Spectrum XT User Guide

Table of Contents

Introduction

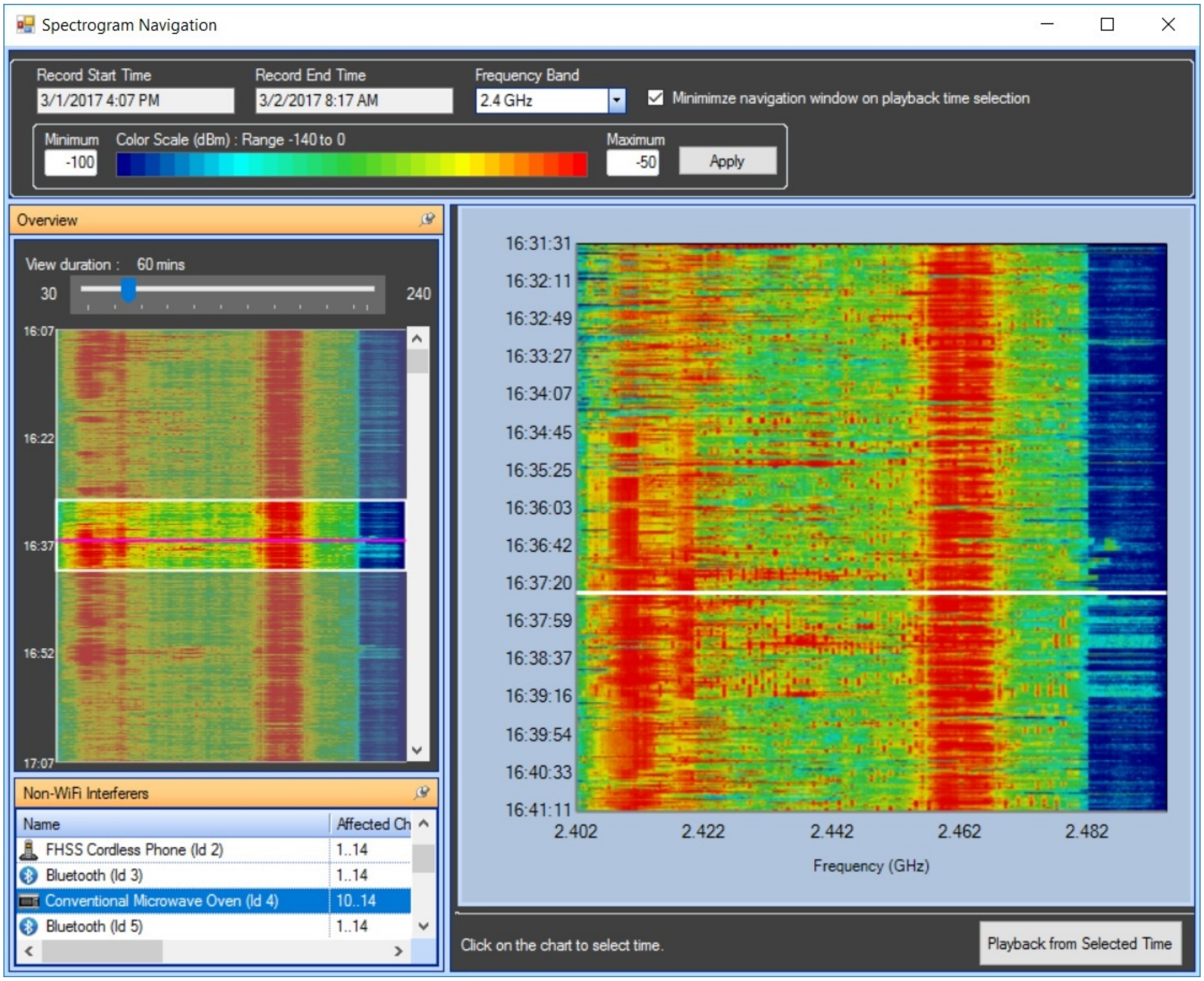
Spectrogram Navigation

During Playback you can select what portion of the recording to analyze. After making a selection, the recording will move to that exact spot and update all the visible charts.

Use this feature as follows:

1. Check the Capture Spectrogram Navigation data check box on the tab **Configure>Record Options**.

2. During Playback, click the **Spectrogram Navigation** icon ( ) on the toolbar. The Spectrum Navigation window appears.



Spectrogram Navigation

Record Start Time: 3/1/2017 4:07 PM

Record End Time: 3/2/2017 8:17 AM

Frequency Band: 2.4 GHz

☑ Minimimze navigation window on playback time selection

Minimum: -100 Color Scale (dBm) : Range -140 to 0 Maximum: -50

View duration : 60 mins

Non-WiFi Interferers

Name	Affected Ch
FHSS Cordless Phone (Id 2)	1..14
Bluetooth (Id 3)	1..14
Conventional Microwave Oven (Id 4)	10..14
Bluetooth (Id 5)	1..14

Click on the chart to select time.

3. The left-hand portion of the Spectrogram Navigation window provides an overview of the current recording. It allows you to select a portion of the recording to review in more detail, which when selected, appears on the right-hand side of the window.
4. Use the slider at the top left to increase or decrease the amount of time (in minutes) for which data is displayed in the Overview window on the left. If the recording is shorter than 30 minutes, the slider is not available.

5. Click an item on the Non-WiFi Interferers portion on the bottom left to display a purple line in the left side overview to indicate the selected interferer which will also display a white horizontal line (shown in the example above). Alternatively, you can select an area of interest in the right-side window with the white line and start playback from there.

6. When done, click **Playback from Selected Time** to playback the time you have selected.

Note: You can change the Frequency Band (from the drop-down on the top) to display a different set of Spectrogram data, if available.

The list of interferers is dependent upon on the current overview area and the current frequency band selection. When the spectrogram overview is changed, the list of interferers is updated to reflect the current overview area.

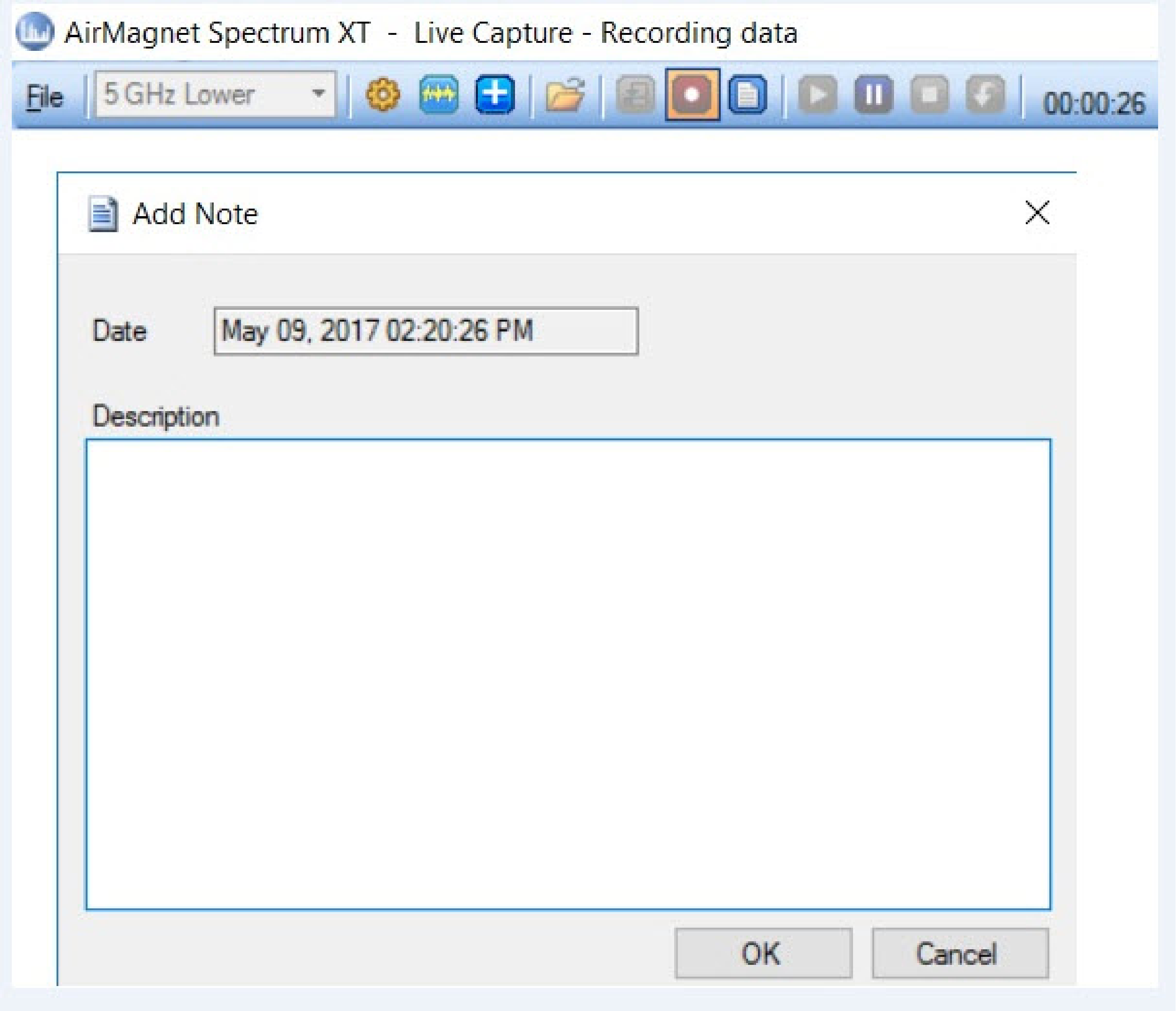
Adding Notes to Captured Data

During the recording and playback of a session, you can add annotation (Notes) at specific points.

Do this as follows:

1. During a recording session, click the **Add Note** button (📄) from the top menu bar.

2. When you select this button, a text box, as shown below, appears.



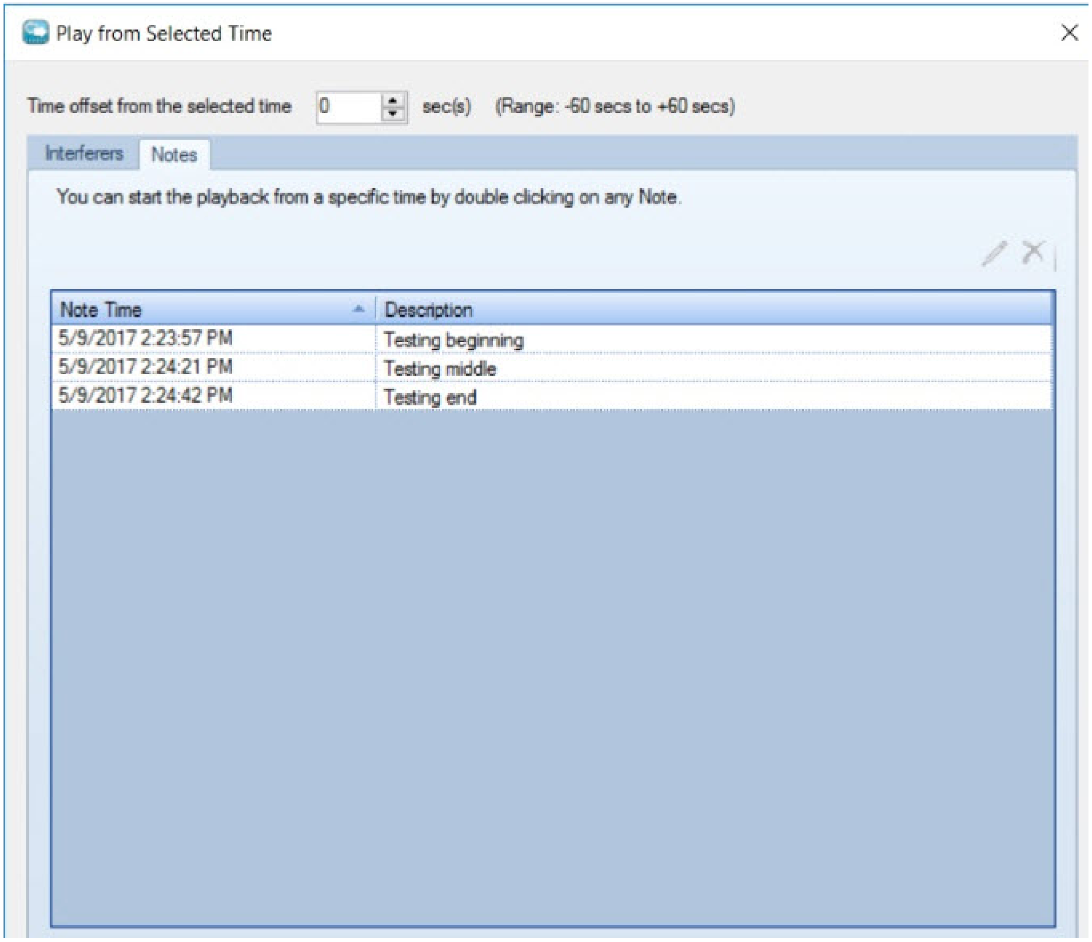
May 09, 2017 02:20:26 PM

3. Enter text in the Description field with a maximum of 512 characters.

4. Select **OK**, and the note gets added to the recording at the timestamp. Notes get saved with the recording to the bundled .amt file.

During playback of a recording, you can access the note(s) you made previously as follows:

When playing back a recording, the list of notes displays under the **Notes** tab in the "Play from Selected Time" window as shown below:



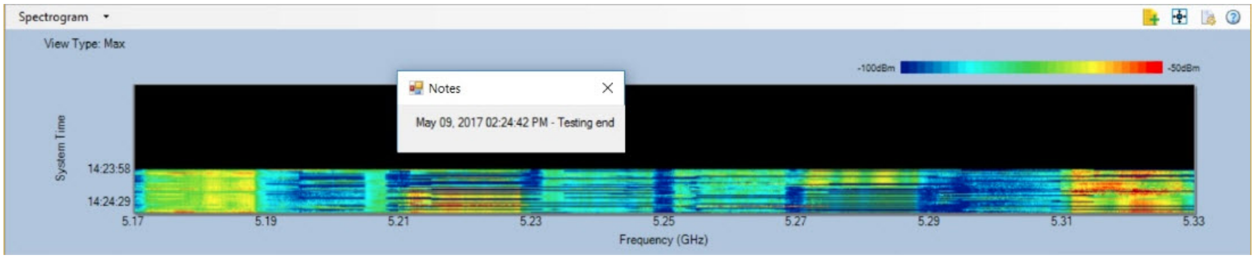
Time offset from the selected time 0 sec(s) (Range: -60 secs to +60 secs)

You can start the playback from a specific time by double clicking on any Note.

Note Time	Description
5/9/2017 2:23:57 PM	Testing beginning
5/9/2017 2:24:21 PM	Testing middle
5/9/2017 2:24:42 PM	Testing end

- Double-click a note and the playback will go to that spot in the recording.
- You can edit a Note by clicking the (✏) **Edit** icon. After you have edited the note, click **Close**.
- Delete a Note by selecting it and clicking the (✗) **Delete** icon.
- When the timestamp of a note is reached in a recording, the note appears in a popup window. Close the window by clicking **Close**.

The pop-up note appears as follows:



May 09, 2017 02:24:42 PM - Testing end

Copyright

AirMagnet® Spectrum XT User Guide.

NETALLY SHALL NOT BE HELD LIABLE FOR ERRORS OR OMISSIONS CONTAINED HEREIN; NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THIS CONTENT.

NetAlly
2075 Research Parkway
Colorado Springs, CO 80920

Spectrum XT version v3.10

Compiled in the United States of America. 04/2020.

General Terms and Conditions

(v01-Oct-19)

These General Terms and Conditions ("General T&Cs") are by and between the legal entity set forth in the applicable Order ("Company"), as further defined below, and sets forth the terms, conditions, rights and restrictions for which LinkRunner, LLC d/b/a NetAlly, and any of its subsidiaries and affiliates (collectively or individually referred to as "NetAlly") is willing to sell devices ("Hardware") and license NetAlly's proprietary software, as well as any firmware residing on such Hardware, ("Software") (The Hardware and Software may be collectively referred to as the "Product(s)"), and provide maintenance and technical support services ("Maintenance"), to Company. Unless otherwise governed by a signed contract between Company and NetAlly, only these General T&Cs will apply to any Orders made for NetAlly's Products. NetAlly's provisioning of Products, Maintenance or any other services to Company is expressly contingent upon Company's acceptance of these General T&Cs, "AS IS".

Receipt without return of any Products from NetAlly by Company shall be deemed as acceptance of this Order and shall also constitutes Company's confirmation that the Products descriptions, quantities, term, and prices set forth in the Order accurately represent Company's intended purchase. All additional and conflicting terms and conditions presented with or in any communication, including but not limited to those set forth in any P.O., except with respect to price, quantity, and location are hereby rejected, and shall be deemed null and void.

1. Definitions.

“API(s)” means the software application interfaces and workflow methods made generally available by NetAlly in certain Products to enable integration, implementation, and interoperability with third party hardware and software.

“Company” means a valid legal entity, in good standing, which has entered into a commercial agreement with NetAlly, allowing for the licensing or re-licensing of Software or distribution, sale, or resale of Products and Service.

“Company Data” means information that Company uploads or uses in conjunction with Company’s use of the Products.

“Data Protection Act” means the Health Information Portability and Accountability Act (HIPAA) (29 U.S. Code § 1181, et seq.), Gramm Leach Bliley Act (GLBA) (15 U.S Code § 1681), General Data Protection Regulation (GDPR) (EU 2016/679), and other applicable regulations which seek to protect the processing and storage of personal information.

“Documentation” means any installation guides, reference guides, operation manuals and release notes provided with the Product in printed, electronic, or online form.

“Evaluation Product” means software that contains a license key, which disables the Software after 30 days, or other term as agreed to by the parties, and which will render the Product unusable.

“Order" means the combination of Company’s P.O., a Quote issued by NetAlly or a NetAlly Company, and these General T&Cs.

“Personal Data” means any information relating to an identified or identifiable natural person (hereafter a “Data Subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

“P.O.” means a purchaser order or document, in tangible or intangible form (e.g. .rtf, .pdf, formats, etc.), issued by Company indicating Company’s acceptance of the Quote and these General T&Cs, without regards to any conflicting terms and conditions presented therein, except with respect to price, quantity, and location of Products or Services.

“Quote” means the document under which NetAlly offers for sale and licenses its Products, Maintenance, and other services.

“Services” means Maintenance as well as any other services offered by NetAlly to Company from time to time.

2. Shipment & Delivery Terms. NetAlly ships all Products hereunder FOB Origin. Unless otherwise agreed to by the parties, all shipments will be made using the carrier designated by Company. If Company does not designate a carrier, NetAlly reserves the right to choose a carrier at Company's expense. For Software available for electronic download, delivery will be deemed to have occurred once NetAlly has made the Software available for download by Company or Company's designate agent or representative. Unless otherwise stated conspicuously on the face of the applicable Order, NetAlly reserves the right to fulfill Orders via multiple shipments. For all Products shipped internationally, Company will be the importer of record. Company agrees that it will not remove any NetAlly General T&Cs or other agreement from the NetAlly Product(s), and/or associated packaging.

3. License Grant and Restrictions. Subject to payment of the applicable license fee and the terms set forth in an applicable Order, NetAlly grants Company a limited, non-exclusive, non-transferable, revocable license to use the Software and the Documentation for Company's own internal business purposes.

(a) Evaluation License: NetAlly hereby grants Company a temporary, non-exclusive, non-transferable, revocable license to use the Evaluation Product set forth in the applicable NetAlly Evaluation Request Form solely for internal testing, evaluation, or demonstration purposes. If Company chooses not to purchase a license for the Evaluation Product, the Evaluation Product must be removed from Company's system(s) and all permitted copies of such Evaluation Product immediately destroyed. A Return Materials Authorization number ("RMA #") for any Hardware Evaluation Product must be obtained prior to return of such Product.

(b) Pre-Released Products. If the Product Company has received with this license is not yet commercially available ("Pre-Released Product"), then NetAlly grants Company a temporary, non-exclusive, non-transferable, revocable license to use the Pre-Released Product and the associated Documentation, if any, as provided to Company by NetAlly solely for internal evaluation purposes. NetAlly may terminate Company's right to use the Pre-Released Product at any time at NetAlly's discretion. Company's use of the Pre-Released Product is limited to thirty (30) days unless otherwise agreed to in writing by NetAlly. Company acknowledges and agrees that (i) NetAlly has not promised or guaranteed to Company that the Pre-Released Product will be announced or made available to anyone in the future; (ii) NetAlly has no express or implied obligation to Company to announce or introduce the Pre-Released Product; (iii) NetAlly may not introduce a product similar to or compatible with the Pre-Released Product; and (iv) any use of the Pre-Released Product or any product associated with the Pre-Released Product is entirely at Company's own risk. During the term of these General T&Cs, if requested by NetAlly, Company will provide feedback to NetAlly regarding use of the Pre-Released Product. Company will not disclose any features or functions of any Pre-Released Product until NetAlly makes the Pre-Released Product publicly available.

(c) API License. NetAlly grants Company a limited, non-exclusive, non-transferable revocable license to use the API, together with applicable documentation, any sample code, and any sample applications provided with the API, solely in connection with the Products for Company's internal business purposes; provided that Company may not use the API in connection with developing a product or service that competes with Products.

(d) License Restrictions. Except as required by law, Company will not, and will not cause or permit others to, derive the source code of the Software, or reverse engineer, disassemble, or de-compile the Products. Company may not (i) create derivative works of the Software,

(ii) lend, rent, lease, assign, sublicense, and/or make available through timesharing or service bureau the Software, or (iii) transfer the Software or provide third party access to the Software.

(e) Third-party Technology. The Products may contain embedded third-party technology ("Third-party Materials"). Such Third-party Materials are licensed for use solely with the Product. Third-party Materials are provided subject to the applicable third-party terms of use ("TOU"). Company agrees to abide by the TOU and/or to obtain any additional licenses that may be required to use the Third-party Materials.

(f) Ownership. NetAlly and its third-party licensors retain all right, title, and interest in and to the Products, Third party Technology and/or APIs. Company retain all right, title and interest in and to the Company Data.

4. Acceptable Use. Company specifically agrees to limit the use of the Products and/or Services to those specifically granted in these General T&Cs. Without limiting the foregoing, Company specifically agrees not to (i) attempt to reverse engineer, decompile, disassemble, or attempt to derive the source code of the Software or any portion thereof; (ii) modify, port, translate, localize or create derivative works of the Software; (iii) remove any of NetAlly's, or its vendors, copyright notices and proprietary legends; (iv) use the Products to (a) infringe on the intellectual property rights of any third party or any rights of publicity or privacy; (b) violate any law, statute, ordinance, or regulation (including but not limited to the laws and regulations governing export/import control, unfair competition, anti-discrimination and/or false advertising); or (c) propagate any virus, worms, Trojan horses or other programming routine intended to damage any system or data; and/or (v) file copyright or patent applications that include the Product or any portion thereof.

5. Company & Personal Data. During the Term, Company may provide to NetAlly Company Data. NetAlly may use Company Data in connection with the performance of its obligations under these General T&Cs. Company hereby agrees to strictly comply with any and all applicable Data Protection Acts with regards to the transfer, handling storage and processing of Personal Data. Company acknowledges and agrees that should Company transfer such Personal Data to NetAlly, or other third-parties, Company will serve as such Personal Data's "Controller", as set forth in the applicable Data Protection Acts. Further, in the event of a breach of Personal Data, attributed to Company's actions or inactions in furtherance of these General T&Cs, in violation of the Data Protection Acts, Company shall promptly (i) take all necessary steps to curtail such breach; (ii) undertake all necessary actions to mitigate damages; (iii) provide the necessary notification and remediation, as set forth in the applicable Data Protection Act; and (iv) aid and assist in NetAlly's efforts to do the same, at Company's sole cost and expense.

6. Term and Termination. These General T&Cs shall continue unless terminated pursuant to this Section; provided, that the applicable subscription term for any licenses purchased hereunder shall continue for the period of time specified in the applicable Quotation. Either party may terminate these General T&Cs immediately upon providing written notice of breach to the other party, if such other party materially breaches any of its obligations hereunder but fails to cure such breach within a period of thirty (30) days following receipt of such written notice. Upon any termination of these General T&Cs (i) all licenses granted hereunder shall immediately terminate, (ii) Company will either return the Software, Documentation, and Copies or, with NetAlly's prior consent, destroy the Software, Documentation, and Copies.

7. Confidentiality. “Confidential Information” shall mean any and all non-public technical, financial, commercial or other confidential or proprietary information, Services, Product roadmaps, pricing, software code, Documentation, techniques and systems, and any and all results of benchmark testing run on the Products. Neither party will disclose Confidential Information to any third party except to the extent such disclosure is necessary for performance of these General T&Cs, or it can be documented that any such Confidential Information is in the public domain and generally available to the general public without any restriction. Each party will use the same degree of care to protect Confidential Information as Company uses to protect Company’s own confidential information but in no event less than reasonable care.

8. Warranties. NetAlly warrants, for Company’s benefit alone, (i) that the Hardware will be free from material defects for a period of twelve (12) months following the date of shipment of the Hardware ("Hardware Warranty Period"); and (ii) the Software, will conform materially and substantially to the Documentation for a period of ninety (90) days

following the date when first made available to Company for download (“Software Warranty Period”). The warranties set forth herein do not apply to any failure of the Software or Hardware caused by (a) Company’s failure to follow NetAlly's installation, operation, or maintenance instructions, procedures, or Documentation; (b) Company’s mishandling, misuse, negligence, or improper installation, de-installation, storage, servicing, or operation of the Product; (c) modifications or repairs not authorized by NetAlly; (d) use of the Products in combination with equipment or software not supplied by NetAlly or authorized in the Documentation; and/or (e) power failures or surges, fire, flood, accident, actions of third parties, or other events outside NetAlly's reasonable control. NetAlly cannot and does not warrant the performance or results that may be obtained by using the Products, nor does NetAlly warrant that the Products are appropriate for Company’s purposes or error-free. If during the Software Warranty Period or Hardware Warranty Period, a nonconformity is reported to NetAlly, NetAlly, at its option, will use commercially reasonable efforts to repair or replace the non-conforming Software or Hardware. THIS REMEDY IS CUSTOMER’S SOLE AND EXCLUSIVE REMEDY, AND NETALLY’S SOLE LIABILITY FOR A BREACH OF WARRANTY. EXCEPT FOR THE EXPRESS WARRANTIES STATED IN THIS SECTION 8, “WARRANTIES” NETALLY DISCLAIMS ALL WARRANTIES ON MERCHANDISE SUPPLIED UNDER THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

9. LIMITATION OF LIABILITY. NETALLY SHALL NOT BE LIABLE FOR ANY LOSS OR DAMAGE UNLESS SUCH LOSS OR DAMAGE IS DUE TO NETALLY’S GROSS NEGLIGENCE AND/OR WILLFUL MISCONDUCT. IF NETALLY IS FOUND LIABLE, THE AMOUNT OF NETALLY’S MAXIMUM LIABILITY FOR ANY AND ALL LOSSES AND/OR DAMAGES (IN CONTRACT, TORT, OR OTHERWISE) SHALL NOT EXCEED THE TOTAL AMOUNT OF ALL LICENSE FEES ACTUALLY PAID TO NETALLY FOR THE RELEVANT NETALLY PRODUCT(S) OR SERVICE(S) WITHIN THE PRIOR SIX (6) MONTHS FROM WHICH SUCH CLAIM ARISES.

10. EXCLUSION OF CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER OR ANY THIRD PARTY FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL, PUNITIVE, AND/OR INCIDENTAL DAMAGES, WHATSOEVER, INCLUDING BUT NOT LIMITED TO LOST PROFITS OR LOSS OF DATA, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH POTENTIAL LOSS OR DAMAGE.

11. ESSENTIAL PURPOSE. THE LIMITATION OF LIABILITY AND EXCLUSION OF CERTAIN DAMAGES STATED HEREIN SHALL APPLY REGARDLESS OF THE FAILURE OF ESSENTIAL

PURPOSE OF ANY REMEDY. BOTH PARTIES HEREUNDER SPECIFICALLY ACKNOWLEDGE THAT THESE LIMITATIONS OF LIABILITY ARE REFLECTED IN THE PRICING.

12. Indemnification. For any claims based on Company's breach of Section 3, "License Grant and Restrictions", 4. "Acceptable Use", 5 "Company & Personal Data", 7 "Confidentiality", 8 "Warranties", 14.4 "Compliance & Export Controls", 14.6 "Anti-Corruption and Anti-Bribery" and/or Company use of Product(s), Company hereby agrees to indemnify, defend, and hold NetAlly harmless against such claim(s) at Company's expense and pay all damages that a court of competent jurisdiction finally awards, provided that NetAlly (i) promptly notifies Company in writing of the claim(s); (ii) allows Company to control the defense or any related settlement negotiations; and (iii) cooperates with Company in the defense of any such claim(s); provided, that, Company will not affect any settlement unless such settlement provides NetAlly with a full release.

13. Relationship with Third parties. The relationship between the parties established by these General T&Cs is that of independent contractors, and nothing contained in these General T&Cs shall be construed to: (i) give either party the power to direct or control the day-to-day activities of the other; (ii) constitute the parties as partners, joint ventures, co-owners or otherwise as participants in a joint or common undertaking or franchise; (iii) allow Company to create or assume any obligation on behalf of NetAlly for any purpose whatsoever; or (iv) allow any customer, End-User, or other person or entity not a party to these General T&Cs to be considered a third-party beneficiary of these General T&Cs.

14. General Provisions.

14.1 Entire Agreement T&Cs & Integration. These General T&Cs and all Exhibits referencing these General T&Cs represent the entire agreement between the parties on the subject matter hereof and supersede all prior discussions, agreements and understandings of every kind and nature between the parties. Neither party shall be deemed the drafter of these General T&Cs. No modification of these General T&Cs shall be effective unless in writing and signed by both parties. All additional and conflicting terms and conditions presented with or in any communication, including but not limited to Company's P.O., except with respect to price, quantity, and location specified in a P.O., are hereby rejected, and shall be deemed null and void.

14.2 Severability & Survival. The illegality or unenforceability of any provision of these General T&Cs shall not affect the validity and enforceability of any legal and enforceable provisions hereof. Should any provision of these General T&Cs be deemed unenforceable by a court of competent jurisdiction then such clause shall be re-construed to provide the maximum protection afforded by law in accordance with the intent of the applicable provision. Any provision contained herein, which by its nature should survive the termination of these General T&Cs shall survive, including, but not limited to, Section 7 "Confidentiality", 9 "Limitation of Liability & Exclusion of Consequential Damages", 12 "Indemnification", and 14 "General Provisions".

14.3 Assignment. Neither party may assign any rights or delegate any obligations hereunder, whether by operation of law or otherwise, except in the case of a sale of either party's business whether by merger, sale of assets, sale of stock or otherwise, or except with the prior written consent of the other party, which consent will not be unreasonably withheld. These General T&Cs binds the parties, their respective participating subsidiaries, affiliates, successors, and permitted assigns.

14.4 Compliance & Export Controls. Company shall comply fully with all applicable laws, rules, and regulations including those of the United States, and any and all other jurisdictions globally, which apply to Company's business activities in connection with these General T&Cs. Company acknowledges that the NetAlly Products and/or NetAlly Services are subject to United States Government export control laws. Company shall comply with all applicable export control laws, obtain all applicable export licenses, and will not export or re-export any part of the Products and/or Services to any country in violation of such restrictions or any country that may be subject to an embargo by the United States Government or to End-Users owned by, or with affiliation to, such countries embargoed by the United States Government.

14.5. U.S. Government Use Notice. The NetAlly Software is a "Commercial Item", as that term is defined at 48 C.F.R. § 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. § 12.212 and 48 C.F.R. § 227.7202, as applicable. Consistent with 48 C.F.R. § 12.212 and 48 C.F.R. § 227.7202-1 through 227.7202-4, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government End-Users (a) only as Commercial Items and (b) with only those rights as are granted to all other End-Users pursuant to the terms and conditions herein. For some components of the Software as specified in the Exhibit, Attachment, and/or Schedule, this Software and Documentation are provided on a RESTRICTED basis. Use, duplication, or disclosure by the United States Government is subject to restrictions set forth in Subparagraphs (c) (1) and (2) of the Commercial Computer Software Restricted Rights at 48 CFR 52.227-19, as applicable.

14.6 Anti-Corruption and Anti-Bribery. Company will not make or permit to be made any improper payments and will comply with the U.S. Foreign Corrupt Practices Act, the UK Bribery Act, the Organization for Economic Co-operation and Development ("OECD") Convention on Anti-Bribery, and other applicable local anti-bribery laws and international anti- bribery standards. Company represents and warrants that it will not pay any commission, finder's fee, or referral fee, or make any political contribution, to any person in connection with activities on behalf of NetAlly.

14.7 Applicable Law & Disputes. The parties specifically agree that the U.N. Convention on the International Sale of Goods, the Uniform Computer Information Transactions Act ("UCITA"), and the International Commercial Terms issued by the International Chamber of Commerce ("Incoterms") shall not apply to any and all actions performed by either party hereunder in furtherance of these General T&Cs. These General T&Cs and all resulting claims and/or counterclaims shall be governed, construed, enforced and performed in accordance with the laws of the State of Colorado, United States of America, without reference and/or regard to its conflicts of laws principles. The parties hereto specifically agree that the exclusive jurisdiction for any and all resulting claims and/or counterclaims arising out of these General T&Cs shall be the federal and local courts of Denver, Colorado.

14.8 Force Majeure. Neither party shall be liable for any failure or delay in performing Services or any other obligation under these General T&Cs, nor for any damages suffered by the other or an End-User by reason of such failure or delay, which is, indirectly or directly, caused by an event beyond such party's foreseeable control including but not limited to strikes, riots, natural catastrophes, terrorist acts, governmental intervention, or other acts of God, or any other causes beyond such party's reasonable control.

14.9 Waiver. Each party agrees that the failure of the other party at any time to require performance by such party of any of the provisions herein shall not operate as a waiver of the rights of such party to request strict performance of the same or like provisions, or any other provisions hereof, at a later time.

15. Notices. All notices under these General T&Cs shall be in English and shall be in writing and given to the address indicated upon the cover page and may be sent either by (i) registered airmail; (ii) overnight delivery through a reputable third-party courier; or (iii) via electronic mail (email) sent "read receipt" and "delivery receipt". With respect to NetAlly's receipt of electronic notice set forth in (iii) above such notice shall only been deemed received once Company receives a confirmation of "read receipt" and "delivery receipt" and such notice shall only be valid if sent to legal@netally.com.

See also https://www.netally.com/web-legal/.

Main Features

AirMagnet Spectrum XT has the following main features:

- ***Ability to scan all available 802.11 radio bands***

  AirMagnet Spectrum XT has the capability to capture live spectrum and Wi-Fi data in the wireless network and display them in real time on the screen, assuming you have an AirMagnet-supported wireless network adapter installed and enabled at the same time. To make it easier for you to focus on a certain part of the 802.11 radio spectrum, AirMagnet Spectrum XT offers six band options: 2.4 GHz, 4.9 GHz, 5.0 GHz Lower, 5.0 GHz Middle, 5.0 GHz Upper, and Mixed which includes all options other than 4.9 GHz. You can choose any of these band options from the Band menu in the toolbar.

- ***Real Time FFT***

  The Real Time FFT graph displays in real time the current, average, and maximum FFT readings. The X-axis represents channel/frequency and the Y-axis shows power readings in dBm.

- ***Spectrum Density***

  The Spectrum Density graph shows the "popularity" of a particular frequency/power reading over time. The X-axis shows the frequency/channel for the selected 802.11 radio band; the Y-axis shows the power readings in dBm. You can also display the signal strength of selected APs across the Spectrum Density graph by selecting APs of interest from the AP List by SSID/Channel section on the left. Click here for more information.

- ***Spectrogram***

The Spectrogram graph shows the distribution (sweep) of energy across the radio band over time and changes in frequency use and the duration of such changes. Click here for more information.

- ***Channel Power***

  The Channel Power graph shows the current and maximum (aggregated) channel energy readings. The graph can display either Envelope Power or Integrated Power. The former refers to the highest power reading at a particular frequency; the latter shows the total summation of power readings over a specific bandwidth. Click here for more information.

- ***Channel Duty Cycle***

  The Channel Duty Cycle graph shows the percentage of time the RF energy (both 802.11 and non-802.11) is present on the channel. Click here for more information.

- **Non-Wi-Fi Devices**

  This table lists all non-Wi-Fi devices whose spectrum information has been detected by the application, along with some key data about each device. The devices are organized by category which includes Bluetooth devices, microwave ovens, cordless phones, baby monitors, wireless cameras, and RF Jammers. Click here for more information.

- ***Event Spectrogram***

  The Event Spectrogram provides a visual presentation of real-time information about events (device detections) that the application has made in the network. Each detection is an event which is represented by a color band. The color of the band indicates the signal strength of the device being detected (refer to the signal scale on top of the graph). If more detections are made of the same device as the application sweeps the spectrum, the band will become thicker (taller). The height of the color band indicates the (length of time in seconds the device has been detected. It stops increasing when the device becomes inactive (meaning that the device has not been detected for a minute). The width of the line/band indicates the channels or frequencies being affected by the device. If the device is a frequency-hopping device, then the line/band may extend sideways as the device hops from one channel to another. Click here for more information.

- ***WiFi Device***

  The WiFi Devices graph (table) displays comprehensive information about all Wi-Fi devices, such as APs, stations, and phones, detected on the Wi-Fi network. Click here for more information.

  Note: To view this graph, you must have an AirMagnet-supported wireless network adapter installed and enabled when running AirMagnet Spectrum XT**.**

- ***AP Signal Strength***

  The AP Signal Strength graph identifies the three APs with the strongest signal strengths on each available channel in the selected radio band. Click here for more information.

  Note: To view this graph, you must have an AirMagnet-supported wireless network adapter installed and enabled when running AirMagnet Spectrum XT.

- ***Channel Occupancy***

  The Channel Occupancy graph shows AP deployment on all available channels in the selected radio band. It identifies all APs deployed on each channel. It also shows their overall signal strength (strong or weak) and the channels that are being affected. Click here for more information.

  Note: To view this graph, you must have an AirMagnet-supported wireless network adapter installed and enabled when running AirMagnet Spectrum XT.

- ***Channels by Speed***

  The Channels by Speed graph displays the relative amount of data (in kilobytes) that has been transmitted at each data rate on each available channel in the selected radio band. The X-axis lists all the available channels and the data rates used on each channel, whereas the Y-axis shows the number of Kilobytes of data transmitted at certain speeds on each channel. Click here for more information.

  Note: To view this graph, you must have an AirMagnet-supported wireless network adapter installed and enabled when running AirMagnet Spectrum XT.

- ***Channels by Media***

  The Channels by Media graph shows that volume of Wi-Fi transmissions in kilobytes recorded on each channel in the selected radio band. It also provides a rough breakdown by 802.11 media type of the transmission on each channel. Click here for more information.

  Note: To view this graph, you must have an AirMagnet-supported wireless network adapter installed and enabled when running AirMagnet Spectrum XT.

- ***Channels by Address***

  The Channels by Address graph shows the volume of data transmission in kilobytes that has been recorded on each channel in the selected radio band. It also provides a rough breakdown of the transmission by the type of address (that is, broadcast, multicast, and unicast) that was used for the transmission. Click here for more information.

  Note: To view this graph, you must have an AirMagnet-supported wireless network adapter installed and enabled when running AirMagnet Spectrum XT.

- ***Channel Utilization***

  The Channel Utilization graph shows the percentage of bandwidth being used on each channel and the breakdown of the utilization by transmission rate. Click here for more information.

  Note: To view this graph, you must have an AirMagnet-supported wireless network adapter installed and enabled when running AirMagnet Spectrum XT.

- ***Top 10 APs by Speed***

  The Top 10 APs by Speed graph shows the 10 APs that have transmitted the most amount of data (in kilobytes) as well as the breakdown of the transmissions by data rate on each AP. Click here for more information.

  Note: To view this graph, you must have an AirMagnet-supported wireless network adapter installed and enabled when running AirMagnet Spectrum XT.

- **Top 10 Active APs' Retry/CRC**

  The Top 10 Active APs’ Retry/CRC graph shows the percentage of packets that are either Retry or CRC packets for the top 10 APs that are transmitting the most data. Click here for more information.

  Note: To view this graph, you must have an AirMagnet-supported wireless network adapter installed and enabled when running AirMagnet Spectrum XT.

- **Interference Power**

  The Interference Power graph displays the average power readings of interfering devices on the selected channel or channels.

- **Channel Duty Cycle vs Time**

  The Channel Cycle vs. Time graph is a trending chart which shows the average power in the channel is above the noise floor over a specific period of time.

- **Interference Power vs Time**

  The Interference Power vs. Time graph is a trending chart which shows the maximum average power readings of interfering devices operating on the selected channel over a specific period of time.

- ***Channel Signal/Noise Ratio***

  The Channel SNR graph shows the signal-to-noise ratio on all available channels in the selected radio band.

- ***Channels by Retry/CRC***

The Channels by Retry/CRC graph allows the user to quickly assess which channels are experiencing high levels of Retry or CRC packets.

- **Finding Devices**

The Find Device tool enables the user to find any device (Wi-Fi or non-Wi-Fi) that the application has detected. You can launch the Find Device screen by clicking (**Find Device**) at the bottom of the screen. Once on the Find Device screen, you can select the device of interest and click **Find**. The screen will show you in real time the signal strength (if the device in question is a non-Wi-Fi device) or signal strength and noise level (if it is a Wi-Fi device). You can also turn on the audio feature to assist in locating the device: the closer you approach the device the louder the sound.

Note: You can also open the Find Device screen by double-clicking a device of interest from the Device List in the Spectrum screen. In this case, the device of interest will be automatically selected and all you need to do is to click **Find**.

- ***Instant Playback of Live Capture Data***

The instant playback feature allows you to revisit something they have noticed on the live screen. It is very useful when you want to take a closer look at what has caught your attention at the first glance. You can switch to instant playback mode by clicking (**Switch to Instant Playback**) on the toolbar. You can also save the data that has just been played back into a file for record or further analysis.

Note: The amount of data that is replayed may last for one or two minutes, depending on the speed of the PC the user is using.

- ***Recording Live Data***

This feature allows you to record live data the application captures to the hard drive of the PC, by clicking (**Start Recording**) on the toolbar. You can interrupt the recording at any time by clicking **(Stop Recording and Save Capture),** which will then prompt the user to save the recorded data to a *.amm* file.

Note: The length of the recording depends on the Max Live Capture Streaming File Size [MB] you have configured **(Settings>Configure)**. The application will stop recording once the limit has been reached. Upon completion of the recording, you will be prompted to save the recorded data. Also, if the available hard drive space is less than the size of the Max Live Capture Streaming File, a message will pop up to remind you of the deficiency so that proper actions can be taken to rectify the problem from the start.

- ***Saving Capture Data***

  This feature allows you to save to an *.amt* file the live data they have recorded.

  Note: To save recorded data, you must first stop recording by clicking **Stop Recording and Save Capture** (on th you clicks **Start Recording**. Also, the application will automatically stop recording and prompt you to save the recorded data once the Max Live Capture Streaming File Size [MB] is reached.

- ***Replaying Capture Data***

  This feature allows the user to replay recorded data saved to an .amt file.

  To replay recorded capture data, click 📂 (Open Capture File) on the toolbar. Then select and open the .amm file of interest. The application will start replaying the recorded data. During the course of the replay, the user can pause or stop the replay using the buttons on the tool bar. When the replay completes, the user can play it again using the replay button.

- ***Right-click to copy graph***

  The feature allows you to easily copy any graph or chart displayed on the screen and paste it into any software document that supports the copy-and-paste.

- **Right-click to save graph**

  The application allows you to save any chart or graph shown in the Graph Window as an image file in any of the following four image formats:

  - .PNG
  - .BMP
  - .JPG
  - .GIF

- **Custom Device Classification**

  Due to the ever changing nature of wireless device technology, there are ever more devices that transmit in the 2.4 and 5GHz regulatory frequency bands. In order to allow customers to identify more potential non-Wi-Fi interferers, users have the ability to identify, classify, and analyze interferers beyond those devices included in the software package.

- **Region-Specific Scanning Control**

  Users in regions with specific wireless range restrictions have the ability to specify precisely which channels shall be scanned in AirMagnet Spectrum XT by simply selecting the desired region from a drop-down provided in the application's configuration window. This streamlines the process of narrowing down the channels needed based on the area in which the network is located to a simple one-click process.

- **Virtual AP Grouping**

  AirMagnet Spectrum XT's Virtual AP Grouping feature allows you to set up specific names for single devices that utilize multiple SSIDs under different BSSIDs. These groups help you identify instances where separate BSSIDs show up and appear to be several different devices, when they actually belong to a single device.

- **BlueSweep Integration**

  BlueSweep software is designed to identify nearby devices with Bluetooth wireless technology and alert users to potential Bluetooth security risks. It identifies and tracks devices up to 300 feet away and lets users know what their own Bluetooth devices are doing.

- **Remote Spectrum Analysis**

  AirMagnet Spectrum XT enables you to connect to remote systems to perform remote troubleshooting capabilities.

  The Remote XT Connection option enables you to view remote, real-time data in their local Spectrum UI. It does this by connecting to a remote computer running an AirMagnet Spectrum Analyzer card.

Product Overview

AirMagnet Spectrum XT is a Wi-Fi troubleshooting and optimization tool from NetAlly, designed to provide W-Fi network professionals with a clear and concise view into their wireless network environment. AirMagnet Spectrum XT's power reaches far beyond its sleek and intuitive design, because it includes the option to complement spectrum analysis with Wi-Fi packets and traffic analysis, using an optional second Wi-Fi card. This allows you to directly connect spectrum information to the real performance of your wireless APs and channels. The software brings everything together in a single, clean interface that ensures that you can easily see the information that you need without digging through pages of data.

