Sensor Operation. When this is enabled ADSP uses information that it has sensed in the environment and critical issues that it has found to determine how much time it should spend monitoring each channel.

In ADSP 9.1 Adaptive Scan was updated with support for Proximity and Analytics. When Adaptive Scan is enabled along with Location Tracking RSSI Scan ADSP will assume that any channels configured on Sanctioned BSSs are Proximity channels. It will then adjust the sensor scanning pattern to better support the Proximity and Analytics requirements on those channels.

✓ ***NOTE*** This setting only affects Dedicated sensor radios not Radio Share sensor

radios.

CAUTION The Adaptive Scan updates for Proximity and Analytics are only available in ADSP 9.1 or later.

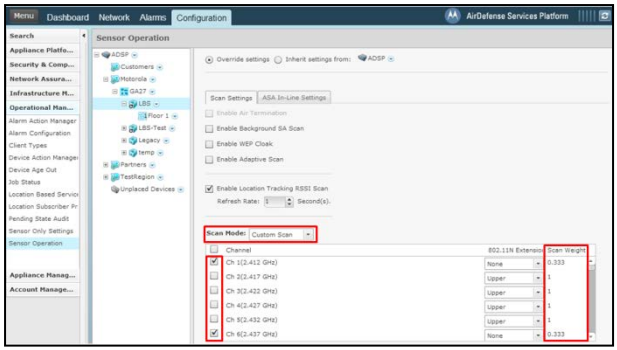


5.2.3 Channel Settings

To meet the Wi-Fi Zone Tracking deployment requirements it may be necessary to limit the channels monitored by dedicated sensors. As mentioned before Adaptive Scan in ADSP 9.1 is updated to automatically adjust channel settings for Proximity and Analytics. In ADSP 9.0.x it may be required to limit the number of channels scanned by a dedicated sensor. For Wi-Fi Zone Tracking the fewer channels that are required to be scanned and the lower the dwell, the faster ADSP will be able to detect a station's zone.

This configuration is also made in the Sensor Operation settings. First change the Scan Mode to Custom Scan. Then use the enable check boxes to select the channels that should be scanned by the dedicated sensors.

The Scan Weight can be adjusted to change the dwell time for a channel. A Scan Weight of '1' is approximately 1 second, so reducing the weight below one will reduce the dwell time. The lowest value is '0.1'.



NOTE The channel setting only affect Dedicated sensors radios not Radio Share sensor radios.

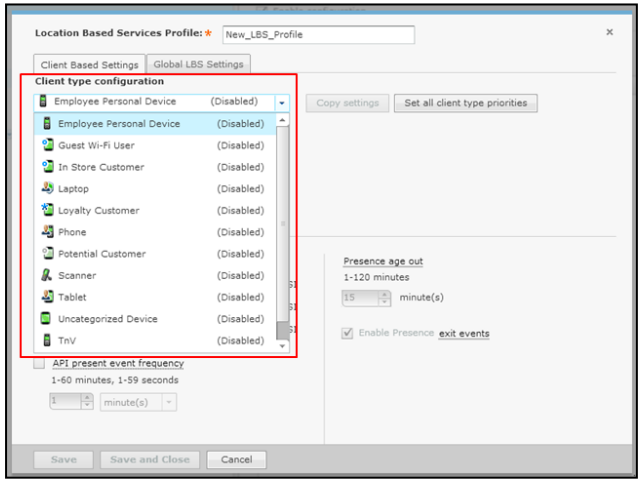
CAUTION Enabling Adaptive Scan is the preferred method of dedicated sensor scanning adjustment in ADSP 9.1.

5.3 Location Based Services Profile

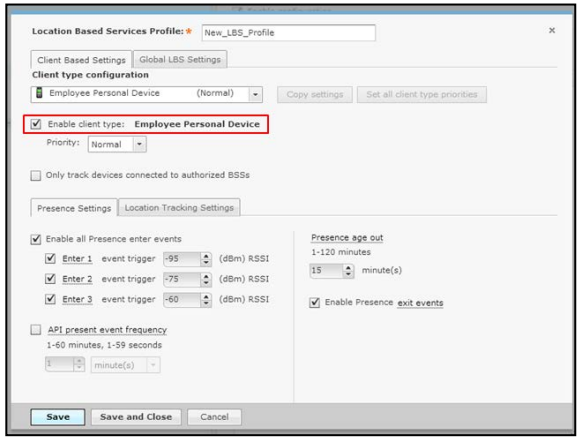
To enable Wi-Fi Zone Tracking, it must be configured in the Location Based Services (LBS) profile located in the Configuration tab in the Operational Management settings. LBS profiles contain all the Proximity settings and unique profiles can be assigned at any scope level.

Most of the Proximity settings are applied per Client Type to allow unique tracking for different groups of devices.

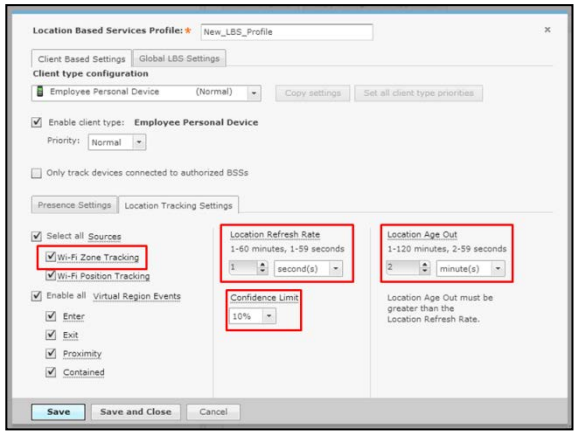
First a Client Type must be selected to configure its settings.



The Client Type should then be enabled.



Once the Client Type is enabled the Location Tracking Settings tab should be selected to access the Wi-Fi Zone Tracking configuration. The first parameters are the Sources and in this case Wi-Fi Zone Tracking should be enabled.

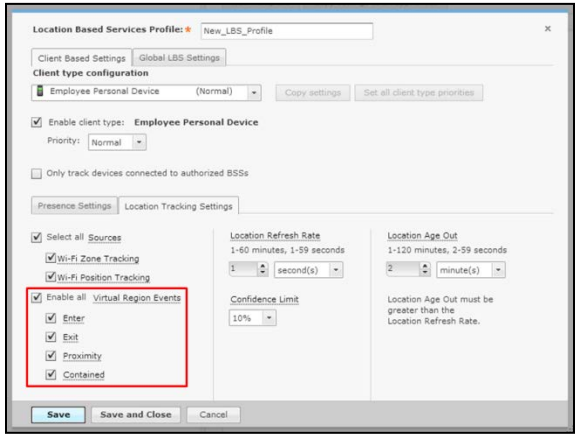


The Location Refresh Rate is the desired rate at which a device's location should be updated. The actual device update time depends on if new data has been received and also on the appliance load.

The Location Age Out is how long the device's last known location will be maintained after a new location cannot be determined. If set to short the device location could drop in and out very quickly. If set to long interval, the last known location will be reported long after the device has left the environment.

When a location is determined there is a confidence associated to that calculation. The Confidence Limit setting restricts only locations that meet a certain confidence level to be used and any locations below that level are thrown out. In most cases this should be set to the lowest level, because the confidence level is going to fluctuate based on many factors.

Now that the tracking behavior is configured, the events that should be triggered should be



enabled. Wi-Fi Zone Tracking uses Virtual Region Events based on a device's location in relation to Virtual Regions. In order for a device to trigger one of these events, its Client Type must have it enabled as well as the Virtual Region it is interacting with.

Enter – device has entered a Virtual Region

Exit – device has exited a Virtual Region

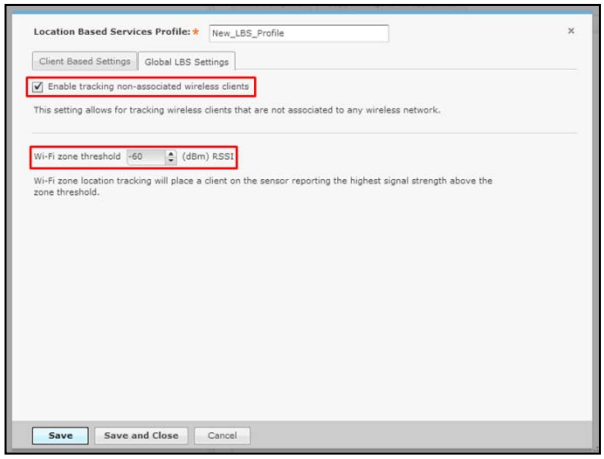
Proximity – device is within a defined distance of a Virtual Region. The distance can be configured while creating virtual regions.

Contained – device has been within a Virtual Region for defined amount of time. The time interval can be configured while creating virtual regions.

Virtual Region configuration is discussed in a follow up section.

In the Global LBS Settings tab, there are two parameters that affect Wi-Fi Zone Tracking. These are called global settings because they affect all Client Types in the LBS profile.