Product Registration

Registering your AirMagnet Spectrum XT allows you expedient access to technical support, product upgrades, and other benefits. It is for this reason that we make product registration an integral part of the installation process. The online product registration form automatically pops up in your Web browser screen when you launch AirMagnet Spectrum XT for the first time after it is installed.

You need to follow the instructions on the screen to register your AirMagnet Spectrum XT now if you do not yet have a AirMagnet Spectrum XT license file (on your laptop PC or network), which is required in order to operate the application. The product registration process will enable you to download and install your software license file from AirMagnet over the Internet.

However, if you already have a software license file at hand and do not want to register right now, you may simply follow the prompt on the screen to upload the license file and close the Product Registration Web page. You can always come back to register your product at a later time using the following instructions.

To register your product at any time, open the following URL:

https://airmagnet.netally.com/support/register_product/

System Requirements

Laptop /Tablet PC

- Operating Systems: Microsoft® Windows 8.1 Pro/Enterprise 64-bit or Microsoft® Windows 10 Pro/Enterprise 64-bit.
- Intel® Core™ 2 Duo 2.00 GHz (Intel® Core™ i5 or higher recommended).
- 2 GB RAM required (4 GB recommended)
- 250 MB free hard disk space.
- Microsoft .NET framework 4.6.1.

Apple® MacBook® Pro

- Operating Systems: MAC OS X Version 10.9 or higher running a supported Windows OS (as noted under Laptop/Notebook PC/Tablet PC section) using Boot Camp®.
- Intel®-based 2.2 GHz Core 2 Duo or higher.
- 2 GB RAM required (4 GB recommended)
- 250 MB free hard disk space.
- Microsoft .NET framework 4.6.1.

Supported Wi-Fi Adapters

AirMagnet Spectrum XT offers Wi-Fi analysis features in addition to the spectrum features supported by the AirMagnet Spectrum USB adapter.

Note: However, keep in mind that an AirMagnet Spectrum USB adapter is required when running AirMagnet Spectrum XT. The application will not work without a supported spectrum USB adapter.

The wireless network adapters supported and tested by NetAlly are listed at:

https://www.netally.com/products/airmagnet-spectrum-xt/#SupportedAdapters

Technical Support

AllyCare Product Support

NetAlly's AllyCare is our comprehensive support and maintenance program that offers expanded coverage for the products.

For more information, visit https://www.netally.com/support/.

Contact Us

Call toll-free in North America: 1-844-TRU-ALLY (1-844-878-2559)

Visit https://www.netally.com/contact-us/ for additional phone numbers. Scroll down and select your region to complete a web form and have a NetAlly representative contact you.

Troubleshooting AirMagnet Spectrum XT

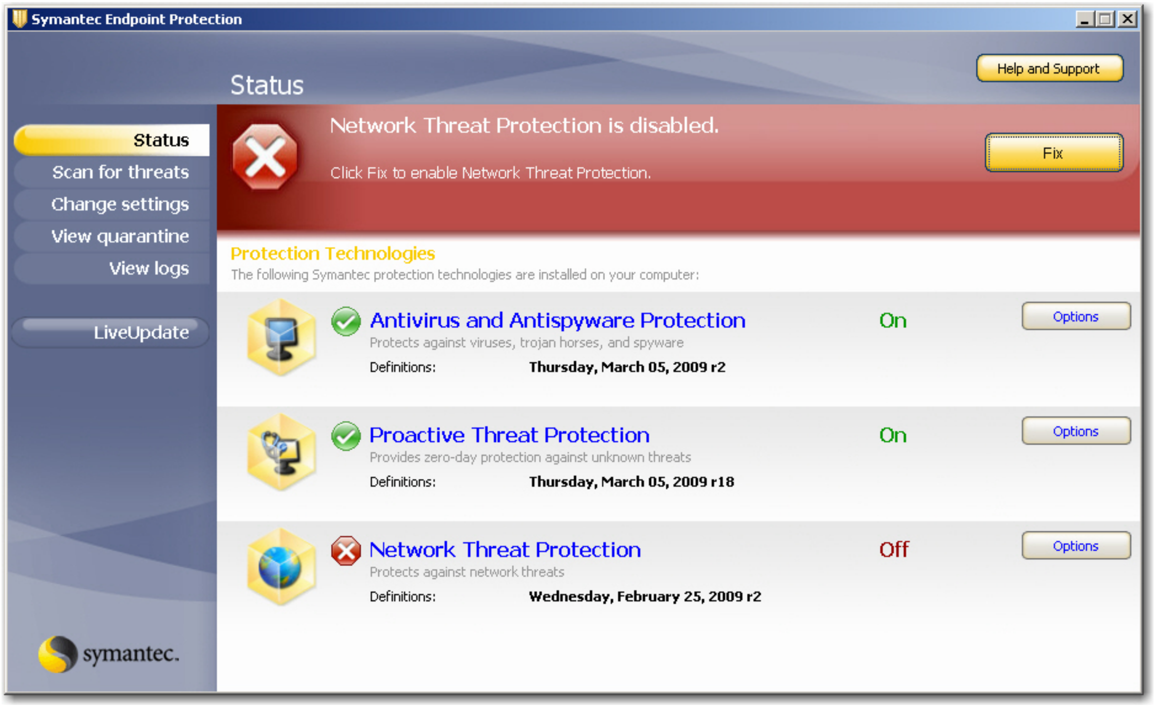
This section explains some typical troubleshooting scenarios related to the use of AirMagnet Spectrum XT.

I have both a spectrum adapter and a wireless network adapter enabled, but why do no Wi-Fi devices show up on the screen?

AirMagnet Spectrum XT has the capability to capture and display both Wi-Fi and spectrum data simultaneously from a network environment. As a result, you should be able to see both Wi-Fi and non-Wi-Fi devices the application has captured. The following steps will help you solve this issue:

1. Make sure that your wireless network adapter is supported by AirMagnet.
   Refer to Supported Wireless Network Adapters.

2. Turn off **Network Threat Protection** on Symantec Endpoint Protection if you have the application installed on the PC. Refer to the illustration below.



Network Threat Protection is disabled.

Click Fix to enable Network Threat Protection.

Protection Technologies

The following Symantec protection technologies are installed on your computer:

Antivirus and Antispyware Protection On

Protects against viruses, trojan horses, and spyware

Definitions: Thursday, March 05, 2009 r2

Proactive Threat Protection On

Provides zero-day protection against unknown threats

Definitions: Thursday, March 05, 2009 r18

Network Threat Protection Off

Protects against network threats

Definitions: Wednesday, February 25, 2009 r2

If this still does not solve the problem, contact AirMagnet Support for assistance.

Getting Started

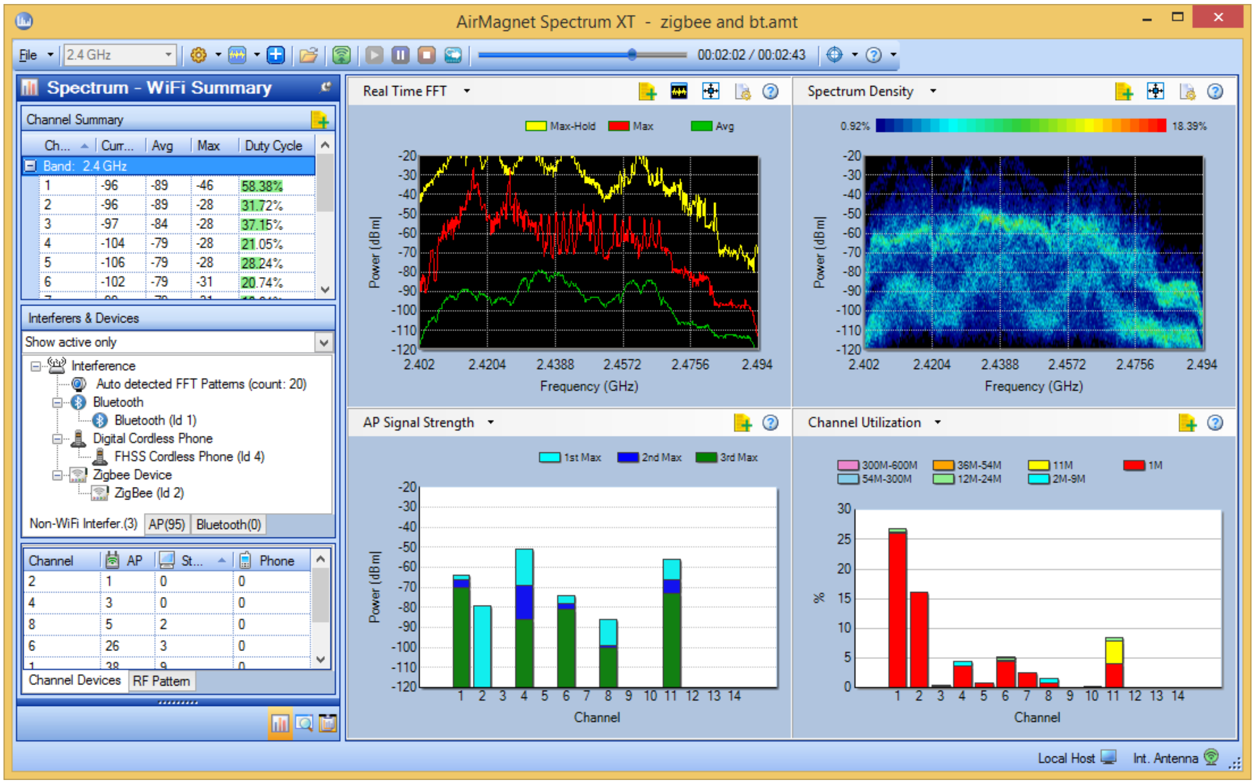
Major Screen Options

AirMagnet Spectrum XT has three major screen options, represented by three buttons in the lower-left part of the application's user interface:

- **Spectrum-WiFi Summary** - presents detailed RF spectrum information about all Wi-Fi and non-Wi-Fi devices detected in the network. For more information, click here.
- **Find Device** - contains tools for locating devices (Wi-Fi or non-W-iFi) that the application has detected. For more information, click here.
- **Reports** - opens the Reports page where you can access the default report or create custom reports of your own. For more information, click here.

By default, the Spectrum-WiFi Summary screen opens when the application is started. You can toggle between these two screen options by clicking the buttons.

About the Spectrum-WiFi Summary Screen



Ch...	Curr...	Avg	Max	Duty Cycle
Band: 2.4 GHz				
1	-96	-89	-46	58.38%
2	-96	-89	-28	31.72%
3	-97	-84	-28	37.15%
4	-104	-79	-28	21.05%
5	-106	-79	-28	28.24%
6	-102	-79	-31	20.74%

Channel	AP	St...	Phone
2	1	0	0
4	3	0	0
8	5	2	0
6	26	3	0
1	38	9	0

The image above shows the Spectrum-WiFi Summary screen which contains the following major components:

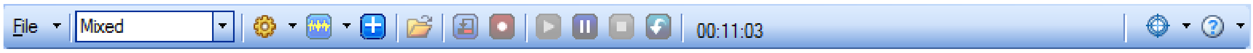
- Toolbar
- Channel Summary
- Device List
- Channel Usage
- Graphs Window
- AutoHide Button

Note: The data shown on the screen vary, depending on whether you have a spectrum adapter alone or both a spectrum adapter and an AirMagnet-supported wireless network adapter running at the same time on the PC when the application is started. The data content also vary with the radio band being selected. The image above shows the user interface when the application is started with both a spectrum adapter and wireless network adapter running using the 2.4 GHz radio band. In this case (that is, the combined mode), the screen shows both spectrum and Wi-Fi data. By design, an AirMagnet-supported spectrum adapter is required to install and operate AirMagnet Spectrum XT, whereas an supported wireless network adapter is required only if you want to view Wi-Fi data on the screen. You will not see live data in the AP List by SSID/Channel, Channel Usage, and all WiFi Graphs if you do not have a supported wireless network adapter running when operating AirMagnet Spectrum XT.

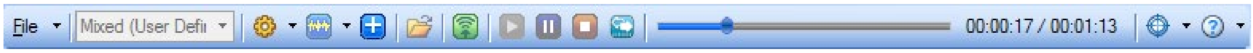
Toolbar

The illustrations below show Spectrum XT's toolbar in live capture and playback mode, respectively. They allow you easy access to the tools you need when working with the application in either mode.

Toolbar - Live Capture Mode



Toolbar Playback Mode



Most of these tools are buttons or icons which come with a tip screen that pops up when you place the cursor over a button. The tip screen shows the name of the tool you are focusing on.

As shown in the image above, the toolbar contains the following tools or menu options:

Menu/Tool Options	Description
File	Contains the following option: ▪ **Open Captured File...** - Opens a AirMagnet Spectrum XT capture (*.amt*) file and starts the playback mode.

	▪ **Save Capture As…** - Saves to a file the data being played or having been played. ▪ **Start/Resume** - Starts or resumes live capture after it has been stopped or paused. ▪ **Pause** - Pauses live data capture. ▪ **Stop** - Stops file playback or data recording. ▪ **Instant Playbac**k - Instantly starts playing back data captured in the last two minutes. ▪ **Record** - Records captured data to the system's hard drive. ▪ **Live Capture** - Switches to live capture mode from playback mode. ▪ **List of Recent Files** - Shows all recently opened capture files. ▪ **Exit** - Ends the operation of the application. Click here for more information.
Band	Contains the following options (which determine the 802.11 radio spectrum the application focuses on): ▪ **2.4 GHz** - Covers the radio frequency range from 2.402 GHz to 2.842 GHz, which is used by Channels 1 through 14. ▪ **5.0 GHz Lower** - Covers the radio frequency range from 5.17 GHz to 5.33 GHz, which is used by Channels 44, 48, 52, 56, 60, and 64. ▪ **5.0 GHz Middle** - Covers the radio frequency range form 5.49 GHz to 5.71 GHz, which is used by Channels 108, 112, 116, 120,124, 128, 132, 136, and 140. ▪ **5.0 GHz** Upper -Covers the radio frequency range from 5.735GHz to 5.835 GHz, which is used by Channels 157, 161, and 165. ▪ **4.9 GHz** - Covers bands used by many public safety organizations, from 4.91 to 4.99 GHz. ▪ **Mixed** - Covers all aforementioned radio frequencies (other than 4.9 GHz) and channels. **Note**: The screen automatically refreshes when you switch from one band to another, emptying out old data before loading new data. Click here for more information.
Settings	Opens the Settings list menu which contains the following options: ▪ **Configure** - Opens the Configure dialog box which has three tabs: ▪ General -Lets you configure certain Wi-Fi and spectrum parameters in the application ▪ Driver -Lets you choose a Wi-Fi driver of your choice if you have more than one installed on the PC. ▪ **SNMP Settings** - Opens SNMP settings configuration dialog ▪ **Custom Device Classification Manager** - Enables you to create custom signatures of devices so they can be detected

	automatically. ▪ **Show Auto Detected Pattern**s - Displays persistent patterns and enables you to create custom pattern signatures.
X-Axis Label Type	This button allows you to modify the labels used on the X-axis for the graph displays. You can specify viewing by band or by channel as desired. See Modifying Display Options for more details.
Add View	Click the drop-down menu arrow next to the + button to provide the following options: • Add a new graph to a report. You can enable up to 9 graphs. Right-click a view to display the close view option. • Select to add all current views to the report.
Open Capture File	This button enables you to browse and load any previously saved capture recordings (*.amt*) and starts the playback mode when the file is loaded.
Record/playback controls	The following buttons are for recording and playing back data capture.
Switch to Instant Playback	Starts playing back data captured in the last two minutes. Once the instant playback is started, the button changes to **Save Capture.** Refer below.
Save Capture	Save to a file the data being played or having been played. **Note:** This button/tool is available only when the application is in Instant Playback mode.
Switch to Live Capture	Stops file or data playback and switch back to live capture mode. **Note**: This option becomes available only when the application is in Instant Playback mode or you are playing back a capture (*.amt*) file.
Start Recording	Enables the application to start recording captured data to the system's hard drive.

Stop Recording and Save Capture

Stops recording data to the hard drive and prompts you to save the captured data to a (*.amt*) file.

Note: All data that have been recorded to the hard drive will be discarded unless you save them to a (*.amt*) file.

Resume/Play

In live capture mode, this button is named **Resume** which allows you to resume live capture after it is paused. In playback mode, it is named **Play** which allows you to play back the data or file after the playback is stopped.

Pause

Pauses live data capture shown on the user interface.

Note: Even though live data capture appears suspended on the user interface after you have clicked this button, the application is still capturing live data. Clicking the **Resume/Play** button again (after live capture is paused) will resume live data capture.

Stop

Stops live capture.

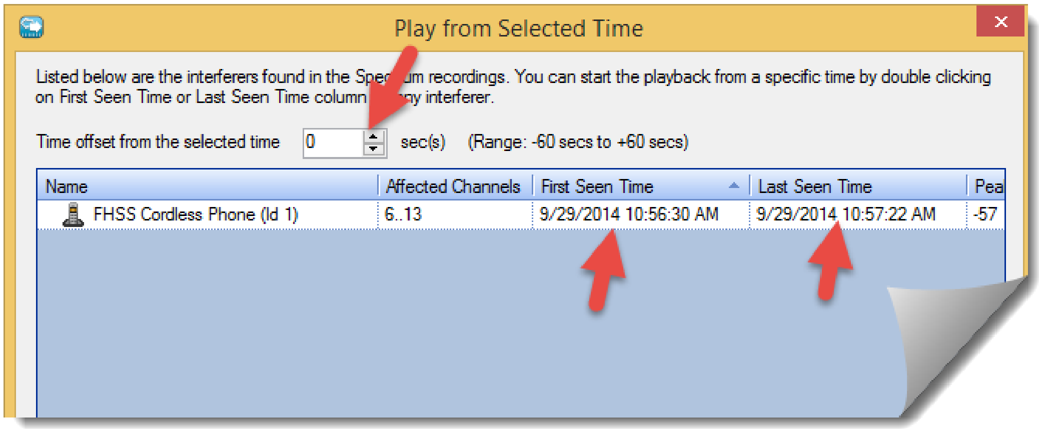
Reset Data

Resets all data in the application.

Note: The screen refreshes every time you click this button. Click here for more information.

Play from Selected Time

Opens the *Play from Selected Time dialog* where you can play back recorded data of a device from a selected point in time:



Play from Selected Time

Listed below are the interferers found in the Spectrum recordings. You can start the playback from a specific time by double clicking on First Seen Time or Last Seen Time column for any interferer.

Time offset from the selected time 0 sec(s) (Range: -60 secs to +60 secs)

Name	Affected Channels	First Seen Time	Last Seen Time	Pea
FHSS Cordless Phone (Id 1)	6..13	9/29/2014 10:56:30 AM	9/29/2014 10:57:22 AM	-57

- Double-click the First Seen time to start play back from the time when the device was first detected.
- Double-click the Last Seen time to start play back from the

	time when the device was last detected. ▪ To start the playback 30 seconds after the First Seen Time, select 30 in the Time Offset from the Selected Time box and then double-click the First See Time. ▪ To start the playback 30 seconds before the First Seen Time, enter a minus sign (-) and select 30 in the Time Offset from the Selected Time box, and then double-click the First Seen Time. ▪ To start the playback 30 seconds after the Last Seen Time, select 30 in the Time Offset from the Selected Time box, and then double-click the Last See Time. ▪ To start the playback 30 seconds before the Last Seen Time, enter a minus sign (-) and select 30 in the Time Offset from the Selected Time box and then double-click First See Time.
Timer	Shows the progress of a file playback or instant data playback.
Easy View	Opens the Easy View list menu which contains the options for organizing data displayed on the screen. Click here for more information.
Help	Opens the Help list menu which contains the following tabs: ▪ **Contents** - Opens the application's online Help. ▪ **Search** - opens the search page of the online Help, where you do a text search. ▪ **About** - Opens the About AirMagnet Spectrum XT dialog box which contains the following three tabs: ▪ AirMagnet Spectrum XT - Displays basic information about the software, including its build and version number. ▪ Licenses - Shows your product's license information, including its serial number and serial key and the MAC address to which the license is tied. ▪ Debug - Contains an option for the application to automatically capture a sampling data need for troubleshooting. ▪ **Tutorial Videos** - Opens the Spectrum XT video tutorials.

Channel Scan Indicator

The channel scan indicator, which appears in the lower left-hand corner of the screen, is available only when AirMagnet Spectrum XT is operated with a supported external wireless network adapter simultaneously with the spectrum adapter. It shows in real time the 802.11 channels that the wireless network adapter has been scanning.

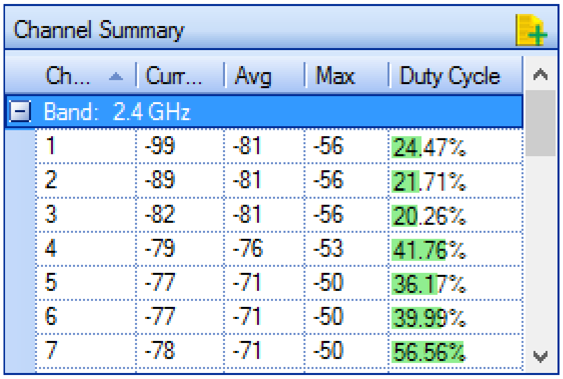
The channels that are scanned vary, depending on the 802.11 radio band in use. Refer to the Channel Summary.

Scanning Channel: 10

Note: If no external wireless network adapter is used, AirMagnet Spectrum XT will still gather limited amounts of Wi-Fi data from Windows Wireless Configurations. This status will be indicated by a message in the bottom-left corner of the screen: "Dynamic Wi-Fi data collected from Windows Wireless Configuration".

Channel Summary

In the upper-left corner of the screen is the Channel Summary which highlights key spectrum statistics the application has detected on all available channels covered by the selected 802.11 radio band. Refer to the illustration below.



Channel Summary

Ch...	Curr...	Avg	Max	Duty Cycle
Band: 2.4 GHz				
1	-99	-81	-56	24.47%
2	-89	-81	-56	21.71%
3	-82	-81	-56	20.26%
4	-79	-76	-53	41.76%
5	-77	-71	-50	36.17%
6	-77	-71	-50	39.99%
7	-78	-71	-50	56.56%

As shown in the image above, the columns, from left to right, shows the following data:

Column	Description
Channel	Shows all available channels for the selected radio band.
Current	Shows the average of current FFT readings in dBm on each channel.
Avg	Shows the average historical FFT readings in dBm on each channel.
Max	Shows the maximum (Max-Hold) FFT reading in dBm on each channel.
Duty Cycle	Shows the percentage of time the RF energy (both 802.11 and non-802.11) is present on the channel.

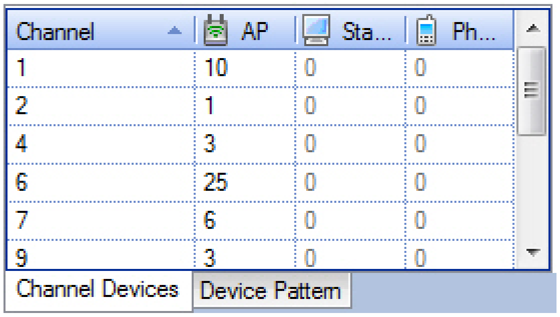
Note: When you select a channel from the Channel Summary, that channel's portion of the wireless spectrum is highlighted in the charts displayed to the right. This makes it easy to identify exactly where a device is appearing in charts like the Spread Spectrogram, among others.

Channel Devices

In the lower-left corner of the screen is Channel Devices, which lists the number of APs, stations, and/or VoFi phones that the application has detected on each channel in the selected 802.11 radio band.

An AirMagnet-supported Wi-Fi adapter is required in order for the application to capture and display such data.

Note: Channels with no data will not be listed in the Channel Devices table.



Channel	AP	Sta...	Ph...
1	10	0	0
2	1	0	0
4	3	0	0
6	25	0	0
7	6	0	0
9	3	0	0

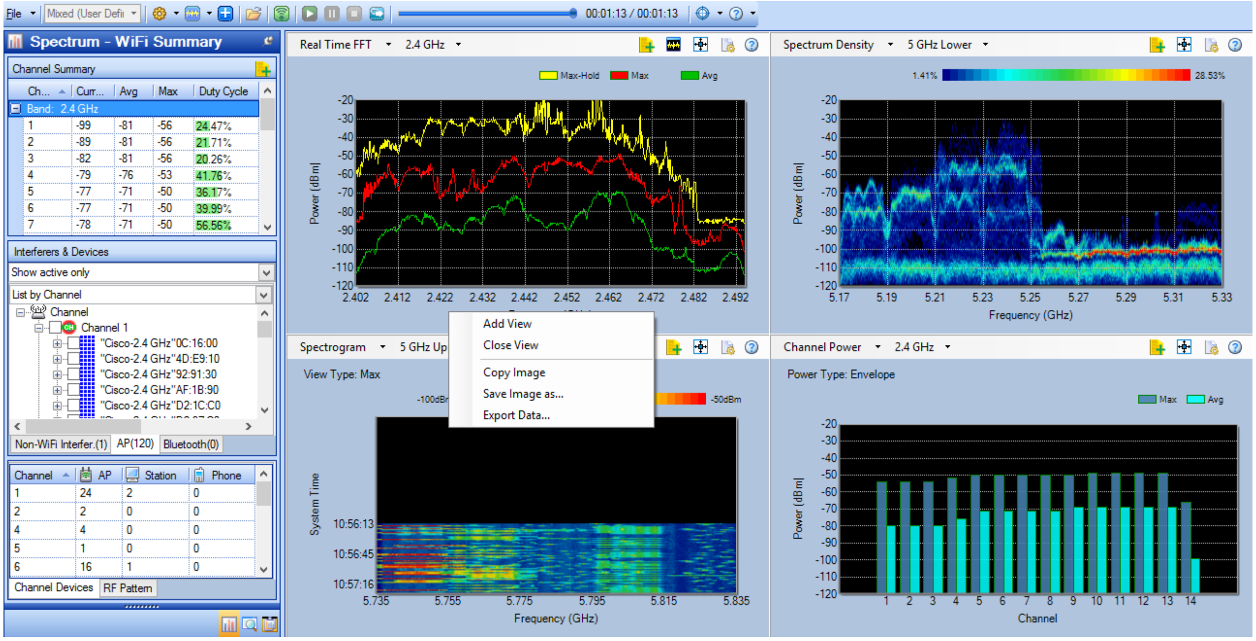
The Channel Devices pane only displays channels on which Wi-Fi devices are detected. If you notice certain channels missing from this section, it means that no Wi-Fi devices have been detected on those channels. Also, the channels shown here vary depending on the option selected from the Band menu in the toolbar. You can click the Device Pattern tab to view a sample image of the detected spectrum pattern of devices detected. Refer to Device Pattern.

Graph Options

Add View

Click the drop-down arrow next to the **+** button on the toolbar give you one of the following options:

- Add an additional graph to the graphs view. This option enables up to 9 graphs to be opened. Right-click a graph to display the close view option.
- Add all current views to a report.



Channel Summary

Ch...	Curr...	Avg	Max	Duty Cycle
Band: 2.4 GHz				
1	-99	-81	-56	24.47%
2	-89	-81	-56	21.71%
3	-82	-81	-56	20.26%
4	-79	-76	-53	41.76%
5	-77	-71	-50	36.17%
6	-77	-71	-50	39.99%
7	-78	-71	-50	56.56%

Interferers & Devices

Show active only

List by Channel

- Channel
  - Channel 1
    - "Cisco-2.4 GHz"0C:16:00
    - "Cisco-2.4 GHz"4D:E9:10
    - "Cisco-2.4 GHz"92:91:30
    - "Cisco-2.4 GHz"AF:1B:90
    - "Cisco-2.4 GHz"D2:1C:C0

Non-WiFi Interfer.(1) | AP(120) | Bluetooth(0)

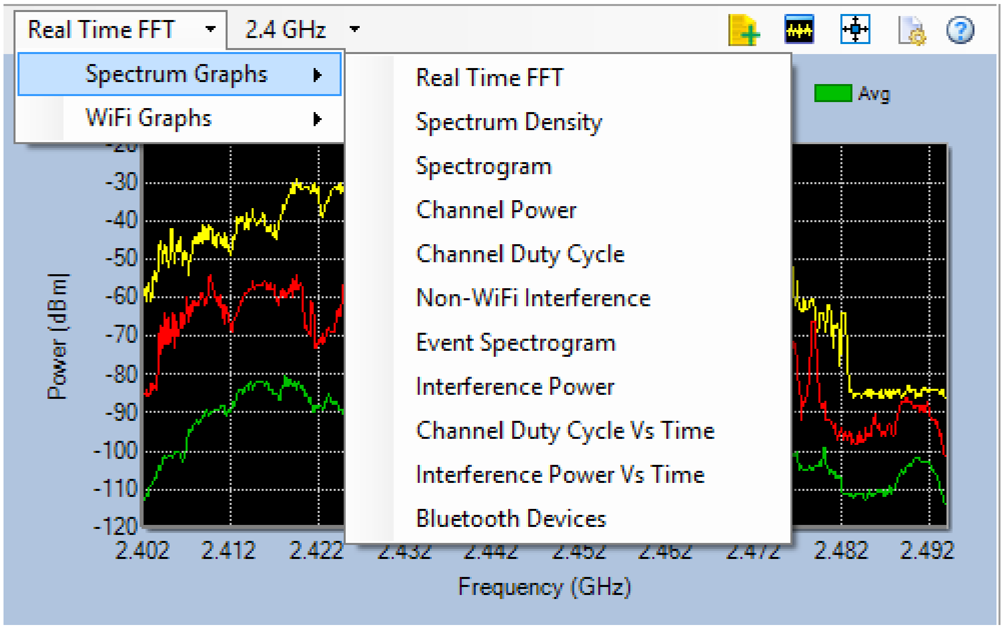
Channel	AP	Station	Phone
1	24	2	0
2	2	0	0
4	4	0	0
5	1	0	0
6	16	1	0

Channel Devices | RF Pattern

In the upper-left corner of each graph you will find the name of the graph. Clicking the name of a graph will open a drop-down list menu which contains all the spectrum and Wi-Fi graph options that the application can generate. You can open eithe rone or all of the list menu simply by clicking the graph name, as shown in the illustrations below. If you need help understanding data contained in a graph, click the ? **(Help)** button In the upper-right corner of the graph. The relevant online Help page will open on the screen.

Spectrum Graphs

This group contains multiple spectrum graph options, as shown below in expanded drop-down list menu.

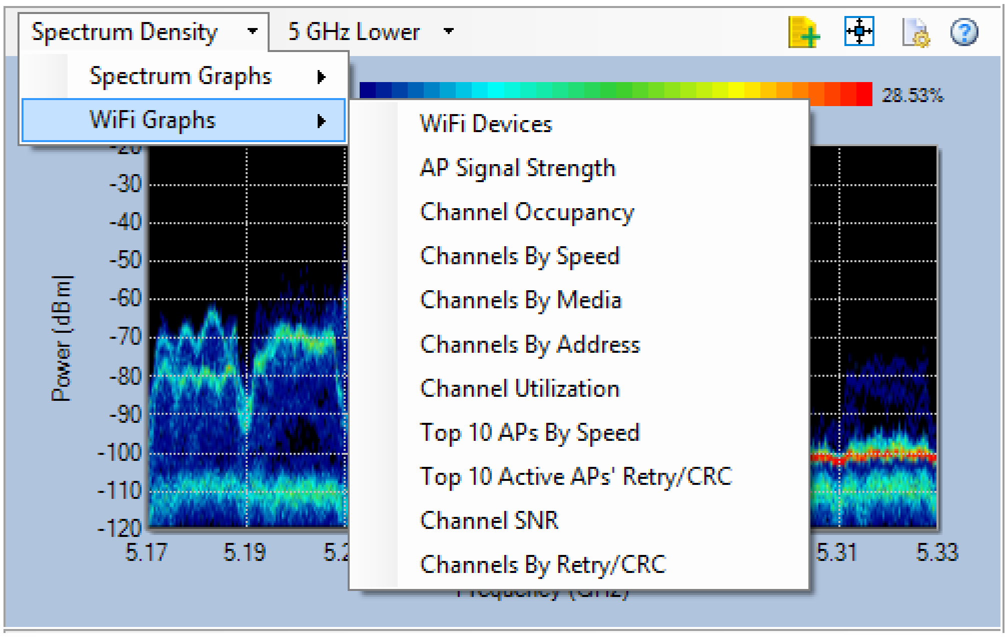


For more information about these Spectrum Graphs, click Spectrum Graphs.

Note: There is a Configuration button in the upper-right corner of every graph in this group. It allows you to set or change certain parameters used in the graphs. Refer to Spectrum Graphs for more information.

WiFi Graphs

This group contains several WiFi graph options, as shown in the expanded drop-down list menu below.

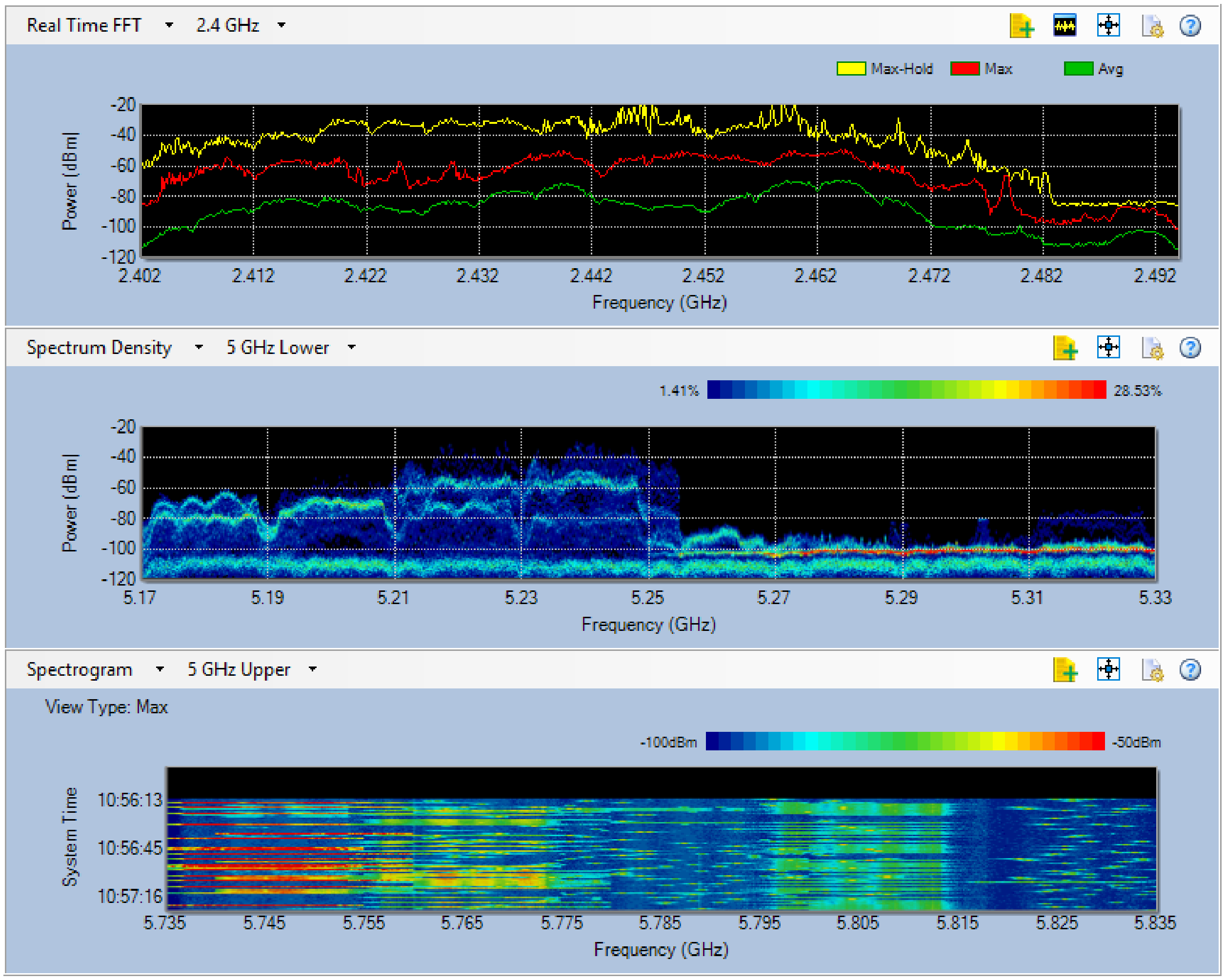


For more information about the WiFi Graphs, click WiFi Graphs.

Note: If no external wireless network adapter is used, Spectrum XT is still able to gather limited amount of Wi-Fi data using Windows Wireless Configuration. This will be indicated by the message in the bottom-left corner of the screen: "Dynamic Wi-Fi data collected from Windows Wireless Configuration".

Graphs Window

The data graph window allows you to view and analyzer all spectrum data and Wi-Fi data (if you have a supported Wi-Fi adapter running at the same time) that the application has captured or is capturing in your network. The data are presented in the form of charts or graphs which are grouped into Spectrum Graphs and WiFi Graphs.



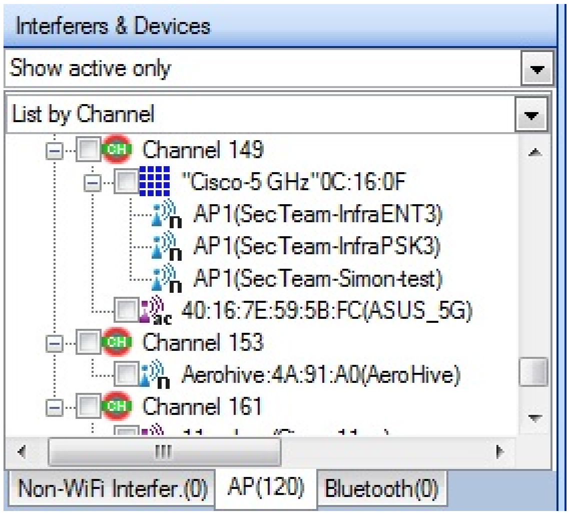
Data shown in this part of the screen vary, depending on whether a spectrum adapter is used alone or alongside with a Wi-Fi adapter as well as the 802.11 radio band being selected. The figure above shows the default screen when both a spectrum adapter and a Wi-Fi adapter are being used to scan the 2.4 GHz band. The content of each chart or graph can be changed using the drop-down list menu in the upper-left corner of each chart or graph. Options in the list menus are the same. Click here for more information.

Note: All graph options in the WiFi Graphs category will be blank if you do not have a supported Wi-Fi adapter running.

Interferers and Devices List

Below the Channel Summary is the Interferers and Devices List. It shows all the Devices (Wi-Fi and non-Wi-Fi) that the application has detected in the network. The Device List contains two tabs that categorize devices based on their wireless characteristics; standard 802.11 Wi-Fi devices are displayed on their own tab, and non-802.11 devices on a second one.

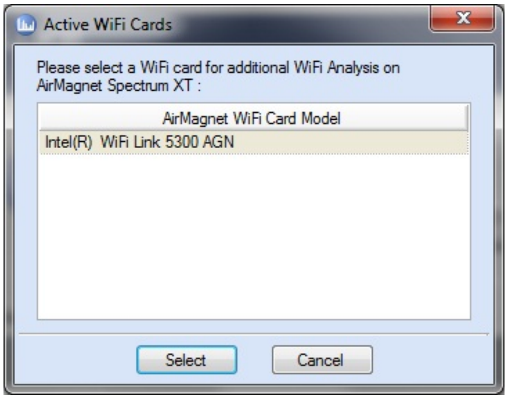
When viewing the 802.11 devices portion,use the drop-down menu across the top of the pane to change the manner in which the devices are displayed, either by SSID or by Channel. Refer to the illustration below.



You can project signal strengths of any APs over the Spectrum Density graph by selecting them (checking the corresponding check boxes in the AP List). Signal strengths of the corresponding APs will appear in the graph in the form of color-coded curves. Click **here** for more in formation.

Enabling Wi-Fi Capability

When launching AirMagnet Spectrum XT, you have the choice of allowing or disallowing the laptop's Wi-Fi adapter from being used by AirMagnet Spectrum XT. Allowing the adapter to be used enables the capture of Wi-Fi data, but makes the adapter unavailable for browsing the Web.



Please select a WiFi card for additional WiFi Analysis on AirMagnet Spectrum XT :

AirMagnet WiFi Card Model
Intel(R) WiFi Link 5300 AGN

To allow an adapter to be used by AirMagnet Spectrum XT, select the adapter and click **Select**. To disallow the adapter from being used, click **Cancel**.

AutoHide Button

In the upper-right corner of the Spectrum-WiFi Summary section is a 📌 **(AutoHide)** button. It is used to hide the Spectrum-WiFi Summary so that you can have more screen space to display the graphs.

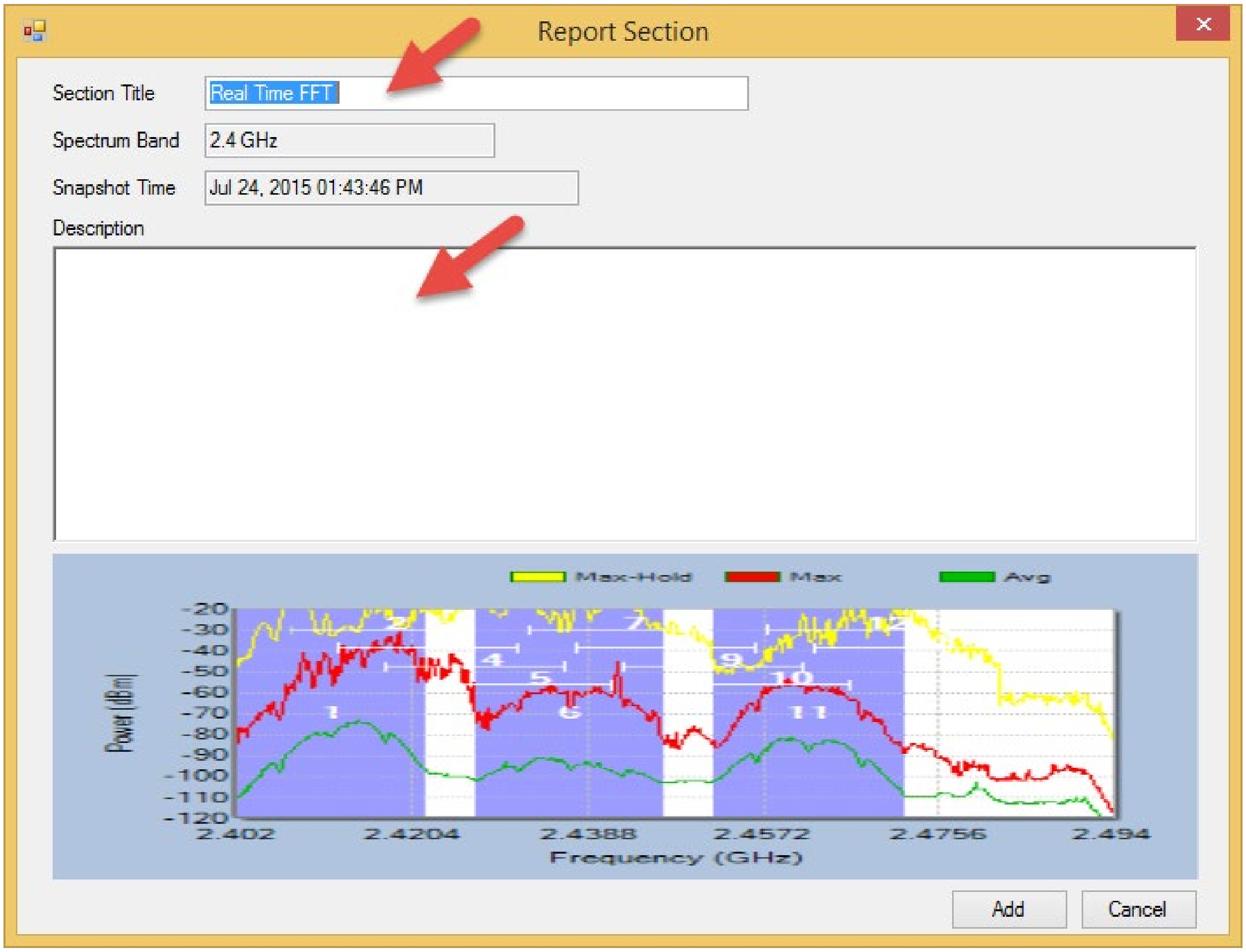
When you click this button, the Spectrum-WiFi Summary will fold up and snap to the left edge of the screen, leaving only its title in the form of a tab in the upper-left corner of the screen. You can unfold the Spectrum-WiFi Summary by clicking the tab. You can also click the pushpin to restore it to its default position.

Capturing Data as Report Sections

On the Spectrum - WiFi Summary page, you will see + (the **Add to Report** button) in the upper-right hand corner of every spectrum and Wi-Fi graph as well as the Channel Summary panel. It allows you to capture the data shown in graphs (panel) with a single click and add it to the Reports page as a report sections, which can be used to create custom reports.

To capture the data in a graph as a report section:

1. Open the graph.
2. Wait until the graph is populated with enough data.
3. Click +. The Report Section dialog opens. Refer to the illustration below.



Report Section

Section Title: Real Time FFT

Spectrum Band: 2.4 GHz

Snapshot Time: Jul 24, 2015 01:43:46 PM

Description

4. In the Section Title field, type a unique section title over the default section title.
5. In the Description field, enter a brief description of the report section.
6. Click **Add.**

Note: Each time you click (**Add to Report**), the application automatically generates a report section with the name of the graph as its default title. We recommend that you rename each report section with a unique name and enter a specific description about it before clicking the **Add** button. This will help you distinguish the report sections and know which report sections to choose when creating a custom report.

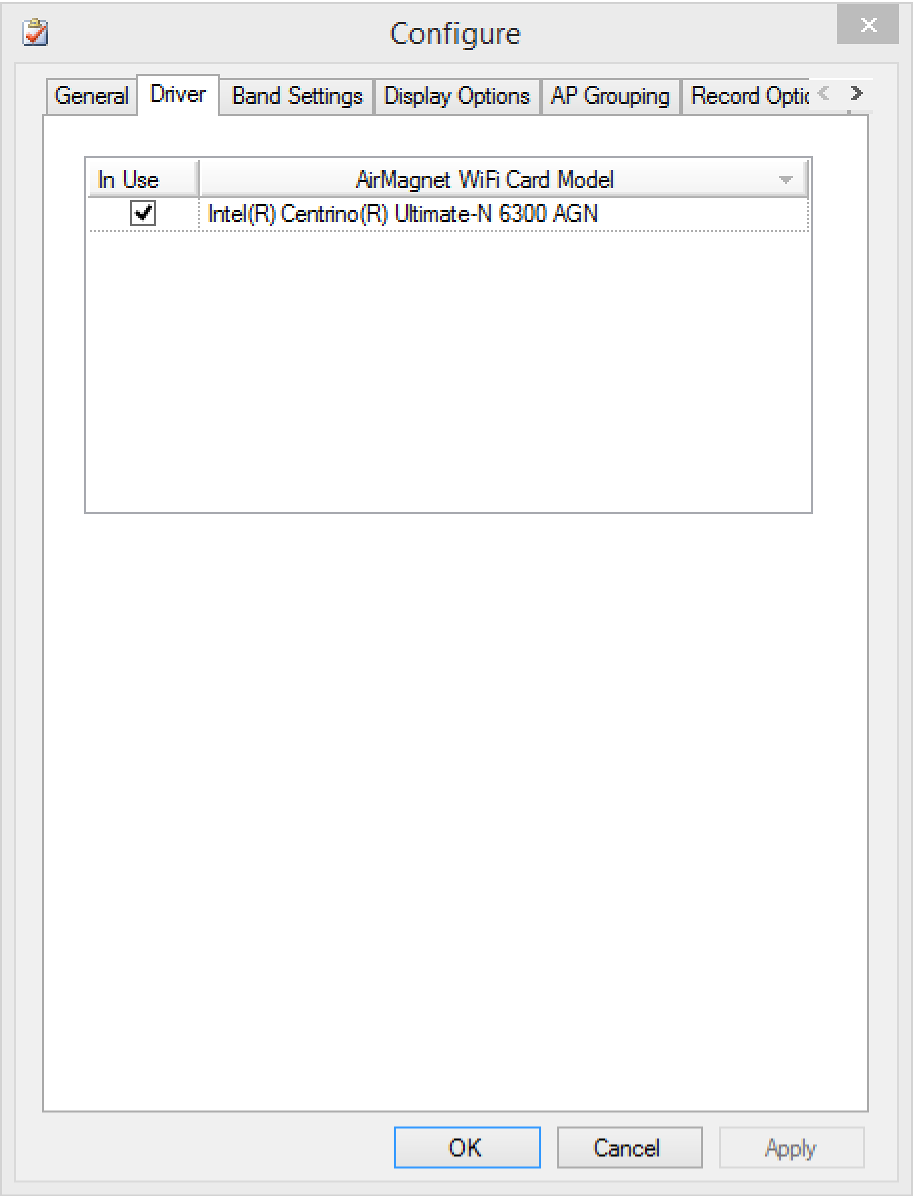
Refer to Creating a Custom Report.

Configuration and Management

Viewing the Current Device Driver

AirMagnet Spectrum XT is designed to work with a number of Wi-Fi adapters. You must install and enable a driver compatible to an adapter in order to operate the application with that adapter.

You can see the wireless network adapter driver Spectrum XT is using by clicking the **Driver** tab in the Configure dialog, as illustrated below.



In Use	AirMagnet WiFi Card Model
☑	Intel(R) Centrino(R) Ultimate-N 6300 AGN

Note: To learn more about supported adapters, refer to Supported Wireless Network Adapters.

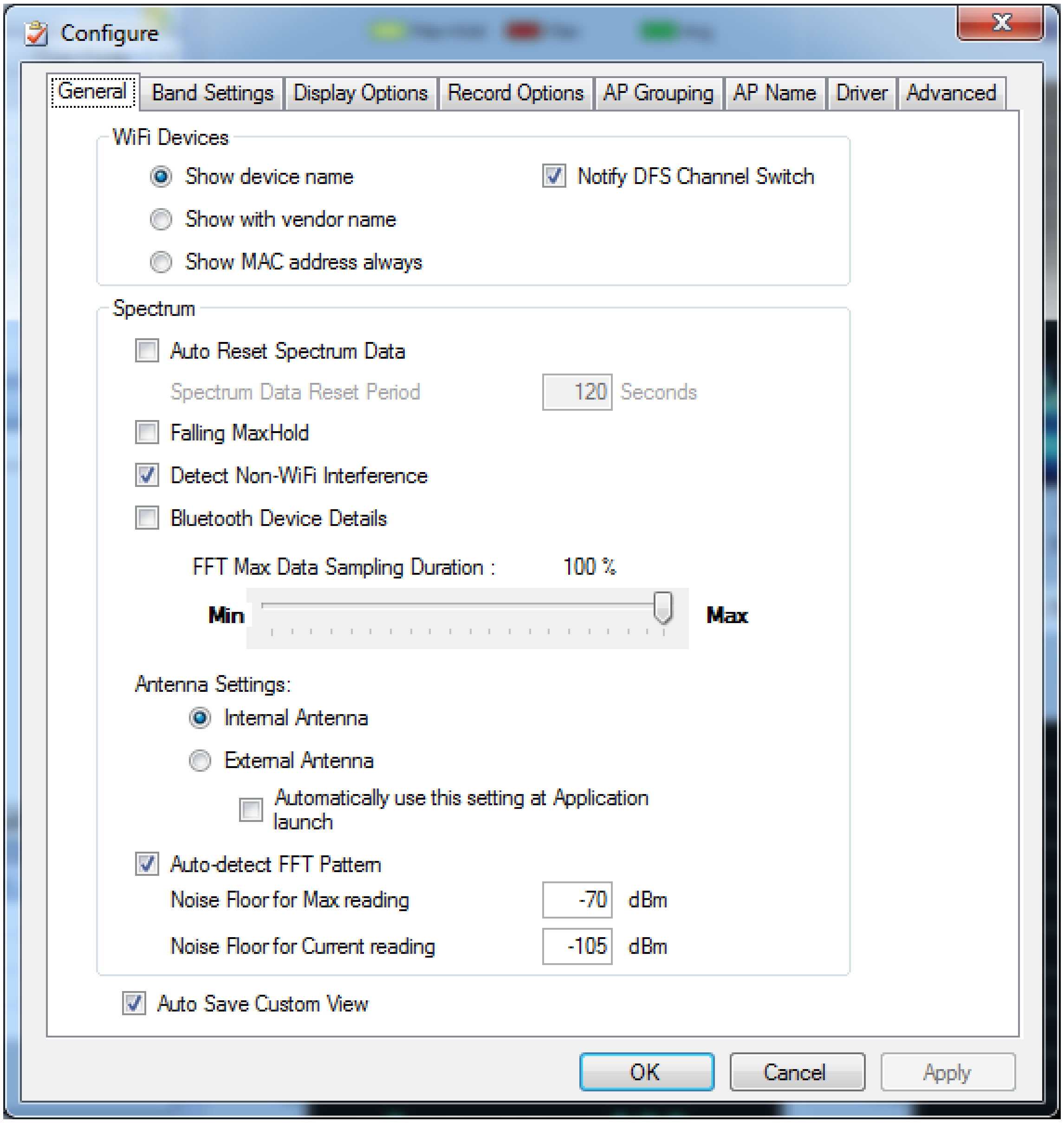
Configuring General Settings

AirMagnet Spectrum XT allows you to set or change general parameters displayed on the screen that relate to the Wi-Fi devices and/or spectrum data captured on your network.

To set or change the display of Wi-Fi or spectrum data:

1. From the Toolbar, click **Settings>Configure.**

2. Click the **General** tab, if not selected.



WiFi Devices

● Show device name

○ Show with vendor name

○ Show MAC address always

☑ Notify DFS Channel Switch

Spectrum

☐ Auto Reset Spectrum Data

Spectrum Data Reset Period 120 Seconds

☐ Falling MaxHold

☑ Detect Non-WiFi Interference

☐ Bluetooth Device Details

FFT Max Data Sampling Duration : 100 %

Antenna Settings:

● Internal Antenna

○ External Antenna

☐ Automatically use this setting at Application launch

☑ Auto-detect FFT Pattern

Noise Floor for Max reading -70 dBm

Noise Floor for Current reading -105 dBm

☑ Auto Save Custom View

3. Make the selection and/or entry as described in the following table.

4. Click **Apply** and then **OK.**

Parameter	Description
WiFi Devices	These parameters apply to Wi-Fi devices only.
• Show device name	If selected, the names of Wi-Fi devices will show on the screen wherever applicable.
• Show with vendor name	If selected, vendor names will show as part of devices names on the screen.
• Show MAC address always	If selected, MAC addresses will always appear as part of device identification.
• Notify DFS Channel Switch	If selected, you will receive a notification whenever an AP operating on a Dynamic Frequency Selection (DFS) Channel switches to a different channel. A Channel Switch can occur when there is any radar signal. This feature is activated by default.
Spectrum	These parameter apply to spectrum data only.
▪ Auto Reset Spectrum Data	If checked, the application will automatically reset spectrum data at the specified interval. (Refer below.)
▪ Spectrum Data Reset Period	If **Auto Reset Spectrum Data** is checked (above), you need to specify the time period for the application to reset spectrum data.
▪ Falling MaxHold	Factors such as noise in the spectrum or DC leak may cause sudden one-time spurts in the FFT plot. These spurts or "false" MaxHold, if left as, will remain on the spectrum plot as MaxHold. This option, if select, enables the application to automatically discount the "false" MaxHold points by letting the "false" MaxHold gradually fall back, thus eliminating false MaxHold.
▪ Detect Non-WiFi Interference	When Device Detection is disabled, Spectrum will not record devices detected during scanning. This can reduce the number of entries that appear in the capture file, particularly when saved in .csv format.

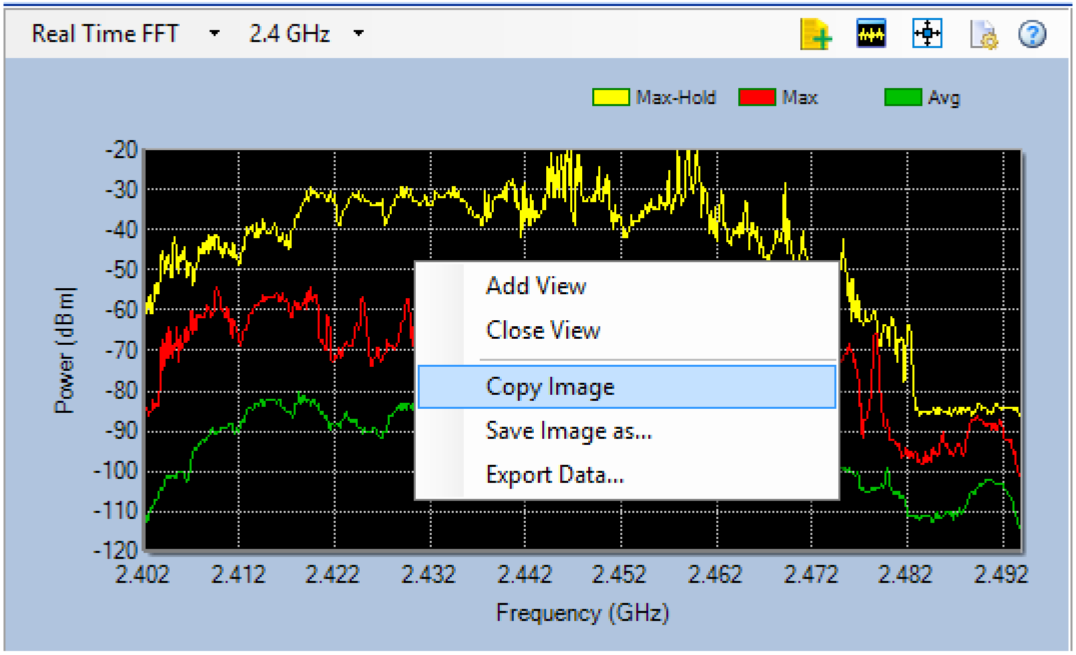
▪ Bluetooth Device Details	This option is used with a Bluetooth adapter to detect different Bluetooth devices in the area.
▪ FFT Max Data Sampling Duration	The FFT Data Sampling feature can effectively reduce noise in order to produce a better distinguishable FFT pattern. For example, adjusting the bar to 50% will reduce sampling by half, thereby smoothing out spikes in the FFT graph that may be caused by interference noise.
▪ Antenna Settings	This option allows you to specify usage of the internal or external antennas with the AirMagnet Spectrum adapter. Check the *Automatically use this setting at application launch* option to store this setting for every time the application is loaded.
▪ Auto Detect FFT Pattern Settings	The Auto Detect feature processes both the "current" and the "max" FFT data. As such these two parameters may be tuned in order to affect the algorithm.
Auto Save Custom View	If checked, the application will automatically save the customized view options that the user has created in Easy View.

Copying and Pasting Screen Images

AirMagnet Spectrum XT allows you to easily copy any chart or graph in the graph window as still images and paste them to other applications such as Paint, MS Word, and so on. This makes it very convenient for saving and sharing data captured on the network.

To copy a graph or chart on the screen:

1. Right-click a chart or graph of interest.
2. From the pop-up menu, select **Copy Image.** Refer to the illustration below.



3. Open an application that supports copy and paste, such as MS Word.
4. Use the Paste command to paste the image to the document.
5. Save the document for archiving and/or sharing.

Instantly Playing Back Captured Data

AirMagnet XT allows you to replay captured data that has recently been displayed on the screen so that you can revisit the data for a closer look.

To replay captured data that has recently passed through the screen:

1. Click **(Switch to Instant Playback)** on the toolbar. The application will switch to playback mode instantly.

   Note: The application can instantly play back about 2 minutes of data at most. The figure above shows that the application has replayed 29 seconds of data captured for the last 2 minutes. The replay stops when the slider reaches the end. You can use the **Play**, **Pause**, or **Stop** buttons to play the data back and forth. You can also set the starting point by dragging the slider to anywhere you want.

2. To save the data that was replayed, click **(Save).**

3. To switch back to live capture mode, click **(Switch to Live Capture).**

During playlback, you can also view various portions of the spectrogram. For information on doing this, refer to Spectrogram Navigation.

Exiting

For security reasons, you need to close AirMagnet Spectrum XT once you are done with it and should never leave it running unattended.

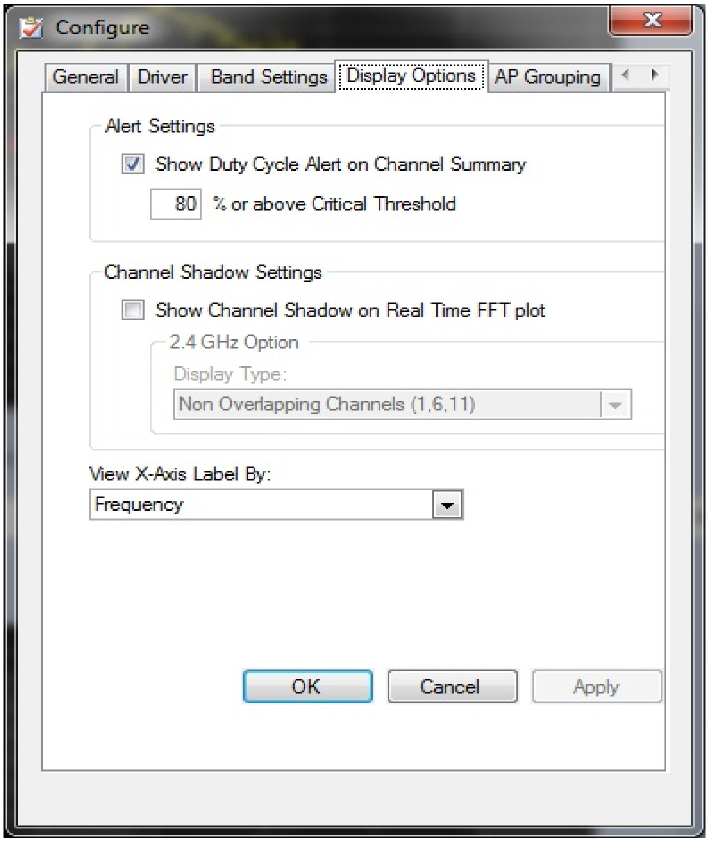
To exit the application:

From the application's user interface, click **File>Exit**.

Note: You can also close the application by clicking the **x** button in the upper-right corner of the screen.

Modifying Display Options

The Display Options tab allows you to alter various aspects of the application's overall appearance.



Alert Settings

☑ Show Duty Cycle Alert on Channel Summary

80 % or above Critical Threshold

Channel Shadow Settings

□ Show Channel Shadow on Real Time FFT plot

2.4 GHz Option

Display Type:

Non Overlapping Channels (1,6,11)

View X-Axis Label By:

Frequency

Refer to the table below for information regarding each of the options provided.

Option	Description

Alert Settings

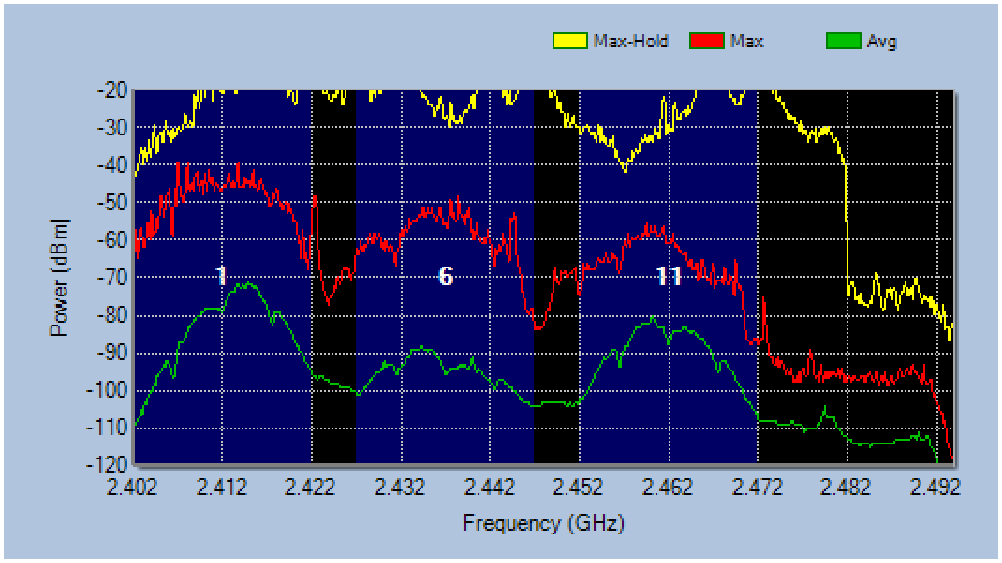
When enabled, this option will highlight the Duty Cycle column in the Channel Summary field when it exceeds the specified threshold. Channels on which the Duty Cycle meets this criteria will be highlighted in red (channels with normal levels are highlighted in green).

Channel Shadow Settings

This feature applies to the 2.4-GHz band only. It allows you to choose whether or not to plot the channel shadows on the Real Time FFT graph.

To use this feature, you must first enable it by checking the **Show Channel Shadow on Real FFT plot** check box. Then you need to click the down arrow to select either of the options from the list menu:

- Non Overlapping Channels (1, 6, 11) (Click *here* for a sample Real Time FFT graph with shadows on the three non-overlapping channels.)



- All Channels

View X-Axis Label By

This allows you to toggle between viewing charts by frequency range and channel number. Although the default setting is Frequency, many users find the Channel selection easier to use and analyze.

Opening a Capture Data File

Captured data are saved to a file using the *.amt* file extension. You can replay those saved capture data by opening the file containing the data.

To open a capture file:

1. Click **(Open Capture File).**
2. Locate the *.amt* file on your PC and click **Open**.

3. Use the buttons (**Start**, **Pause**, and **Stop**) to play the file back and forth, if you wish to.
4. To switch back to Live Capture mode, click **(Switch to Live Capture).**

You can also add notes to a playback recording and later review these notes. To do this, refer to Adding Notes to Captured Data.

Pausing and Resuming Live Capture

Pausing live capture allows you to suspend the dynamic display of live data on the screen; it does not stop the application from capturing live data at all. In other words, the application still keeps capturing live data and storing them in the memory even after you have clicked the **Pause Live Capture** button.

To suspend the display of live data capture on the screen:

From the toolbar, click ⏸ **(Pause).**

To resume the display of live data capture on the screen:

From the toolbar, click ▶ **(Resume).**

Recording Capture Data

Normally, the application automatically sends all data it has captured to the buffer. Due to the buffer size, the application discards old data as new data come in. However, if you want to retain data captured during a session, you can let the application send the data to the system's hard drive. This is the so-called "stream to file" feature.

To use this feature, you must set the Max Live Capture Streaming File Size (MB) which is 500 MB by default. You can set it to any value (up to 2 GB) as long as you have enough hard drive space to accommodate it. This can be done using *Configure>General>Max Live Capture Streaming File Size (MB)*.

To record capture data:

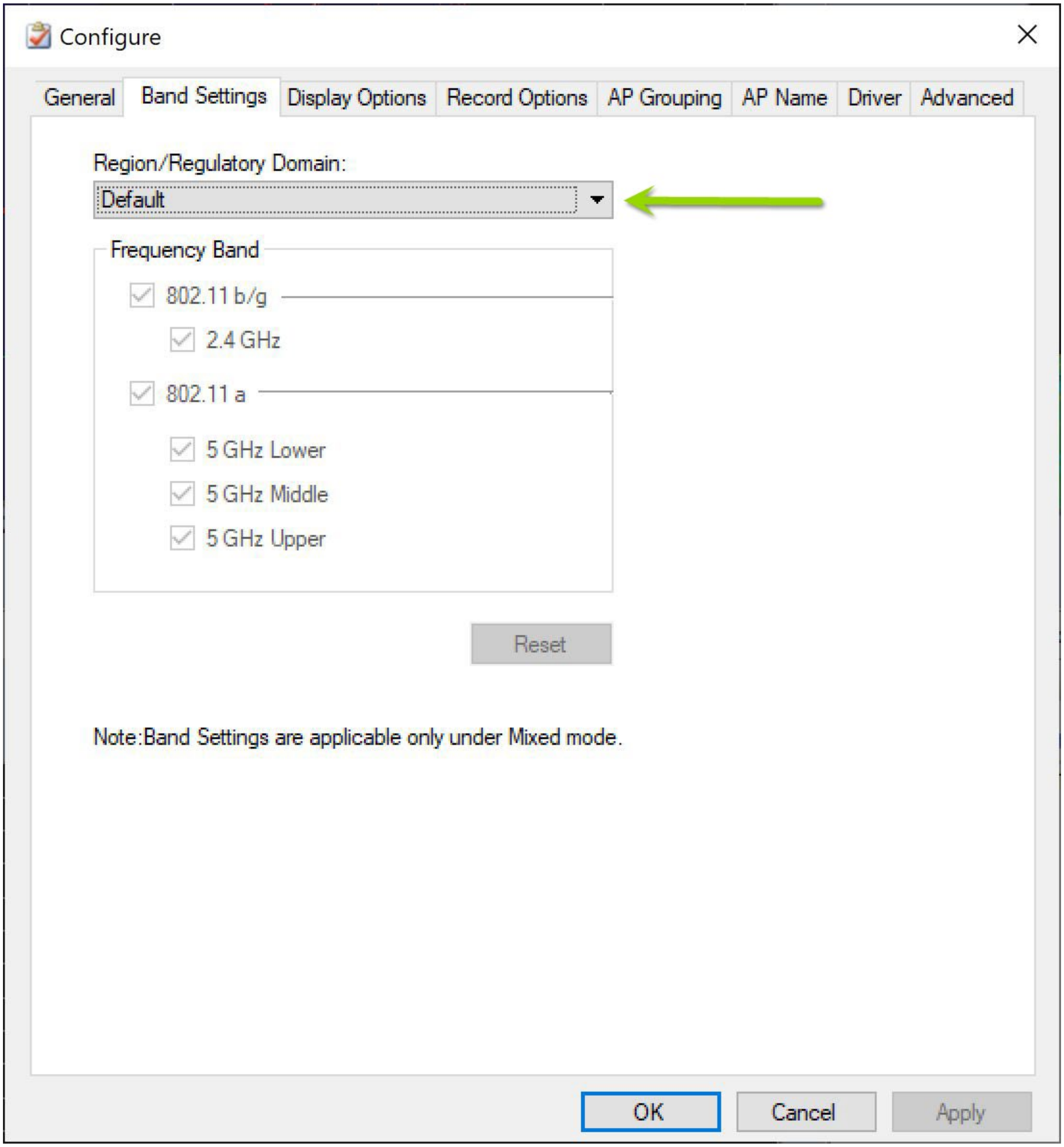
1. Click ● **(Start Recording)**.
2. When enough data has been collected, click ● **(Stop Recording and Save Capture).**
3. Save the file when prompted.

Note: All recorded data will be lost unless you save them to a file.

You can also add notes during a playback recording and later review these notes. To do this, refer to Adding Notes to Captured Data.

Region Specific Scanning Control

If you are in regions with specific wireless range restrictions, you can specify precisely which channels to be scanned in AirMagnet Spectrum XT by selecting the desired region from a drop-down menu provided in the application's configuration window. This streamlines the process of narrowing down the channels needed, based on the area in which the network is located to an easy one-click process.



Region/Regulatory Domain: Default

Frequency Band

☑ 802.11 b/g

☑ 2.4 GHz

☑ 802.11 a

☑ 5 GHz Lower

☑ 5 GHz Middle

☑ 5 GHz Upper

Note:Band Settings are applicable only under Mixed mode.

Remote Spectrum Analysis

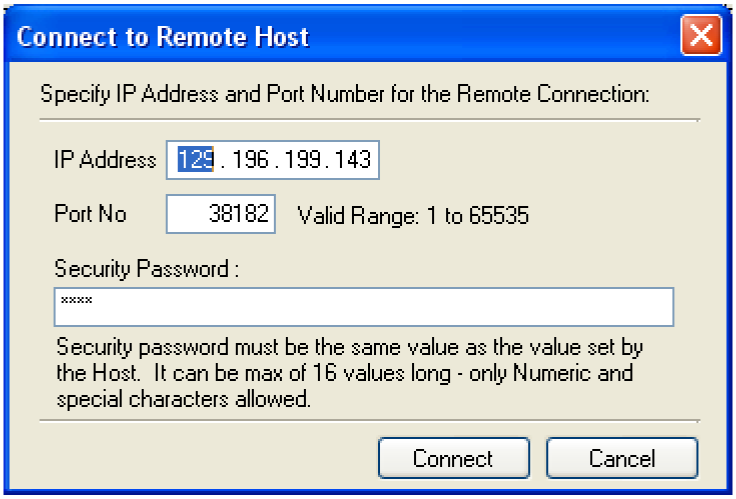
You can remotely log into the user interface and monitor ambient traffic patterns using a separate computer. In order to connect to the Spectrum XT remote interface, you must install AirMagnet Spectrum XT (including valid license) or a AirMagnet Spectrum XT Viewer-Only license (provided with the purchase of a valid AirMagnet Spectrum XT license) on the second computer.

Note: Connecting to a remote system is not supported in a Network Address Translation (NAT) environment.

To Connect to a Remote Host:

From the **File** menu, select **Remote XT Connection**> **Connect to Remote Host**.

Type the required remote connection information: Remote Host IP Address, Port Number and (Security Password) Authentication key. Click **Connect**. Refer to "Setting up Authentication Key on the Remote Host" below for information about the authentication key.



Connect to Remote Host

Specify IP Address and Port Number for the Remote Connection:

IP Address 129 . 196 . 199 . 143

Port No 38182 Valid Range: 1 to 65535

Security Password :

****

Security password must be the same value as the value set by the Host. It can be max of 16 values long - only Numeric and special characters allowed.

To Disconnect from Remote Host:

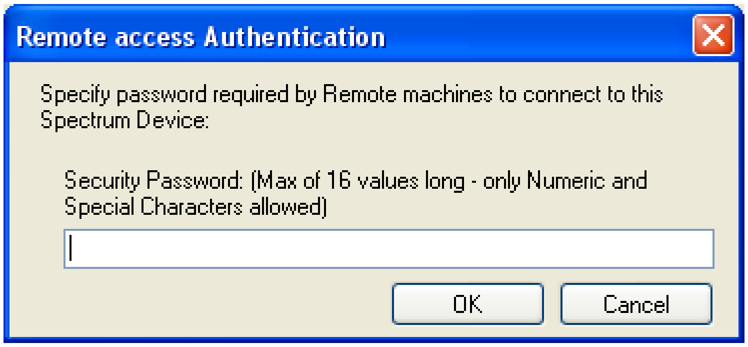
This connects the application from the remote Spectrum Analyzer mode. Live Capture will be stopped.

From the **File** menu, select **Remote XT Connection**> **Disconnect from Remote Host**.

Setting up Authentication Key on the Remote Host:

Before connecting to a remote computer, you should have received an authentication key from the remote user. The Remote user should set the authentication key with the Remote Access Authentication menu which opens a dialog where the user can set the authentication key.

From the **File** menu, select **Remote XT Connection**> **Remote Access Authentication**



Remote access Authentication

Specify password required by Remote machines to connect to this Spectrum Device:

Security Password: (Max of 16 values long - only Numeric and Special Characters allowed)

Remote Access Authentication Screen

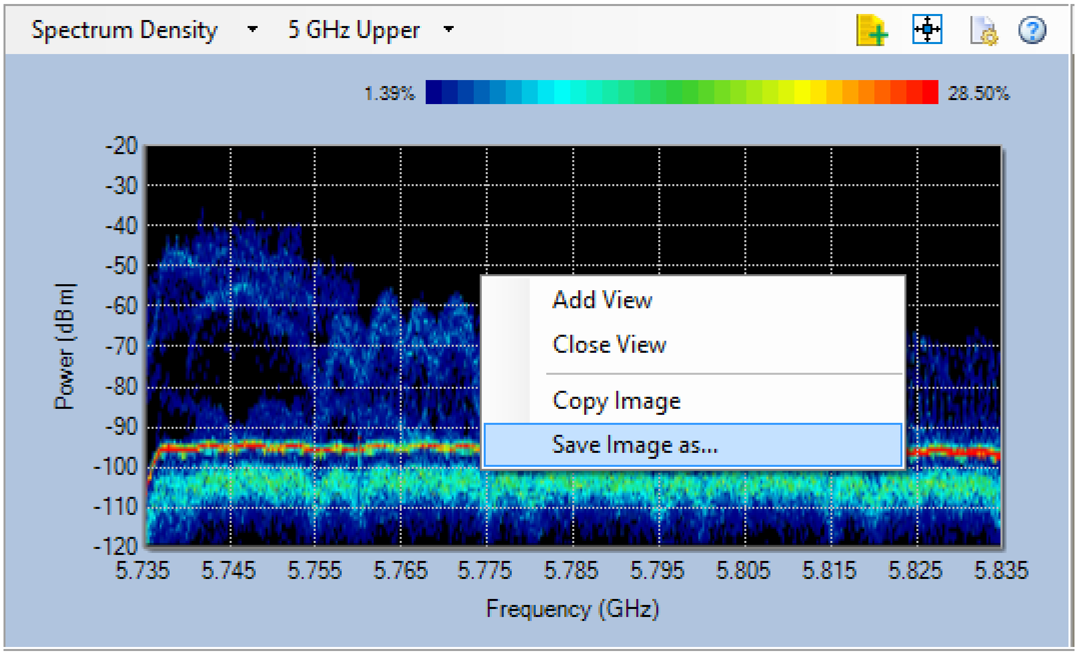
Saving Screen Data as Image Files

AirMagnet Spectrum XT allows you to save any chart or graph shown in the Graph Window as an image file in any of the following four image formats:

- .PNG
- .BMP
- .JPG
- .GIF

To save a chart or graph as an image file:

1. From the graph window, right-click the chart or graph.



2. From the pop-up menu, select **Save Image As....**
3. From the Save As dialog box, choose a location, name, and format for the file.
4. Click **Save.**

Selecting an 802.11 Radio Band

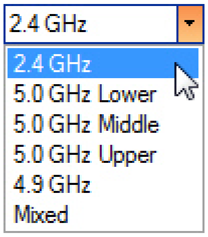
AirMagnet Spectrum XT can scan all available 802.11 radio bands. To enable you to conduct more focused analysis of their spectrum and Wi-Fi environment. the application provides the following five radio bands for easy selection:

Radio Band	Frequency Range (in GHz)	Applicable Channels (US/North America only)
2.4 GHz	2.402 ~ 2.494	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
5 GHz Lower	5.17 ~ 5.33	36, 40, 44, 48, 52, 56, 60, 64
5 GHz Middle	5.49 ~ 5.71	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
5 GHz Upper	5.735 ~ 5.835	149, 153, 157, 161, 165
4.9 GHz	4.91 ~ 4.99	184, 188,192, 196
Mixed	All radio frequencies listed above (except 4.9 GHz)	All channels listed above (except 4.9 GHz)

By default, the application scans the 2.4 GHz radio band when it is started. You can switch to any of the other bands at any time using the Band drop-down list menu.

To change to another radio band:

1. From the toolbar, click the **Band** button.
2. Select the desired band, as illustrated below.

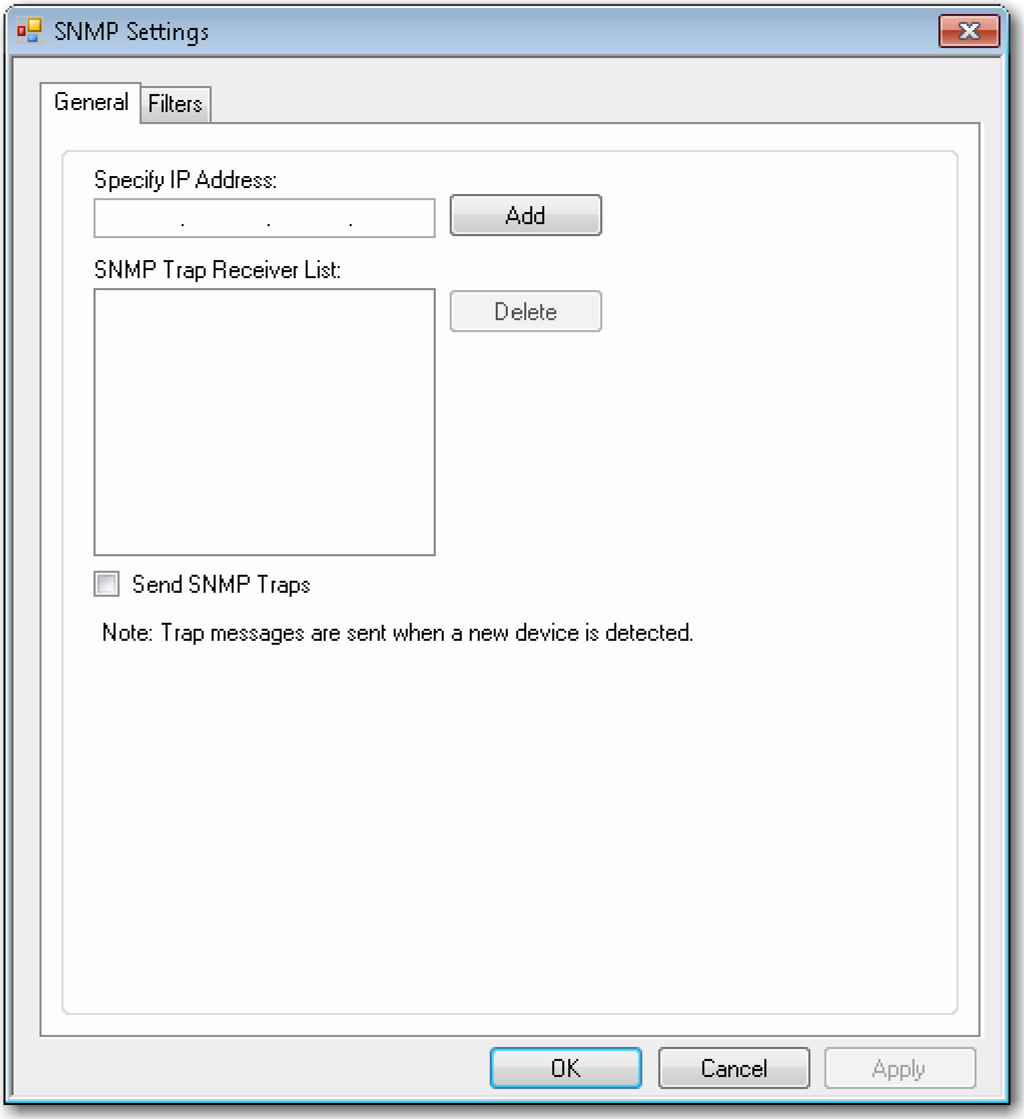


SNMP Integration

AirMagnet Spectrum XT provides a MIB file (*AirMagnetSpectrumInterferer.mib*) that allows AirMagnet Spectrum XT to send SNMP traps to multiple SNMP management stations when an interferer is detected by AirMagnet Spectrum XT. When you receive a trap from the AirMagnet Spectrum XT, it is possible to view detailed description of the trap in AirMagnet Spectrum XT and thereby functioning of your wireless network.

To receive traps from the AirMagnet Spectrum XT on your SNMP management station, do the following:

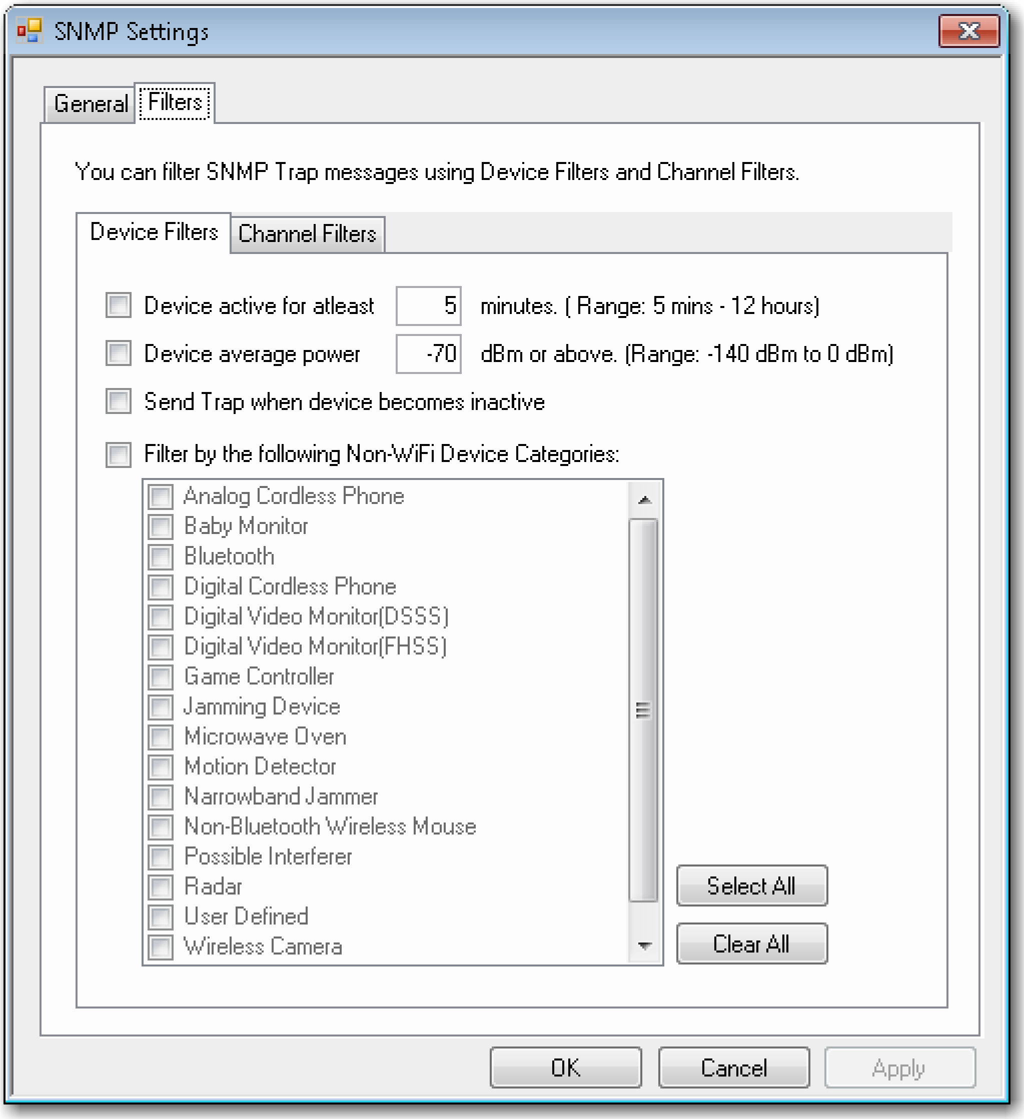
- From the AirMagnet Spectrum XT launch the SNMP settings dialog box by clicking the **Settings>SNMP Settings** menu. In the General tab specify the IP addresses of all your SNMP management stations. You should select the check box **Send SNMP Traps** to send the SNMP traps.



□ Send SNMP Traps

Note: Trap messages are sent when a new device is detected.

You can set various filters to control SNMP traps send by AirMagnet Spectrum XT as follows:



You can filter SNMP Trap messages using Device Filters and Channel Filters.

□ Device active for atleast 5 minutes. (Range: 5 mins - 12 hours)

□ Device average power -70 dBm or above. (Range: -140 dBm to 0 dBm)

□ Send Trap when device becomes inactive

□ Filter by the following Non-WiFi Device Categories:

□ Analog Cordless Phone
□ Baby Monitor
□ Bluetooth
□ Digital Cordless Phone
□ Digital Video Monitor(DSSS)
□ Digital Video Monitor(FHSS)
□ Game Controller
□ Jamming Device
□ Microwave Oven
□ Motion Detector
□ Narrowband Jammer
□ Non-Bluetooth Wireless Mouse
□ Possible Interferer
□ Radar
□ User Defined
□ Wireless Camera

1. Download the *AirMagnetSpectrumInterferer.mib* from the download page of the AirMagnet Spectrum XT in your SNMP management station.
2. Compile the MIB file and enable your SNMP management station to receive traps. Currently there is a trap that is generated by the AirMagnet Spectrum XT for each detected device based on the Filter conditions set in the Filter Tab.

The IANA assigned Private Enterprise Number for AirMagnet is 16603.

Trap Details generated by AirMagnet Spectrum XT:

Trap Number SNMP Trap-V2 Related Alarm Title of Dist AirMagnet

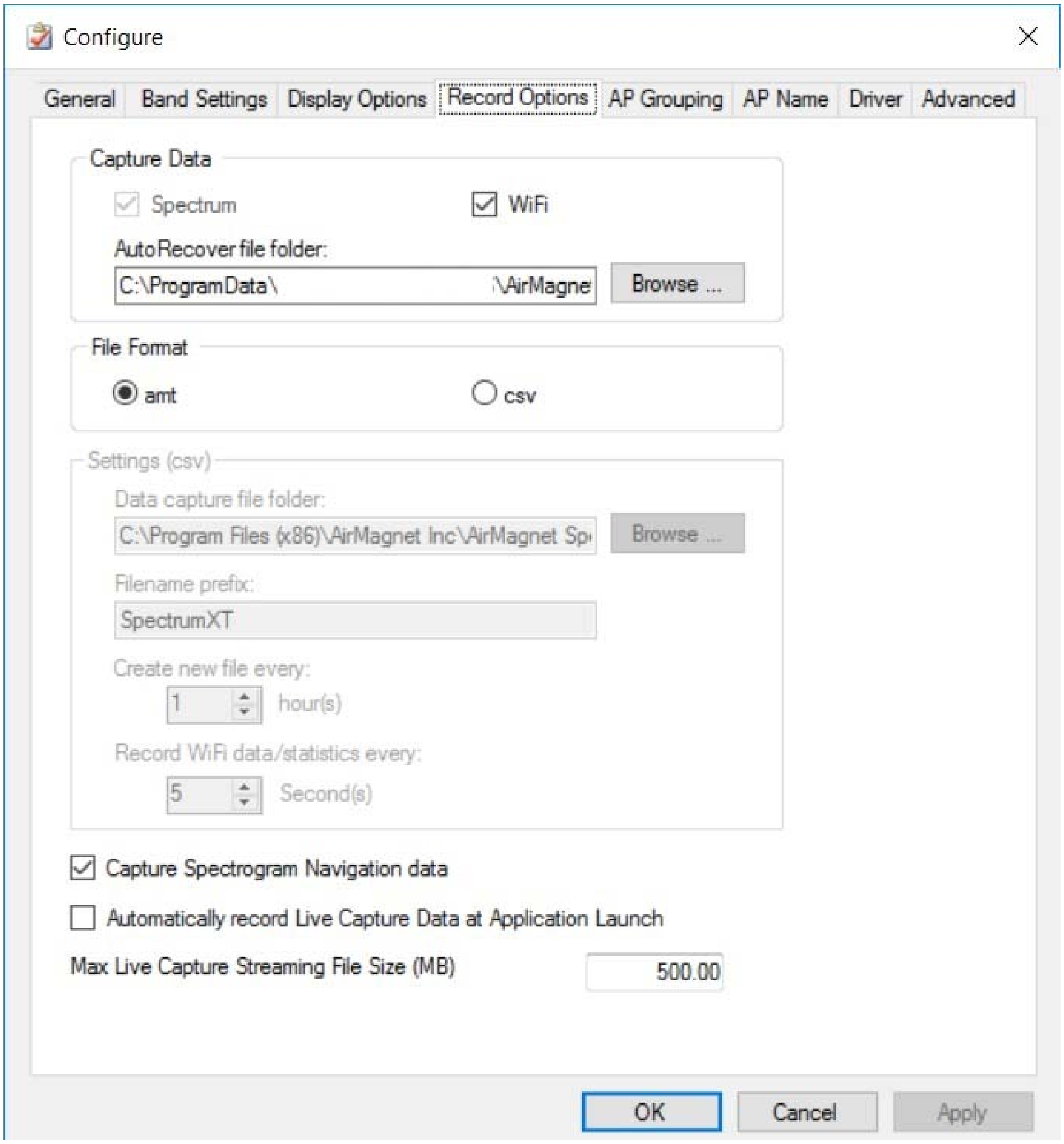
1 amSpectrumTrap Interferer detected

The trap will have the following details:

Device Type
Device Identifier
Device Description
First Seen Time
Last Seen Time
Channel
Max Power at the Channel
Average Power at the Channel
Center Frequency of the Channel

Specifying Record Settings

By default, AirMagnet Spectrum XT saves collected data in AirMagnet's *.amt* format. However, the Record Options tab allows you to save information in *.csv* format for analysis in other applications. It also allows you to activate the Capture Spectrogram Navigation Data feature.