The first is tracking non-associated wireless clients. When enabled, associated and non-

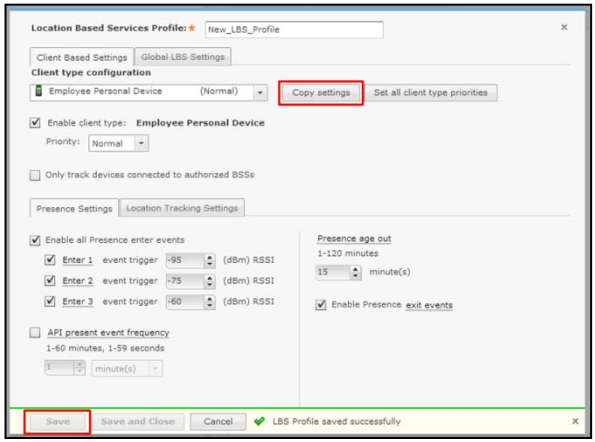


associated stations will be tracked. If it is disabled then only stations associated to a wireless network will be tracked.

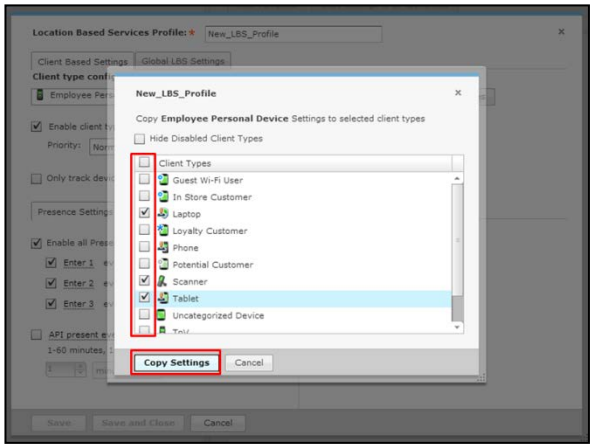
The Wi-Fi Zone Threshold is the RSSI level that a station must reach in relation to an AP/ Sensor before it is considered in that AP/Sensor's zone. The higher the RSSI setting the smaller the zone will be, because a station would have to be closer to the AP/Sensor to cross the threshold.

Once the Client Type is configured others can be selected and configured as well. If there are several Client Types that will have the same settings then the settings from one can be copied to the others. First save the settings by pressing the Save button.

Then verify that the Client Type you want to copy is selected and press the Copy Settings button to open the selection window.



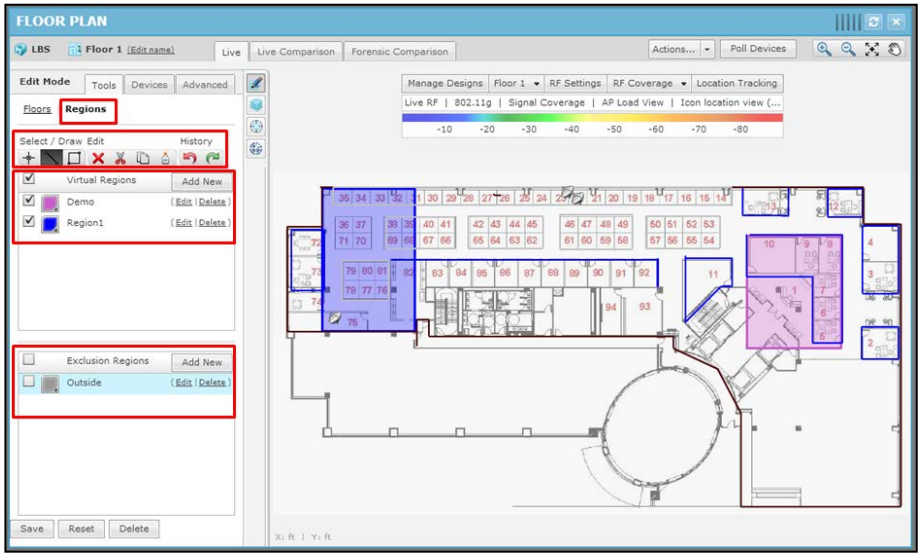
In the selection window select all the Client Types that the settings should be copied to and then press the Copy Settings button. Then in the main LBS profile window press the Save button.



5.4 Virtual/Exclusion Regions

Virtual and Exclusion Regions are designated in the environment by drawing areas on the floor plan map. Virtual Regions are areas used to interact with device's location and trigger events. Exclusion Regions are used to indicate areas where devices cannot or should not be located. If a device's location is determined to be within an Exclusion Region, that location is not used and the last known location will be reported.

To create Regions, Live RF / Floor plan for that building must first be opened. From there the edit menu should be accessed and the Regions settings selected.

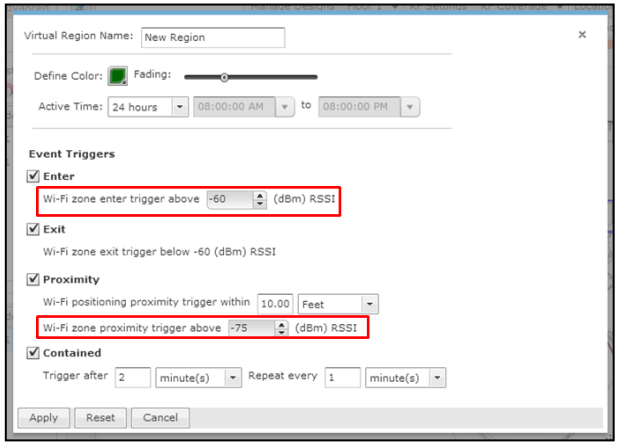


To create a Region, first add a new Region in either the Virtual Regions list or the Exclusion Regions list. Select the new Region from the list and then use either the line tool or the box tool to trace it out on the floor plan.

⚠ ***CAUTION*** The sensors must be contained within a Virtual Region for a Region event to be triggered based on Wi-Fi Zone Tracking.

When creating new Regions there are settings associated to them. Exclusion Regions only have the color and fading settings. But Virtual Regions have additional settings related to Position Tracking and Wi-Fi Zone Tracking.

The color and fading can be set along with when the Virtual Region is active. It can either be



active 24 hours or can be active for a range of time during the day.

The event triggers affect all location tracking. As mentioned in the LBS Profile configuration, the Virtual Region and the device's Client Type must both have an event type enabled for that event to be triggered for that device.

The Contained event has some extra parameters for how long a device must be contained within the Virtual Region before triggering the event. It also allows for setting how often this event should be repeated while the device is still contained in the Virtual Region.

The Enter and Proximity events have additional settings specifically for Wi-Fi Zone Tracking. The RSSI trigger level setting is used to determine how close the client must be to the AP/Sensor before the event is triggered.

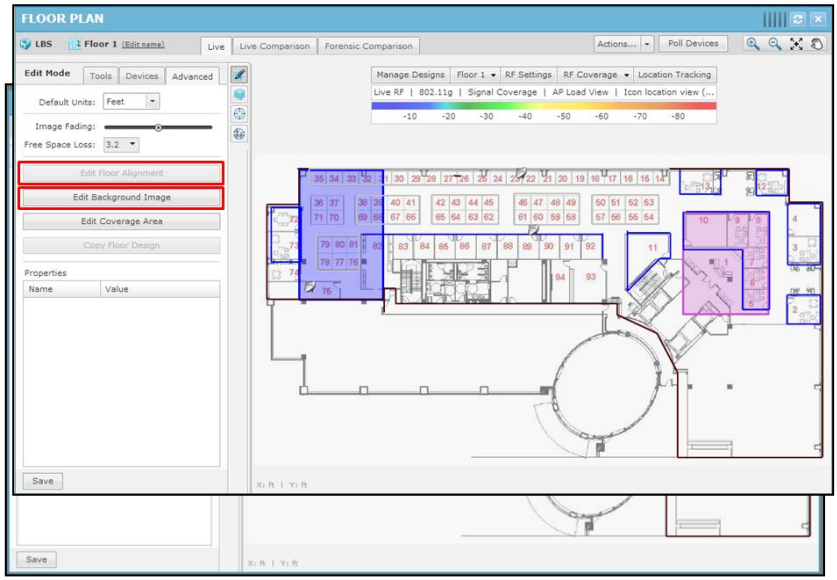
⚠ ***CAUTION*** For a device with Wi-Fi Zone Tracking to trigger a Virtual Region event it must be within an AP/Sensor Zone's RSSI trigger that is located within the Virtual Region and also meet the RSSI trigger requirements for the Virtual Region.

6 Configuring Position Tracking

Wi-Fi Position Tracking is the calculation of a devices location within the environment using information from several sensors. It is used to track a device's movement throughout the environment.