Capture Data

☑ Spectrum ☑ WiFi

AutoRecover file folder: C:\ProgramData\ \AirMagne

File Format

● amt ○ csv

Settings (csv)

Data capture file folder: C:\Program Files (x86)\AirMagnet Inc\AirMagnet Sp

Filename prefix: SpectrumXT

Create new file every: 1 hour(s)

Record WiFi data/statistics every: 5 Second(s)

☑ Capture Spectrogram Navigation data

□ Automatically record Live Capture Data at Application Launch

Max Live Capture Streaming File Size (MB) 500.00

Note: Files saved in *.csv* format cannot be played back using AirMagnet Spectrum XT.

To record *.csv* files:

1. From the Record Options tab, click the **csv** radio button.
2. Specify the folder in which the files should be saved, either by entering the path manually or by clicking the **Browse...** button.
3. Enter a prefix for the files, if desired.
4. Specify the frequency with which the files should be saved off.
5. Click **OK** to save the changes.

Using the Capture Spectrogram Navigation data checkbox:

- When checked, recordings made afterwards will include Spectrogram data.
- When unchecked, recordings made afterwards will NOT include Spectrogram data.
- This checkbox does not affect the access to Spectrogram Navigation feature, but instead affects whether or not Spectrogram data is captured in recordings. If a recording does NOT have spectrogram data, then you will not be able to access the Spectrogram Navigation feature (icon will be greyed out) and vice-versa.

Using Easy View

The Easy View allows you to filter data to be displayed on the screen so that you can focus more on data of interest. The Easy View button provides the following viewing options:

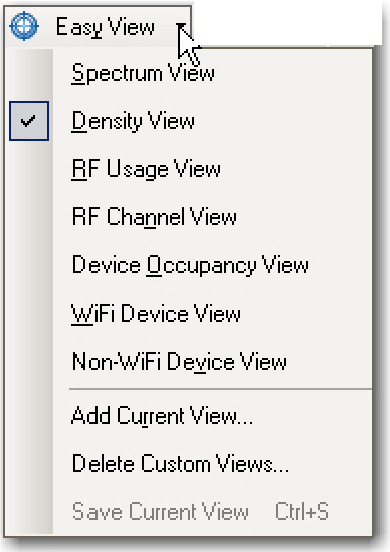
- **Spectrum View** - (default) Displays the Real-Time FFT graph, along with the Spectrum Density and AP Signal Strength graphs.
- **Density View** - Displays the Spectrum Density graph, along with Channels by Speed graph.
- **RF Usage View** - Displays the Real-Time FFT, Spectrogram and Spectrum Density graphs.
- **RF Channel View** - Displays the Real-Time FFT, Channel Duty Cycle, and Channel Power graphs.
- **Device Occupancy View** - Displays the Real-Time FFT and Channel Occupancy graphs.
- **WiFi Device View** - Displays the WiFi Devices table that list all Wi-Fi devices (that is, APs, stations, and so on) detected on each channel.
- **Non-WiFi Device View** - Displays the Non-WiFi Devices table that list all non-Wi-Fi devices detected.
- **Add Current View...** - Allows you to create a unique view option using what is shown on the current screen and add it to the Easy View menu.
- **Delete Custom Views... -** Allows you to remove custom view options off the Easy View menu.
- **Save Current View** - Allows you to save any custom view you have created and/or any configuration changes you have made in any graph currently shown in the graph window.
- **Saved Custom View** - Shows all custom view options the user has saved.

Changing View Options

By default, the application opens in the Spectrum View, but you can switch to any other options in the Easy View menu.

To display data using Easy View:

1. From the toolbar, click **Easy View** and select an option from the drop-down menu. Refer to the illustration below.

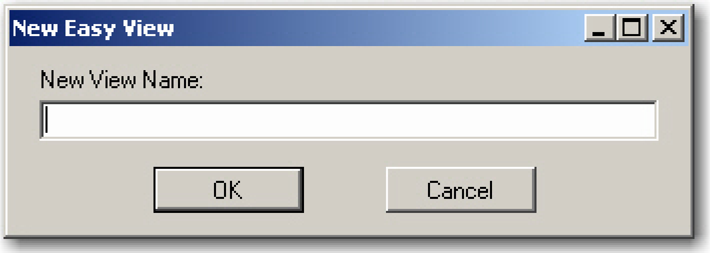


Creating a Custom View Option

Since the application can display multiple graphs on one screen, you can display the graphs of interest and save the current screen view as a custom view option and add it to the list of option in the Easy View menu.

To create a custom view option:

1. Open the graphs of your choice on the screen.
2. Click **Easy View** and select **Add Current View…** from the list menu. The New Easy View window appears, as shown below.



3. Type a name for the new view and click **OK**.

Note: You can create more Easy View options by following the same steps outlined above. All custom view options you create will be automatically appended to the end of the Easy View list menu.

Deleting a Custom View Option

Unlike those built-in Easy View options, the custom Easy View options can be deleted if desired.

To delete a custom Easy View option:

1. Click the **Easy View** button and select **Delete Custom Views....** The Delete Easy Views window appears.
2. Select the custom view option or options to be deleted and click **Delete**.

Resetting Collected Data

While the **Pause/Resume Live Capture** and **Stop/Start Live Capture** functions apply to the entire application, the **Reset Spectrum Data** button applies only to the spectrum part of the application. Clicking this button causes the application to discard all spectrum and Wi-Fi data it has captured and then starts all over again. Although the effect is visible in all parts of the user interface where spectrum data are shown, it has no effect on the Wi-Fi data.

To reset data:

From the toolbar, click ↻ **(Reset Data).**

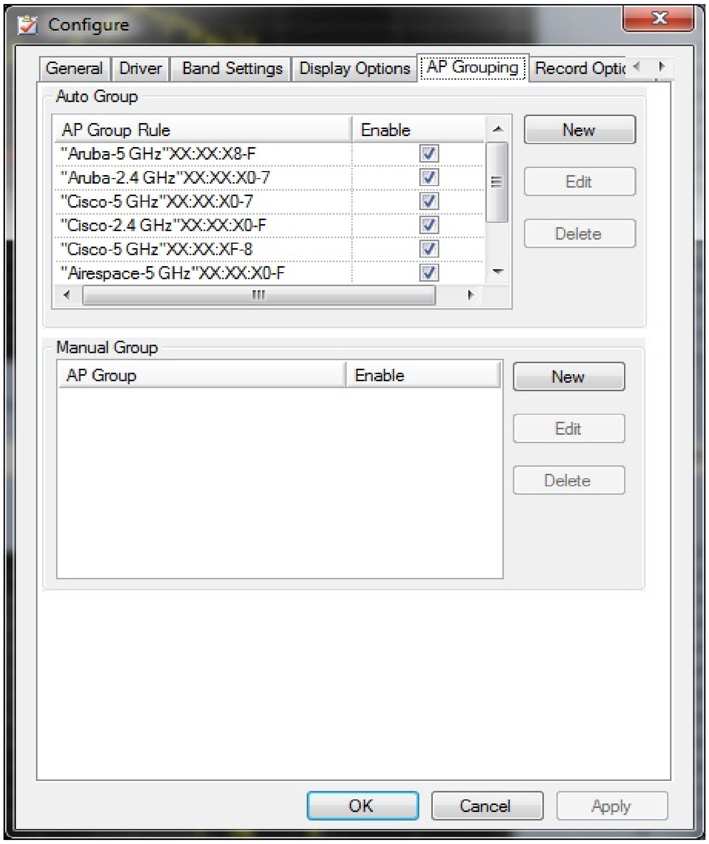
Virtual AP Grouping

AirMagnet Spectrum XT’s Virtual AP Grouping feature allows you to set up specific names for single devices that use multiple SSIDs under different BSSIDs. These groups help you identify instances where separate BSSIDs show up and appear to be several different devices, when they actually belong to a single device.

Spectrum comes with several built-in “automatic” AP Group rules. If you enable them, they will automatically group all devices meeting the criteria specified in the rule under a single AP Group.

To configure AP Grouping settings:

1. From the Configure window, click the **AP Grouping** tab.



Auto Group

AP Group Rule	Enable
"Aruba-5 GHz"XX:XX:X8-F	☑
"Aruba-2.4 GHz"XX:XX:X0-7	☑
"Cisco-5 GHz"XX:XX:X0-7	☑
"Cisco-2.4 GHz"XX:XX:X0-F	☑
"Cisco-5 GHz"XX:XX:XF-8	☑
"Airespace-5 GHz"XX:XX:X0-F	☑

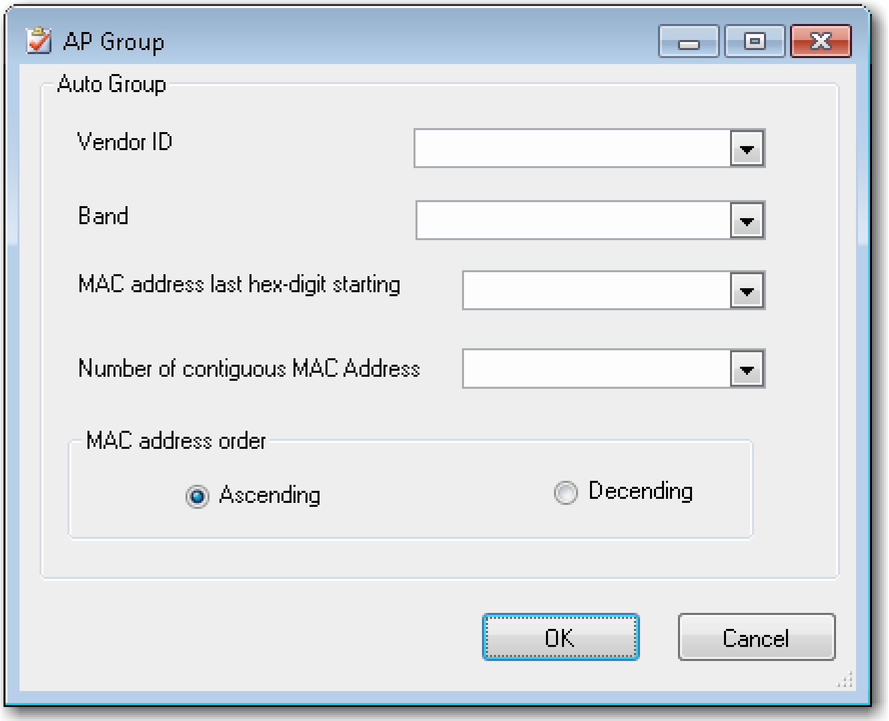
Manual Group

AP Group	Enable

2. This tab provides two different types of rules for grouping APs. See the sections below for instructions on configuring each type.

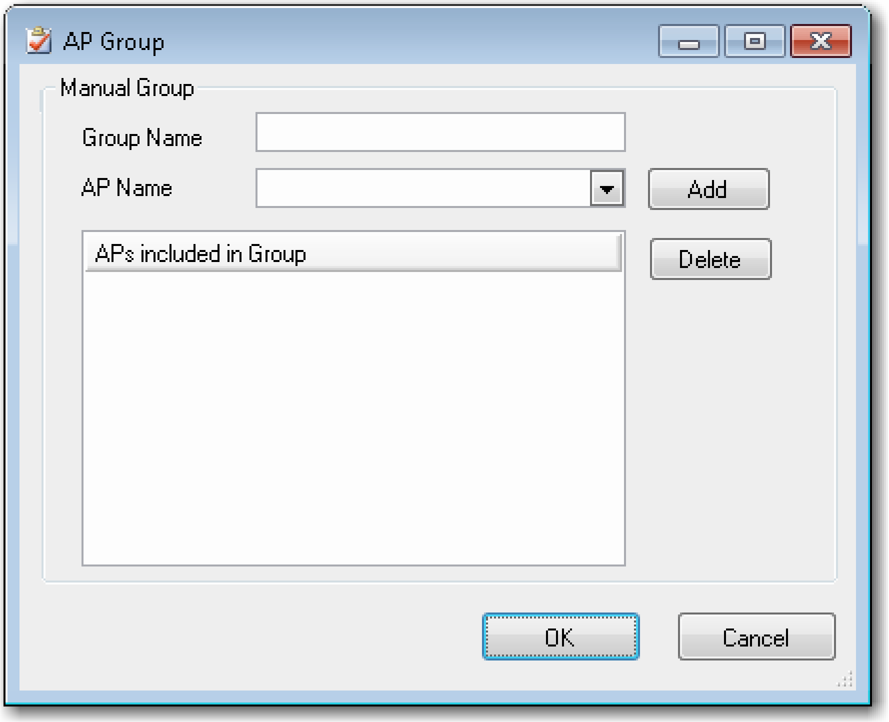
Auto Group Rules

Configure different fields in the Auto AP Group Rules by clicking on the **New** button.



Manual Group Rules

Manually add groups by clicking the **New** button for Manual Group and add a Group name and AP Name.



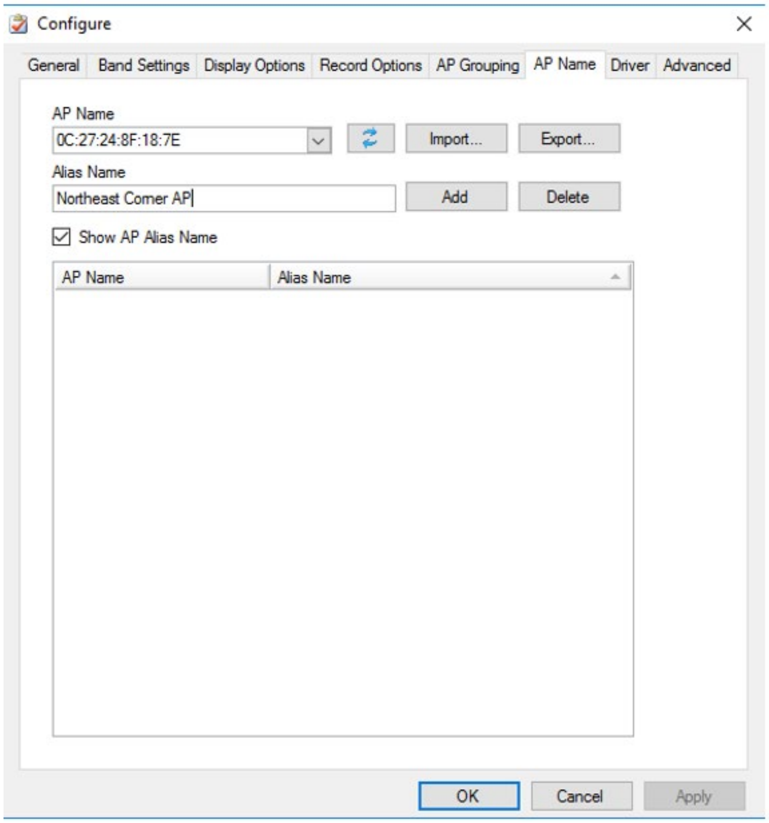
Assigning an AP Alias Name

You can assign an alias name to an Access Point (AP) to display that AP's instance throughout the user interface with a user-friendly name.

To assign an AP Alias Name:

1. From the Toolbar, click **Settings>Configure.**

2. Click the **AP Name** tab, if not selected. Refer to the example below.



AP Name
0C:27:24:8F:18:7E

Alias Name
Northeast Corner AP

☑ Show AP Alias Name

3. Type an Alias name in the **Alias Name** field.
4. Click the **Show AP Alias Name** check box.
5. Click **Add**.
6. Click **OK**.

Spectrum XT Report

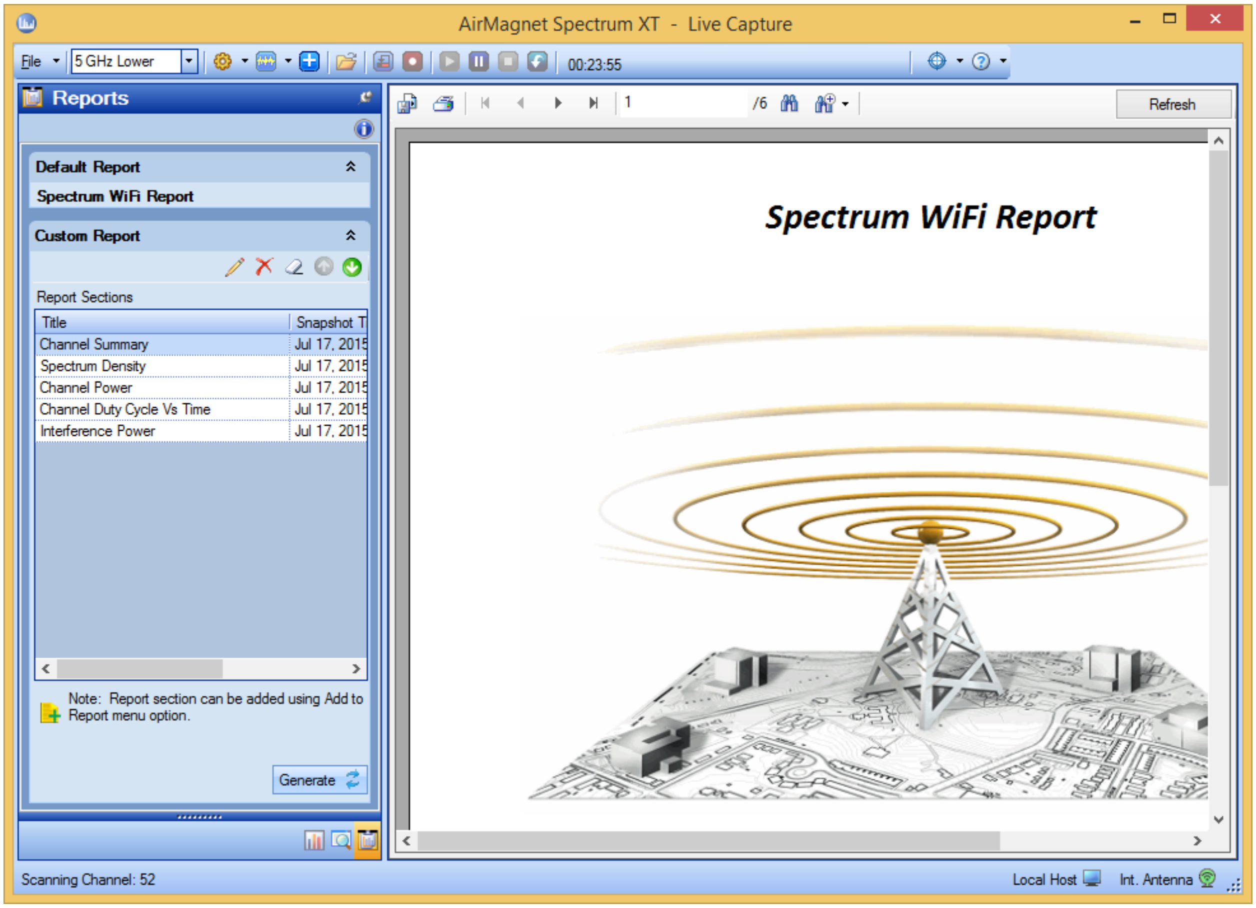
AirMagnet Spectrum XT Report will display a formatted report that summarizes RF spectrum data such as any detected non-Wi-Fi interferers along with Wi-Fi data such as detected APs (if a Wi-Fi adapter is active). The report may be printed and exported.

Export options: .pdf, .rtf, .doc, .xls, and .rpt.

To use the Report feature:

1. When installing AirMagnet Spectrum XT, accept the request to install the report viewer.
2. From the Navigation Bar, click **Report**.
3. Use the **page forward** and **page back** controls at the top of the report to navigate from page to page.
4. The report menu bar also provides options to **Print** and **Export**.

The first time the report is opened, it takes a snapshot of the data at that time. To update the data, click **Refresh**.

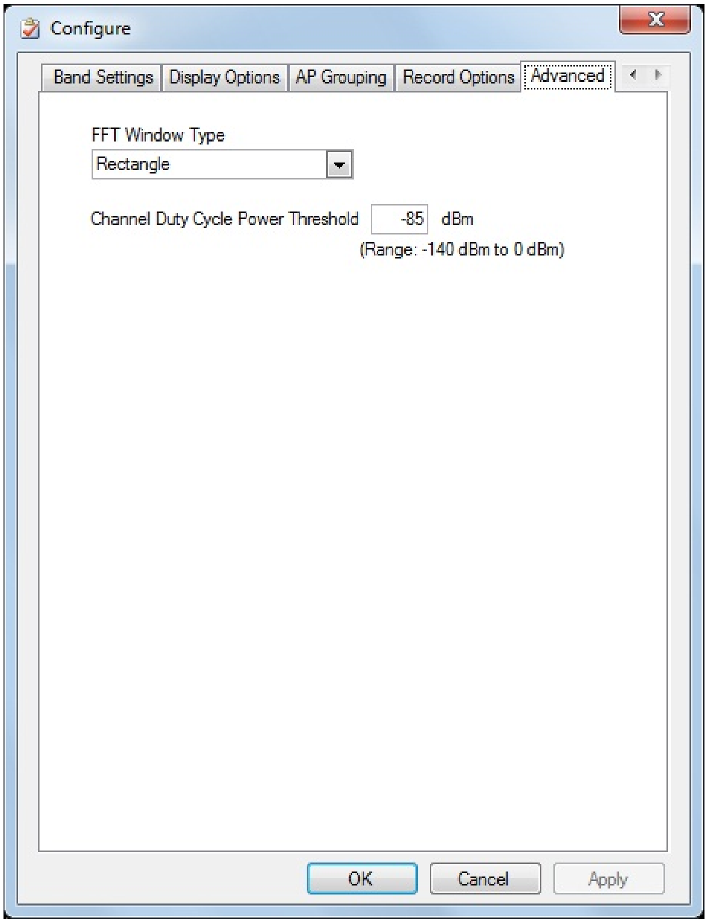


Title	Snapshot T
Channel Summary	Jul 17, 2015
Spectrum Density	Jul 17, 2015
Channel Power	Jul 17, 2015
Channel Duty Cycle Vs Time	Jul 17, 2015
Interference Power	Jul 17, 2015

Note: Report section can be added using Add to Report menu option.

Scanning Channel: 52

Configuring FFT Window Types



FFT Window Type: Rectangle

Channel Duty Cycle Power Threshold -85 dBm

(Range: -140 dBm to 0 dBm)

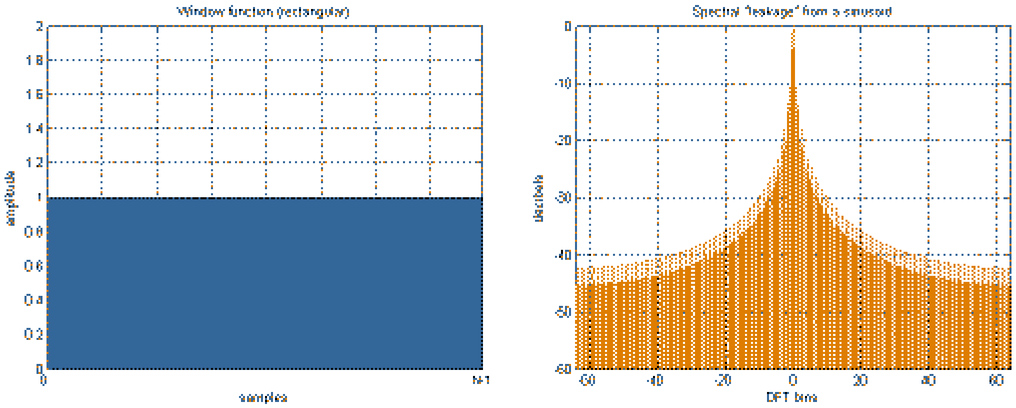
You can choose the desired method to be used to process FFT data: Rectangular, Hamming, Hann and Blackman Harris. Rectangular is the default.

1. From the Toolbar, click **Settings>Configure.**
2. Click the **Advanced** tab.
3. Select the desired FFT Window Type from the drop-down menu.

When FFT is computed from a signal sample which is non-periodic, an effect known as leakage, causes errors in amplitude and/or frequency. Windowing functions are used to correct (or minimize) this problem. In the latest release, Spectrum XT offers user-selectable FFT Windows. In previous versions of the Spectrum XT, a rectangular FFT Window was used by default. Now, you have the choice between: Rectangular, Hamming, Hann and Blackman-Harris FFT Window Types. You should choose the appropriate window function, based on the input signal and/or specific application. FFT Windows do not eliminate leakage entirely, but alters the shape of the leakage.

The following FFT window types descriptions are excerpts from a Wikipedia article, *Window Function* located at this Web address: *http://en.wikipedia.org/wiki/Window_function*.

Rectangular Window

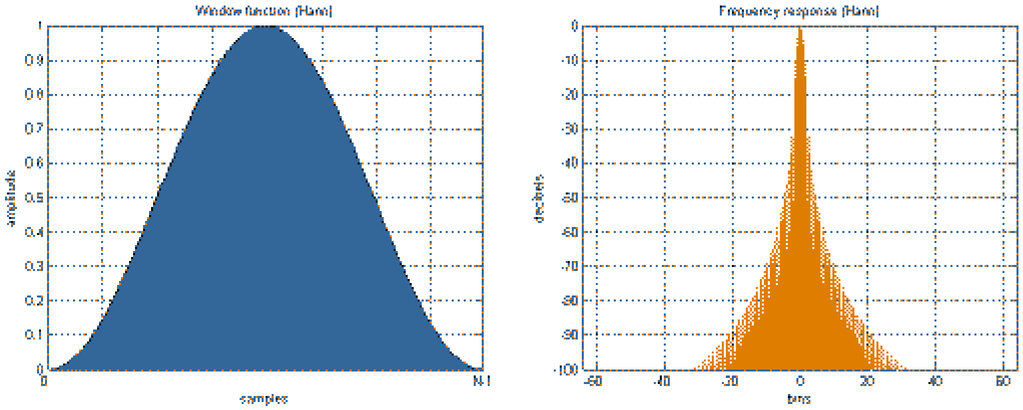


Rectangular window; B=1.00

$$w(n) = 1$$

The rectangular window (sometimes known as the boxcar or Dirichlet window) is the simplest window, equivalent to replacing all but N values of a data sequence by zeros, making it appear as though the waveform suddenly turns on and off. Other windows are designed to moderate these sudden changes because discontinuities have undesirable effects on the discrete-time Fourier transform (DTFT) and/or the algorithms that produce samples of the DTFT.

Hann Window



Hann window; B = 1.50

$$w(n) = 0.5\ \left(1 - \cos\left(\frac{2\pi n}{N-1}\right)\right)$$

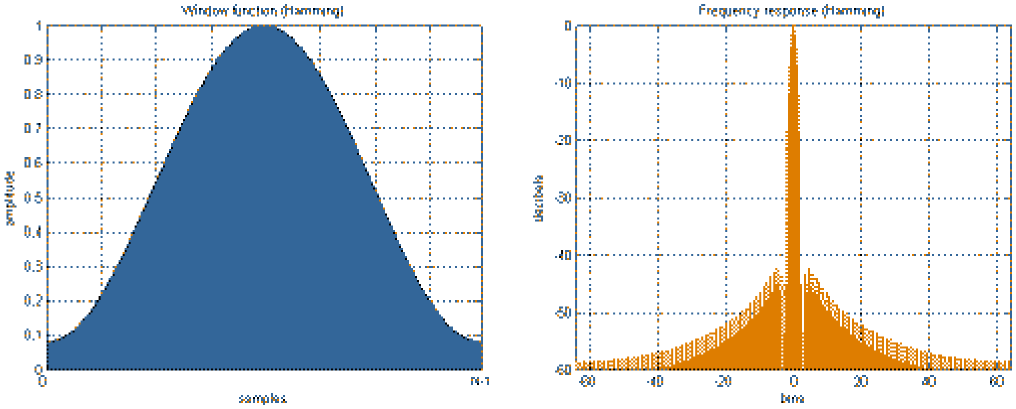
Note that:

$$w_0(n) = 0.5\ \left(1 + \cos\left(\frac{2\pi n}{N-1}\right)\right)$$

The ends of the cosine just touch zero, so the side-lobes roll off at about 18 dB per octave.

The Hann and Hamming windows, both of which are in the family known as "raised cosine" or "generalized Hamming" windows, are respectively named after Julius von Hann and Richard Hamming. The erroneous term "Hanning window" is sometimes used to refer to the Hann window.

Hamming Window



Hamming window; B=1.37

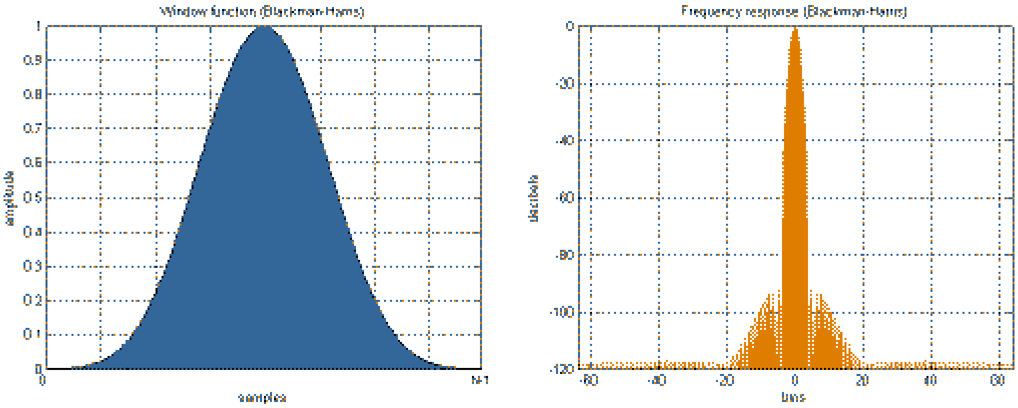
The "raised cosine" with these particular coefficients was proposed by Richard W. Hamming. The window is optimized to minimize the maximum (nearest) side lobe, giving it a height of about one-fifth that of the Hann window, a raised cosine with simpler coefficients.

$$w(n) = 0.54 - 0.46\ \cos\left(\frac{2\pi n}{N-1}\right)$$

Note that:

$$\begin{aligned} w_0(n) &\overset{\text{def}}{=} w(n+\tfrac{N-1}{2}) \\ &= 0.54 + 0.46\ \cos\left(\frac{2\pi n}{N-1}\right) \end{aligned}$$

Blackman–Harris window



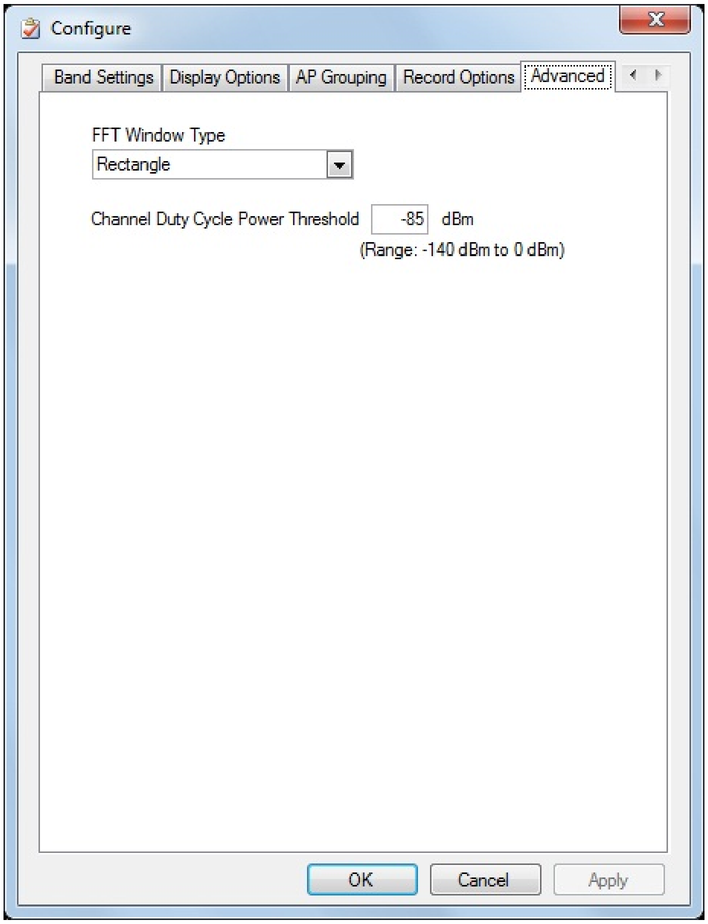
Blackman–Harris window; B=2.01

A generalization of the Hamming family, produced by adding more shifted sinc functions, meant to minimize side-lobe levels.

$$w(n) = a_0 - a_1 \cos\left(\frac{2\pi n}{N-1}\right) + a_2 \cos\left(\frac{4\pi n}{N-1}\right) - a_3 \cos\left(\frac{6\pi n}{N-1}\right)$$

$$a_0 = 0.35875; \quad a_1 = 0.48829; \quad a_2 = 0.14128; \quad a_3 = 0.01168$$

Channel Duty Cycle Power Threshold



FFT Window Type
Rectangle

Channel Duty Cycle Power Threshold -85 dBm
(Range: -140 dBm to 0 dBm)

Use this option to setup the integrated power threshold level that will count towards the duty cycle calculation.

- All received integrated channel power in a 20MHz bandwidth above the threshold level will be counted in the duty cycle calculation.
- All received integrated channel power in a 20MHz bandwidth below the threshold level will not be counted in the duty cycle calculation.
- The default value for the channel utilization power threshold is -85 dBm.
- The default value for the channel utilization threshold is -85 dBm.

1. From the Toolbar, click **Settings>Configure.**
2. Click the **Advanced** tab.
3. Adjust the threshold level value as desired.
4. Click **OK**.

Analyzing Spectrum Data

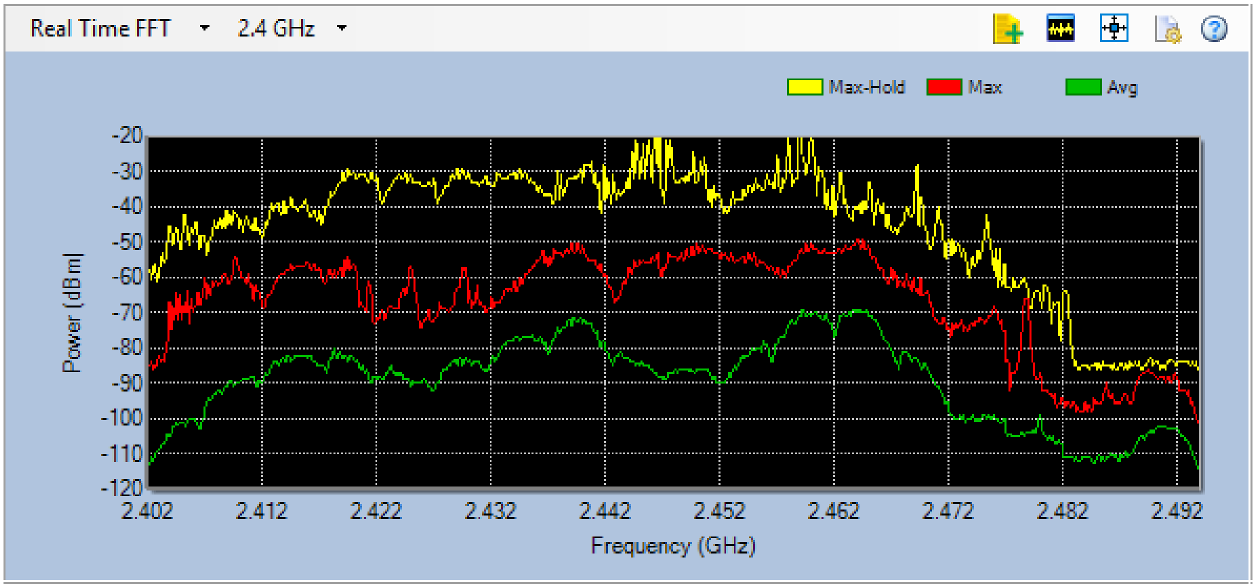
Spectrum Graphs

AirMagnet Spectrum XT has the capability to capture spectrum data from various radio devices and display the data in the following graphs:

- Real Time FFT
- Spectrum Density
- Spectrogram
- Channel Power
- Channel Duty Cycle
- Non-WiFi Devices
- Event Spectrogram
- Interference Power
- Channel Duty Cycle vs Time
- Interference Power vs Time

Real Time FFT

The Real-Time FFT (Fast Fourier Transform) graph displays in real time the value of RF power as a function of radio frequency. The X-axis shows the frequency range of each channel in the selected radio band; the Y-axis shows power readings in dBm.

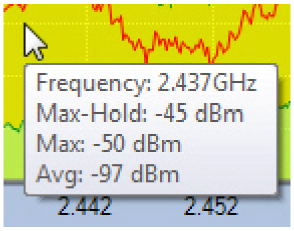


Real Time FFT Graph

The Real Time FFT graph can display four types of spectrum data that are color-coded. The number of data types displayed depends on the configuration settings.

Real Time FFT Graph Parameters **Color**	**Spectrum Data**	**Description**
Yellow	Max-hold	The highest power readings that have been recorded since the session began.
Red	Max	The maximum power in the RF Spectrum of a single channel sweep. Each FFT consists of 256 samples in 6.4 microseconds. A 100ms dwell on a channel results in 15,625 FFTs.
Green	Average	The average historical power readings recorded since the beginning of the session.
Blue	Current	The last sampling power in the RF Spectrum of a single channel sweep. ***Note:*** *The Current option is disabled by default; it can be enabled by modifying the Graph Options.*

You can see a brief text description of the spectrum data such as the Maximum, Average, and Current power readings as well as the radio frequency using the tool tip which, if enabled, it will pop up where you place the causer in graph.



Frequency: 2.437GHz
Max-Hold: -45 dBm
Max: -50 dBm
Avg: -97 dBm

Using Tool Tip

The tool tip shows the following information about the point of interest in the Real-Time FFT graph:

- (RF) Frequency
- Max-hold (power reading)
- Maximum (power reading)
- Average (power reading)
- Current (power reading - if enabled)

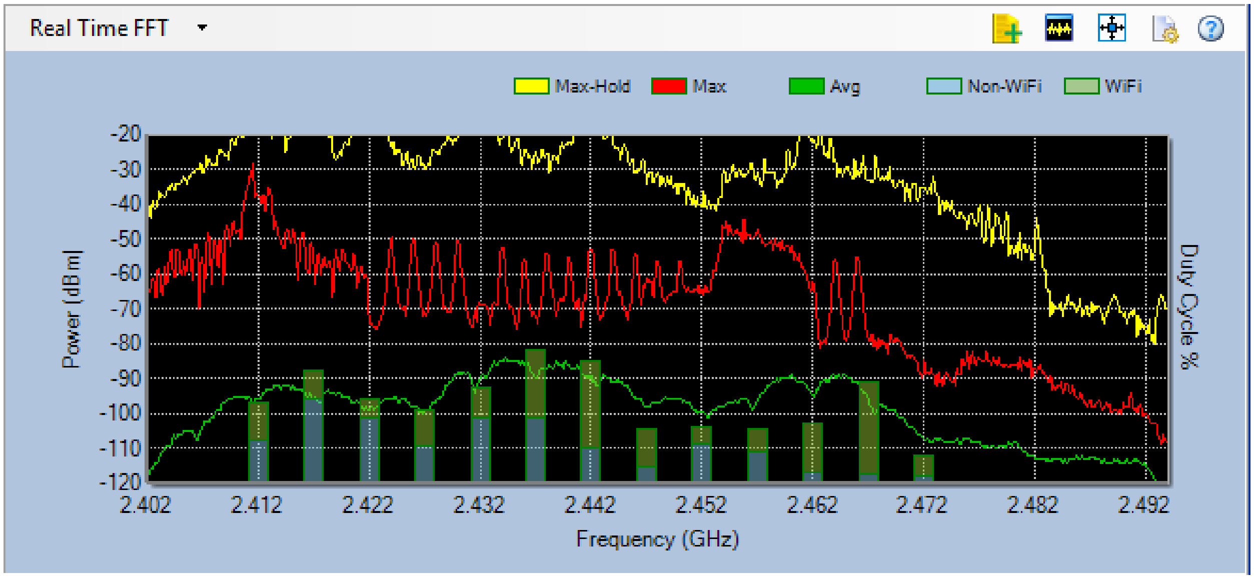
Technically, the power range in the Real Time FFT graph can be set as low as -140 dBm (Minimum Power) and/or as high as 0 dBm (Peak Power). When a narrower power range is used, for example, -120 dBm ~ -30 dBm, you may notice some discrepancy between what is shown in the Real Time FFT graph and what is displayed in the tool tip when the actual power readings fall beyond either or both the Minimum Power and/or Peak Power limit. For instance, if the power range is set between -120 dBm and -20 dBm, you will not be able to see any power reading lower than -120 in the graph because it falls beyond the Minimum Power. However, you will be able to see the actual power readings in the tool tip even when they fall outside the specified power range because the tool tip is not affected by the power range set for the Real Time FFT graph.

The power readings shown in the tool tip are not updated in real time and may not match what is shown in the Real Time FFT graph.

Channel Duty Cycle Overlay on FFT Graph

The FFT Graph can be configured to show an overlay of Channel Duty Cycle data. This setting option is added to the FFT Chart Configuration settings as “Show Duty Cycle.”

With this option enabled, the duty cycle data will overlay the FFT graph as semi-transparent bars. Both Wi-Fi and non-Wi-Fi data are displayed as indicated by the legend in the upper right of the graph. The Duty Cycle percentage is shown on the far right Y-axis.



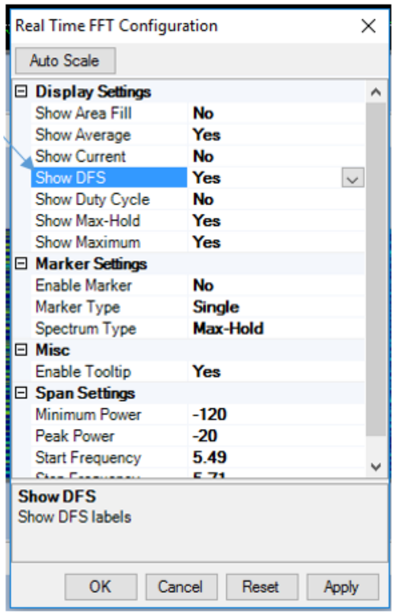
FFT Graph Showing Channel Duty Cycle

Setting FFT Graph Parameters

In the upper-right corner of the Real Time FFT graph comes with a Configuration button which allows you to set or change a number of parameters in the Real Time FFT graph.

To configure Real-Time FFT graph parameters:

1) From the upper-right corner of the Real Time FFT graph, click (**Chart Configuration**). The Real-Time FFT Configuration dialog box appears.



Display Settings	
Show Area Fill	No
Show Average	Yes
Show Current	No
Show DFS	Yes
Show Duty Cycle	No
Show Max-Hold	Yes
Show Maximum	Yes
Marker Settings	
Enable Marker	No
Marker Type	Single
Spectrum Type	Max-Hold
Misc	
Enable Tooltip	Yes
Span Settings	
Minimum Power	-120
Peak Power	-20
Start Frequency	5.49
Stop Frequency	5.71

Show DFS
Show DFS labels

Configuring Real Time FFT Configuration Dialogue Box

2) Make the entries and/or selections as described in the following table.

3) Click **Apply** and then OK.

Setting Real Time FFT Graph Parameters **Parameter**	**Description**
Show Area Fill	Enables or disables the graph's ability to fill the area below the displayed line. **Note:** This option can be fairly CPU-intensive; consequently, you can

	experience improved application performance if this is set to No.
Show Average	Allows you to show or hide the average power readings in the FFT graph. Click in the field and use the down arrow to select either of the following: • Yes - Displays the average power readings. • No - Hides the average power readings.
Show Current	Allows you to show or hide the current power readings in the FFT graph. Click in the field and use the down arrow to select either of the following: • Yes - Displays the current power readings. • No - Hides the current power readings.
Show DFS	When you have selected a band including Dynamic Frequency Selection (DFS) channels, the Show DFS option appears on the Real Time FFT Configuration window. Select one of the following: • Yes - Displays the DFS channel range. • No - Hides the DFS channel range.
Show Duty Cycle	The duty cycle data will overlay the FFT graph as semi-transparent bars • Yes - Displays the duty cycle overlay. • No - Hides the duty cycle overlay.
Show Max-hold	Allows you to show or hide the max-hold power readings in the FFT graph. Click in the field and use the down arrow to select either of the following: • Yes - Displays the max-hold power readings. • No - Hides the max-hold power readings.
Show Maximum	Allows you to show or hide the maximum power readings in the FFT graph. Click in the field and use the down arrow to select either of the following: • Yes - Displays the maximum power readings. • No - Hides the maximum power readings.

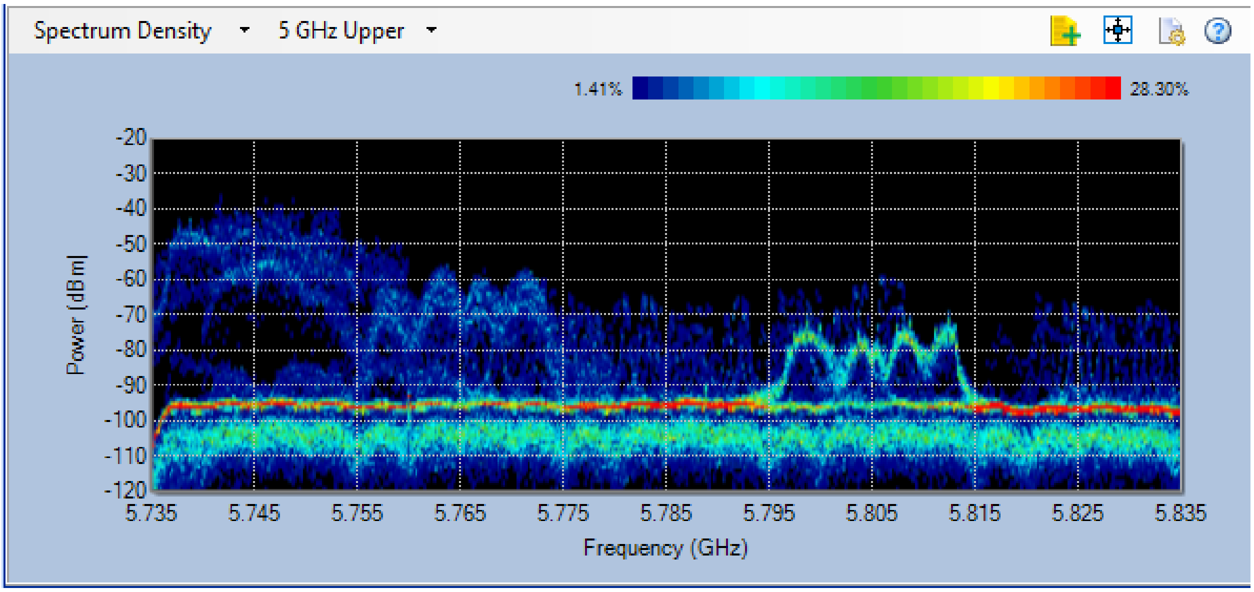
Enable Marker	Allows you to enable or disable the marker or markers (which is or are tiny blue dots) on the FFT graph. The marker or markers help you to highlight a specific point of interest in the FFT graph. Click in the field and use the down arrow to select either of the following: • Yes - Displays the marker. If selected, You then have to specify a marker type which can be Single or Delta. See below. • No - Hides the marker.
Marker Type	Used only when you select **True** in the Enable Marker field. It allows you to choose between Single and Delta. The former only shows one marker, as the name suggests. The latter shows two markers: one of them stays at a fixed location on the FFT graph while the other can be dragged around. To effectively use this feature, you should start with a Single marker and drag it to a point of interest on the FFT graph. Then select Delta to bring up the second marker. This will cause the first marker to remain fixed at where you leave it. You can then drag the second marker to compare the power readings between a fixed data point and any other data point on the FFT graph. Click in the field and use the down arrow to select either of the following: • Single - Displays a single maker which can dragged to any point of interest on the FFT graph. • Delta - Displays two markers: one fixed at a particular location and the other can be dragged across the FFT plot for comparison. See the above paragraph. **Note:** When Marker is enabled, power readings of the data points marked by the markers also appear in the upper-left corner of the FFT graph.
Spectrum Type	Allows you to decide where (which part of the FFT graph) the marker or markers should fall. Click in the field and use the down arrow to select one of the following: • Current - Places the marker or markers on the Current power readings. (The marker may jumps up and down as the curve line changes, because this curve reflects the real-time change of power readings across the spectrum.) • Average - Places the marker or markers on the Average power readings. • Maximum - Places the marker or markers on the Maximum power readings.

Enable Tool Tip	Allows you to show or hide the tool tip (on the FFT graph), which provides the current, average, and maximum power readings as well as the frequency at the point the cursor rests upon. Click in the field and use the down arrow to select either of the following: • Yes - Shows the tool tip. • No - Hides the tool tip.
Minimum Power	Allow syou to set or change the minimum power level on the Y-axis. By default, it is set at -120 dBm, but it can be set to as low as -140 dBm. Highlight the existing value and override it with a new value.
Peak Power	Allows you to set or change the maximum power level on the Y-axis. By default, it is set at -20 dBm, but you can change it to any value less than 0 dBm. Highlight the existing value and override it with a new value.
Start Frequency	Allows you to set or change the start point of a frequency range. Highlight the existing value and override it with a new value.
Stop Frequency	Allows you to set or change the end point of a frequency range. Highlight the existing value and override it with a new value.

The text message at the bottom of the Real Time FFT Configuration dialog box changes with the parameter you select. It provides a brief description of the parameter being selected.

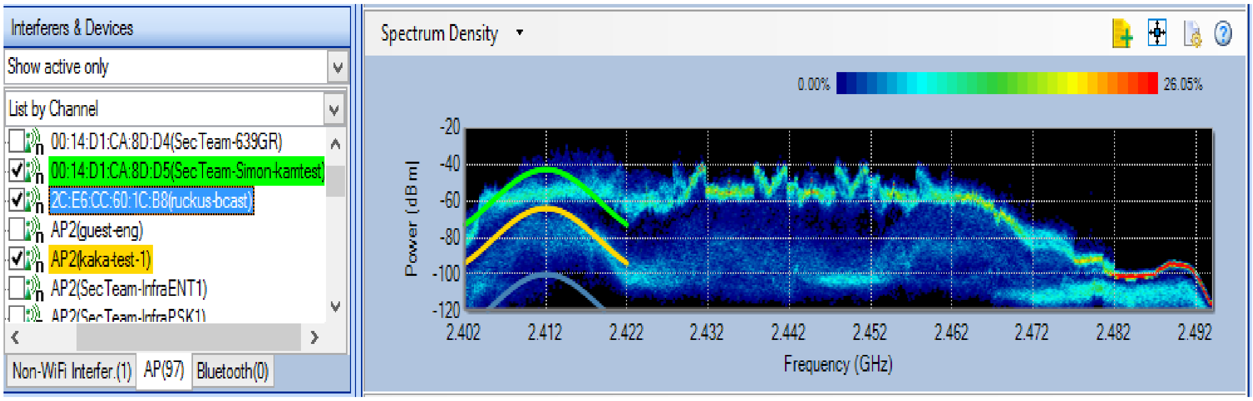
Spectrum Density

The Spectrum Density graph shows the “popularity” of a particular frequency/power reading over time. The X-axis shows the frequency or channel for the selected 802.11 radio band; the Y-axis shows the minimum and maximum power readings in dBm. Refer to the illustration below.



Viewing AP Signal Strengths Across Frequency Range

You can also display the signal strengths of APs selected from the Device List on the left. The signal strengths of the selected APs are projected over the Spectrum Density graph in the form of curves across the corresponding frequency range used by the APs. Notice that the selected APs and their signal strength readings are color-coded with matching colors for easy identification. Refer to the illustration below.



□ 00:14:D1:CA:8D:D4(SecTeam-639GR)
☑ 00:14:D1:CA:8D:D5(SecTeam-Simon-kamtest)
☑ 2C:E6:CC:60:1C:B8(ruckus-bcast)
□ AP2(guest-eng)
☑ AP2(kaka-test-1)
□ AP2(SecTeam-InfraENT1)
□ AP2(SecTeam-InfraPSK1)

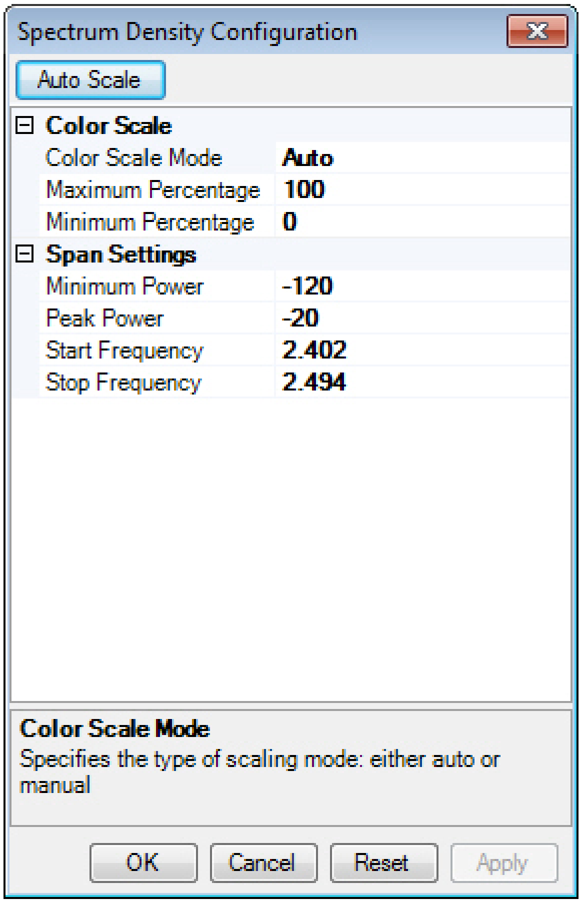
Note: The AP signal strength curves are based on Wi-Fi data captured by the wireless network adapter in use and may not completely match the data in the Spectrum Density graph. As illustrated above, AP signal strengths as represented by the colored curves appear higher than the maximum signal strength shown in the Spectrum Density graph. This is because AP signal strengths (and the curve representing them) are based on RSSI data captured by the external wireless network adapter. While RSSI is usually calculated over a packet or averaged over multiple packets, RF power as measured by the spectrum analysis engine includes packets and background noise, plus RF silence in between the packets. For this reason, it is no surprise that the RSSI value (the AP curve in this case) differs from the peak of the spectrum graph for the same AP.

Setting or Changing Spectrum Density Plot Parameters

You can change the settings of the Spectrum Density plot using the **(Chart Configuration)** button in the upper-right corner of the Spectrum Density plot.

To Change the settings of the Spectrum Density plot:

1. Click the **Configure Plot** button to open the Spectrum Density Configuration dialog box, as illustrated below.



⊟ Color Scale	
Color Scale Mode	**Auto**
Maximum Percentage	**100**
Minimum Percentage	**0**
⊟ Span Settings	
Minimum Power	**-120**
Peak Power	**-20**
Start Frequency	**2.402**
Stop Frequency	**2.494**

Color Scale Mode
Specifies the type of scaling mode: either auto or manual

2. Make the desired changes as described in the table below.

3. Click **Apply** and then **OK.**

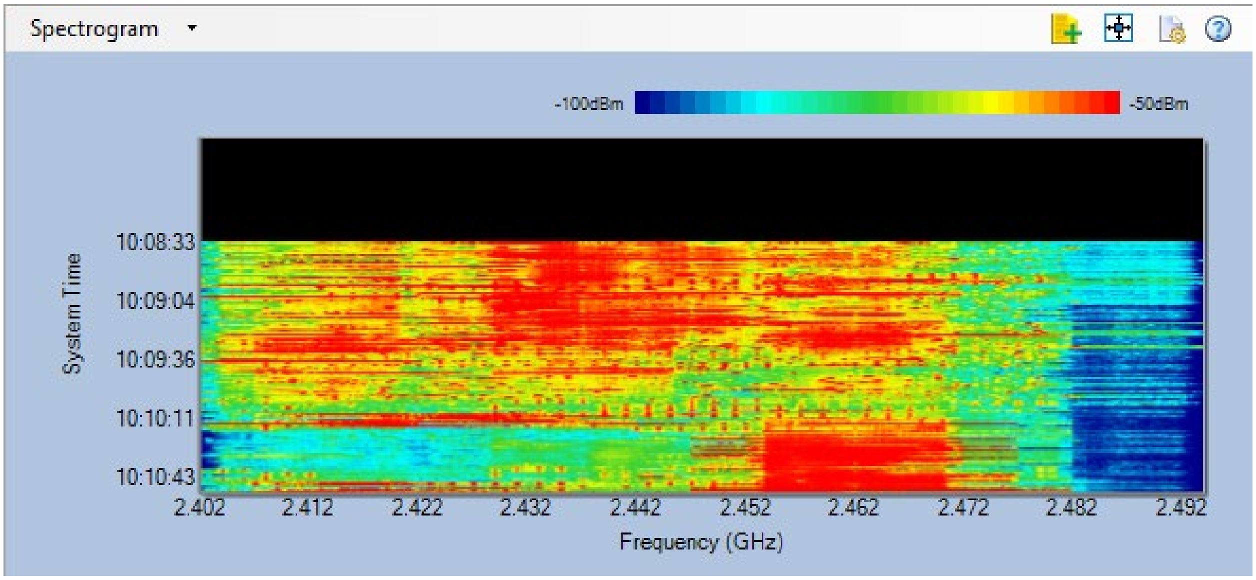
Parameter	Description
Color Scale Mode	This options allows you to set or change the color scale modes of the Spectrum Density plot. As indicated by the legend in the upper-right corner of the plot, the color scale mode range from blue (Minimum Percentage) to red (Maximum Percentage). Click in the field and use

	the down arrow to select either of the following: ▪ Auto - (Default) If selected, the application will automatically and dynamically change the color scale on the Spectrum Density plot. ▪ Manual - If selected, you can manually set or change the Maximum Percentage and/or Minimum Percentage values. Highlight the existing Minimum Percentage and Maximum Percentage values and override them with new values. Once the Minimum Percentage and Maximum Percentage values are set, any values that fall outside the range will be ignored by the Spectrum Density plot. Those that are below the Minimum Percentage value will show as blue while those that are above the Maximum Percentage value will show as red on the Spectrum Density plot.
Maximum Percentage	This option allows you to set or change the maximum percentage value (shown on the right-hand side) of the color scale. It is 100 by default, but you can change this value to any value if you select Manual in the Color Scale Mode. Simply highlight the existing value and override it with a new value.
Minimum Percentage	The minimum percentage (shown on the left-hand side) of the color scale. It is 0 by default, but you can change it to any value between 0 and 100, if you select Manual in the Color Scale Mode. Simply highlight the existing value and override it with a new value.
Minimum Power	This option allows you to set or change the Minimum Power value in dBm in the Y-axis of the Spectrum Density plot. By default, the Minimum Power value is -120, but you can change it to any value as low as -140.
Peak Power	This option allows you to set or change the Peak Power value in dBm in the Y-axis of the Spectrum Density plot. By default, the Peak Power value is -20, but you can change it to any value less than 0 dBm. Highlight the existing Peak Power value and override with a new value.
Start Frequency	This option allows you to set or change the start point of a frequency range. Highlight the existing value and override it with a new value.
Stop Frequency	This option allows you to set or change the end point of a frequency range. Highlight the existing value and override it with a new value.

Note: You can get some rough idea about any parameter you highlight from the brief description at the bottom of the screen.

Spectrogram

The Spectrogram graph provides another way to present the same data as shown in the Real-Time FFT graph. It allows you to visualize the changes in the spectrum over a period of time and to easily identify any shift in frequency use and the duration of such shifts. The X-axis shows the frequency range covered by the selected radio band. The Y-axis shows in real time the number of sweeps the spectrum adapter scans the RF spectrum, which ranges from 0 to 100. Refer to the illustration below.



Each time the adapter scans the RF spectrum makes one sweep cycle, which is represented by a horizontal (colored) line across the spectrogram plot. The spectrogram scrolls dynamically upward as the application scans the spectrum. New data appear at the bottom of the graph while old data are constantly pushed to the top.

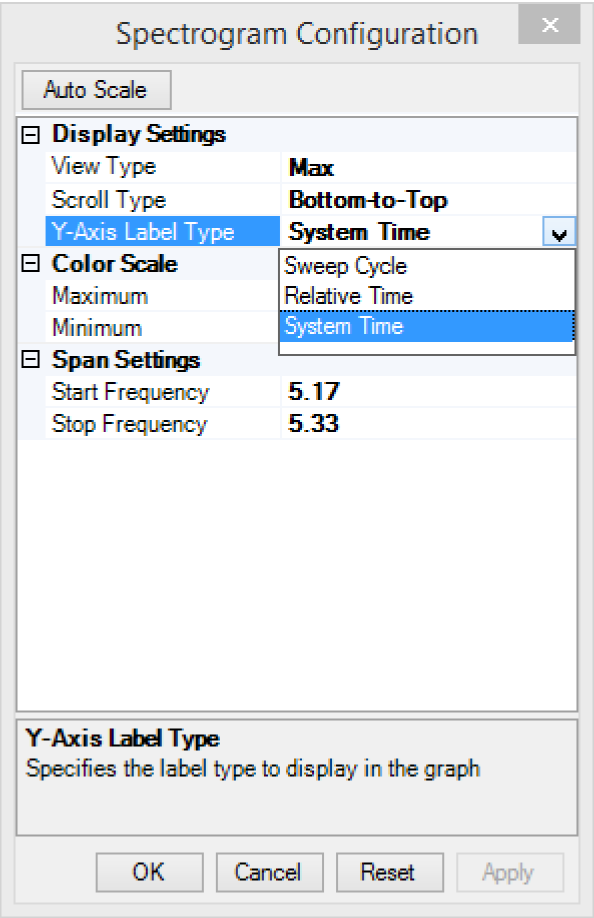
The sweep cycle values are mapped to a range of colors which corresponds to color range shown in the color legend in the upper-right corner of the graph. Blue represents the Minimum power values while red represents the Maximum power values.

Setting or Changing Spectrogram Parameters

You can change the settings of the Spectrogram using the **(Chart Configuration)** button in the upper-right corner of the Spectrogram graph.

To Change the settings of the Spectrogram graph:

1. Click the **Chart Configuration** button to open the Spectrogram Configuration window. Refer to the illustration below.



Display Settings
View Type: Max
Scroll Type: Bottom-to-Top
Y-Axis Label Type: System Time
Sweep Cycle
Relative Time
System Time

Color Scale
Maximum
Minimum

Span Settings
Start Frequency: 5.17
Stop Frequency: 5.33

Y-Axis Label Type
Specifies the label type to display in the graph

2. Make the selections and/or entries as described in the table below.
3. Click **Apply** and then **OK.**

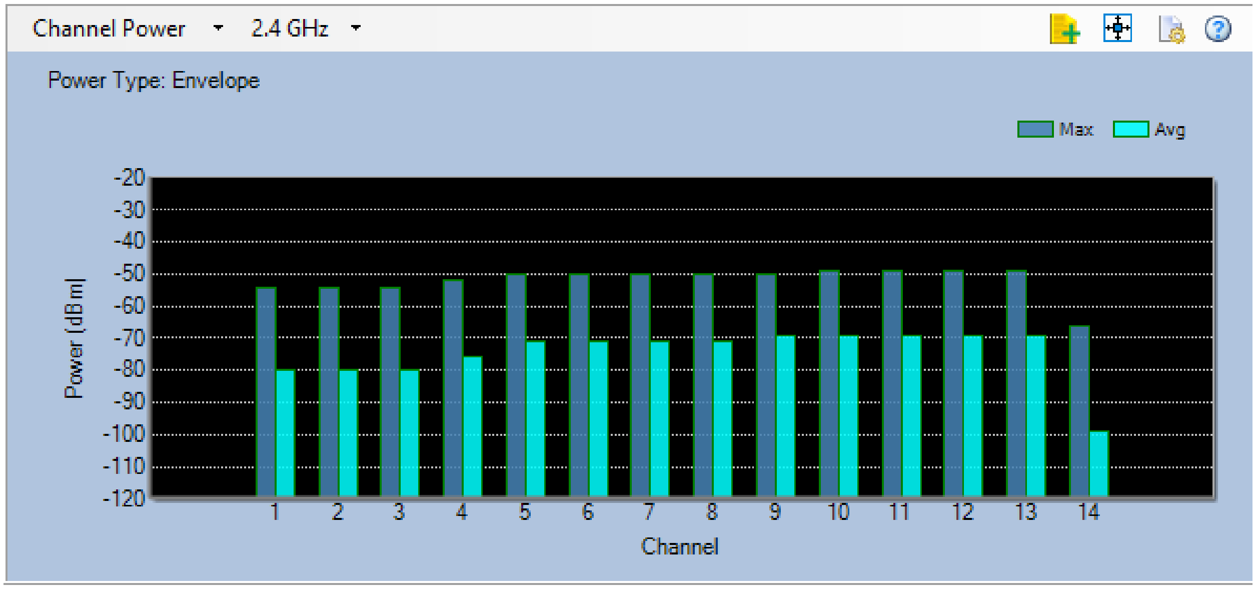
Parameter	Description
View Type	This option allows you to decide which type of spectrum data to be displayed on the Spectrogram. Click in the field and use the down arrow to select one of the following: ▪ Current - Plots Current power readings on the Spectrogram. ▪ Average - Plots the Average power readings on the Spectrogram. ▪ Maximum - Plots the Maximum power readings on the Spectrogram. ▪ Duty Cycle - Plots Duty Cycle readings on the Spectrogram.
Scroll Type	This option allows you to set the direction in which the graph scrolls (for example, up or down).
Y-Axis Label	This setting allows you to choose the type of data to be displayed on

Type	the Y-axis of the Spectrogram graph. There are three choices: ▪ Sweep Cycle - Shows the number of scans of the spectrogram. ▪ Relative Time - Shows the time relative to the start of either the Spectrum XT or a live capture session (which is 00:00:00 by default). For example, a value of 00:00:05 means five seconds after the start of the spectrogram, a value of 00:00:10 means 10 minutes after the start of the spectrogram, and so on. ▪ System Time - Shows the time of the system (that is, your laptop PC) on which Spectrum XT is running.
Maximum	This option allows you to set or change the maximum power value in dBm in the Spectrogram graph. By default, the Maximum Power value is -20, but you can change it to any value less than 0 dBm. The Maximum value appears on the right-hand end of the color scale. Any value that exceeds the set maximum will appear in red. Highlight the existing Maximum value and override with a new value.
Minimum	This option allows you to set or change the Minimum Power value in dBm in the Spectrogram graph. By default, the Minimum Power value is -100 dBm, but you can change it to any value as low as -140. The Minimum value Specify the minimum value of the color scale, which can be equal to or greater than -140 dBm.
Starting Frequency	This option allows you to set or change the start point of a frequency range. Highlight the existing value and override it with a new value.
Stop Frequency	This option allows you to set or change the end point of a frequency range. Highlight the existing value and override it with a new value.

Note: You can get some rough idea about any parameter you highlight from the brief description at the bottom of the screen.

Channel Power

The Channel Power graph shows the maximum and average power levels across all channels in the selected radio band. The X-axis shows all available channels for the selected radio band and the y-axis shows the rough energy readings. Refer to the illustration below.



The Channel Power can be defined either as Envelope or Integrated. Envelope power is defined as the maximum, or peak, energy level in a channel's frequency range. Integrated power is similar, and is defined as the average power of all frequency power levels in a channel's frequency range. In the bar chart, the Max bar corresponds to the Max data line on the FFT chart, while the Avg bar corresponds to the Average data line on the FFT graph.

With the chart set to the Envelope power type, the Max bar will show the dBm power of the strongest received signal within the 20MHz channel frequency width as recorded by the Max data line in the FFT chart, while the Avg bar will show the highest dBm value of the Average data line for the same channel frequency width.

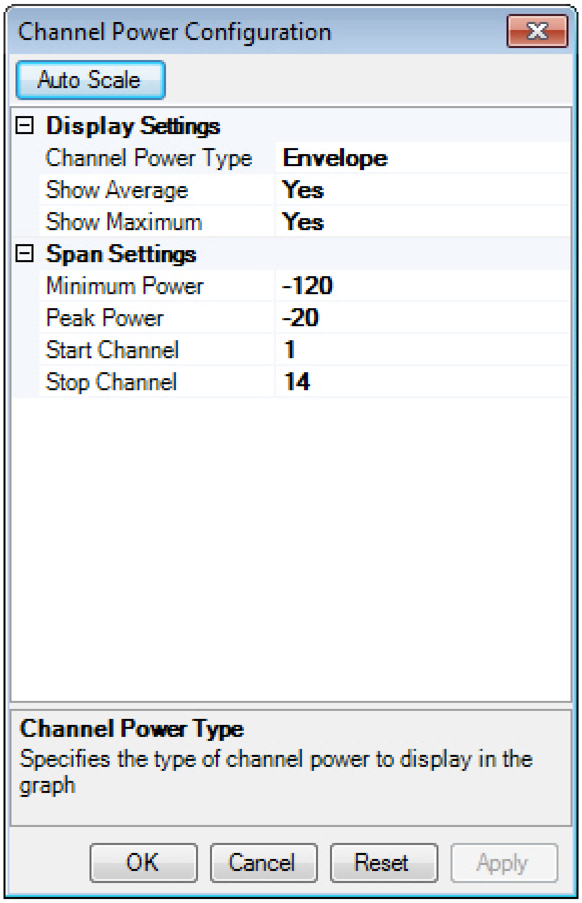
With the chart set to the Integrated power type, the application first samples the data from the Max and Average data lines in the FFT graph, then calculates the average power of all the sampled frequencies within the 20MHz channel frequency width. These values are then represented by the Max and Avg bars in the chart.

Note: If you place the cursor over a channel, a tooltip will pop up showing the Maximum and Average power readings on that channel.

Setting or Changing Channel Power Parameters

You can change the settings of the graph using the **(Chart Configuration)** button in the upper-right corner of the Channel Power graph.

1. Click the **Chart Configuration** button in the upper-right corner of the graph to bring up the Channel Power Configuration dialog box. Refer to the illustration below.



Display Settings

Channel Power Type	Envelope
Show Average	Yes
Show Maximum	Yes

Span Settings

Minimum Power	-120
Peak Power	-20
Start Channel	1
Stop Channel	14

Channel Power Type

Specifies the type of channel power to display in the graph

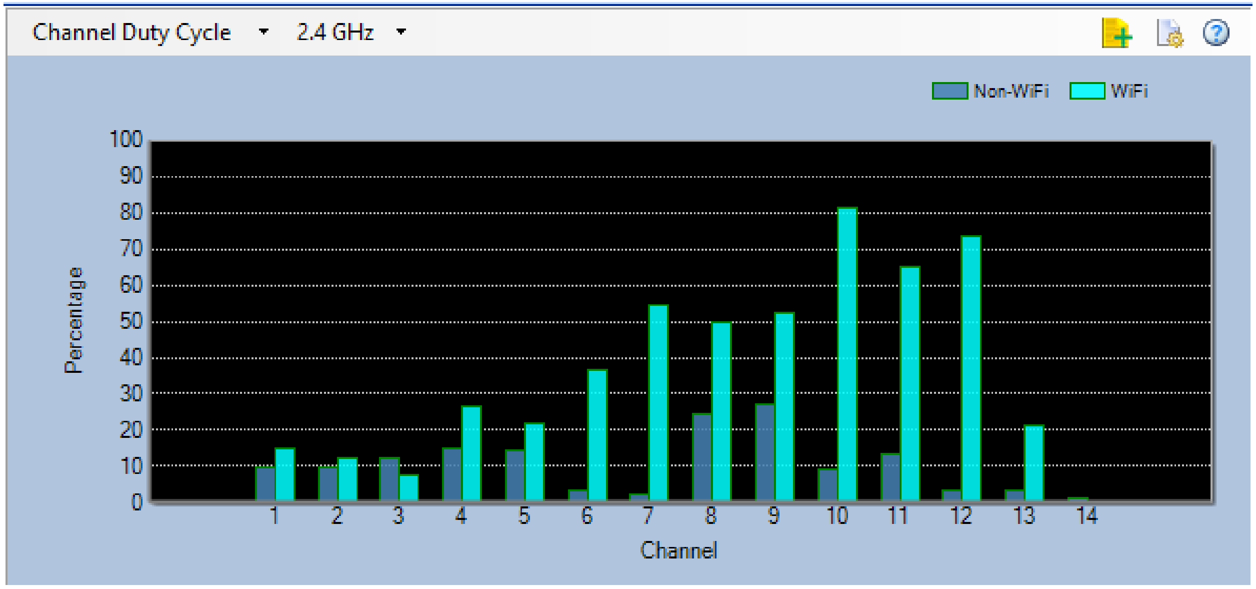
2. Make the selections and/or entries as described in the table below.
3. Click **Apply** and then **OK.**

Parameter	Description
Show Average	This option allows the user to show or hide the average power (aqua) readings in the graph. Click in the field and select one of the following: ▪ **True** - Shows the average power in the graph (default). ▪ **False** -Hides the average power in the graph.
Show Maximum	This option allows the user to show or hide the maximum power (blue) readings in the graph. Click in the field and select one of the following: ▪ **True** - Shows the maximum power in the graph (default). ▪ **False** - Hides the maximum power in the graph.
Channel Power Type	▪ **Envelope** - The highest energy reading that has been reached at a particular frequency with a frequency range. See the description at the top of the page. ▪ **Integrated** - The total summation of energy reading of an entire frequency range. Refer to the description at

	the top of the page.
Minimum Power	This option allows you to set or change the Minimum Power value in dBm in the Y-axis of the Spectrum Density plot. By default, the Minimum Power value is -120, but you can change it to any value as low as -140.
Peak Power	This option allows you to set or change the Peak Power value in dBm in the Y-axis of the Spectrum Density plot. By default, the Peak Power value is -20, but you can change it to any value less than 0 dBm. Highlight the existing Peak Power value and override with a new value.
Start Channel	This is the first channel in the range of channels to be selected. Highlight the existing value and override it with a new value.
Stop Channel	This is the last channel in the range of channels to selected. Highlight the existing value and override it with a new value.

Channel Duty Cycle

This screen shows the percentage of time that the RF energy is present in the channel above the noise floor. The duty cycle calculation is done by summing up the duration of all pulses that are detected within the bandwidth of a channel.   There are actually two accumulators, one for pulses that are determined to be 802.11 pulses and another for pulses that are not 802.11 packets. The WLAN duty factor (or channel utilization as we refer to it) is computed by dividing the accumulated 802.11 WLAN pulse time by the time the radio was dwelling on that channel. The non-WLAN duty factor is computed by dividing the accumulated time of non-WLAN pulses with the total channel dwell time. Refer to the illustration below.



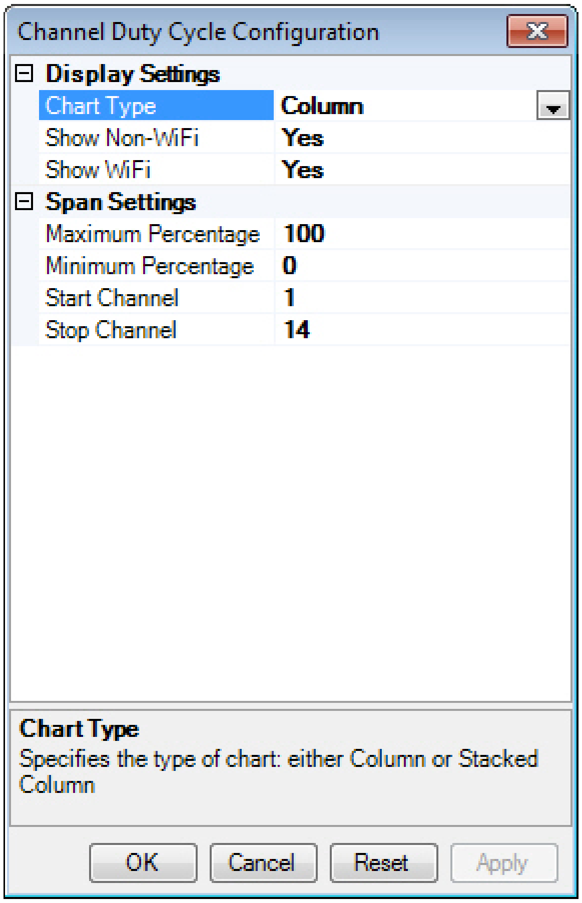
Note: If you place the cursor over a channel, a tooltip will pop up showing the Maximum and Current power readings on that channel.

Setting or Changing Channel Duty Cycle Graph Parameters

You can change the settings of the graph using the (**Configure**) button in the upper-right corner of the Channel Power graph.

To set or change Channel Duty Cycle graph parameters:

1. From the upper-right corner of the Channel Duty Cycle graph, click the **Configuration** button to bring up the Channel Duty Cycle Configuration dialog box.
2. Make the selections and/or entries as described in the table below.
3. Click **Apply** and then **OK.**



Channel Duty Cycle Configuration

⊟ **Display Settings**

Chart Type	**Column**
Show Non-WiFi	**Yes**
Show WiFi	**Yes**

⊟ **Span Settings**

Maximum Percentage	**100**
Minimum Percentage	**0**
Start Channel	**1**
Stop Channel	**14**

Chart Type
Specifies the type of chart: either Column or Stacked Column

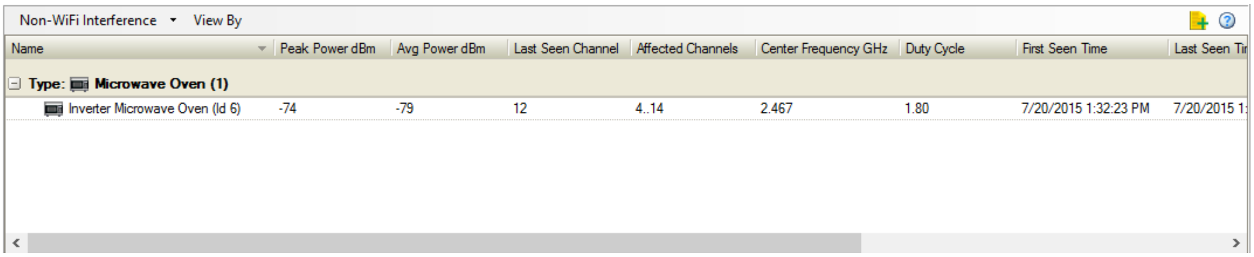
Parameter	Description
Chart Type	Toggles between column and stacked column displays. When viewing by stacked column, the data for Wi-Fi and non-Wi-Fi data will be

	displayed in a single column, with Wi-Fi data stacked on top of the non-Wi-Fi information.
Show Non-WiFi	Enables or disables display of non-W-iFi data.
Show WiFi	Enables or disables display of Wi-Fi data.
Maximum Percentage	The highest percentage value on the Y-axis. By default, the Maximum Percentage is 100. The application will discard any value that exceeds the Maximum Percentage. To change this value, highlight the existing value and override it with a new value.
Minimum Percentage	The lowest percentage value on the Y-axis. By default, it is 0, but you can change it to any value greater than 0. Any value below the set Minimum Percentage will be discarded. To change this value, highlight the existing value and override it with a new value.
Start Channel	This is the first channel in the range of channels to be selected. Highlight the existing value and override it with a new value.
Stop Channel	This is the last channel in the range of channels to selected. Highlight the existing value and override it with a new value.

Non-Wi-Fi Interference

The Non-Wi-Fi Devices table displays all non-Wi-Fi devices that the application has detected in the network environment. The devices are organized in the following categories:

- Bluetooth Devices
- Digital Cordless Phones
- Analog Cordless Phones
- Wireless Cameras
- Microwave Ovens
- Baby Monitors
- Digital Video Monitors
- Wireless Game Controllers
- RF Jammers
- Zigbee Devices
- Non-Bluetooth Wireless Mouse
- Motion Detector
- Radar



Name	Peak Power dBm	Avg Power dBm	Last Seen Channel	Affected Channels	Center Frequency GHz	Duty Cycle	First Seen Time	Last Seen Ti
⊟ **Type: Microwave Oven (1)**								
Inverter Microwave Oven (Id 6)	-74	-79	12	4..14	2.467	1.80	7/20/2015 1:32:23 PM	7/20/2015 1:

Non-WiFi Devices

The Non-WiFi Devices table shows the following information about each non-WiFi device that are listed:

- **Name (Device Type)** - The device category a device belongs to (refer to the bullet list above).

- **Peak Power dBm** - The highest energy reading in dBm ever recorded of device.

- **Avg Power dBm** - The average energy reading in dBm of the device.

- **First Seen Time** - The time when the device was detected for the first time.

- **Last Seen Time** - The most recent time when the device was detected.

- **Event Count** - The number of times the device was detected (refer to the Event Spectrogram).

- **Last Seen Channel** - The channel on which the device was last detected.

- **Affected Channels** - Channels that are affected by the device.

- **Center Frequency GHz** - The center frequency used by the device.

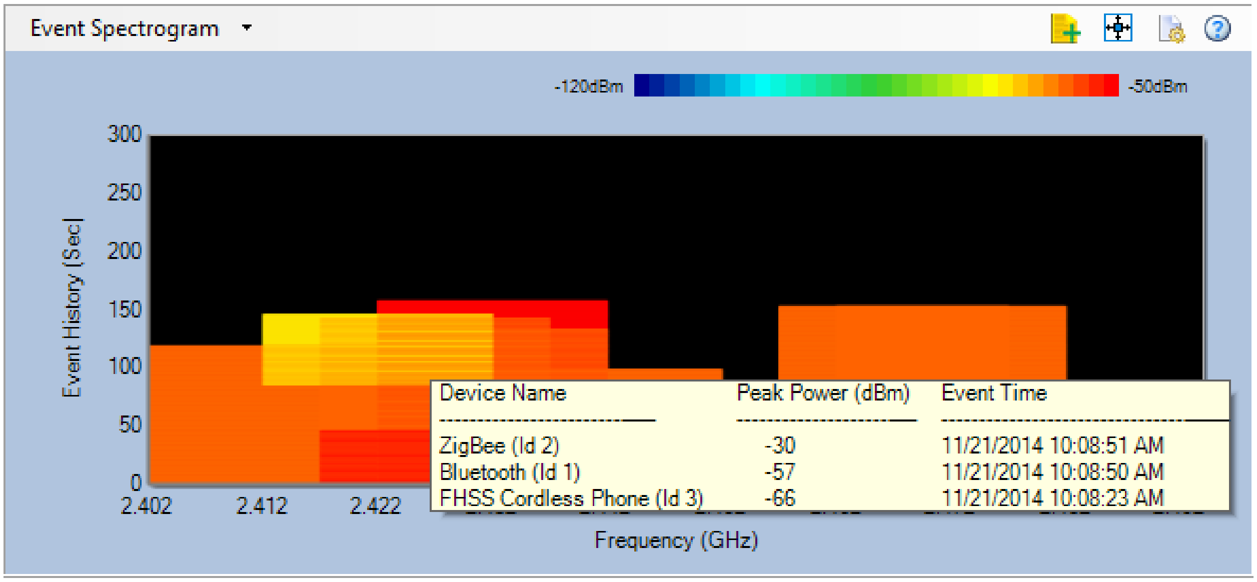
- **Duty Cycle** - The percentage of time that the RF energy is present in the channel above the noise floor.

- **Is Active** - Indicates if the device is active or not. You’ll see a check mark if it is active, or a cross mark if otherwise.

- **Is Hopping** - Indicates if the device is a frequency-hopping device. You’ll see a check mark if it is a frequency-hopping device, or a cross mark if it is otherwise.

Event Spectrogram

The Event Spectrogram provides a visual presentation of real-time information about events (device detections) that the application has made in the network. Each detection is an event which is represented by a color band. The color of the band indicates the signal strength of the device being detected (refer to the signal scale on top of the graph). If more detections are made of the same device as the application sweeps the spectrum, the band will become thicker (taller). The height of the color band indicates the (length of time in seconds the device has been detected. It stops increasing when the device becomes inactive (meaning that the device has not been detected for a minute). The width of the line/band indicates the channels or frequencies being affected by the device. If the device is a frequency-hopping device, then the band may extend sideways as the device hops from one channel to another.



Device Name	Peak Power (dBm)	Event Time
ZigBee (Id 2)	-30	11/21/2014 10:08:51 AM
Bluetooth (Id 1)	-57	11/21/2014 10:08:50 AM
FHSS Cordless Phone (Id 3)	-66	11/21/2014 10:08:23 AM

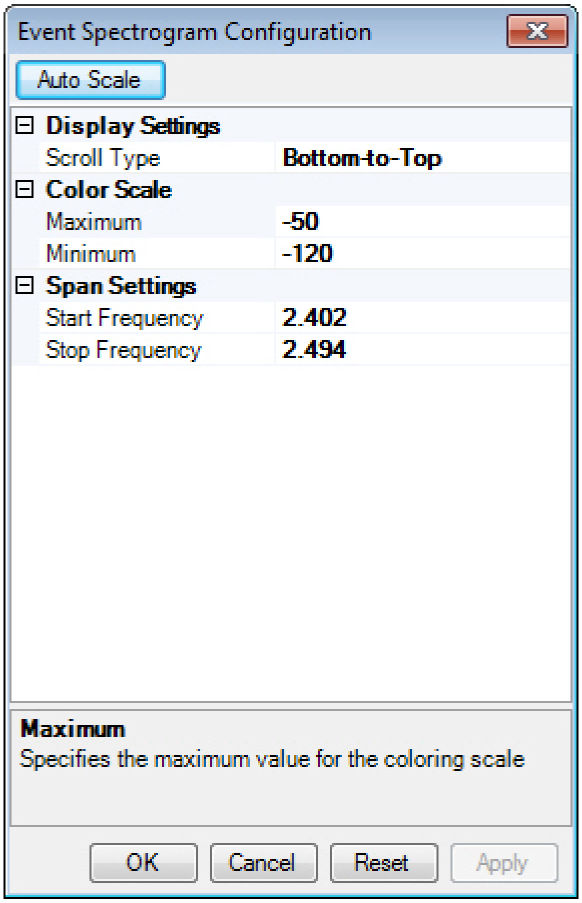
Note: If you place the cursor over the line/band, a tooltip will pop up showing some basic information about that device, such as the type of the device, its peak power, and the time of it being detected.

Configuring Event Spectrogram

In the upper-right corner of the plot is a configuration button which allows you to configure and change a number of parameters in the Event Spectrogram plot.

To set or change parameters in the Event Spectrogram plot:

1. Click (**Chart Configuration**). The Event Spectrogram Configuration dialog box opens. Refer to the illustration below.



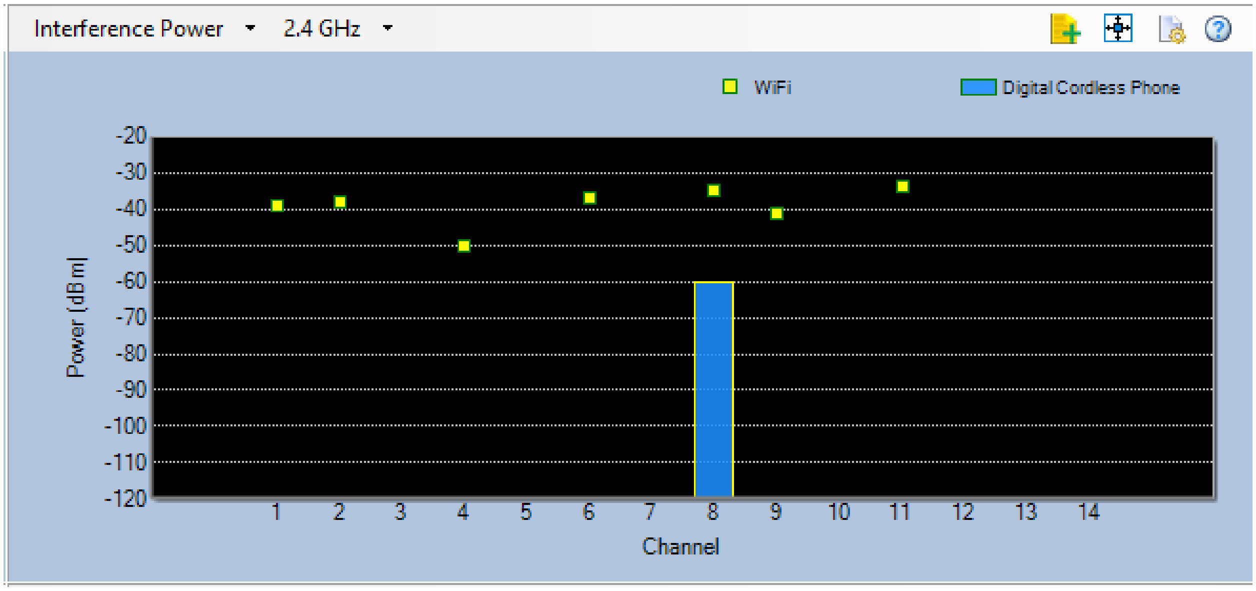
⊟ **Display Settings**	
Scroll Type	**Bottom-to-Top**
⊟ **Color Scale**	
Maximum	**-50**
Minimum	**-120**
⊟ **Span Settings**	
Start Frequency	**2.402**
Stop Frequency	**2.494**

Maximum
Specifies the maximum value for the coloring scale

2. Make the desired changes to the following parameters:
   - **Maximum** - The maximum energy level to show in the Event Spectrogram, which is on the red end of the color legend.
   - **Minimum** - The minimum energy level to show in the Event Spectrogram, which is on the blue end of the color legend.
   - **Start Frequency** - The lowest frequency of the frequency range.
   - **Stop Frequency** - The highest frequency of the frequency range.
3. Click **OK** when done.

Interference Power

The Interference Power chart provides a quick display of all devices, both Wi-Fi and non-Wi-Fi, that are causing potential interference in the wireless spectrum. Using this function, you can quickly identify which channels are experiencing unusually high levels of network interference and plan or adjust the deployment accordingly.



As noted in the color legend above the main portion of the chart, the yellow points on the graph represent the current signal strength of the strongest AP detected on each channel; hovering over the point provides the device's name and MAC address. The point's location on the chart indicates the level of interference that it is experiencing; as the interference level climbs, the device's performance can suffer as a result.