6.1 Floor Plan Setup

Floor plans are used for several functions in ADSP, but Wi-Fi Position Tracking requires that the AP/Sensors be placed on the building floor plan, otherwise the device locations will not be tracked. The floor plan for the building should be as accurate as possible and scaled properly. The Edit Background Image tool under the Advanced tab in the Edit menu can be used to adjust the scale. The floor alignment also needs to be as accurate as possible as well. In the same menu the Edit Floor Alignment tool can be used for adjustment.



When placing the AP/Sensors on the floor plan they need to be placed as accurately as possible.

To place the AP/Sensor select it from the device list in the editor menu and drag it to the correct location.

6.2 Sensor Operation

Wi-Fi Position Tracking can be performed by Dedicated and Radio Share sensors. Sensor Operation settings are used to adjust the scanning functions of dedicated sensor radios.

6.2.1 Location Tracking RSSI Scan

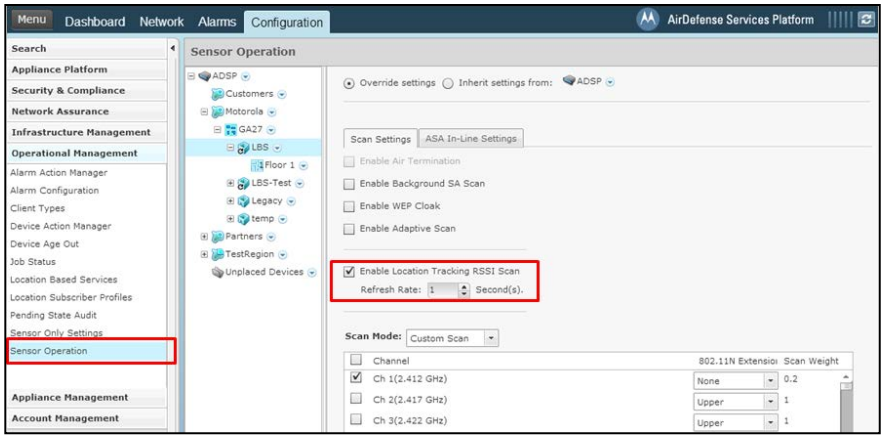
Enabling the Location Tracking RSSI Scan in the Sensor Operation settings instructs the sensors to send client RSSI data back to ADSP at the designated rate. The default value is 1 second and it is recommended to use this value.

When the Location Tracking RSSI Scan is disabled the sensor will send client RSSI data back to ADSP at 1 minute intervals. Depending on the Wi-Fi Position Tracking requirements this may delay client detection for too long.

✓ ***NOTE*** This setting affects both Dedicated and Radio Share sensors.

⚠ ***CAUTION*** This setting only works with sensor APs running WiNG 5.2 or later firmware.

It does not work with M400 or M5x0 sensors.



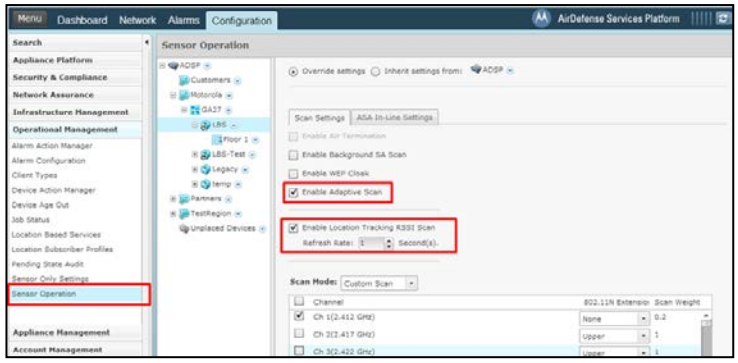
6.2.2 *Adaptive Scan*

Adaptive Scan is a feature that is enabled in the Sensor Operation. When this is enabled ADSP uses information that it has sensed in the environment and critical issues that it has found to determine how much time it should spend monitoring each channel.

In ADSP 9.1 Adaptive Scan is updated with support for Proximity and Analytics. When Adaptive Scan is enabled along with Location Tracking RSSI Scan ADSP will assume that any channels configured on Sanctioned BSSs are Proximity channels. It will then adjust the sensor scanning pattern to better support the Proximity and Analytics requirements on those channels.

✓ ***NOTE*** This setting only affects Dedicated sensor radios not Radio Share sensor radios.

⚠ ***CAUTION*** The Adaptive Scan updates for Proximity and Analytics are only available in ADSP 9.1 or later.

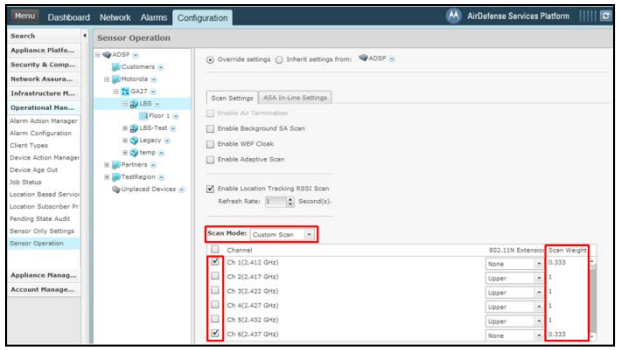


6.2.3 *Channel Settings*

To meet the Wi-Fi Position Tracking deployment requirements it may be necessary to limit the channels monitored by dedicated sensors. As mentioned before Adaptive Scan in ADSP 9.1 is updated to automatically adjust channel settings for Proximity and Analytics. In ADSP 9.0.x it may be required to limit the number of channels scanned by a dedicated sensor. For Wi-Fi Zone Tracking the fewer channels that are required to be scanned and the lower the dwell the faster ADSP will be able to detect a station's zone.

This configuration is also made in the Sensor Operation settings. First change the Scan Mode to Custom Scan. Then use the enable check boxes to select the channels that should be scanned by the dedicated sensors.

The Scan Weight can be adjusted to change the dwell time for a channel. A Scan Weight of '1' is approximately 1 second, so reducing the weight below one will reduce the dwell time. The lowest value is '0.1'.



✓ ***NOTE*** The channel setting only affect Dedicated sensors radios not Radio Share sensor radios.

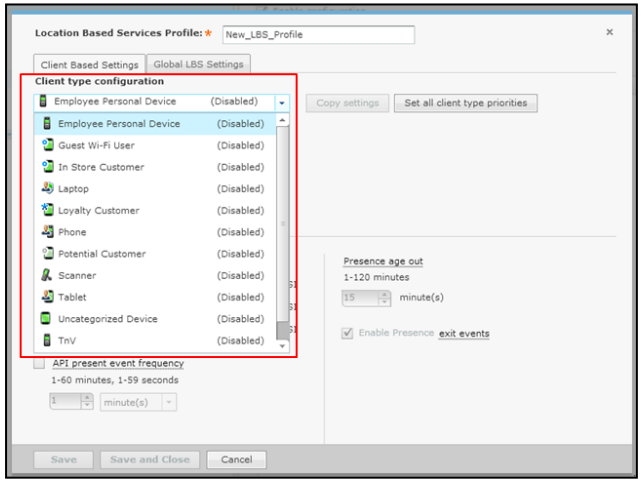
⚠ ***CAUTION*** Enabling Adaptive Scan is the preferred method of dedicated sensor scanning adjustment in ADSP 9.1.

6.3 Location Based Services Profile

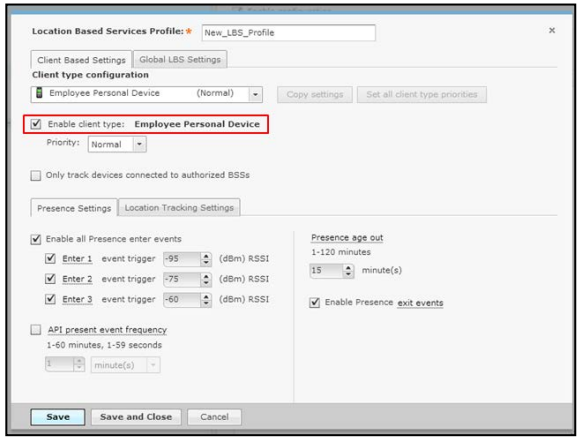
To enable Wi-Fi Position Tracking it must be configured in the Location Based Services (LBS) profile located in the Configuration tab in the Operational Management settings. LBS profiles contain all the Proximity settings and unique profiles can be assigned at any scope level.

Most of the Proximity settings are applied per Client Type to allow unique tracking for different groups of devices.

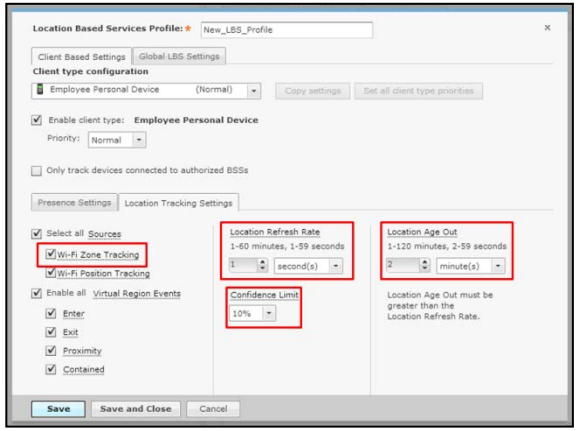
First a Client Type must be selected to configure its settings.