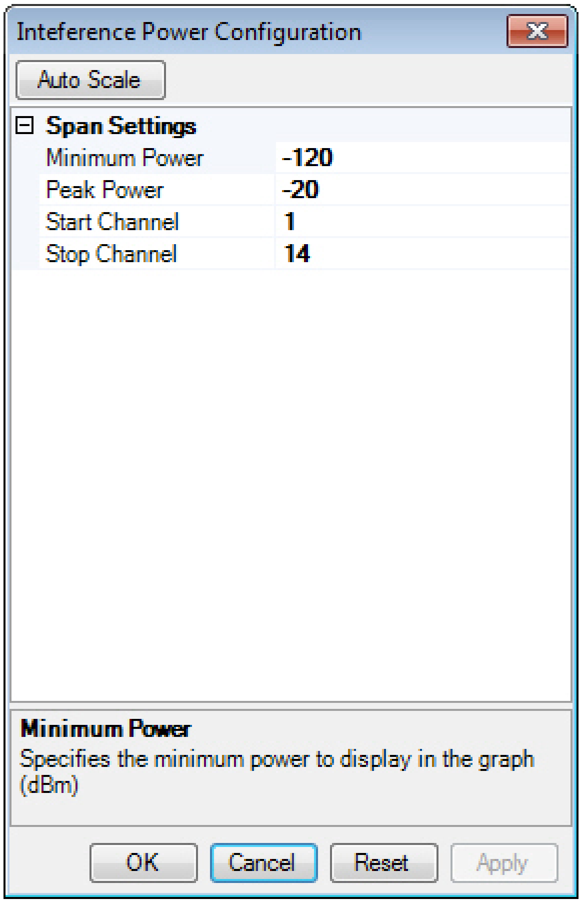
Non-Wi-Fi devices are color-coded to make it easy for users to quickly assess which devices are present at any given time. Hovering over the color bar of a given interferer provides a pop-up display that indicates the level of interference caused by the device as well as the device's type (if known).

Configuring the Interference Power Display

In the upper-right corner of the plot is a configuration button which allows you to configure and change a number of parameters in the Interference Power plot.

To set or change parameters in the Interference Power plot:

1. Click the **Chart Configuration** button in the upper-right corner. The Interference Power Configuration dialog box opens.



Inteference Power Configuration

Span Settings

Minimum Power	-120
Peak Power	-20
Start Channel	1
Stop Channel	14

Minimum Power
Specifies the minimum power to display in the graph (dBm)

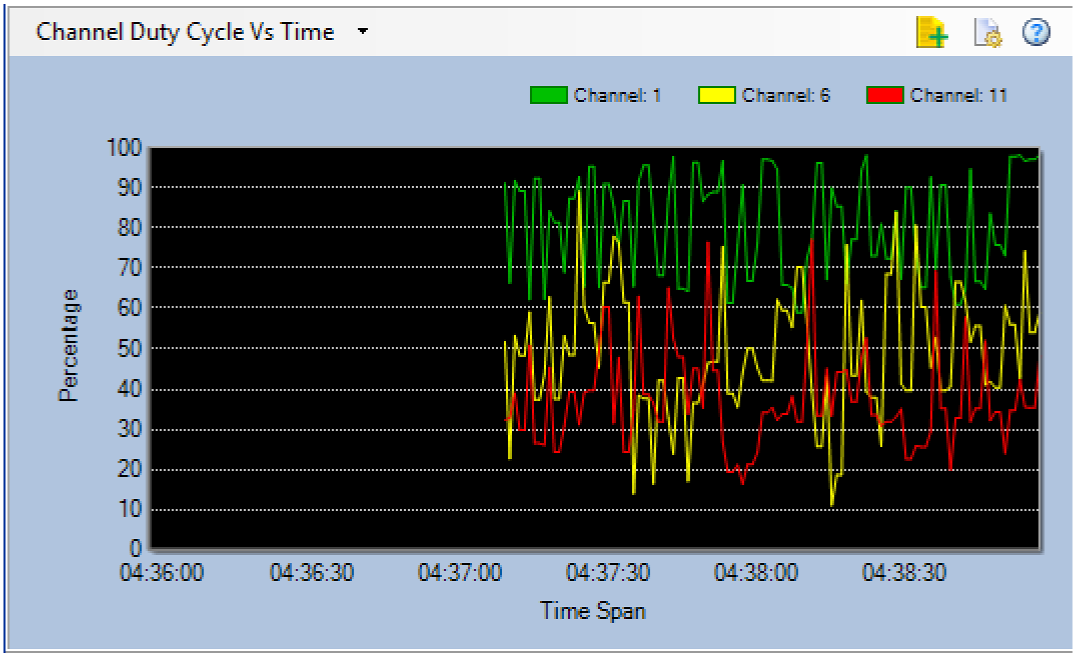
2. Make the desired changes to the following parameters:

- **Minimum Power**—The minimum power level that will be displayed on the graph.
- **Peak Power**—The maximum power level that will be displayed on the graph.
- **Start Channel**—The first channel that will be displayed.
- **Stop Channel**—The last channel that will be displayed.

3. Click **OK** when done

Channel Duty Cycle vs Time

The Channel Duty Cycle vs Time graph shows the recorded duty cycle over the course of time, allowing you to easily identify channels that are experiencing a high percentage of traffic steadily over for an extended period. The X-axis shows the amount of time elapsed and the Y-axis displays the duty cycle percentage.



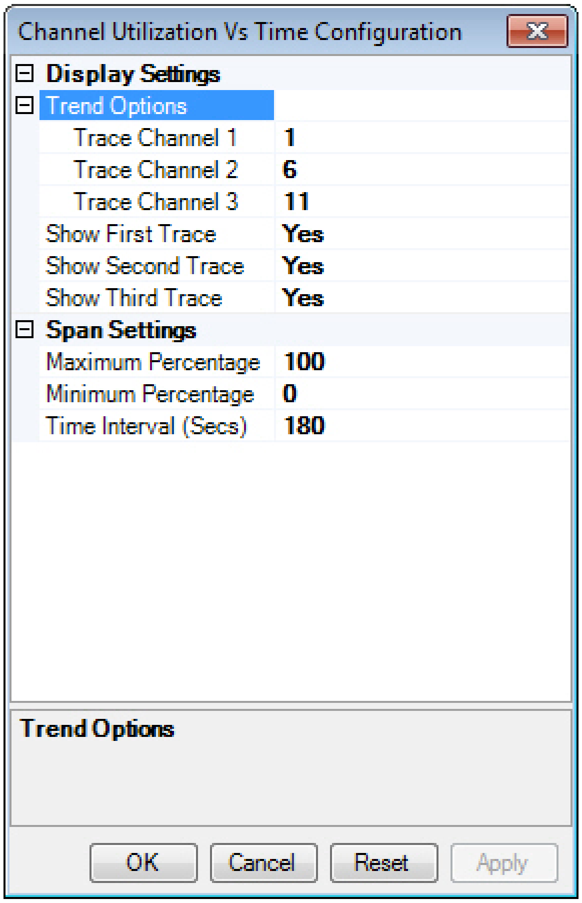
As shown above, the graph will display up to three channels at a time in color-coded lines. The channels can be modified via the chart configuration, as explained below.

Configuring Channel Duty Cycle vs Time

You can set or change the parameters in the Channel Duty Cycle vs Time graph using the Chart Configuration button.

To configure Channel Duty Cycle vs Time graph parameters:

1. From the upper-right corner of the graph, click **Chart Configuration**. The Channel Duty Cycle vs Time Configuration dialog box appears.



⊟ Display Settings

⊟ Trend Options

Trace Channel 1	1
Trace Channel 2	6
Trace Channel 3	11
Show First Trace	Yes
Show Second Trace	Yes
Show Third Trace	Yes

⊟ Span Settings

Maximum Percentage	100
Minimum Percentage	0
Time Interval (Secs)	180

Trend Options

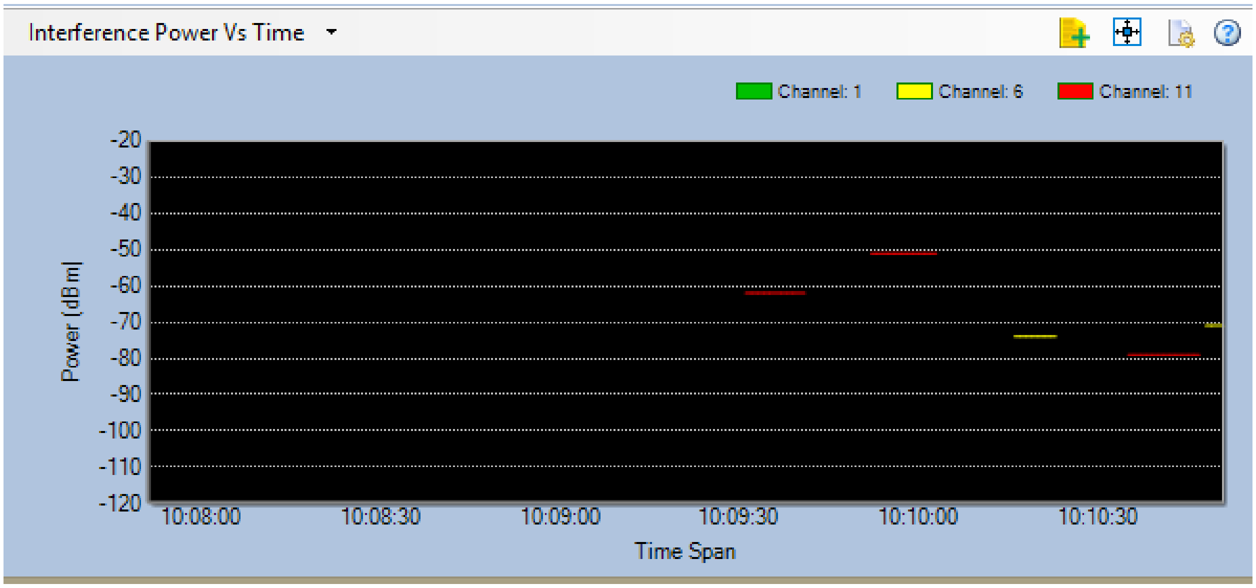
2. Make the desired selections and/or entries as described in the table below.
3. Click **Apply** and then **OK**.

Parameter	Description
Trend Options	Use these fields to specify the channels that should be displayed in the graph. You can select up to three channels at any single time.
Show First/Second/Third Trace	These fields activate or deactivate the trace options specified in the first portion of the configuration. Select 'Yes' to activate (for example., display) each trace as needed. Selecting 'No' will remove the trace from the graph.
Maximum Percentage	Allows you to specify the maximum percentage to be displayed in the graph. Highlight the existing value and then override it with a new value.

Minimum Percentage	Allows your to specify the minimum percentage to be displayed in the graph. Highlight the existing value and then override it with a new value.
Time Interval (Secs)	The maximum number of seconds that will be displayed on the chart at any given time.

Interference Power vs. Time

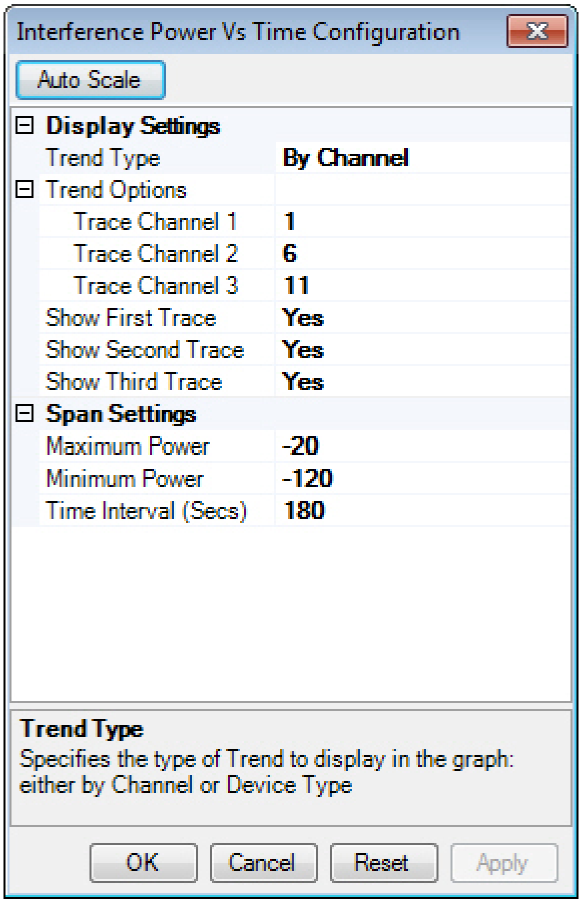
The Interference Power vs. Time graph provides a visual representation of the length of time in which interferers are active. This graph displays non-Wi-Fi interference only, and can help you identify non-802.11 interferers that are active consistently over time.



By default, the graph is set to display interferers separated into individual channels, allowing you to troubleshoot problems on up to three channels at a time. This configuration can be modified, however, to display lines for each interferer present instead, making it significantly easier to identify multiple sources of interference as well as their impact on the network. Hovering over the lines in the graph provides additional details regarding the information displayed, including interference level and the type of interferer (if known).

Configuring the Interference Power vs Time Graph

As mentioned above, the configuration menu for the Interference Power vs Time graph allows the user to alternate between displaying interference data by channel and by device type. Refer to the table below for specific options that can be configured in the graph, as shown below.



⊟ **Display Settings**

Trend Type	By Channel

⊟ Trend Options

Trace Channel 1	1
Trace Channel 2	6
Trace Channel 3	11
Show First Trace	Yes
Show Second Trace	Yes
Show Third Trace	Yes

⊟ **Span Settings**

Maximum Power	-20
Minimum Power	-120
Time Interval (Secs)	180

Trend Type
Specifies the type of Trend to display in the graph: either by Channel or Device Type

Parameter	Description
Trend Type	Select whether to display data by channel or by device as desired.
Trend Options	Depending on the selection made in the Trend Type field, these fields allow you to select the channels or devices that should be displayed.
Show First/Second/Third Trace	These fields activate or deactivate the trace options specified in the first portion of the configuration. Select 'Yes' to activate for example, display) each trace as needed. Selecting 'No' will remove the trace from the graph.
Maximum Power	Allows you to specify the maximum power to be displayed in the graph. Highlight the existing value and then override it

	with a new value.
Minimum Power	Allows you to specify the minimum power to be displayed in the graph. Highlight the existing value and then override it with a new value.
Time Interval (Secs)	The maximum number of seconds that will be displayed on the chart at any given time.

BlueSweep Integration

BlueSweep is designed to identify nearby devices using Bluetooth wireless technology and alert you to potential Bluetooth security risks. It identifies and tracks devices up to 300 feet away and informs you of the activity of their own Bluetooth devices.

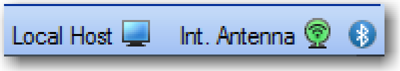
Additional Bluetooth Analysis

AirMagnet Spectrum XT offers enhanced Bluetooth interferer information using an optional Windows-compatible Bluetooth adapter. The enhanced information includes details on the name, ID, services, and so on. for Bluetooth devices.

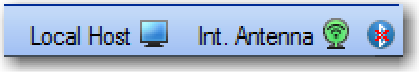
You can either use the Bluetooth adapter that is built into their PC or you can use an external adapter.

Note: We recommend that you always use the Microsoft driver for Bluetooth devices instead of the vendor-supplied driver. Refer to the Microsoft's website to obtain drivers.

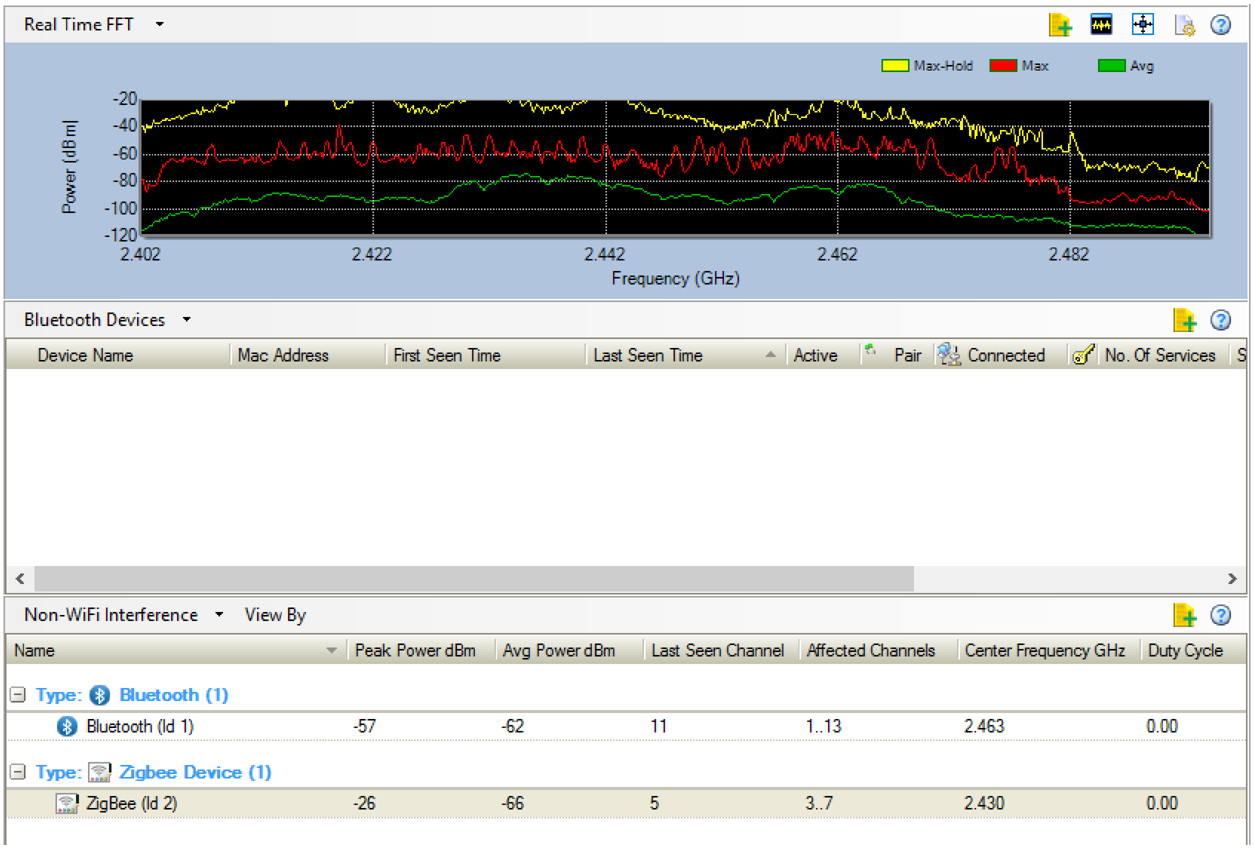
For effective customized signature detection and classification, we recommend that you not insert the optional Bluetooth adapter at the same time.



BlueSweep Active



BlueSweep Inactive



Device Name	Mac Address	First Seen Time	Last Seen Time	Active	Pair	Connected	No. Of Services	S

Name	Peak Power dBm	Avg Power dBm	Last Seen Channel	Affected Channels	Center Frequency GHz	Duty Cycle
⊟ Type: Bluetooth (1)						
Bluetooth (Id 1)	-57	-62	11	1..13	2.463	0.00
⊟ Type: Zigbee Device (1)						
ZigBee (Id 2)	-26	-66	5	3..7	2.430	0.00

BlueSweep Integration Screen

Analyzing WiFi Data

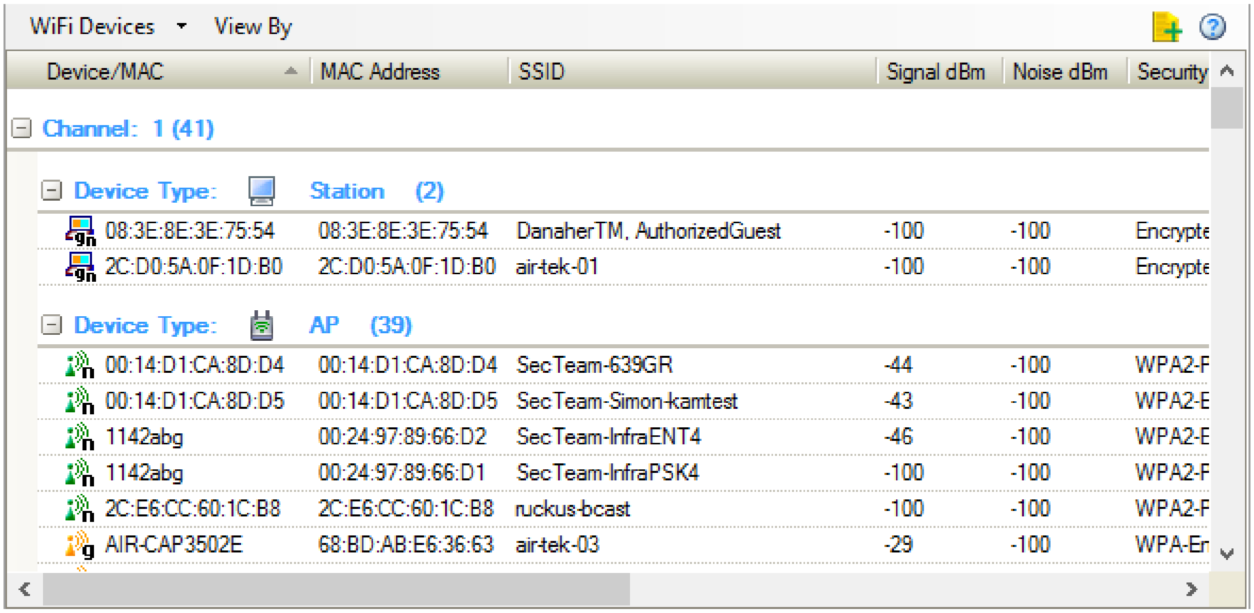
WiFi Graphs

When an AirMagnet-supported Wi-Fi adapter is used, the application is able to capture and display the following Wi-Fi data:

- Wi-Fi Devices
- AP Signal Strength
- Channel Occupancy
- Channels by Speed
- Channels by Media
- Channels by Address
- Channel Utilization
- Top 10 APs by Speed
- Top 10 Active APs' Retry/CRC
- Channel Signal/Noise Ratio
- Channels by Retry/CRC

WiFi Devices

The WiFi Devices graph (table) option shows all Wi-Fi devices that AirMagnet Spectrum XT has detected on all available channels in the selected radio band. The devices are displayed by channel. Like the Channel Usage section, channels with no devices detected on them will not be listed in the WiFi Devices table. Within the same channel, the devices are then organized in three groups: AP, Station, and Phone. If no device has been detected for a certain group, then the group will not be listed either. Refer to the illustration below.



Device/MAC	MAC Address	SSID	Signal dBm	Noise dBm	Security
Channel: 1 (41)					
Device Type: Station (2)					
08:3E:8E:3E:75:54	08:3E:8E:3E:75:54	DanaherTM, AuthorizedGuest	-100	-100	Encrypte
2C:D0:5A:0F:1D:B0	2C:D0:5A:0F:1D:B0	air-tek-01	-100	-100	Encrypte
Device Type: AP (39)					
00:14:D1:CA:8D:D4	00:14:D1:CA:8D:D4	SecTeam-639GR	-44	-100	WPA2-F
00:14:D1:CA:8D:D5	00:14:D1:CA:8D:D5	SecTeam-Simon-kamtest	-43	-100	WPA2-E
1142abg	00:24:97:89:66:D2	SecTeam-InfraENT4	-46	-100	WPA2-E
1142abg	00:24:97:89:66:D1	SecTeam-InfraPSK4	-100	-100	WPA2-F
2C:E6:CC:60:1C:B8	2C:E6:CC:60:1C:B8	ruckus-bcast	-100	-100	WPA2-F
AIR-CAP3502E	68:BD:AB:E6:36:63	air-tek-03	-29	-100	WPA-Er

The following information is provided for each device:

- **Device/MAC -** This can be a device's name or MAC address, or a combination of vendor name and partial MAC address of a device (depending on the option that has been selected using **Settings>General>WiFi Devices**).
- **MAC Address -** A device's MAC address.
- **SSID -** A device's SSID.
- **Signal dBm -** A device's signal strength in dBm.
- **Noise dBm -** A device's noise level.
- **Security -** The security mechanism used on a device.
- **Bandwidth MHz -** The max channel bandwidth supported by the device.
- **First Frame Time -** The time the first frame involving a device was detected.
- **Last Frame Time -** The time the last frame involving a device was detected.
- **AP Name** - The name of the AP itself or of the one that provides service to a station or phone.

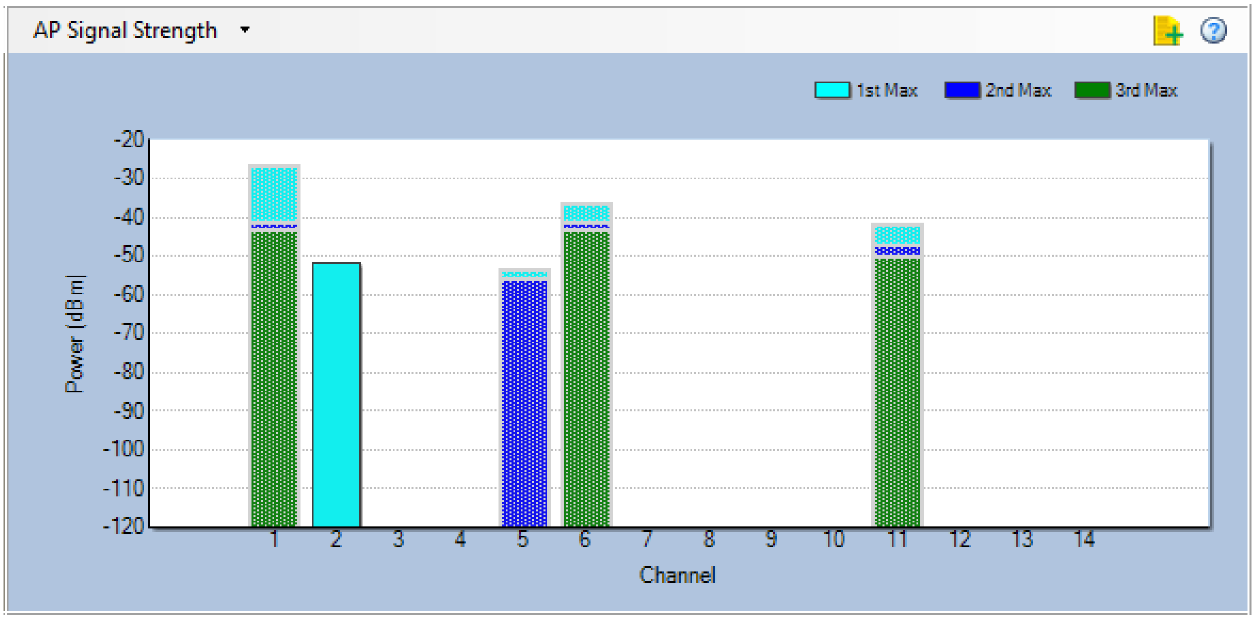
Since the WiFi Devices graph contains a great deal of data that require a lot of screen space, you may need to custom AirMagnet Spectrum XT's user interface in a way to make it easy for you to view Wi-Fi device data. You can customize your screen space by doing either or both of the following, depending on your screen resolution:

- Hide the entire **Spectrum-WiFi Summar**y section by clicking **(AutoHide).**
- From the toolbar, click **Settings** and then uncheck (hide) all the graphs except for the one that corresponds to the WiFi Devices graph.

Note: Even though that the screen can display three categories of devices (that is, station, AP, and phone), a category does not show on the screen if no device in that category has been detected. Also, the order in which data are presented in the WiFi Devices graph can be changed. All you need to do is to drag and drop, one at a time, the title of a column to where you want it to be.

AP Signal Strength

The AP Signal Strength graph displays the three APs with the strongest signal strength readings on each channel in the selected radio band. The X-axis shows all available channels in the radio band, and the Y-axis shows AP signal strength readings in dBm. Refer to the illustration below.



AP signal strength readings are color-coded as follows:

- Aqua = 1st Max (the AP with the highest signal strength recorded).
- Blue = 2nd Max (the AP with the second highest signal strength recorded).
- Green = 3rd Max (the AP with the third highest signal strength recorded).

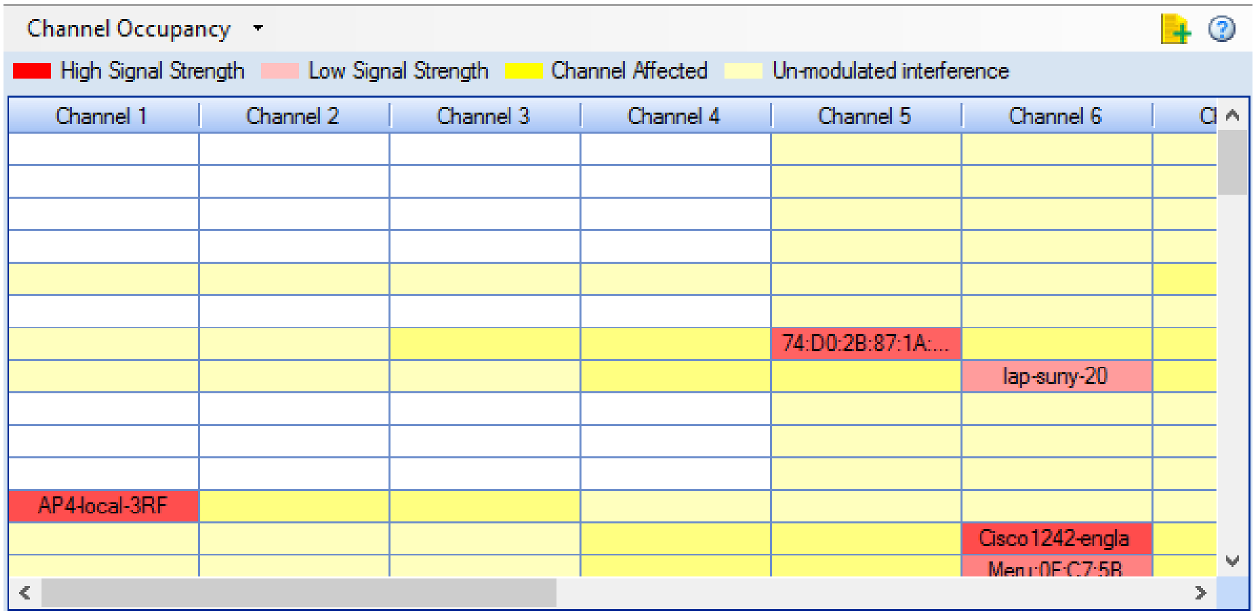
If you place the cursor over a portion of a channel bar marked by any of the colors, a tip screen will appear showing the information about the AP:

- **MAC Address -** The MAC address of the AP.
- **AP -** Which can be the AP's name, the combination of the AP's vendor name and part of its MAC address, or the AP's MAC address (depending on the option you have selected using **Settings>General>WiFi Devices**).
- **Signal Strength** - The signal strength of the AP being recorded.

Note: When you select a specific channel in the Channel Summary pane (in the upper-left corner of the screen), all channel bars in the graph will become tinted except the one corresponding to the channel being selected. This helps you focus on the channel being selected. You can find more information about APs on any of these channels by selecting WiFi Devices from the drop-down list menu in the upper left corner of the graph.

Channel Occupancy

The Channel Occupancy graph shows all the available channels for the selected radio band and which APs are occupying which channels. Refer to the illustration below.



Channel 1	Channel 2	Channel 3	Channel 4	Channel 5	Channel 6	Cl
				74:D0:2B:87:1A:...		
					lap-suny-20	
AP4-local-3RF						
					Cisco1242-engla	
					Meru:0F:C7:5B	

As seen from the illustration above, each column represents a channel. Each row represents one AP. The fields can be one of the following colors:

- Red = High signal strength of APs identified by name or SSID.
- Light Red = Low signal strength of APs identified by name or SSID.
- Yellow = Channels affected by the modulated inference from APs in the center frequencies.
- Light Yellow = Channels affected by unmodulated interference from APs in the center frequencies.

Based on the information presented on the screen, you can then reallocate your APs to optimize their performance. The information is very helpful for making AP channel allocation decisions to optimize AP performance.

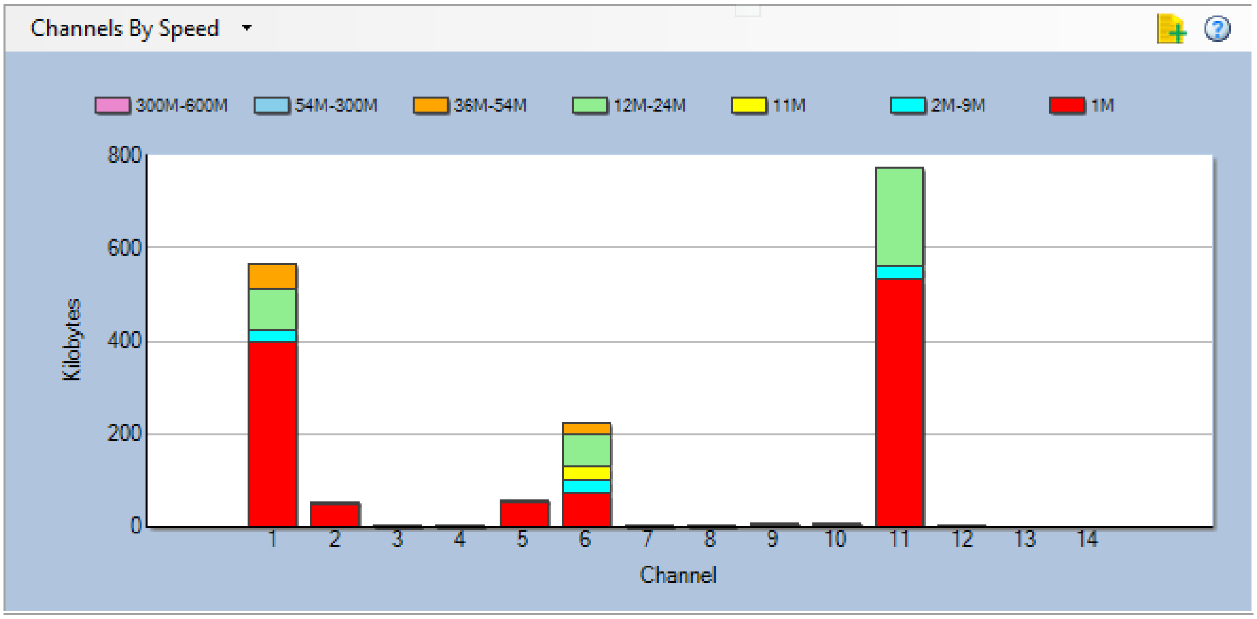
Note: Modulated interference refer to interference that occurs within a device's modulated spectrum (that is, within the device's operating channel width), whereas unmodulated interference refers to interference caused by the "bleed over" of signals beyond the modulated portion of the transmission.

Like the WiFi Devices graph, the Channel Occupancy graph requires more screen space to display its content. Therefore, you may need to custom AirMagnet Spectrum XT's user interface in a way to make it easy for you to view the data. You can custom your screen space by doing either or both of the following, depending on your screen resolution:

- Hide the entire **Spectrum-WiFi Summary** section by clicking **(AutoHide).**
- Click **Settings** and then uncheck all graphs except for the one that corresponds to the Channel Occupancy graph.

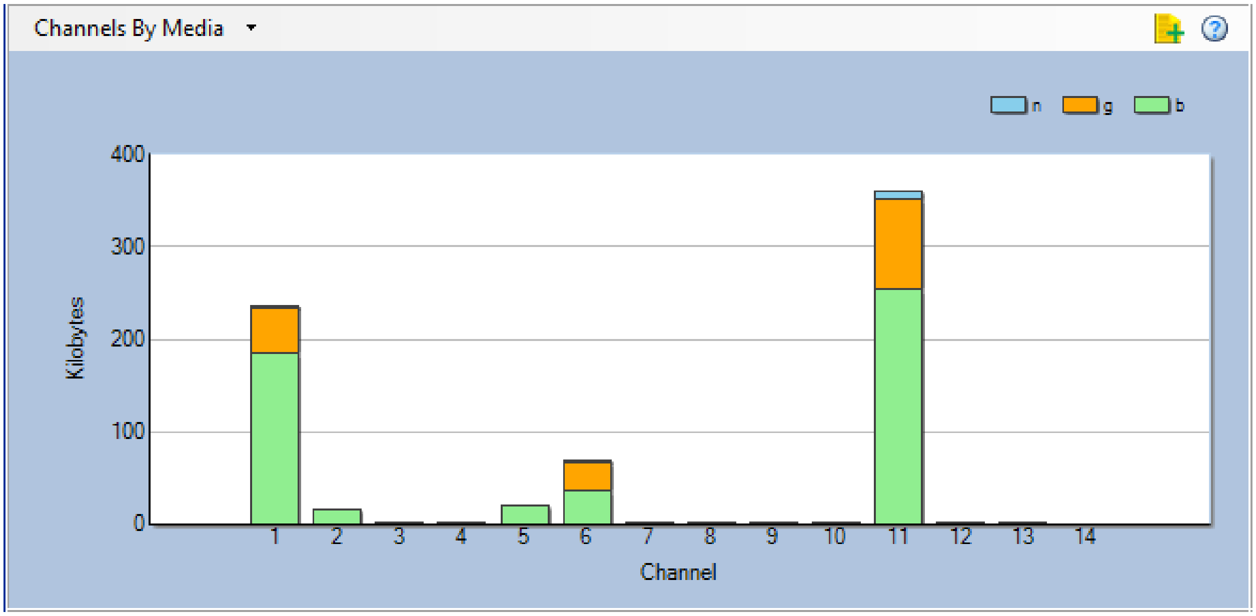
Channels by Speed

The Channels by Speed graph displays the relative amount of data (in kilobytes) that has been transmitted at each data rate on each available channel in the selected radio band. The X-axis shows all available channels in the radio band and the data rate used on each channel, whereas the Y-axis shows the amount of the data (in kilobytes) transmitted on each channel as well as a visual breakdown by data rate of the volume of data being transmitted. Refer to the illustration below.



Channels by Media

The Channels by Media graph shows that volume of Wi-Fi transmissions in kilobytes recorded on each channel in the selected radio band. It also provides a rough breakdown by 802.11 media type of the transmission on each channel. The X-axis shows all available channels in the selected band and the types of media used for the transmission; the Y-axis shows the volume of transmission in kilobytes. Refer to the illustration below.



Each bar in the Channels by Media graph represents the total amount of data in kilobytes that has been transmitted on a channel. Wi-Fi traffic is categorized by the type of 802.11 media being used.

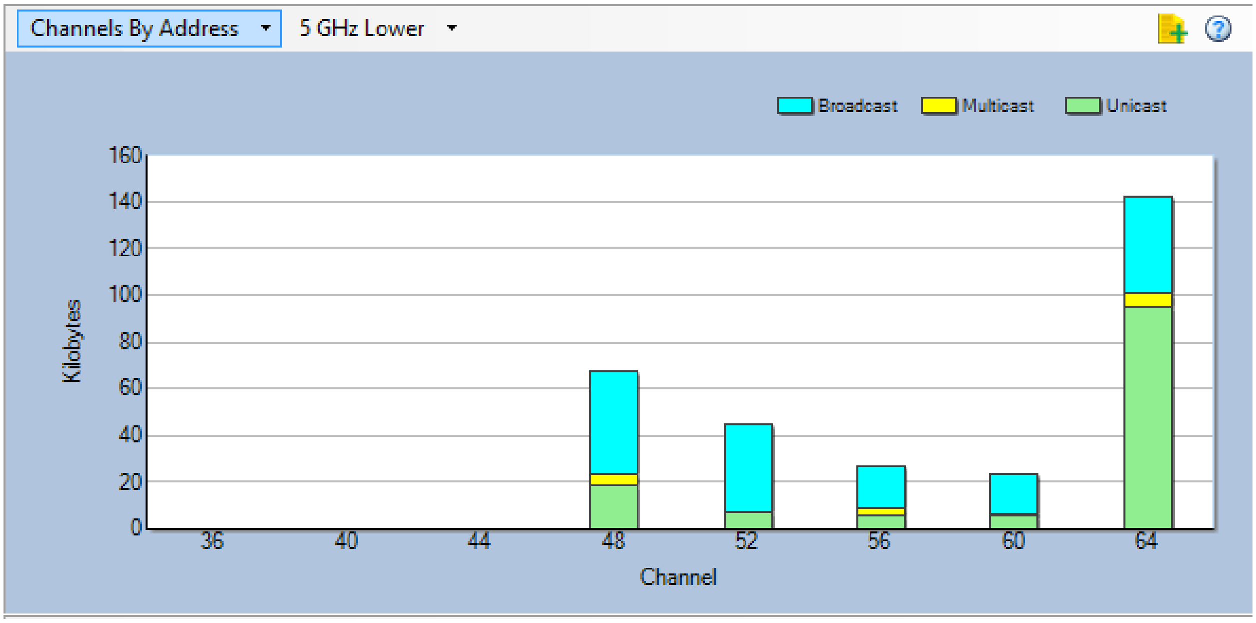
The 802.11 media are broken down into the following categories, each represented by a unique color:

- Purple = 802.11ac
- Blue = 802.11n
- Orange = 802.11g
- Green = 802.11b
- Aqua = 802.11a

Note: If you place the cursor over a channel, a tip screen will pop up showing the volume of data transmitted using each type of media.

Channels by Address

The Channels by Address graph shows the volume of data transmission in kilobytes that has been recorded on each channel in the selected radio band. It also provides a rough breakdown of the transmission by the type of address (that is, broadcast, multicast, and unicast) that was used for the transmission. The X-axis shows the available channels and the type of address on each channel; the Y-axis shows the volume of data in kilobytes being transmitted. Refer to the illustration below.



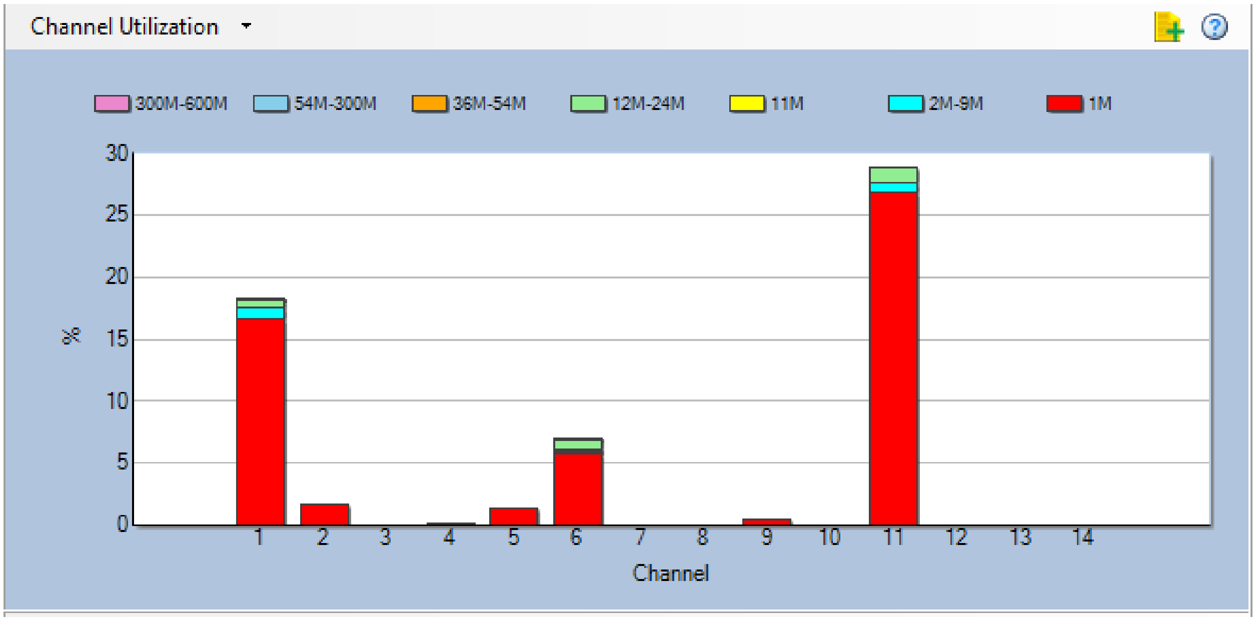
The traffic is broken down into three categories, each represented by a unique color:

- **Broadcast** - The process of sending the same data to all stations on the network.
- **Multicast** - The process of sending a single message to multiple destinations simultaneously. It is a one-to-many transmission similar to broadcasting, except that multicasting means transmission to specific groups, whereas broadcasting implies sending to everybody. Multicasting can save considerable bandwidth when sending large volumes of data because the bulk of the data is transmitted once from the source through major backbones and are multiplied, or distributed out, at switching points closer to the recipients.
- **Unicast** - The process of sending duplicates of the same message to multiple destinations on the network. In unicast, even though multiple users might request the same data from the same server at the same time, duplicate data streams are transmitted, one to each destination.

Note: If you place the cursor over a channel, a tool tip will pop up showing the volume of transmission carried by each address type.