The Client Type should then be enabled.



Once the Client Type is enabled the Location Tracking Settings tab should be selected to access the Wi-Fi Position Tracking configuration. The first parameters are the Sources and in this case Wi-Fi Position Tracking should be enabled.

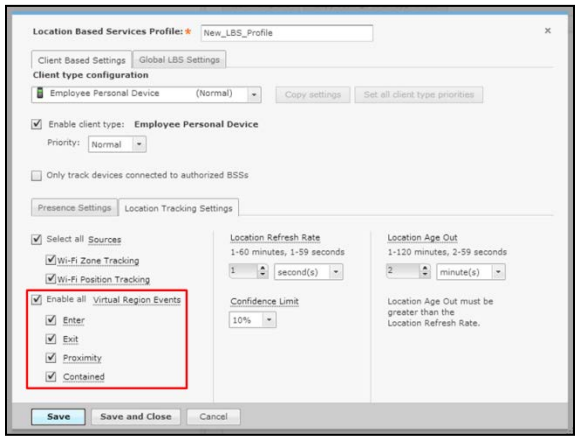


The Location Refresh Rate is the desired rate at which a device's location should be updated. The actual device update time depends on if new data has been received and also on the appliance load.

The Location Age Out is how long the device's last known location will be maintained after a new location cannot be determined. If set to short the device location could drop in and out very quickly. If set to long the last known location will be reported long after the device has left the environment.

When a location is determined there is a confidence associated to that calculation. The Confidence Limit setting restricts only locations that meet a certain confidence level to be used and any below that level are thrown out. In most cases this should be set to the lowest level, because the confidence level is going to fluctuate based on many factors.

Now that the tracking behavior is configured the events that should be triggered should be



enabled. Wi-Fi Position Tracking uses Virtual Region Events based on a device's location in relation to Virtual Regions. In order for a device to trigger one of these events its Client Type must have it enabled as well as the Virtual Region it is interacting with.

Enter – device has entered a Virtual Region

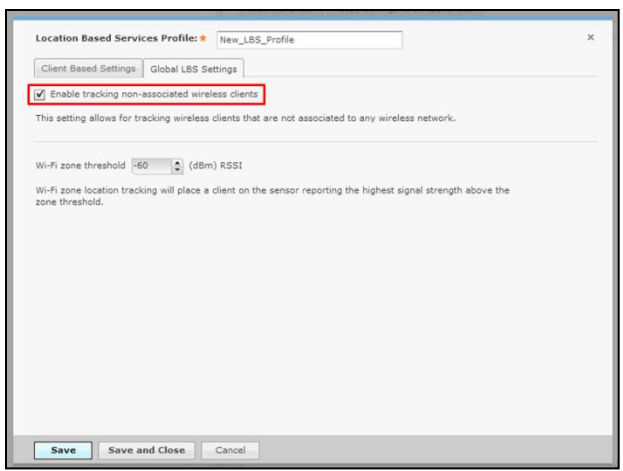
Exit – device has exited a Virtual Region

Proximity – device is within a defined distance of a Virtual Region. The distance can be configured while creating virtual regions.

Contained – device has been within a Virtual Region for defined amount of time. The time interval can be configured while creating virtual regions.

Virtual Region configuration is discussed in a follow up section.

In the Global LBS Settings tab, there is one parameter that affects Wi-Fi Position Tracking.

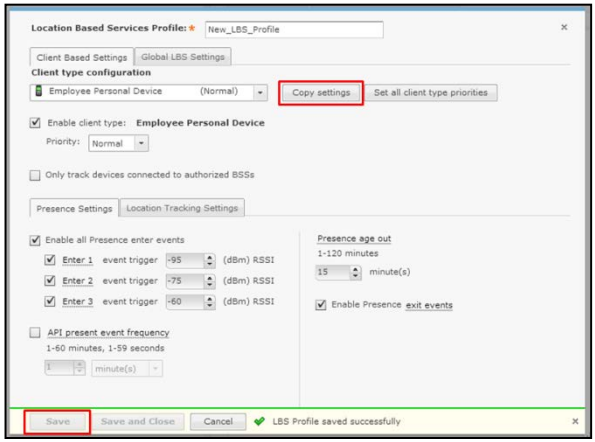


These are called global settings because they affect all Client Types in the LBS profile.

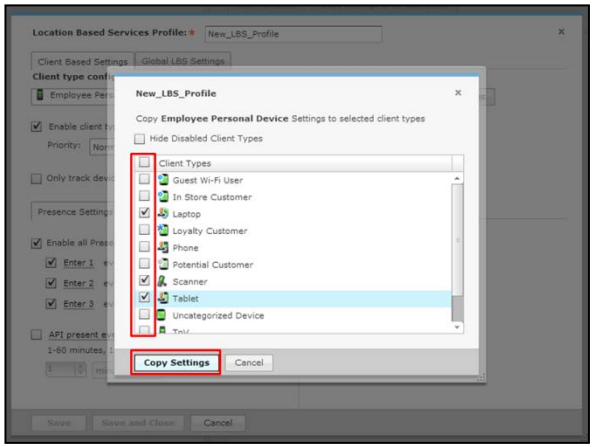
When tracking non-associated wireless clients is enabled, associated and non-associated stations will be tracked. If it is disabled then only stations associated to a wireless network will be tracked.

Once the Client Type is configured others can be selected and configured as well. If there are several Client Types that will have the same settings then the settings from one can be copied to the others. First save the settings by pressing the Save button.

Then verify the Client Type you want to copy is selected and press the Copy Settings button to open the selection window.



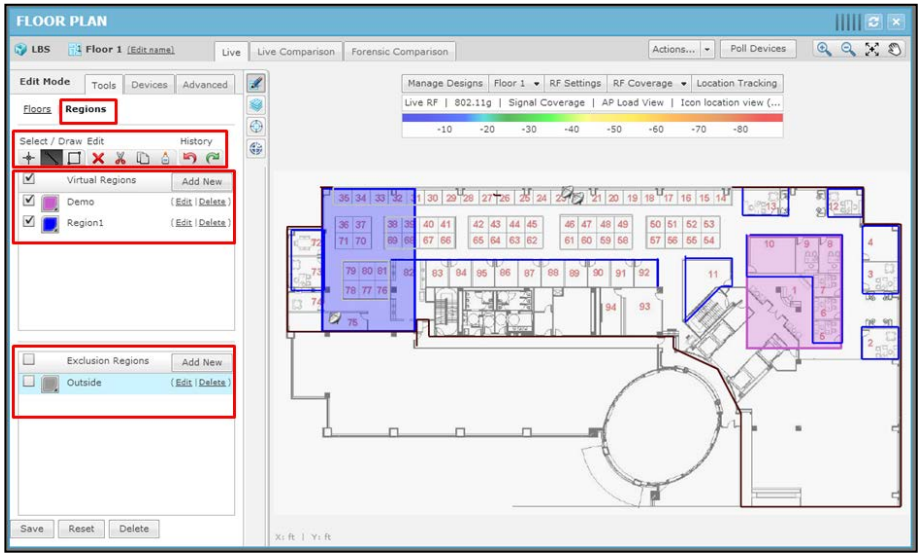
In the selection window select all the Client Types that the settings should be copied to and then press the Copy Settings button. Then in the main LBS profile window press the Save button.



6.4 Virtual/Exclusion Regions

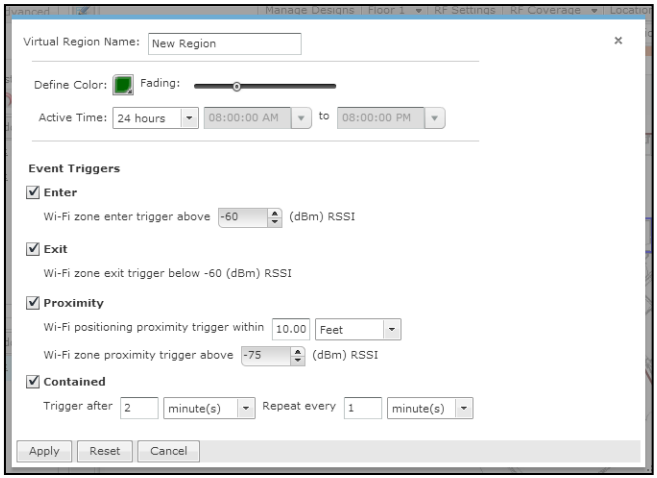
Virtual and Exclusion Regions are designated in the environment by drawing areas on the floor plan map. Virtual Regions are areas used to interact with a devices location and trigger events. Exclusion Regions are used to indicate areas where devices cannot or should not be located. If a device's location is determined to be within an Exclusion Region, that location is not used and the last known location will be reported.