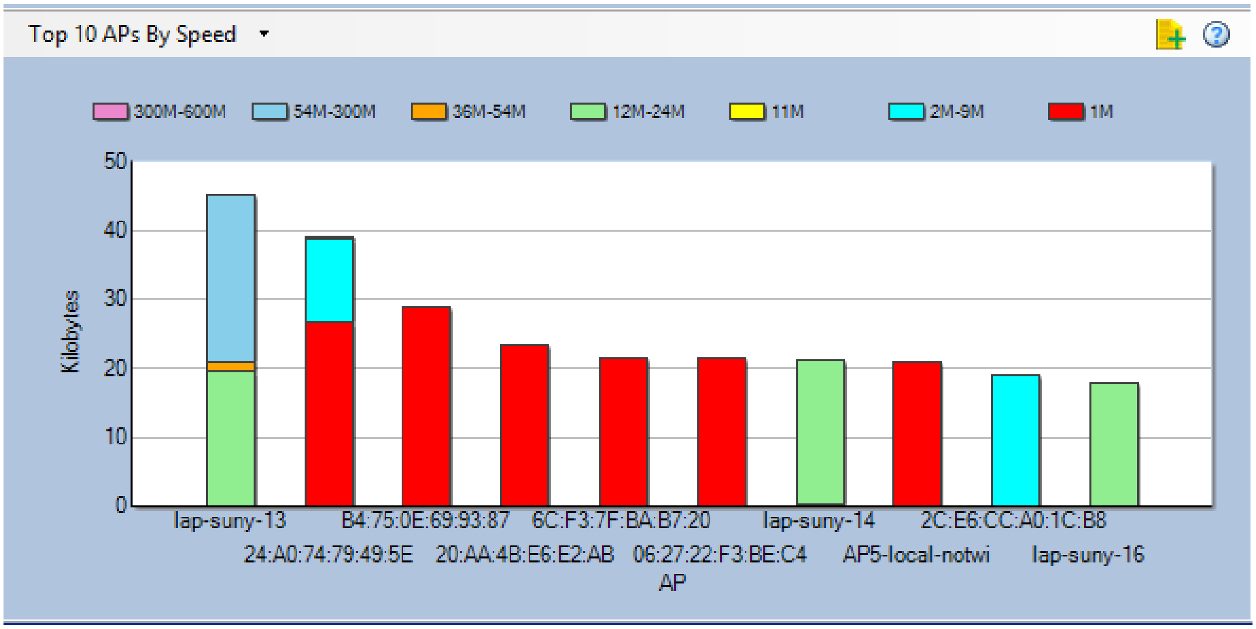
Channel Utilization

The Channel Utilization graph shows the percentage of bandwidth being used on each channel and the breakdown of the utilization by transmission rate. The X-axis shows all available channels for the selected radio band as well as the transmission rates being used on each channel; the Y-axis shows the overall percentage of bandwidth being used on each channel. Refer to the illustration below.



Top 10 APs by Speed

The Top 10 APs by Speed graph shows the 10 APs that have transmitted the most amount of data (in kilobytes) as well as the breakdown of the transmissions by data rate on each AP. The X-axis shows the names of the top 10 APs and the transmission rates being used by the APs; the Y-axis shows the volume of data in kilobytes being recorded. Refer to the illustration below.

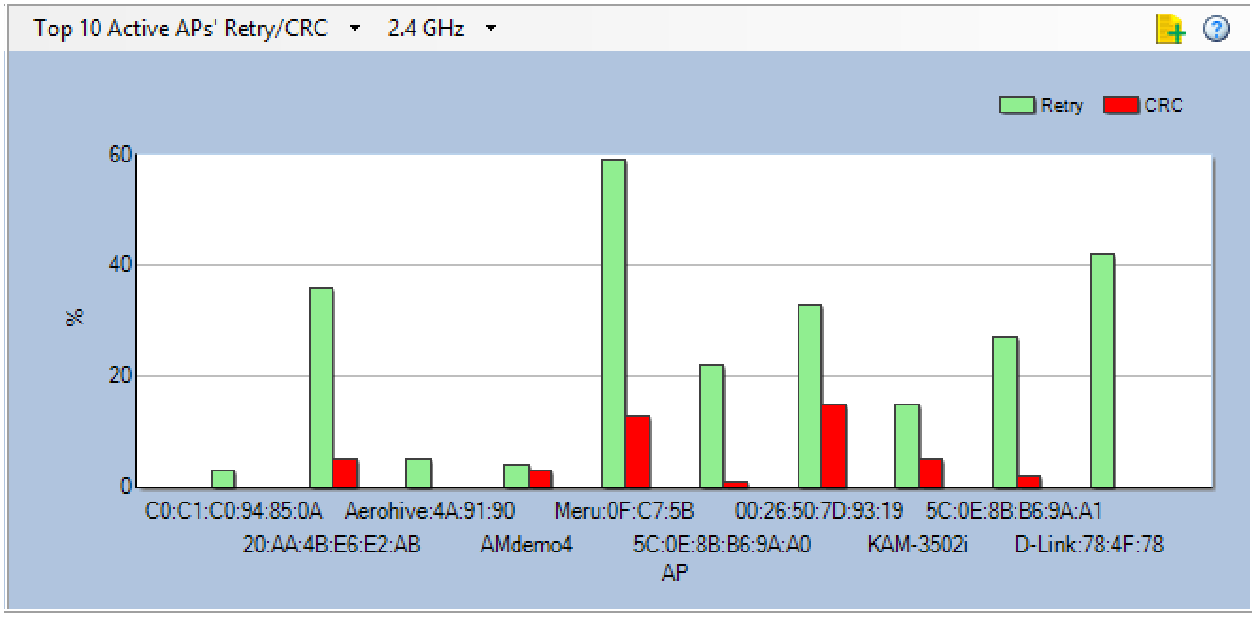


Each bar in the Top 10 APs by Speed graph represents the volume of data transmission being recorded involving a specific AP. It also provides a breakdown of the transmission by transmission rate. The various transmission rates are also color-coded, as shown in the legend.

If you place the cursor over a bar, a tooltip will pop up showing the breakdown of the volume of transmission by transmission rate by that AP. The tooltip also shows basic information about the AP, such as its name or IP address, the channel it is using, its SSID, and its MAC address.

Top 10 Active APs' Retry/CRC

The Top 10 Active APs' Retry/CRC graph shows the percentage of packets that are either Retry or CRC packets for the top 10 APs that are transmitting the most data. The X-axis display APs that have been detected and the types of packets being transmitted (Retry vs. CRC); the Y-axis shows the percentages of Retry and/or CRC packets. Refer to the illustration below.

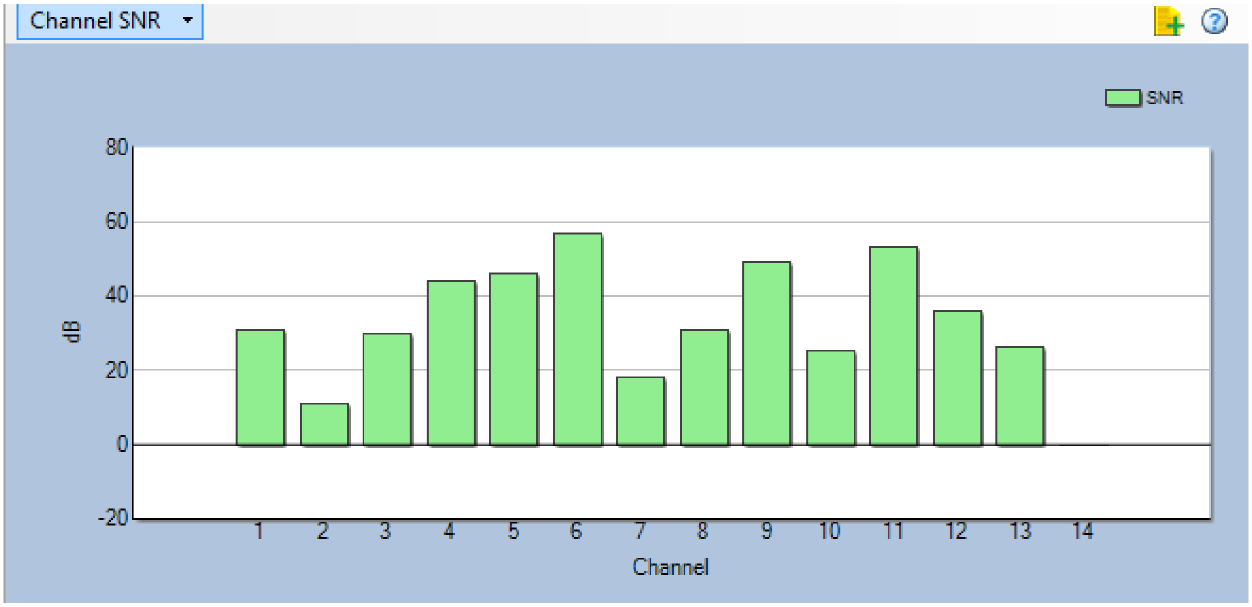


As shown above, the CRC and Retry packets are color-coded, with red for CRC and green for Retry. The APs are identified by name, IP address, or whatever identification is used on the network. If you place the cursor on an AP, a tooltip will pop up showing the following basic information about the AP, in addition to the percentages of Retry and CRC packets transmitted by the AP:

- **AP:** The name or IP address of the AP.
- **Channel:** The channel used by the AP.
- **SSID:** The SSID to which the AP belongs.
- **MAC Address:** The MAC address that identifies the AP.
- **Data Rate(s):** The data rate or rates used by the AP, as indicated by different colors in the legend.

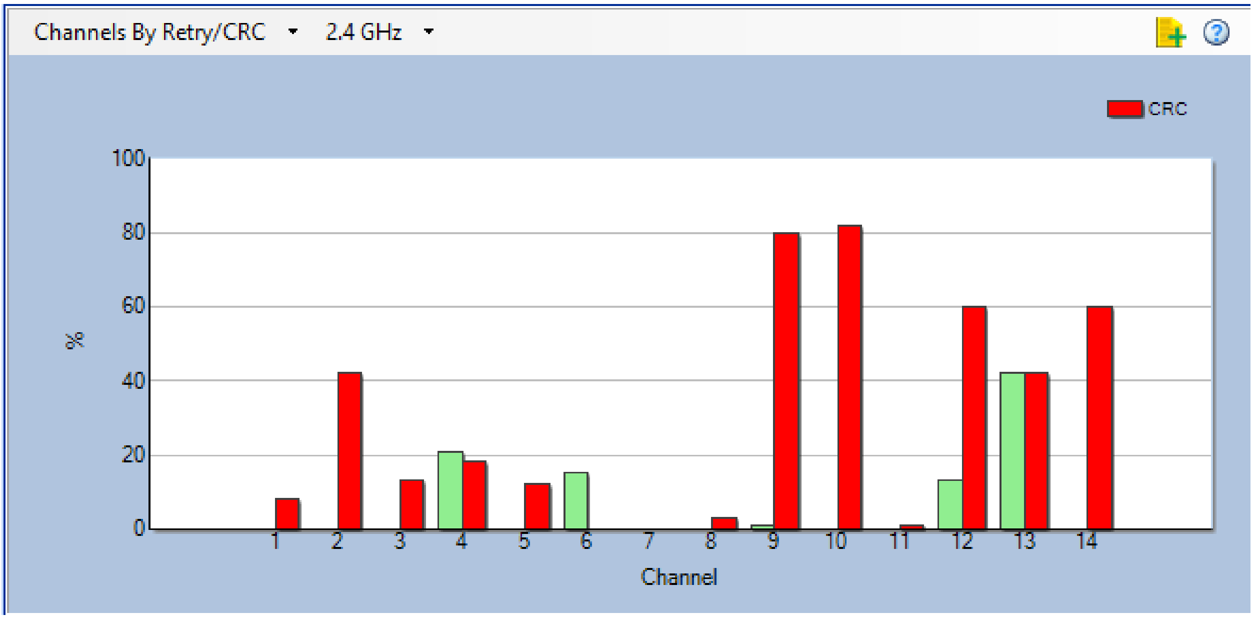
Channel Signal/Noise Ratio

The Channel Signal/Noise Ratio graph shows the ratio of signal to noise present on each displayed channel. The X-axis shows the list of selected channels while the Y-axis displays the ratio in terms of dB.



Channels by Retry/CRC

The Channels by Retry/CRC graph shows the percentage of traffic present on each channel composed of Retry and Cyclic Redundancy Check (CRC) packets. The X-axis shows the list of selected channels while the Y-axis displays the percentage level. As shown in the color legend, Retry traffic is displayed in green while red represents CRC transmissions.



Auto Pattern Detection and Custom Device Classification

Summary of Auto Pattern Detection

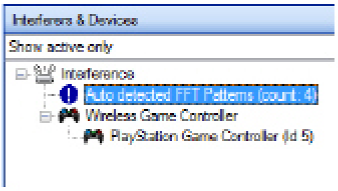
Auto Pattern Detection and Custom Device Classification features enable you to identify, classify, and analyze interferers beyond those devices included in the software package.

- **Auto Pattern Detection:** The system identifies and lists persistent RF patterns that do not match its database of interferers. You can name and save the pattern in order to have it show up as a named interferer in the future when that pattern is detected.

- **Custom Device Classification:** You can create a custom signature of an RF pattern in order to have it show up as a named interferer in the future when that pattern is detected.

Auto Pattern Detection

During the course of an AirMagnet Spectrum XT session, if a particular RF pattern is persistently detected, a list item is created in the "Interferers & Devices" area named "Auto detect FFT Patterns." This list item shows a sum count of the number of patterns detected. The count may rise and fall depending on whether a detected pattern continues to be persistent.



Auto Detected FFT Pattern in Interferers List

This feature is somewhat different from the Custom Device Classification Manager in that these patterns are defined by the system whereas you may manually define the pattern in the Custom Device Classification Manager.

You may view the pattern(s) and create custom signatures of any patterns using the "Auto detect – FFT Patterns" window.

Note: If a pattern is no longer detected after one minute, it will be removed from the Detected Patterns list and the pattern count will be reduced by one to reflect that the pattern is no longer detected.

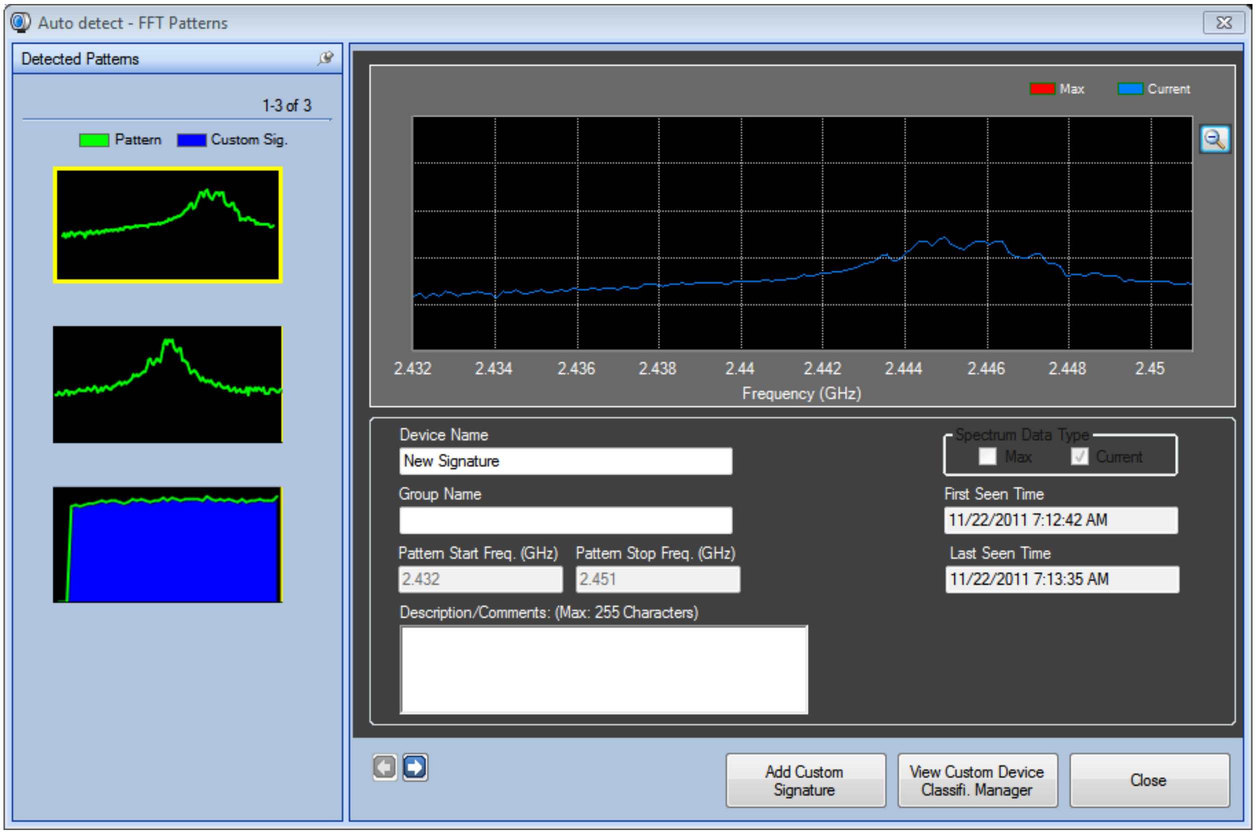
You can open this window using two methods:

- Double-click the **Auto detected FFT Patterns** line item under "Interferers & Devices"

- From the Gear drop-down, select **Show Auto Detected Patterns**

With this window open, you will see the list of detected patterns on the left. The highlighted pattern is displayed in the FFT graph on the right. The pattern will either be "Max" or "Current" data depending on how the pattern was originally detected. The color coded legend in the upper right of the graph will indicate whether the data is "Max" or "Current."

The legend above the patterns indicates that if a custom signature was previously created for a particular pattern, it will be highlighted in blue.



Device Name: New Signature

Group Name:

Pattern Start Freq. (GHz): 2.432

Pattern Stop Freq. (GHz): 2.451

Description/Comments: (Max: 255 Characters)

Spectrum Data Type: ☐ Max ☑ Current

First Seen Time: 11/22/2011 7:12:42 AM

Last Seen Time: 11/22/2011 7:13:35 AM

Auto Detect FFT Patterns Window

To create a custom signature of a pattern:

1) From the Settings drop-down menu, select **Show Auto Detected Patterns**.

2) Click the desired pattern from the pattern list on the left side of the window.

3) Replace **New Signature** with a custom name for the signature.

4) You can also assign the signature to a group using **Group Name**. All signatures assigned to the same group will show up as children of that group in the **Device Signature List** that is part of the Custom Device Classification Manager.

Note: Both Pattern Start and **Stop** fields are auto-filled with the frequency range.

5) Add any description comments, if desired.

6) Click **Add Custom Signature** to save the signature.

Once a signature is created it can be viewed and edited using the Device Classification Manager.

Note: Custom signatures can be imported and exported using the Custom Device Classification Manager.

Best Practices

The Auto Detect FFT Pattern feature in Spectrum XT looks for repeating patterns in the incoming FFT data. It does this by performing the following steps:

1) Performs a 7 point weighted average of the signal, to smooth out small changes in the FFT data.

2) Looks for points in the line that exit/enter the noise floor, producing FFT shape start/stop points.

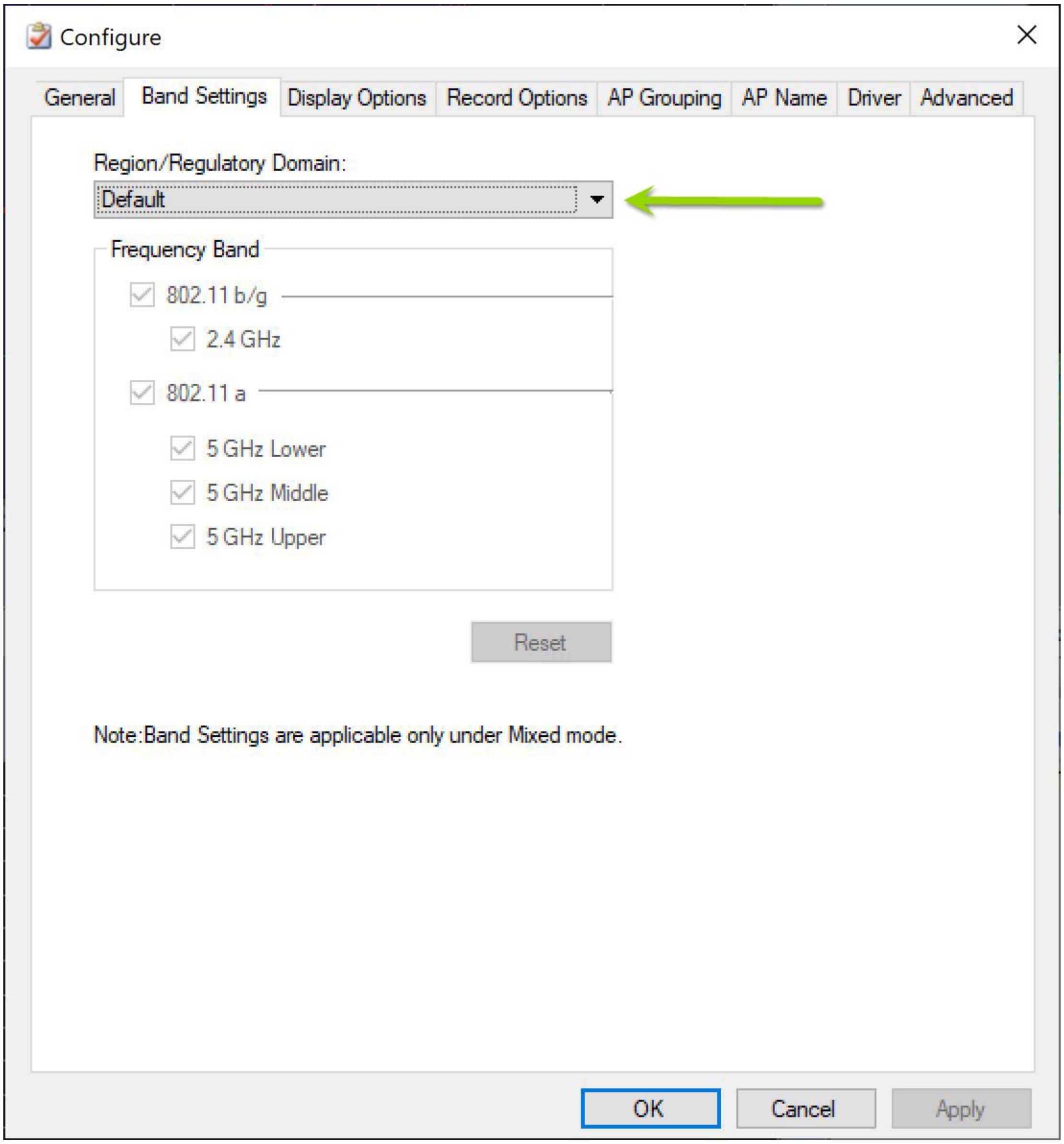
3) These FFT shape start/stop points are categorized based on their start/stop frequency. They are compared against patterns seen in previous iterations of the algorithm. When the mean delta between patterns with the same start/stop frequencies is less than 5 dB, the pattern is said to have been *observed* again.

4) When the observation count for a particular pattern reaches 6, the pattern is said to have been Auto Detected and is now available for inspection in the UI.

5) Patterns which are not seen again within a 1 minute duration are recycled (thrown away). Thus, the user may observe the Auto Detected FFT Pattern count increase and decrease over time.

What you can tune:

The Auto Detect feature processes both the “current” and the “max” FFT data. As such there are two parameters you can tune in order to affect the algorithm: “Noise Floor for max Reading” and “Noise Floor for Current Reading”.



Region/Regulatory Domain: Default

Frequency Band

☑ 802.11 b/g

☑ 2.4 GHz

☑ 802.11 a

☑ 5 GHz Lower

☑ 5 GHz Middle

☑ 5 GHz Upper

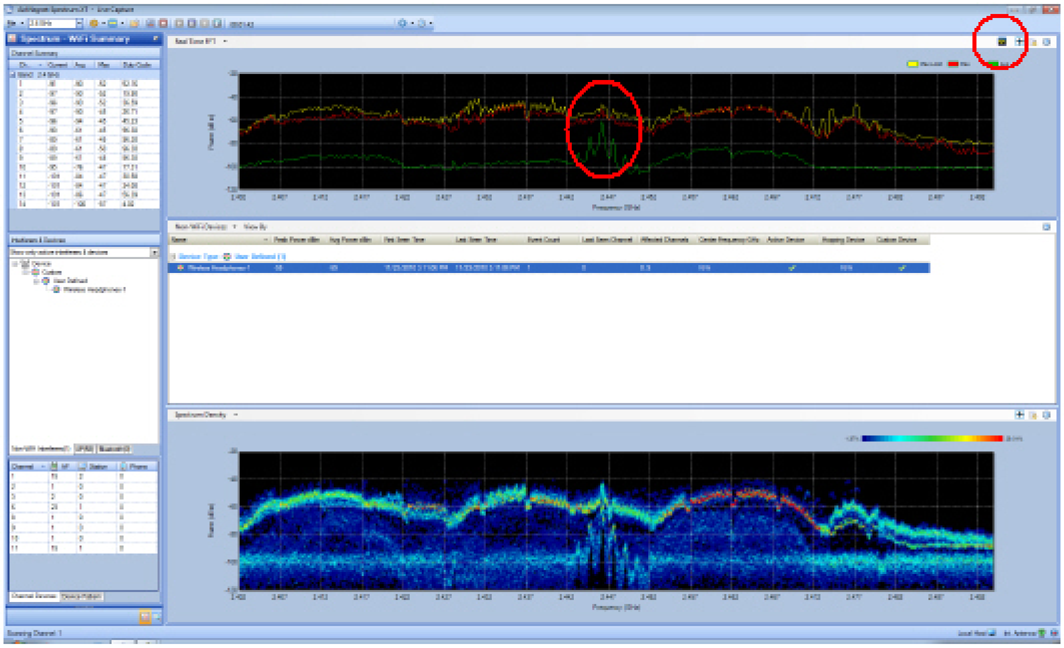
Note:Band Settings are applicable only under Mixed mode.

Configure Auto Detect Settings Window

Custom Device Classification Manager

The first step in using custom classification is determining whether there may be an unclassified device detected in your environment. Each RF interferer has its own signature pattern on the Real Time FFT chart. This helps you recognize a distinct pattern for the device.

As shown in the following example, a pattern shows up that looks like a narrowband transmitter. At this point, if the device is not known, a directional antenna would work best to locate the device within the environment for labeling in the custom classification.



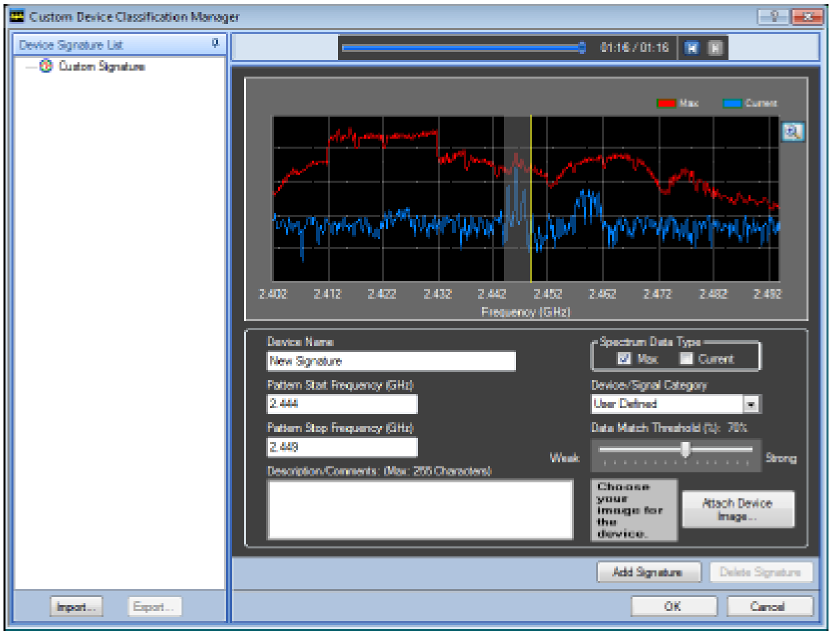
Device Detected

To create a custom device classification signature:

1. Wait until you see a distinct pattern for the device on the Max or Current Line of the FFT graph. By default, the visibility of Current Line is not enabled on the Real Time FFT chart. You can enable it from the chart configuration window.

2. Click the **Add Custom Device Classification** button (this is located at the top left of the FFT graph).

3. You can use the slider bar on top of the Custom Device Window to move forward or backward on the frames to capture a perfect pattern. This slider is isynchronized with the Instant Playback data with a maximum of 2 minutes worth of data. The slider bar is enabled only for the signature which is currently being defined. To get the most accuracy out of the custom signature feature, you should select only the portion of the band which contains the interferer’s distinct pattern.



Device Name: New Signature

Pattern Start Frequency (GHz): 2.444

Pattern Stop Frequency (GHz): 2.449

Description/Comments: (Max: 255 Characters)

Spectrum Data Type: ☑ Max ☐ Current

Device/Signal Category: User Defined

Data Match Threshold (%): 70%

Range Defined Custom Classification Window

4. Narrow down the pattern window from the entire spectrum to just the frequencies that are relevant to the device. To do this, click the left edge of the desired range and drag to the right edge of the range.

5. Replace **New Signature** with a custom name for the signature.

6. You can also assign the signature to a group using **Group Name**. All signatures assigned to the same group will show up as children of that group in the Device Signature List that is part of the Custom Device Classification Manager.

Note: Both Pattern Start and Stop fields are auto-filled with the frequency range.

7. Select whether to use the **Current** or **Max** data line for the Spectrum Data Type. This may depend on which is best based on which one provides a consistent, distinct pattern. You can select both data sources in order to have the system detect the defined pattern on either of the data sources. For example, hopping or short-burst devices should use the max setting for the **Spectrum Data Type** instead of the current, as the Max data gives a more distinct pattern in this situation.

8. Use the **Category** drop-down to choose a pre-defined category to assign to the new signature.

9. Use the **Data Match Threshold** to define how loosely or tightly defined the signal pattern is. The Data Match Threshold value is 70%, and you can change this to any value between 30% and 100%. For environments with high amounts of spectrum data, most loosely constrained patterns can yield

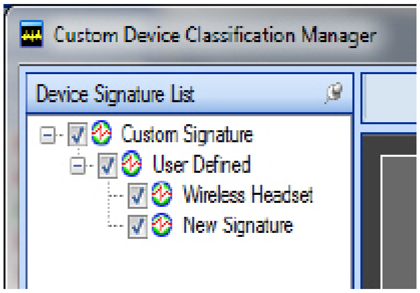
better detection rates, and can also lead to potential false detections. More tightly constrained patterns, meaning a higher threshold, means that there will be fewer false detections, with a chance that there will also be fewer actual detections that fall just out of range of the constraints.

10. Add any description comments, if desired.

11. To attach an image to the new signature that can be used to easily identify the signature, click **Attach Device Image** to browse to an image.

12. Click **Add Signature** to save the signature.

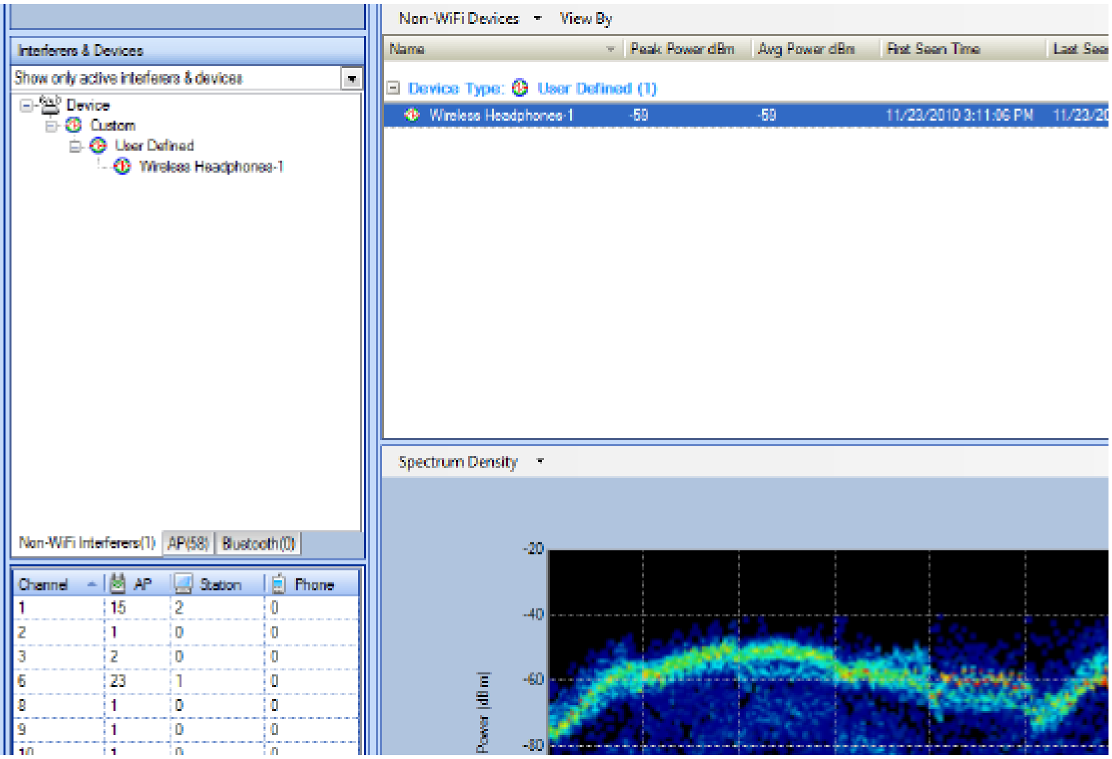
The system allows you to create a maximum of 50 custom signatures and at the most 10 signatures can be enabled. For an enhanced system performance, it is best to enable only the signatures which are of current interest to the user.



Enable and Disable Custom Device Signatures

Verification

The created custom signature is tightly coupled with the associated frequency of the pattern. If the device switches the channel and needs to classify on the new channel, you must create signatures for those frequencies. Once the custom device has been defined and saved, the next time the correct conditions are met, the device will appear in the Device List and in the Non-Wi-Fi devices panel.



Name	Peak Power dBm	Avg Power dBm	First Seen Time	Last Sea
Device Type: User Defined (1)				
Wireless Headphones-1	-59	-59	11/23/2010 3:11:06 PM	11/23/20

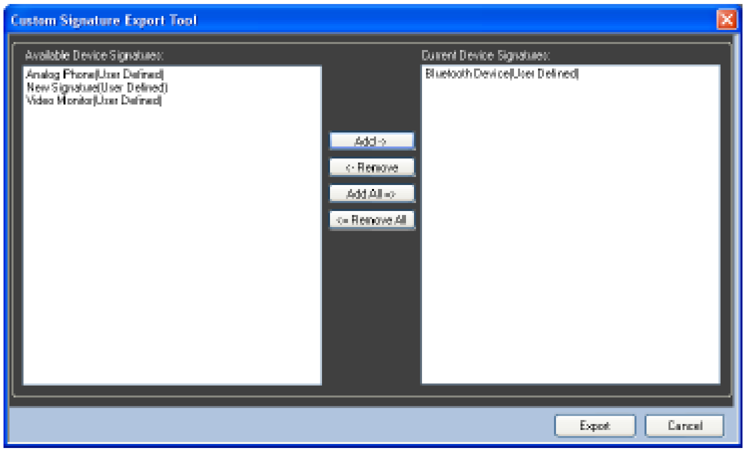
Channel	AP	Station	Phone
1	15	2	0
2	1	0	0
3	2	0	0
6	23	1	0
8	1	0	0
9	1	0	0
10	1	0	0

Device List and Non-WiFi Devices Panel

Export/Import Custom Signatures

AirMagnet Spectrum XT supports the ability to share the defined signatures between users. You can export the interested signatures to a file which can be shared with other users. The user who received a signature file should import the signature into their system to make use of it.

The custom device classification window has buttons to export and import the custom signatures. The system has the ability to selectively export one or more signatures. The exported signatures will be saved into a file (*.amdp*) which you can share with other users.

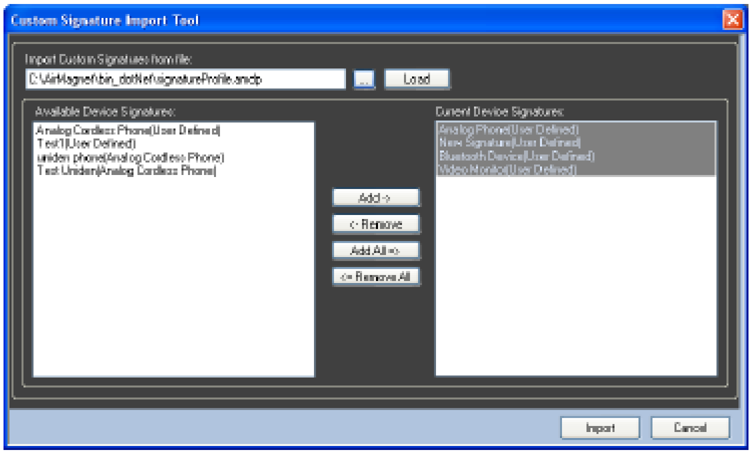

Custom Signature Export Tool
Available Device Signatures:
Current Device Signatures:
Add->
<- Remove
Add All =>
<= Remove All
Export
Cancel

Analog Phone[User Defined]
New Signature(User Defined)
Video Monitor[User Defined]

Bluetooth Device[User Defined]

Signature Export

Import the exported signatures from the file into the system by clicking the **Import** button and selecting the appropriate file. The available device signatures list all the signatures available on the file. You can selectively import one or more signatures into the system. The imported signatures will be merged into the signature file persistent on the system. By default, the imported signature is not enabled and you must enable them by clicking the check box on the **Device Signature List**.



Import Custom Signatures from file: C:\AirMagnet\bin_dotNet\signatureProfile.amdp

Available Device Signatures:
Analog Cordless Phone(User Defined)
Test1(User Defined)
uniden phone(Analog Cordless Phone)
Test Uniden(Analog Cordless Phone)

Current Device Signatures:
Analog Phone(User Defined)
New Signature(User Defined)
Bluetooth Device(User Defined)
Video Monitor(User Defined)

Signature Import

Custom Signature During File Playback

The custom devices classified during recording phase will not be saved into the trace file. Custom signatures will be re-evaluated during file playback for possible classification of the custom devices. AirMagnet Spectrum XT enables you to create a new custom signature in playback mode. Signatures defined during playback will be evaluated against the captures data for the device detection. The creation and application of custom signature during file playback is no different from the Live Capture.

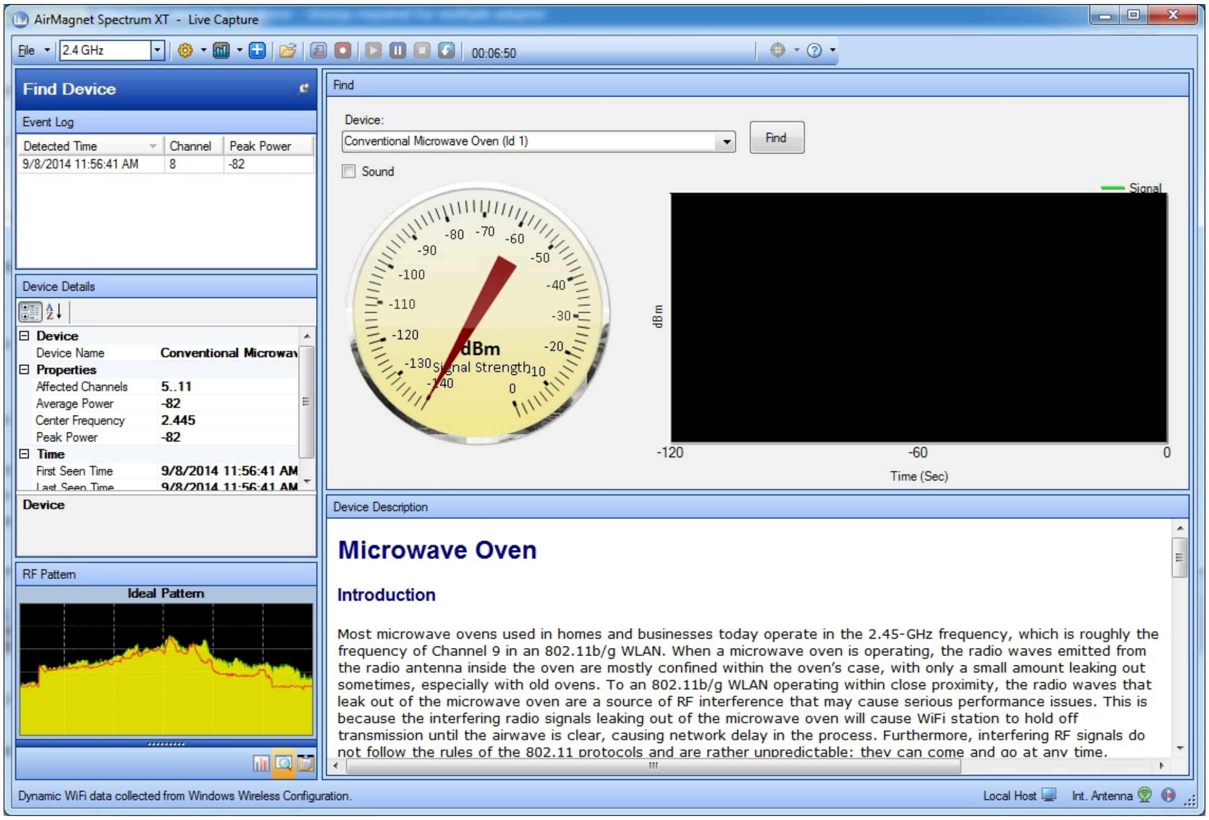
Finding Devices

Using Find Device Tool

AirMagnet Spectrum XT comes with a robust Find Device tool that enables you to find any device (Wi-Fi or non-Wi-Fi) detected in your network. You can access this tool either by clicking **(Find Device)** in the lower left past of the screen or by double-clicking a device in the Device List on the Spectrum-WiFi Summary screen. The former enables you to switch to the Find Device screen where you can select the device of interest and then try to use the Find Device tool to find it, whereas the latter directly opens the Find Device screen with the device of interest automatically selected so that all you have to do is to click the **Find** button to look for it.

The image below shows the Find Device tool screen. It contains the following components:

- Event Log
- Device Details
- Device Pattern
- Find Device Tool
- Device Description



Event Log

Detected Time	Channel	Peak Power
9/8/2014 11:56:41 AM	8	-82

Device:
Conventional Microwave Oven (Id 1)

Device Details

Device	
Device Name	**Conventional Microwav**
Properties	
Affected Channels	**5..11**
Average Power	**-82**
Center Frequency	**2.445**
Peak Power	**-82**
Time	
First Seen Time	**9/8/2014 11:56:41 AM**
Last Seen Time	**9/8/2014 11:56:41 AM**

Device

Device Description

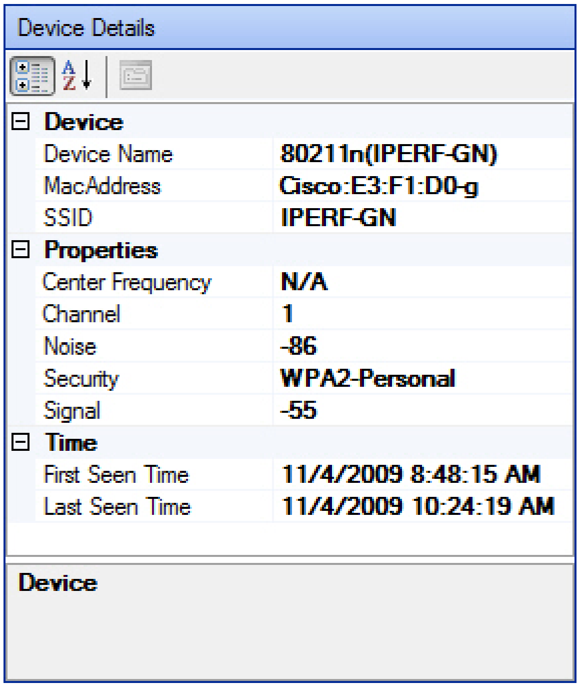
Microwave Oven

Introduction

Most microwave ovens used in homes and businesses today operate in the 2.45-GHz frequency, which is roughly the frequency of Channel 9 in an 802.11b/g WLAN. When a microwave oven is operating, the radio waves emitted from the radio antenna inside the oven are mostly confined within the oven's case, with only a small amount leaking out sometimes, especially with old ovens. To an 802.11b/g WLAN operating within close proximity, the radio waves that leak out of the microwave oven are a source of RF interference that may cause serious performance issues. This is because the interfering radio signals leaking out of the microwave oven will cause WiFi station to hold off transmission until the airwave is clear, causing network delay in the process. Furthermore, interfering RF signals do not follow the rules of the 802.11 protocols and are rather unpredictable: they can come and go at any time.

Device Details

The Device Details pane provides detailed information about the device being selected. Refer to the illustration below.



Device	
Device Name	80211n(IPERF-GN)
MacAddress	Cisco:E3:F1:D0-g
SSID	IPERF-GN
Properties	
Center Frequency	N/A
Channel	1
Noise	-86
Security	WPA2-Personal
Signal	-55
Time	
First Seen Time	11/4/2009 8:48:15 AM
Last Seen Time	11/4/2009 10:24:19 AM

Device

The information displayed will vary, depending on the type of device detected (802.11 or non-802.11). As shown above, the Device Details pane shows the following information for standard 802.11 devices:

- **Device Name** - The device category the selected device belongs to (that is, Bluetooth Device, Digital Cordless Phone, and so on.)
- **Mac Address** - The MAC address of the device.
- **SSID** - The SSID detected from the device.
- **Center Frequency** - The middle point of the frequency range detected for the device.
- **Channel** - The channel on which the device is operating.
- **Noise** - The level of noise detected from the device.
- **Security** - The security mechanism in use by the device.
- **Signal** - The signal level detected from the device (in dBm).
- **First Seen Time** - The first time the device was detected.
- **Last Seen Time** - The most recent time the device was detected.

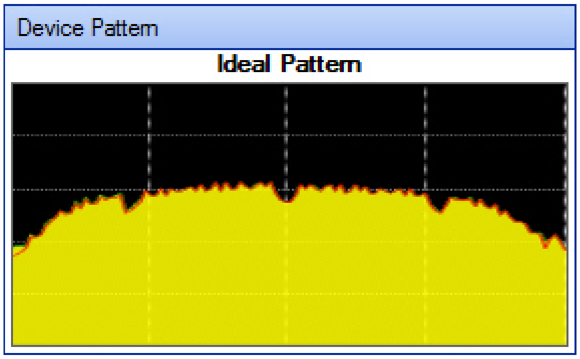
For non-802.11 devices, the information differs:

- **Device Name** - The device category the selected device belongs to (that is, Bluetooth Device, Digital Cordless Phone, and so on.)