To create Regions, Live RF / Floor plan for that building must first be opened. From there the edit menu should be accessed and the Regions settings selected.



To create a Region, first add a new Region in either the Virtual Regions list or the Exclusion Regions list. Select the new Region from the list and then use either the line tool or the box tool to trace it out on the floor plan.

When creating new Regions there are settings associated to them. Exclusion Regions only have the color and fading setting, but Virtual Regions have several general location tracking settings.



The color and fading can be set along with when the Virtual Region is active. It can either be active 24 hours or can be active for a range of time during the day.

The event triggers affect all location tracking. As mentioned in the LBS Profile configuration, the Virtual Region and the device's Client Type must both have an event type enabled for that event to be triggered for that device.

The Contained event has some extra parameters for how long a device must be contained within the Virtual Region before triggering the event. It also allows for setting how often this event should be repeated while the device is still contained in the Virtual Region.

6.5 Sensor Survey

To complete the configuration for Wi-Fi Position Tracking, a Sensor Survey should be performed. The process for performing this procedure can be found in the "Zebra ADSP Sensor Survey for RTLS Calibration How To Guide" located on the Zebra Support site.

7 Proximity API Configuration

When the Proximity and Analytics license is loaded on to the AirDefense Services Platform, the Proximity API is enabled. There will be no data seen on the API until the Wi-Fi Presence, Wi-Fi Zone Tracking, or Wi-Fi Position Tracking is setup and configured.

The API has two basic connection methods: inbound and outbound. Both are made with an HTTPS socket connection either to the appliance or out from the appliance.

7.1 LBS API Toolkit

The LBS API Toolkit download can be found on the toolkit download page on the ADSP appliance. The download page can be accessed from two places: link at the top right of the ADSP GUI login page or in the Menu after logging in.

There is a Java file included in the SDK called LBSClient.jar that can be consumed by the third party application to access the proximity classes. The SDK also includes the Java Docs with the API and their descriptions and two sample applications implementing both inbound and outbound connections.

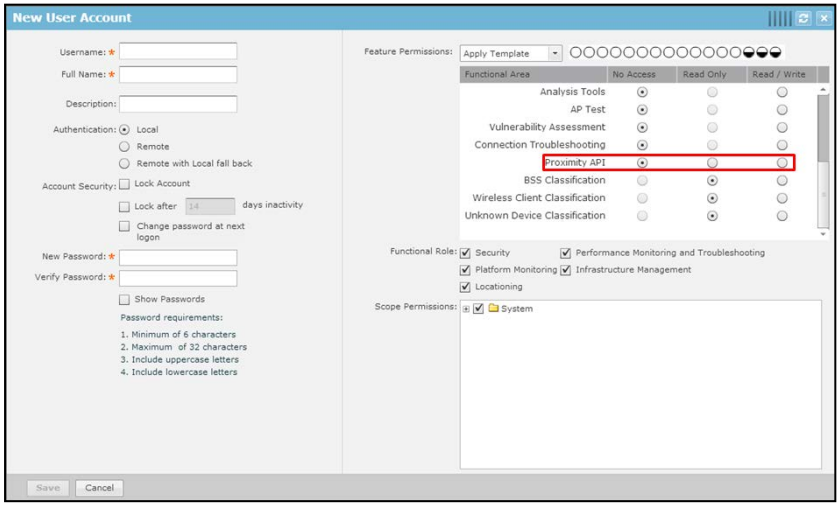
7.2 Inbound API (Pull)

The inbound API methods are available from ADSP 9.0.0 to the current version. When a third party application is using the inbound API methods it must initiate the connection to the ADSP appliance and request the data it wants. The inbound methods use the same TCP port as the appliance web user interface, which defaults to 8543.

There are a couple of functions that can only be performed using the inbound methods. Any type of historical data must be retrieved using the inbound methods. Functions that write data to the appliance are only available through the inbound methods.

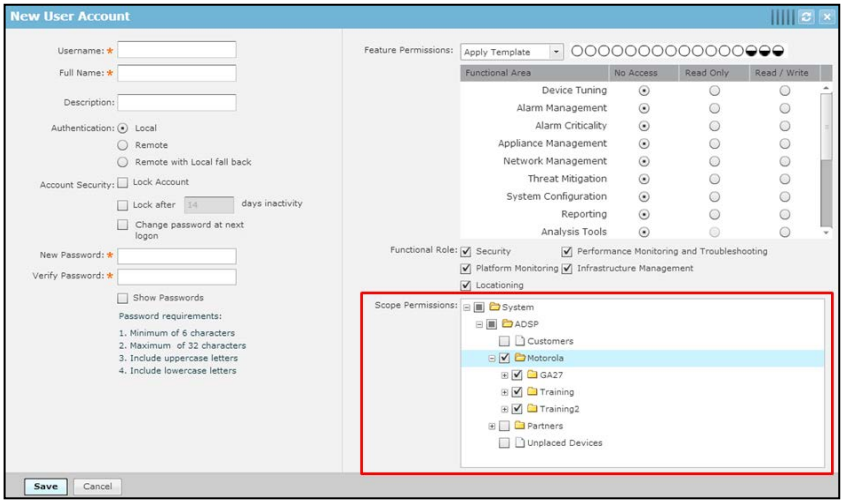
7.2.1 Authentication Setup

The third party application must authenticate with the appliance before it can retrieve or send data to the ADSP appliance. Username/password authentication is used to verify a connection to the inbound methods. A username must be setup in Account Access in Account Management. At the very least the account must have Read Only access to the Proximity API functional area. Read Only allows the account to use the methods that retrieve information from the appliance. Read/Write access allows the account to use the methods that write data back to the appliance.



7.2.2 Limiting Scope Access

The account can also be limited to specified scopes. In the Scope Permissions section of the account setup, select the scope levels the account should have access to. The account would then only have access to Proximity data from those scope levels it has been assigned.



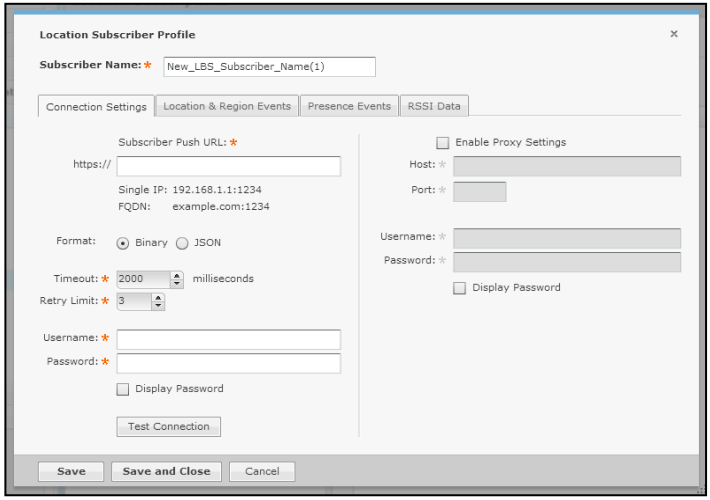
7.3 Outbound API (Push)

The outbound API methods are available from ADSP 9.0.3. When using the outbound API methods, ADSP initiates the connection to the third party application. ADSP opens up a connection to the third party application and sends the data defined in the Location Subscriber Profile. The third party application must implement a web service that ADSP understands how to communicate with.

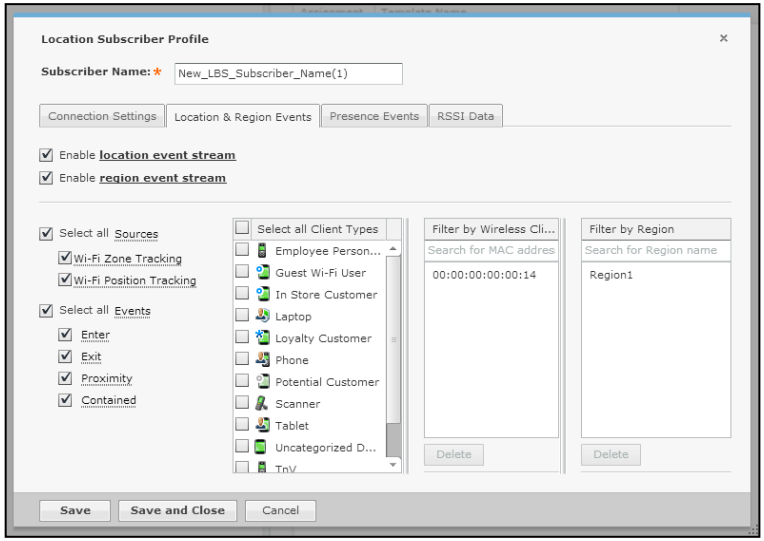
7.3.1 Location Subscriber Profile

The Location Subscriber Profile is where the connection settings and data filters are setup for a particular third party application end point. It can be found in Configuration under the Operational Management menu. Data from particular scopes can be limited simply by assigning the Location Subscriber Profile to specific scope levels.

Once a Location Subscriber Profile is created, the Connection Settings should be configured. These are the settings that ADSP uses to connect to the third party applications web service.



Also, on this tab the data format can be selected: either Binary or JSON. Binary is using protocol buffers which are more efficient, but are not human readable and is more difficult to parse. JSON is an XML based format that is human readable and much easier to parse.



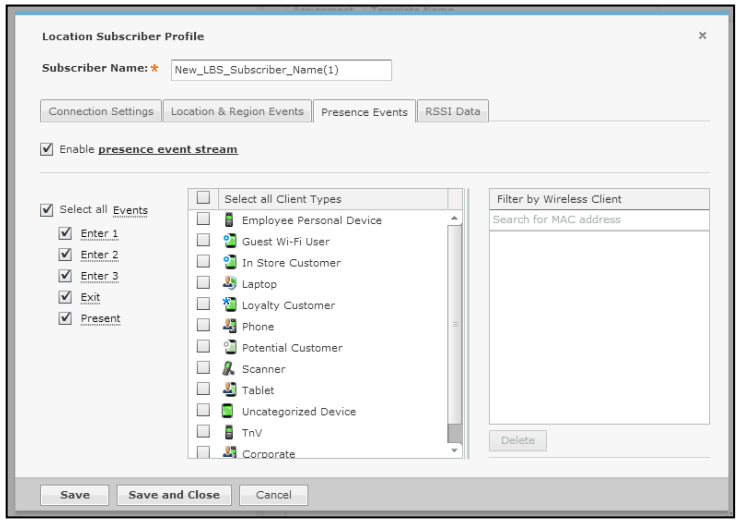
Once the connection settings are setup, the desired data streams must be enabled and appropriate filters are applied. In the Location & Region Events tab, the location data (XY) and Region event streams can be enabled. These two streams share the same filters.

First, the desired sources that the location and events are coming from must be selected. Then select which events are to be sent.

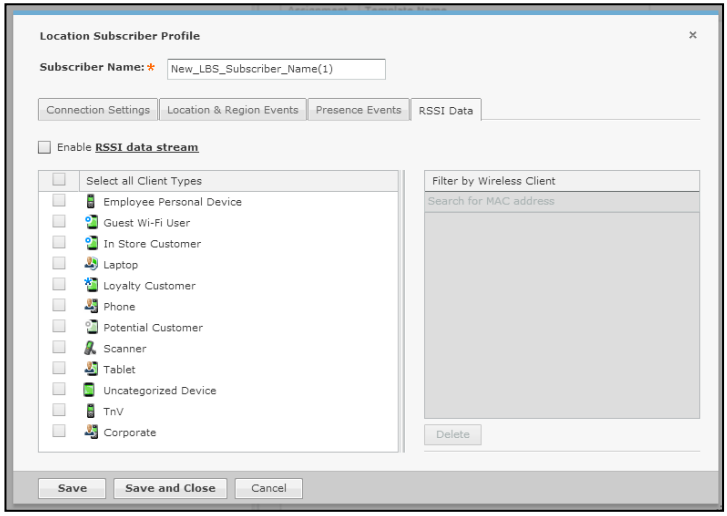
Further filtering can be performed by selecting Client Types, entering specific wireless client MAC addresses, or selecting specific Virtual Region. If specific Client Types are selected then the subscriber will only receive location and Region Events for those Client Types.

If any MAC addresses are entered in the Wireless Client filter then only location data and Region Events for those clients will be sent. If it is left blank then all data will be sent.

The Region filter works a little differently. If there was a region named *Electronics* on all the floor plans in the scope and that region was added to the filter then all Region Events triggered for that region name on all floor plans would be sent.



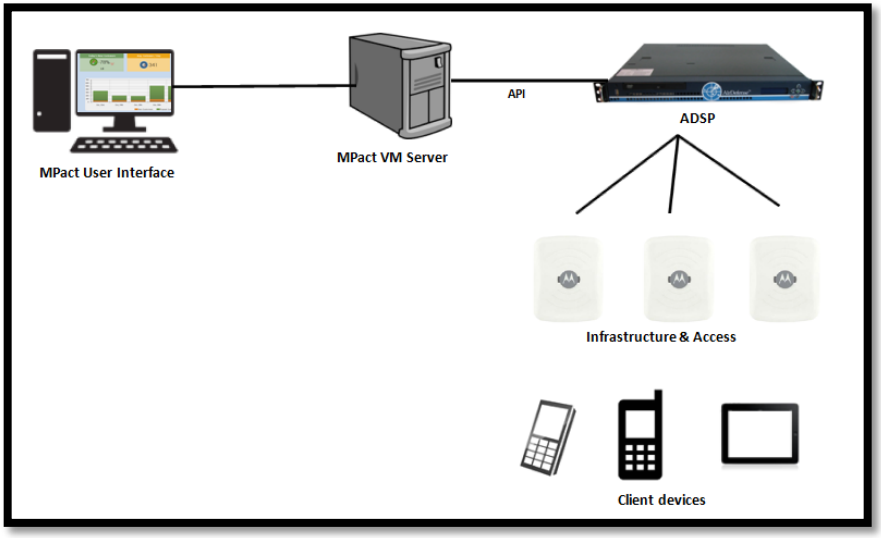
The Presence Event settings are very similar, but there is no source selection, and it has fewer filters. First select the event types that are to be sent to the subscriber. If sending Presence Events for certain Client Types is desired then select only those Client Types. Finally if Presence Events for specific wireless clients are to be sent then enter those MAC addresses. If the MAC filter is left blank then all data is sent.



The RSSI stream sends the raw RSSI data for the wireless clients. There are very few situations that this data is needed and should only be enabled in those cases. The filtering works just like the Presence Events.

8 MPact Integration

MPact platform offers unified BLE and Wi-Fi location tracking and analytics. Existing AirDefense customers who use Wi-Fi location based services, can migrate to MPact if they want to track visitors carrying BLE and/or Wi-Fi devices. In order to track both BLE and Wi-Fi devices from MPact, ADSP needs to be configured to feed LBS data and events to MPact server. The following picture depicts how an overall system looks like when ADSP is integrated with MPact.



From an integration perspective, the following things need to be configured.

a. Sync-up floor designs from ADSP with MPact

b. Configure MPact server as a Subscriber to LBS services on ADSP

8.1 Version Compatibility

The integration of MPact and ADSP is supported in the following releases. So, you would need

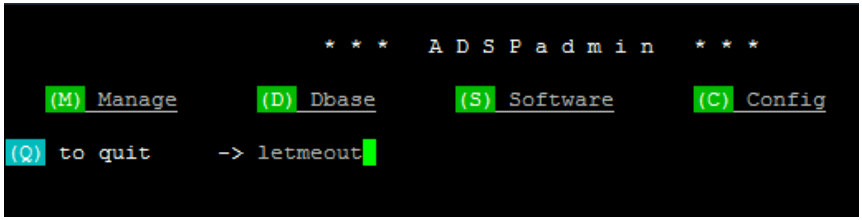
- MPact 1.0.1 Release
- ADSP 9.1.2 Release

8.2 Sync-up Floor Designs

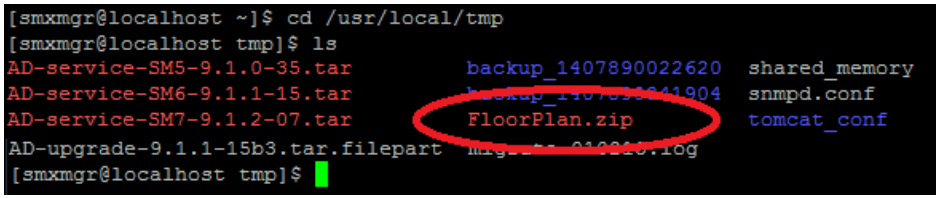
In order to migrate tracking of Wi-Fi client devices from ADSP to MPact, the floor map(s) from ADSP needs to be exported first. If there are any regions defined on ADSP floor plan, those regions would be automatically preserved on MPact server when these floor designs are imported.

Follow the steps below to copy floor designs from ADSP to MPact

- Logon to ADSP console using *smxmgr* account
- Enter *letmeout* command as shown below.



- $cd /usr/local/tmp
- $exportFloorplan
- This creates a file called FLoorPlan.zip



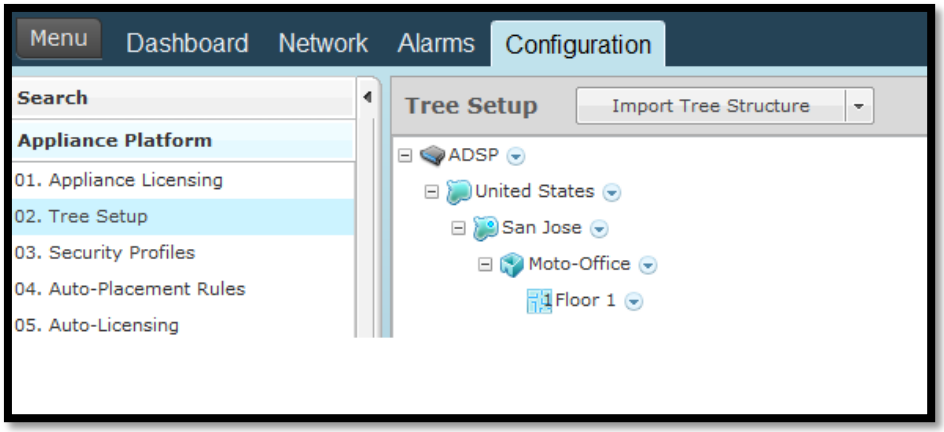
- Copy above file into “/tmp” directory on MPact using any FTP client
- Logon to MPact console using SSH
- cd /usr/nuxi/scripts/bin
- Run the following command to import floor designs on ADSP to MPact for all sites.

  ./atls importADSPPlanningData /tmp/FloorPlan.zip

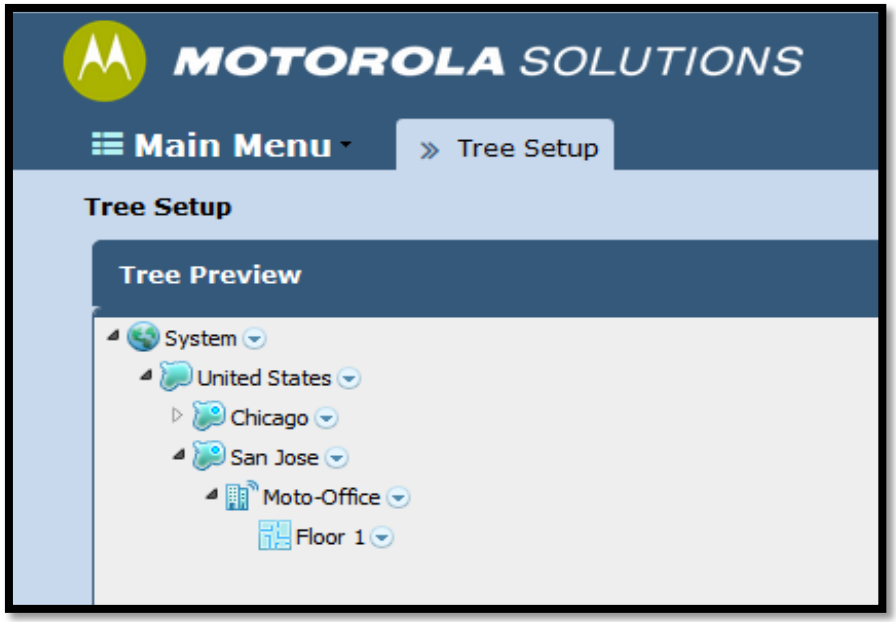
Note that the Country, Region, City, Campus, and Site names for any floor on ADSP tree hierarchy will be automatically created in MPact when the script runs. Verify the presence matching tree hierarchy both on ADSP and MPact, as shown below.

To check the tree setup on ADSP GUI, go to *Configuration -> Appliance Platform ->Tree Setup.*

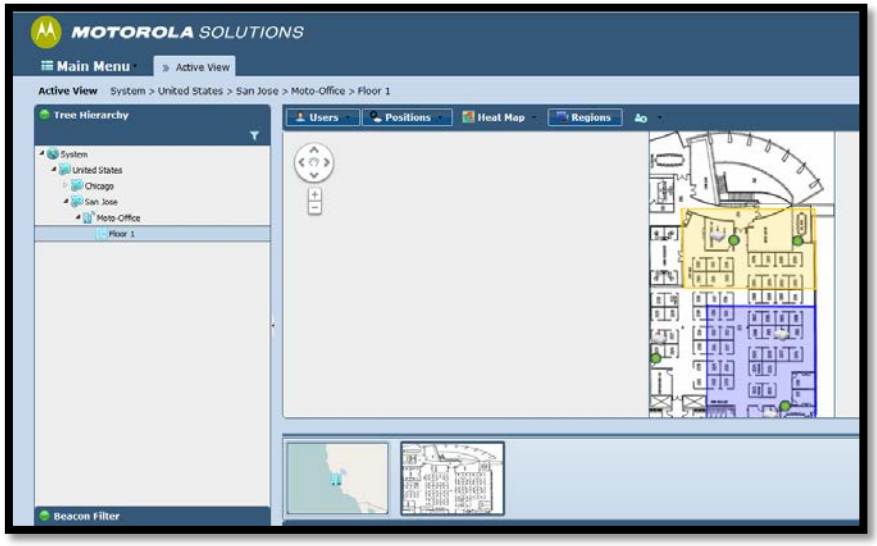
.



To verify the matching tree setup on MPact GUI, go to *Main Menu ->Tree Setup.*



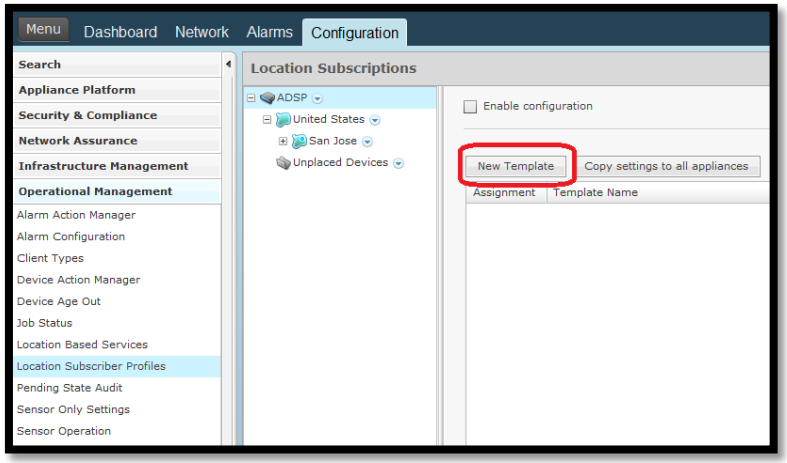
Once, tree hierarchy is verified, you can check the presence of new floor plans in Active View on MPact GUI, as shown below.



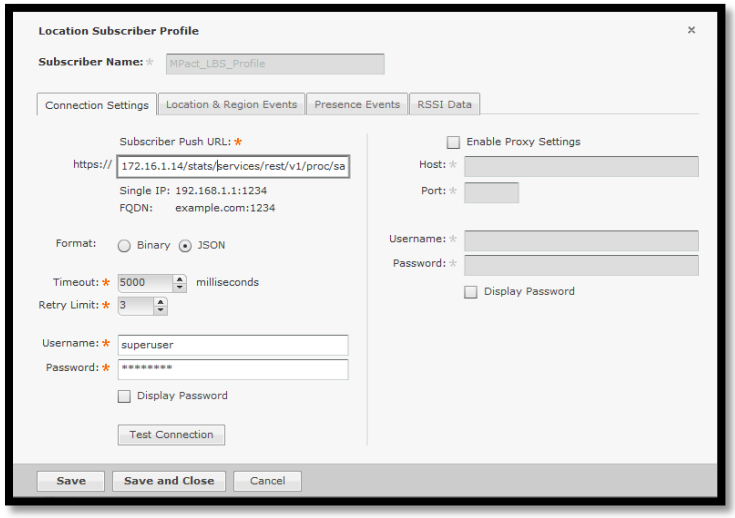
8.3 Setting MPact as a Subscriber

In order to track Wi-Fi and BLE clients from single console on MPact, ADSP should be configured to stream LBS data and events to MPact server for all Wi-Fi clients. This can done using Subscriber profile for location based services in ADSP.

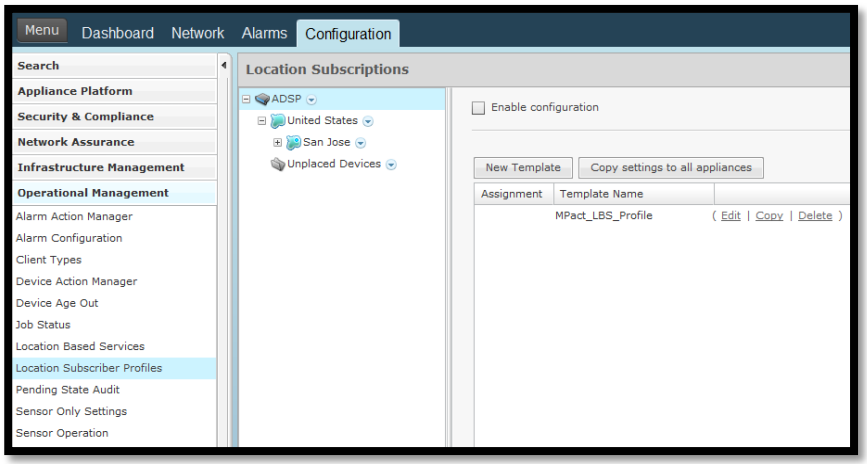
- Logon to ADSP GUI
- Navigate to “Configuration -> Operational Management -> Location Subscriber Profiles”
- Create a new profile by pressing “New Template” button as shown below.



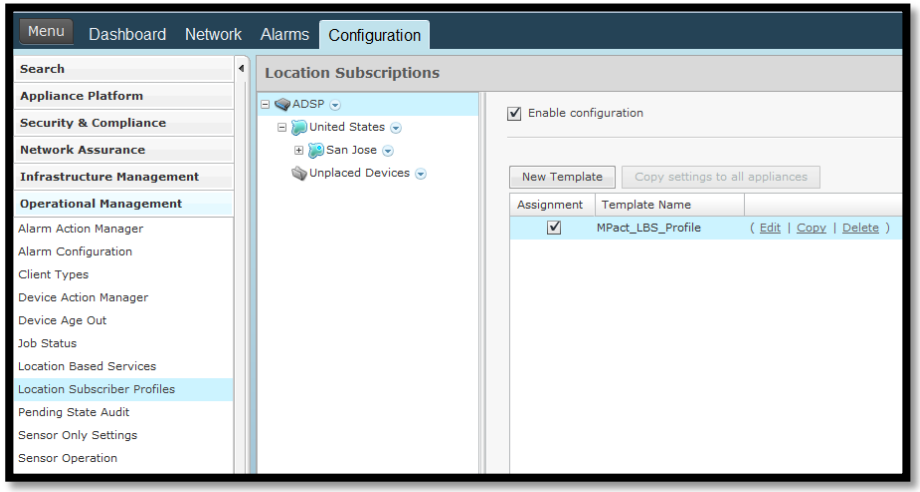
- You will see the following screen.



- Go to “Connection Settings” and enter the following link in Subscriber Push URL *<MPact-IP-Address>/stats/services/rest/v1/proc/save_gzip/ss/updateClientStatusADSP*
- Select JSON format and specify appropriate username and password.
- You can enable location data and events in “Location & Region Events” tab
- Enable Presence notifications in “Presence Events” tab and Ignore “RSSI Data” tab.
- Press “Save and Close” button. You will see the following screen.



- Select “Enable Configuration” and the new Subscriber profile that was created, as shown below and press “Apply” button at the bottom.

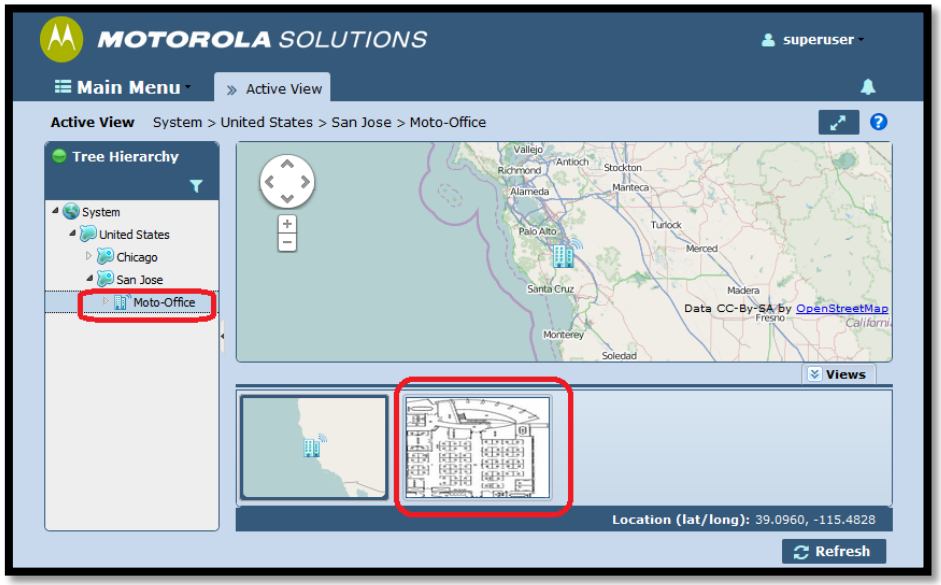


At this point, MPact will start receiving LBS data and events from ADSP.

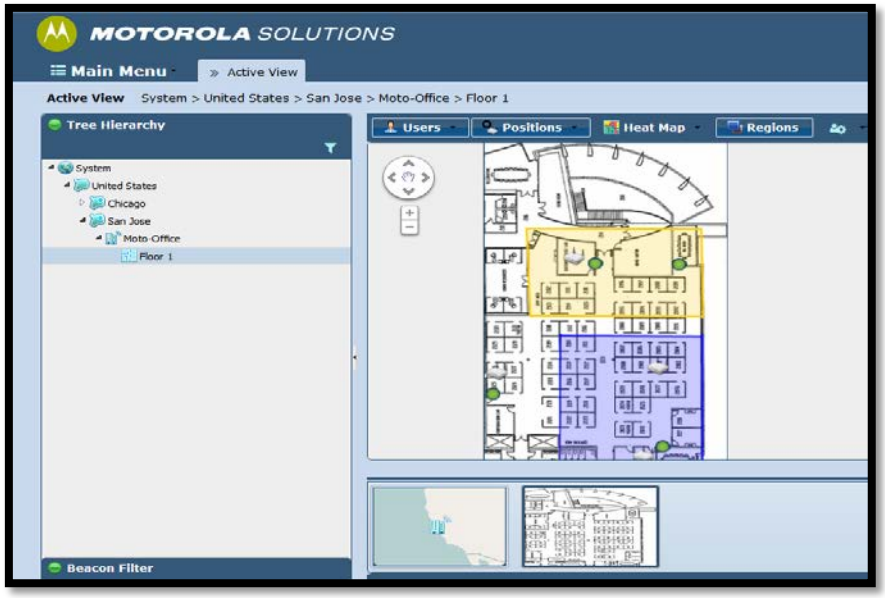
8.4 Tracking Wi-Fi and BLE Clients

One can track both Wi-Fi and BLE clients from *Active View* in MPact GUI, after following the steps mentioned in above sections.

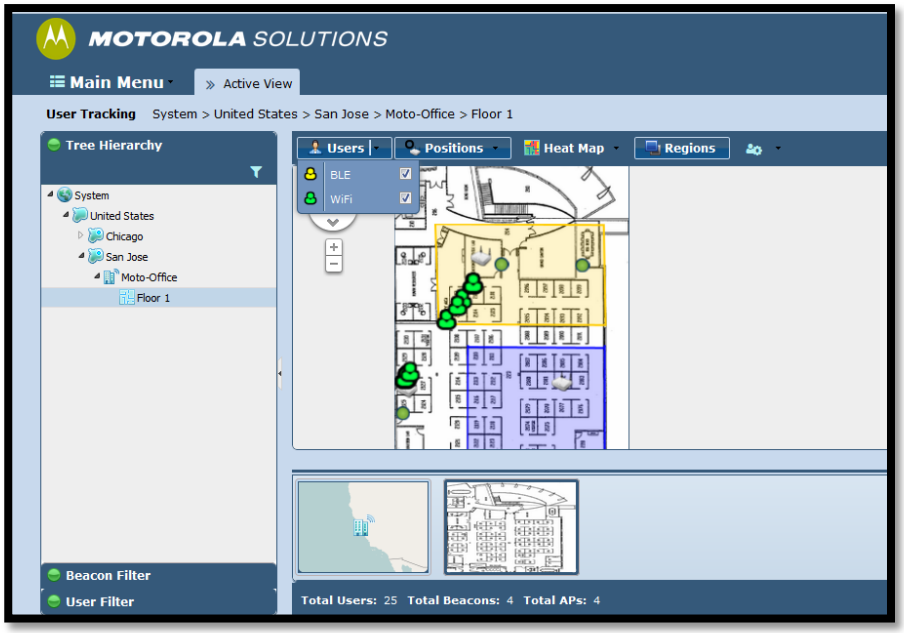
Logon to MPact GUI. Select *Active View* and navigate to the desired site in the Tree Hierarchy. The system will automatically displays icons of all floors in that site, as shown below.



Select the floor for which you want to track the clients. You will see the following screen.



In “Users” drop down menu, make sure that both BLE and WiFi tracking is enabled. This is shown below. All Wi-Fi clients are shown in green and BLE clients are shown in yellow.



The regions can be enabled or disabled using “Regions” button shown above.

Version 2
Nov 2014