- **Affected Channels** - The range of channels being affected by the device.
- **Average Power** - The average energy reading of the device recorded since it was detected.
- **Center Frequency** - The middle point of the frequency range detected for the device.
- P**eak Power** - The maximum energy reading of the device since it was detected.
- **First Seen Time** - The first time the device was detected.
- **Last Seen Time** - The most recent time the device was detected.

Device Pattern

In the lower-left corner of the screen is the Device Pattern pane which shows the RF spectrum pattern of the device being selected. Refer to the illustration below.



The Device Pattern pane shows the spectrum pattern the application has detected of the selected device.

If the selected device is a Wi-Fi device, the Device Pattern pane will show the Ideal Pattern only. If the selected device is a non-Wi-Fi device, then it will show both the Ideal Pattern and the Detected Pattern. The application uses the Ideal Pattern as a reference when classifying devices it has detected and determines the type of device by matching the Detected Pattern with the Ideal Pattern. For example, if the application finds that a detected spectrum pattern matches that of the ideal spectrum pattern of a Bluetooth device, it will categorize the device as a Bluetooth device.

You can also access the Device Pattern pane from the Spectrum-WiFi Summary screen by highlighting an entry in the **Non-WiFi Devices** table.

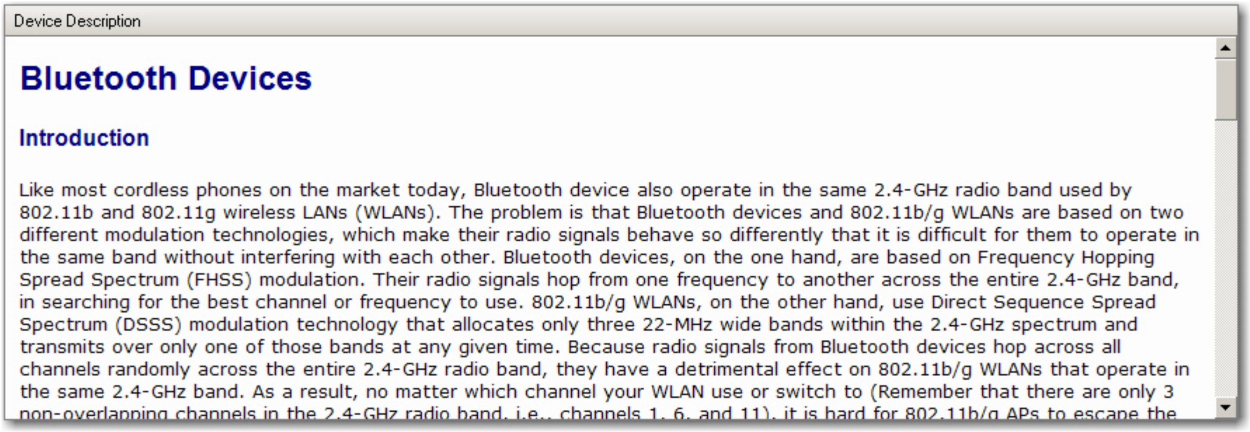
Note: The device pattern examples provided with AirMagnet Spectrum XT are intended to be baselines, not exact matches for the devices detected. The device pattern can vary even between two similar devices (that is, two microwaves from different vendors). Consequently, the device's pattern may not always be an exact match for the example provided in the application.

Device Description

In the lower-right part is the Device Description pane, as sown the illustration below, which contains detailed information about the (type of) device you are trying to find, which includes the following:

- An brief introduction of the RF characteristics of the device, such as radio frequencies or channels, modulation, transmit rate, and so on. of the device.
- The typical RF spectrum pattern of the device.
- Its impact on the WLAN.
- Recommendations on how to minimize the device's interference on a Wi-Fi network.

Note: You can use the scroll bar or arrows on the right to view the full description.



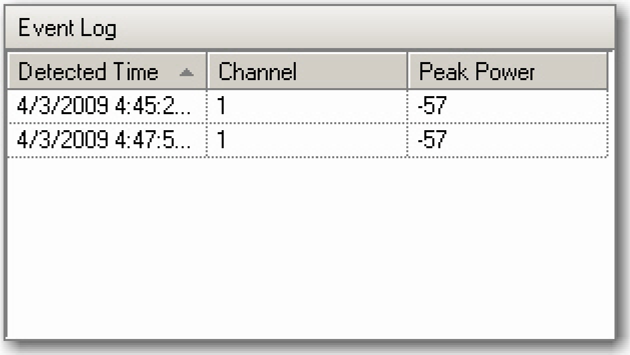
Bluetooth Devices

Introduction

Like most cordless phones on the market today, Bluetooth device also operate in the same 2.4-GHz radio band used by 802.11b and 802.11g wireless LANs (WLANs). The problem is that Bluetooth devices and 802.11b/g WLANs are based on two different modulation technologies, which make their radio signals behave so differently that it is difficult for them to operate in the same band without interfering with each other. Bluetooth devices, on the one hand, are based on Frequency Hopping Spread Spectrum (FHSS) modulation. Their radio signals hop from one frequency to another across the entire 2.4-GHz band, in searching for the best channel or frequency to use. 802.11b/g WLANs, on the other hand, use Direct Sequence Spread Spectrum (DSSS) modulation technology that allocates only three 22-MHz wide bands within the 2.4-GHz spectrum and transmits over only one of those bands at any given time. Because radio signals from Bluetooth devices hop across all channels randomly across the entire 2.4-GHz radio band, they have a detrimental effect on 802.11b/g WLANs that operate in the same 2.4-GHz band. As a result, no matter which channel your WLAN use or switch to (Remember that there are only 3 non-overlapping channels in the 2.4-GHz radio band, i.e., channels 1, 6, and 11), it is hard for 802.11b/g APs to escape the

Event Log

In the upper-left pane of the Find Device screen is the Event Log. Refer to the illustration below.



Detected Time	Channel	Peak Power
4/3/2009 4:45:2...	1	-57
4/3/2009 4:47:5...	1	-57

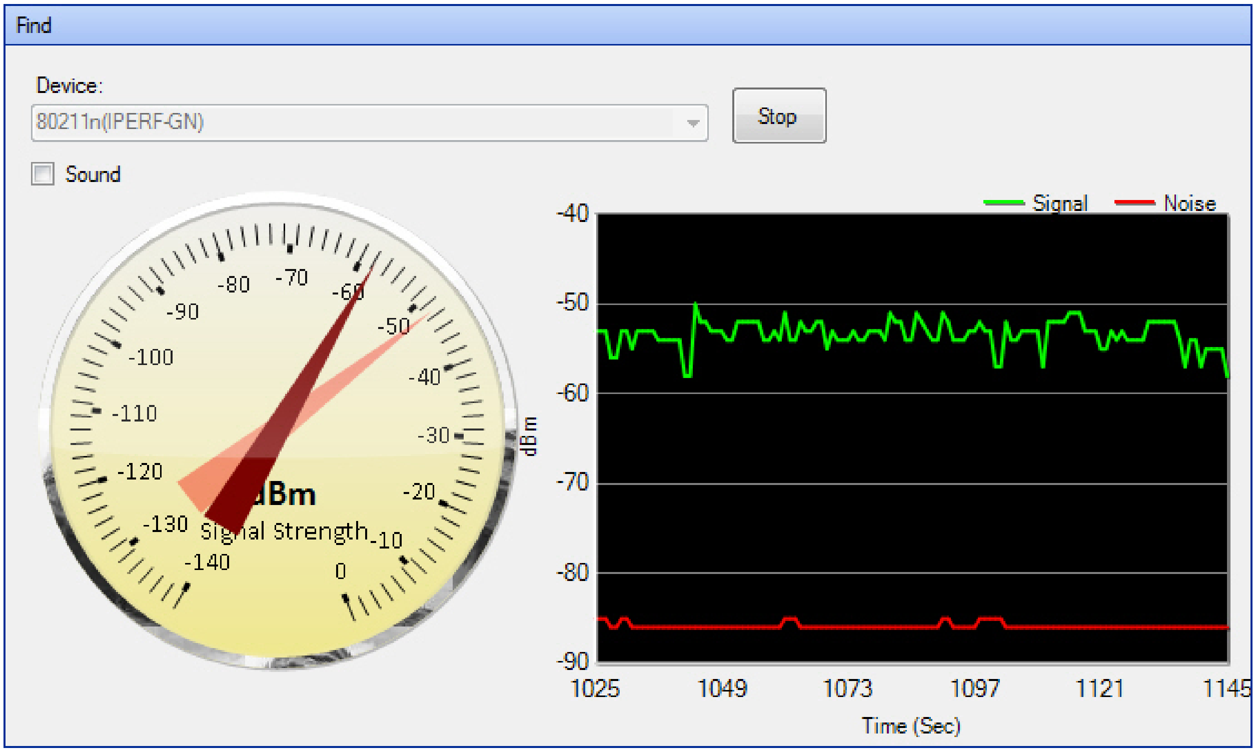
The Event Log records every instance the selected device was been detected. It provides the following information about each event:

- **Detected Time** - The data and time of each instance when the device was detected.

- **Channel** - The channel on which the device was detected.
- **Peak Power** - The maximum energy reading of the device at the time it was detected.

Finding a Device Tool

The Find Device tool contains tools for locating any device (Wi-Fi or non-Wi-Fi) that the application has detected on the network. Refer to the illustration below.



The Find Device tool has the following components:

- **Device Drop-Down List Menu** – Allows you to select an entry among all detected devices in the selected radio band.
- **Find/Stop Button** – Allows you to start or stop a device-locating operation.
- **Sound Check Box** – If checked, the application will start ticking while searching for a device. The sound becomes louder as you get closer to the device.
- **Signal Strength Gauge** – Shows the change in signal strength as you move closer to the device. The lighter hand indicates the highest signal strength that has been recorded of the device and the darker one the signal strength reading of the device at the moment. Signal strength should become stronger as you move closer to the device you are intend to find.

- **Signal/Noise Graph** – Shows the changes in signal strength and/or noise level during a search operation. Both signal strength and noise level are graphed if the device you are trying to find is a Wi-Fi device; only signal strength is shown if it is a non-Wi-Fi device. Signal strength and noise level should rise as you move closer to the device you are trying to find.

To physically locate a device on the network:

1. Make sure that the device is selected in the **Device Drop-Down List Menu**.

2. Click **Find.**

3. Check the Sound check box, if desired.

4. Pick up your laptop PC and move in the direction the ticking sound gets louder and the signal strength get stronger until you finally reach the location of the device.

Best Practices

This section contains recommendations for best results when attempting to locate devices using AirMagnet Spectrum XT.

Note: When attaching the antenna to the Spectrum USB Adapter, ensure that you *firmly* push the antenna cord connector into the adapter port until a pronounced click is audible.

With an Omni-Directional Antenna

1. Begin in the area where interference of the Wi-Fi network has been reported.
2. On the Summary page, identify the non-Wi-Fi device responsible for the interference on your network.
3. Go to the Find page.
4. From the drop down list, select the device you identified in Step 2.
5. Start the **Find Too**l.
6. Because the signal strength can greatly vary from second to second, begin a slow patrol of the area, covering a meter in 3 to 5 seconds.
7. When you reach an area where the signal has climbed to its highest level, look around to locate the device.

With a Directional Antenna

1. Begin in the area where interference of the Wi-Fi network has been reported.
2. On the Summary page, identify the non-Wi-Fi device responsible for the interference on your network.
3. Go to the Find page.
4. From the drop down list, select the device you identified in Step 2.

5. Start the **Find Too**l.
6. Slowly turn around until you locate the direction in which the device's signal strength is the strongest.
7. As directly as possible, move in the direction of the strongest signal. Move slowly, covering about one meter every three to five seconds.
8. When the signal has climbed to its highest point, or appears to be roughly the same no matter what direction the antenna is facing, observe the area to locate your interfering device.

Radar Detection Tool

Radar Detection Tool Overview

The 5-GHz band is an Unlicensed National Information Infrastructure (UNII) band, which is divided into several segments, each designated for a specific use. The UNII-2 (5.25 GHz~5.35 GHz) and UNII-2 extended (5.47 GHz~5.725 GHz) bands used to be set aside exclusively for military and weather radar systems. When the FCC decided to open these bands up for Wi-Fi networks, its ruling came with an important caveat: Dynamic Frequency Selection version 2, or DFS2, compliance.

DFS is a mechanism that tells the transmitter to dynamically listen for radar signals in the airwave and automatically switch to another channel if a radar signal is detected. The mechanism is designed to protect the incumbent military and weather radar systems from the RF interference from 802.11a/n/ac/ax devices in their vicinity. With DFS2, the transmitter on a Wi-Fi device will continuously listen for radar signals, both before and during transmission. IF a radar signal is detected on a channel, it will either vacate that channel or flag it as unavailable.

DFS2 is a must-have on 802.11a/n/ac/ax APs in order for 802.11a/n/ac/ax network systems to co-exist with military and weather radar systems. According to the latest FCC ruling, all Wi-Fi devices operating in the UNII-2 and UNII-2 extended bands are required to support DFS, to detect and automatically switch channels to prevent WLAN operations from interfering with military or weather radar systems. The mandate became effective on July 20, 2007 in the US and Canada. A similar mandate became effective on April 1, 2008 in the EU.

Since then, in April 2009 new EN 301 893 v1.5.1 requirements also called DFS-3 Compliance have also been enforced for 802.11 APs operating in Europe.

AirMagnet Spectrum XT Radar Detection Tool

The only radar signals that AirMagnet Spectrum XT can detect are those described by the regulatory bodies as part of the DFS requirements.

AirMagnet Spectrum XT supports all six of the FCC radar types, all six of the ETSI EN 301 893 V1.5.1 radar types, and all eight of the ETSI EN 302 502 V1.2.1 radar types.

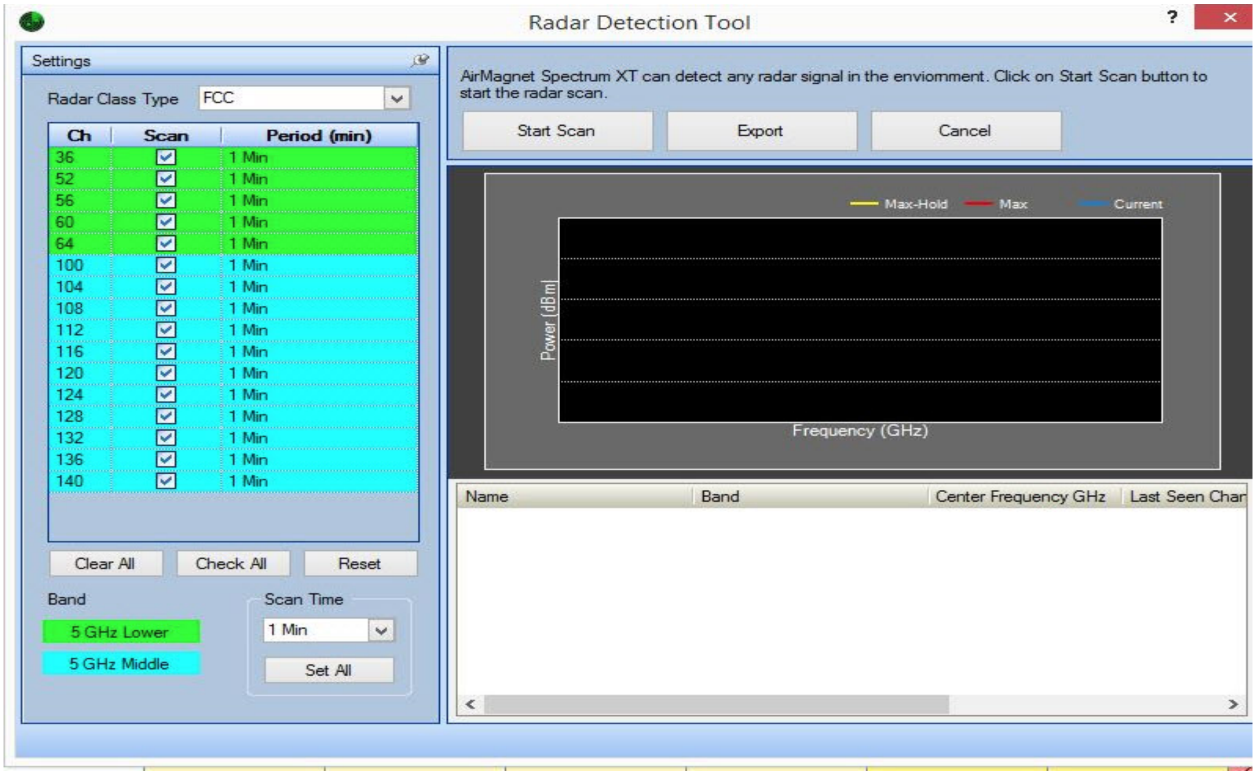
Of the ten radar types defined by the Japanese DFS requirements, AirMagnet Spectrum XT supports Type 1, and Types 5-10, which have exact equivalents in the FCC types.

Japanese radar Types 2-4 are currently not supported.

Note: Most radar signals come in short bursts, followed by dead time. Detection by Spectrum XT would require that the bursts arrive while the Spectrum XT is on the correct channel. The chances of this happening in the short-term may be very low. The best way to detect the radar is to dwell on each channel for a period of time that includes several sweeps of the radar. This could range from 10ths of seconds to several minutes.

Radar Detection Tool UI Components

This section describes the options in the Radar Detection Tool user interface.



AirMagnet Spectrum XT can detect any radar signal in the enviornment. Click on Start Scan button to start the radar scan.

Radar Class Type: FCC

Ch	Scan	Period (min)
36	☑	1 Min
52	☑	1 Min
56	☑	1 Min
60	☑	1 Min
64	☑	1 Min
100	☑	1 Min
104	☑	1 Min
108	☑	1 Min
112	☑	1 Min
116	☑	1 Min
120	☑	1 Min
124	☑	1 Min
128	☑	1 Min
132	☑	1 Min
136	☑	1 Min
140	☑	1 Min

Scan Time: 1 Min

Name	Band	Center Frequency GHz	Last Seen Char

Radar Detection Tool User Interface

Radar Detection Tool UI Components Option	Description
Settings bar	This is the heading for the Settings panel. You may collapse the Setting panel by clicking the push pin icon located to the right of the Settings bar. Once collapsed, to view the panel, click the Settings tab in the top left corner. To re-establish the default view, click the push pin.

Radar Class Type

FCC: Federal Communications Commission channels for United States.

ETSI: European Telecommunications Standards Institute channels for Europe.

TELEC: Telecommunications Engineering Center channels for Japan.

Ch (Channel)

This column lists the channels for the selected Radar Class Type.

Scan

When you check the box next to a channel listing, this channel will be scanned during a scanning session.

Period (min)

This column provides a drop-down menu for each channel that can be used to manually set the time the associated channel will be scanned during the session.

Clear All

Click this button to un-check all the channels.

Check All

Click this button check all the channels.

Reset

Click this button to check all the channels and reset the "Period" column to the default setting of 1 min.

Band

This is a color legend that indicates the media type for the channel listing.

Scan Time

Using this option will automatically set all the channels to the period set using the drop-down.

Start Scan

Click this button to begin a radar scanning session.

Stop Scan

Click this button to end a radar scanning session.

Export

Select a radar device listing and click **Export** to export the data in *.csv* format.

Cancel

Click this button at any time to cancel a scanning session and close the Radar Detection Tool window.

Radar Graph

During an active scanning session, the radar graph charts real-time data by plotting a function of the frequency range and the power in dBm for the current channel being scanned.

Radar Device Table

The table below the graph lists any radar devices detected during the scanning session.

Name: The device signature detected.

Band: The UNII band the device was detected in.

Center Frequency GHz: Refers to the center frequency of the device.

Affected Channel: The channel that is affected by the device.

First Seen Time: When the device was detected for the first time.

Last Seen Time: The most recent time when the device was detected.

Status bar

Scanning Channel: During a scanning session, the current channel being scanned will be displayed in the lower left side of the status bar.

Scan Time: During a scanning session, the time remaining for the scan of the current channel will be displayed in the lower right side of the status bar. The format is min min: sec sec.

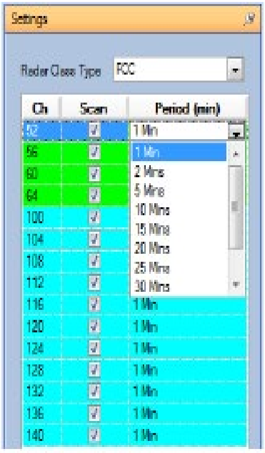
Using the Radar Detection Tool

To use the Radar Detection Tool:

1. From the **File** menu select **Radar Detection Tool**. This will open the Radar Detection Tool window.
2. In the **Settings** panel, select the desired **Radar Class Type** from the drop-down menu.

3. Set the desired channels to scan by adjusting the checked options in the **Scan** column.

4. Set the scan period for each channel by adjusting either a) each channel individually by using the **Period (min)** column drop-down for each channel (refer to the figure)—or— b) set the scan time for all checked channels using the **Scan Time** drop-down menu. To use **Scan Time**, select a time from the drop-down and click **Set All**.



Radar Class Type: FCC

Ch	Scan	Period (min)
52	☑	1 Min
56	☑	
60	☑	
64	☑	
100	☑	
104	☑	
108	☑	
112	☑	
116	☑	1 Min
120	☑	1 Min
124	☑	1 Min
128	☑	1 Min
132	☑	1 Min
136	☑	1 Min
140	☑	1 Min

Period (min) Drop-down Menu

5. Click **Start Scan** to begin the channel scanning session.

   The graph will begin to chart the power and frequency data for the channel being scanned. The channel being scanned will be listed at the bottom left of the window in the status bar. If radar is detected, the device detected will be listed in the table below the graph.

6. Click **Stop Scan** to end the session.

7. If at least one radar device is listed in the table below the graph, the listing data may be exported in *.csv* format. To do this, select the listing and click **Export**. Browse to a folder location to store the data file.

Note: You can close the Radar Detection Tool at any time by clicking **Cancel**.

Spectrum XT in Action

Detecting and Identifying Devices on the Network

AirMagnet Spectrum XT can identify various 802.11 or non-802.11 devices that are operating in your W-iFi network by looking at the unique patterns of energy emitted from those devices. This section shows the Real Time FFT, Spectrum Density, and Spectrogram graphs involving non-802.11 devices that can be easily detected using AirMagnet Spectrum XT.

Non-Wi-Fi Devices

- Bluetooth Devices
- Digital Cordless Phones
- Analog Cordless Phones
- Microwave Ovens
- Baby Monitors
- Wireless Cameras
- RF and Narrowband Jammers
- Digital Video Monitor
- Wireless Game Controllers
- Motion Detectors
- Non-Bluetooth Wireless Mouse
- Possible Interferer
- Radar
- RF Signal Generator
- Zigbee Devices
- Canopy Devices
- Frequency-Hopping Spread Spectrum

Wi-Fi Devices

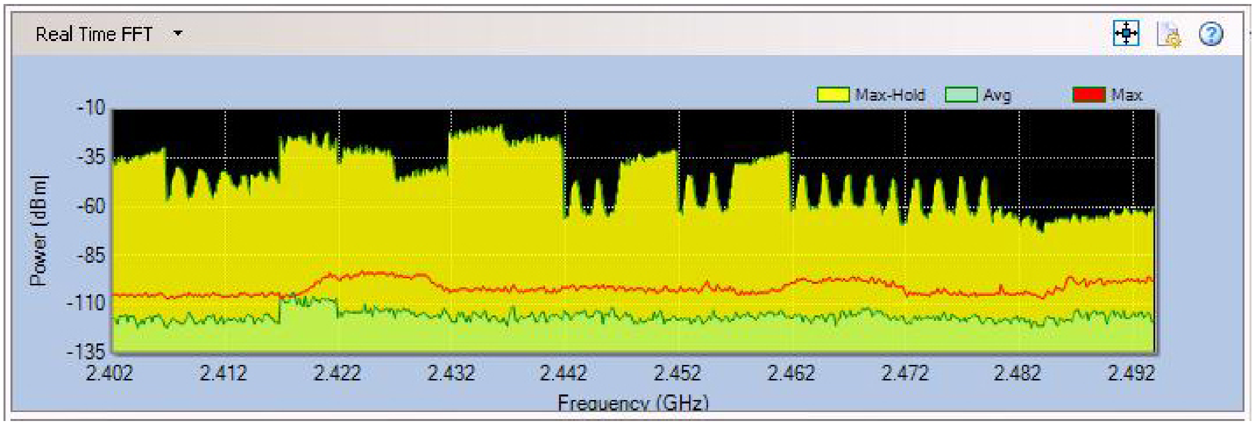
- 802.11a/b/g APs
- 802.11b APs

Bluetooth Devices

Like most cordless phones on the market today, Bluetooth device also operate in the same 2.4-GHz radio band used by 802.11b/g/n/ax wireless LANs (WLANs). The problem is that Bluetooth devices and 802.11b/g/n/ax WLANs are based on two different modulation technologies, which make their radio signals behave so differently that it is difficult for them to operate in the same band without interfering with each other. Bluetooth devices, on the one hand, are based on Frequency Hopping Spread Spectrum (FHSS) modulation. Their radio signals hop from one frequency to another across the entire 2.4-GHz band, in searching for the best channel or frequency to use. 802.11b/g WLANs, on the other hand, use Direct Sequence Spread Spectrum (DSSS) modulation technology that allocates only three 22-MHz wide bands within the 2.4-GHz spectrum and transmits over only one of those bands at any given time. Because radio signals from Bluetooth devices hop across all channels randomly across the entire 2.4-GHz radio band, they have a detrimental effect on 802.11b/g/n/ax WLANs that operate in the same 2.4-GHz band. As a result, no matter which channel your WLAN use or switch to (Remember that there are only 3 non-overlapping channels in the 2.4-GHz radio band, that is, channels 1, 6, and 11), it is hard for 802.11b/g/n/ax APs to escape the RF interference caused by Bluetooth devices operating on or in the vicinity of your network. Bluetooth devices can cause performance degradation when used in close proximity to 802.11 stations, especially when the latter are relatively far away from the APs or stations they are associating with, because of weak signal strength.

RF Spectrum Pattern

The figure below shows the RF spectrum pattern of a Bluetooth iPhone.



RF Spectrum Pattern of a Bluetooth-Enabled iPhone

Impact on 802.11b/g/n/ax WLAN

Because the 2.4-GHz radio band is unlicensed (free to all), there are numerous Bluetooth-enabled devices by different manufacturers available on the market. The following is a short list of such devices:

- Laptops
- PDAs
- Headsets
- Headphones
- Mice
- Keyboards
- Dongles
- Adapters

- Speakers, and so on.

Bluetooth devices are popular in homes and businesses where 802.11b/g/n/ax WLANs are deployed and have been recognized as a source of RF interference to 802.11b/g/n/ax WLANs. You may tackle these interfering Bluetooth devices by identifying and locating them in your WLAN.

Recommended Courses of Action

Once interfering Bluetooth devices are successfully located, we recommend the following actions to minimize or eliminate the RF interference they cause to your 802.11b/g/n/ax WLAN:

- Set your WLAN to run in the 5-GHz channels or frequencies, which will not only avoid RF interference from Bluetooth devices operating in the crowded 2.4-GHz band, but also offer greater throughput.

- Try to use Bluetooth devices that are based upon Bluetooth specification version 1.2 or later which uses Adaptive Frequency Hopping (AFH) which limit the use of pseudo-random frequencies by Bluetooth devices when interference is detected. It helps prevent Bluetooth devices from interfering with other transmissions in the 2.4-GHz band.

WiFi Devices

AirMagnet Spectrum XT not only can detect and present spectrum data of various Wi-Fi devices as it does with non-Wi-Fi devices, but also has the capability to capture various Wi-Fi data about those devices and pinpoint their physical locations in a Wi-Fi network with the help of an AirMagnet-supported wireless network adapter.

This section discusses 802.11 APs. It breaks them up into two groups: 802.11a/g/n/ac/ax APs and 802.11b APs, and talks about their spectrum patterns, impact on the network, and best ways to use them in a wireless network environment.

802.11a/g/n/ac/ax APs

In general, 802.11a/g/n/ac/ax WLANs offer great advantage over 802.11b WLANs in terms of data rate, signal modulation, and so on. The table below provides a brief summary of some key parameters involving all APs built upon different IEEE 802.11 standards.

IEEE 802.11 Standard	Key Technical Parameters				
	RF Band (MHz)	Channel Width (MHz)	Maximum Data Rate (Mbps)	Modulation	Number of Spatial Streams

802.11a	5.0	20	54	OFDM/CCK	1
802.11b	2.4	20	11	DSSS/CCK	1
802.11g	2.4	20	54	DSSS/CCK/OFDM	1
802.11n	2.4 or 5.0	20 or 40	600	DSSS/CCK/OFDM	1~4
802.11ac	5.0	20, 40, 80, 160	6933	DSSS/CCK/OFDM	1~8
802.11ax	2.4 or 5.0	20, 40, 80, 160	9607	DSSS/CCK/OFDM/OFDMA	1~8

The 802.11a standard uses Orthogonal Frequency Division Multiplexing (OFDM) modulation which is a more efficient data transmission method than DSSS used by 802.11b, enabling raw data rates up to 54 Mbps. Unfortunately, despite its greater data rates, the 802.11a WLAN never reached the point to replace the 802.11b WLAN due to the fact that it operates in the 5-GHz radio frequency which is incompatible to 802.11b.

The 802.11g standard which uses the same radio frequencies and channels as the 802.11b standard but also supports OFDM offers the best of both worlds: 802.11g WLANs can achieve raw data rates up to 54 Mbps on the same radio frequencies and channels used by 802.11b WLANs. Nowadays, the vast majority of commercial wireless network devices support the 802.11g standard. Much of the WLAN client devices are dual-band supporting both 802.11a and 802.11g.

The 802.11n standard employed several techniques that improved throughput, reliability, and stability of WLANs. The key 802.11n technological breakthroughs included the capability to support up to 4 spatial streams (MIMO), transmission bursts of multiple data packets (Packet Aggregation), doubling the channel width from 20 MHz to 40 MHz (Channel Bonding), and an improved OFDM.

The 802.11ac standard introduced major improvements that were designed to provide very high throughput and data rates of up to 6933 Mbps. Some of the new technologies introduced with 802.11ac include 80MHz and 160 MHz channel widths (extended channel binding), support for up to 8 spatial streams, the ability to support multiple transmit or receive independent data streams simultaneously (MU-MIMO), and 256-QAM modulation options.

The 802.11ax standard is designed to operate on all ISM bands between 1 and 6 GHz, in addition to the 2.4-GHz and 5.0-GHz bands. To improve efficient utilization of the spectrum, this version introduces technologies like the following:

- **Spatial Frequency Reuse** - Without spatial reuse capabilities devices refuse transmitting concurrently to transmissions ongoing in other, neighboring networks. With it, a wireless transmission is marked at its very beginning helping surrounding devices to decide if a simultaneous use of the wireless medium is permissible or not. A station is allowed to consider the wireless medium as idle and start a new transmission even if the detected signal level from a neighboring network exceeds legacy signal detection threshold, provided that the transmit power for the new transmission is appropriately decreased.

- **OFDMA** - OFDMA segregates the spectrum in time-frequency resource units (RUs). A central coordinating entity (the AP in 802.11ax) assigns RUs for reception or transmission to associated stations. Through the central scheduling of the RUs contention overhead can be avoided, which increases efficiency in scenarios of dense deployments.

- **1024-QAM** - New modulation schemes allow for higher throughput.

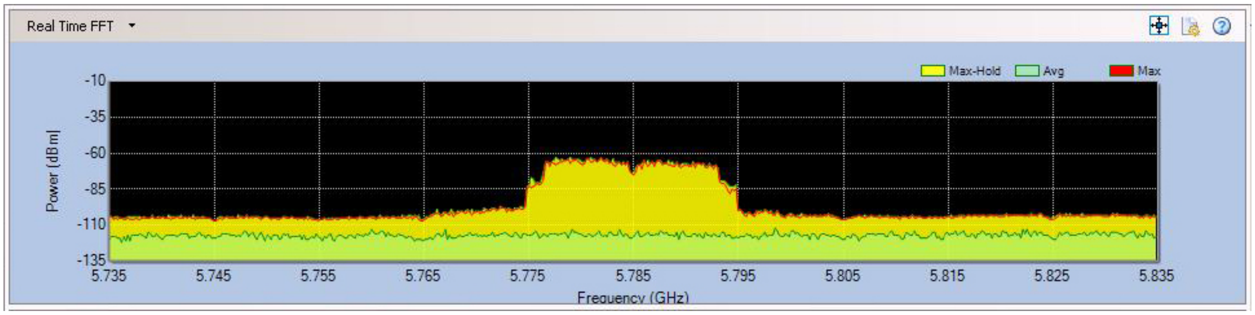
- **Downlink and Uplink MU-MIMO** - With Downlink MU-MIMO an AP may transmit concurrently to multiple stations and with Uplink MU-MIMO an AP may simultaneously receive from multiple stations. Whereas OFDMA separates receivers to different RUs, with MU MIMO the devices are separated to different spatial streams. In 802.11ax, MU-MIMO and OFDMA technologies can be used simultaneously. To enable uplink MU transmissions, the AP transmits a new control frame (Trigger) which contains scheduling information (RUs allocations for stations, modulation and coding scheme (MCS) that shall be used for each station). Furthermore, Trigger also provides synchronization for an uplink transmission, since the transmission starts SIFS after the end of Trigger.

- **Target Wake Time** - It allows devices to wake up at other periods than the beacon transmission period. Furthermore, the AP may group devices to different TWT periods thereby reducing the number of devices contending simultaneously for the wireless medium.

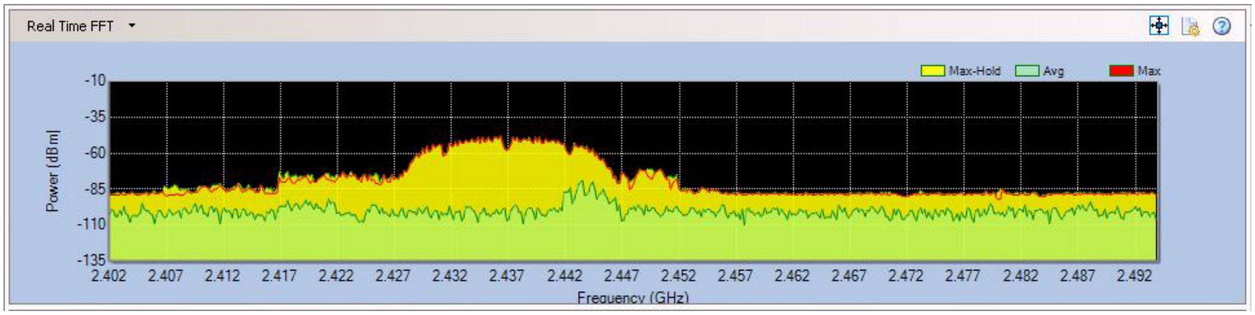
- **Guard Interval Duration** - Extended guard interval durations allow for better protection against signal delay spread as it occurs in outdoor environments.

RF Spectrum Pattern

802.11a/g/n/ac/ax APs operate in the 5-GHz, 2.4-GHz, or 2.4 and 5-GHz frequency bands. Unlike 802.11 b/g WLANs which have only three non-overlapping channels, 802.11a/n/ac/ax WLANs have 25 non-overlapping channels to choose from. The figures below show the RF spectrum pattern of 802.11g/n APs for OFDM and CCK.



RF Spectrum Pattern of an 802.11g/n AP (OFDM)



RF Spectrum Pattern of an 802.11g/n AP (CCK)

Impact on Wi-Fi Networks

802.11a uses Orthogonal Frequency-Division Multiplexing (OFDM) signal modulation method, which differs from DSSS signal modulation used by 802.11b WLANs. Since 802.11a WLANs are installed mostly indoors, OFDM is the perfect choice in that it offers better data rates than DSSS and reduces effects of multipath on signal quality and WLAN throughput.

Even though the 802.11a standard helps improve WLAN performance and reduce interference, radio signals from an 802.11a AP can travel a much shorter distance than those of 802.11b/g APs. An 802.11a AP transmitter may cover less than a quarter of the area of a comparable 802.11b AP. Brick walls and other obstructions affect 802.11a WLANs far more than they do to comparable 802.11b/g WLANs.

802.11g APs are backward-compatible with 802.11b APs but offer greater data rates. However, since they operate in the same radio frequencies as their 802.11b counterparts, they are susceptible to RF interference caused by all wireless devices operating in the 2.4-GHz frequency band. Refer to 802.11b APs.

802.11n/ac/ax APs, by design, can co-exist with 802.11a APs in the 5-GHz band and 802.11g APs in the 2.4-GHz band since they all use OFDM. The presence of 802.11b devices makes communications a little challenging in the 2.4-GHz band because it cannot understand OFDM which is used by both 802.11b and n standards. In that case, OFDM client devices may have to switch to the older signal modulation (DSSS) to protect their high-rate OFDM transmissions, resulting reduced network efficiency.

Recommended Courses of Action

If you are running an 802.11a/g/n/ac/ax WLAN, take the following actions into consideration when installing and managing your WLAN:

- Since radio signals from 802.11a/n/ac/ax APs working on the 5.0-GHz band travel a much shorter distance, make sure that you have enough APs to offer adequate WLAN coverage if you are using an 802.11a/n/ac/ax WLAN.
- If you need more than one AP, make sure to point them to different non-overlapping channels.
- Be aware of other wireless devices that may also be operating in the same radio frequencies and channels as your WLAN APs do. Make sure that your 802.11 WLAN APs use different channels than those used by those competing devices.
- Upgrade your WLAN to the 802.11ax standard, if you can.

802.11b APs

802.11b APs operate at frequencies in the unlicensed 2.4-GHz Industrial, Medical and Scientific (IMS) band. Because the band is free and used globally, it is crowded with all kinds of 2.4-GHz-compliant commercial products, including:

- WLAN devices (802.11g)
- Cordless phones (digital or analog)
- Bluetooth devices
- Wireless (security) cameras
- Baby Monitors (video and/or audio)
- Microwave ovens

As the number of these devices increases, the 2.4-GHz IMS band is becoming more and more congested. As a result, network performance degradation has become a major issue facing network administrators managing 802.11b/g WLANs. It has long been recognized that the main culprit for WLAN performance degradation is RF interference caused by these competing devices in the 2.4-GHz band. RF interference occurs when two or more RF devices are transmitting at the same frequency at the same time. RF interference causes over-the-air collision which can lead to data corruption and loss.

802.11b APs can operate on one of 13 (11 in the US) channels in the 2.4-GHz IMS band, each being 22 MHz wide and 5 MHz apart. Because each of these channels takes up roughly a quarter of the 2.4-GHz spectrum and adjacent channels tend to interfere with each other, 802.11b WLANs are typically installed using one of three non-overlapping channels, namely Channels 1, 6, and 11.

The table below shows the operating channels for 802.11b WLANs in North America, with Channels 1, 6 and 11 highlighted in grey as non-overlapping channels.

Channel	Minimum Frequency	Center Frequency	Maximum Frequency

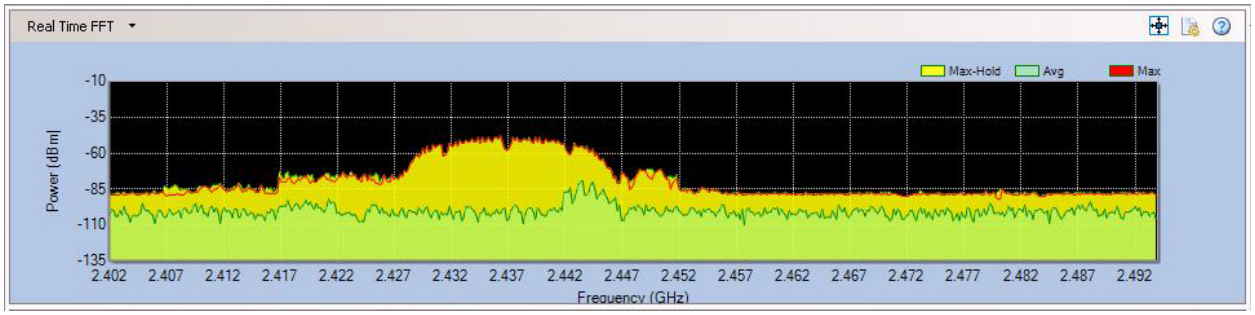
1	2.401	2.412	2.423
2	2.405	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.446	2.457	2.468
11	2.451	2.462	2.473

RF Spectrum Pattern

802.11b APs use Direct Sequence Spread Spectrum (DSSS) signal modulation method which is very susceptible to signal multipath. Signal multipath occurs when radio signals are reflected on their way between the transmitter and the receiver. This could happen when radio signals from an AP are blocked by metal furniture, dry walls, and other structural elements common in office buildings. Signal multipath has a huge impact on data quality and WLAN throughput because it causes transmission errors and requires retransmission.

802.11b WLAN APs typically use up to +20 dBm (100mW) transmit power and -80 dBm ~ -90dBm of receive sensitivity. Their bit transfer rate is 11 Mbps (maximum).

The figure below shows the typical RF pattern of an 802.11b AP.



RF Spectrum Pattern of an 802.11b AP

Impact on Wi-Fi Networks

Since 802.11b APs use a fixed bandwidth of 22 MHz in the 2.4-GHz spectrum, the probability of collisions or interference between 802.11b APs or with other 2.4-GHz devices largely depends on the channel they operate. If they are on the same channel or overlapping channels, the probability is high. Otherwise, the chances of collision are low.

Recommended Courses of Action

Since 802.11b/g WLANs are operating in the crowded 2.4-GHz IMS band with so many competing devices (including 802.11b/g devices themselves), we recommend the following actions in order to minimize or eliminate RF interference to 802.11b/g WLANs:

- Prior to installing an 802.11b WLAN, conduct a thorough RF survey of the WLAN site to know all 2.4-GHz devices operating in the Wi-Fi environment and the channels they are using.
- Install 802.11b WLANs by setting the APs to non-overlapping channels 1, 6, and 11, especially when more than one AP is needed.
- Try to avoid the use of HFSS devices in close proximity of an 802.11b WLAN to minimize RF interference.
- If you have more than one 802.11b AP, adjust the transmit power levels on the APs to minimize mutual interference between APs.
- Try to keep WLAN APs at a good physical distance to avoid mutual interference.
- Upgrade your WLAN to 802.11ac or 802.11ax standard.

Analog Cordless Phones

Analog cordless phones are another source of interference to 802.11a/b/g/n/ac/ax wireless LANs (WLANs). Unlike digital cordless phones, analog cordless phones use narrowband transmission which occupies only a narrow bandwidth of the RF spectrum. Because of this, they can cause severe interference to an 802.11a/b/g/n/ac/ax AP operating in the same channel or frequency even though no significant interference to APs on other non-overlapping channels has been noticed.

One lab study found that an analog cordless phone transmitting on 2.412-GHz frequency which happens to be the center frequency of Channel 1 of the 802.11b/g/n/ax WLAN can effectively take out the wireless connection on that channel the moment the phone which is placed next to an AP is turned on, whereas connections on the other two non-overlapping channels (6 and 11) were barely affected. The study also found that network throughput could drop by 99% with the analog cordless phone placed at 50 feet away from the AP, 20% at 100 feet away, and 5% at 150 feet away. The study concluded that analog cordless phones, if placed close to APs, can virtually disrupt wireless connection on the channel they operate.

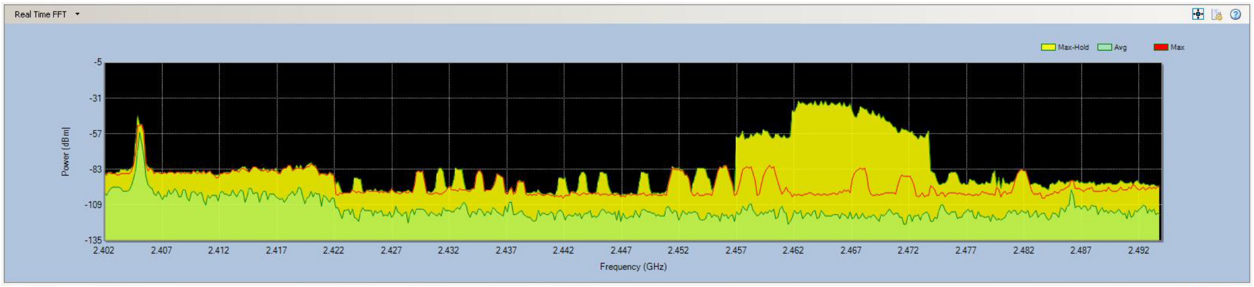
RF Spectrum Pattern

There are numerous analog cordless phones available on the market today. They are widely used in homes and businesses and are also a source of RF interference to the 802.11 WLAN.

Below is a short list of analog cordless phones:

- GE 27923GE (2.4-GHz)
- Uniden EXP4540 (2.4-GHz)

The following figure shows the RF spectrum pattern of a 2.4-GHz analog cordless phone.



RF Spectrum Pattern of a 2.4-GHz Analog Cordless Phone

Impact on 802.11 WLAN

Because the 2.4-GHz and 5-GHz radio bands are unlicensed (free to all), there are numerous 2.4-/5-GHz analog cordless phones by different manufacturers available on the market. They are widely used in homes and businesses where 802.11a/b/g/n/ac/ax WLANs are deployed. They have been recognized as a major source of RF interference for 802.11a/b/g/n/ac/ax WLANs. You may tackle these interfering 2.4-/5-GHz analog cordless phones by first identifying and locating them in your WLAN.

Recommended Courses of Action

Once interfering analog cordless phones are successfully located, you can take the following actions to minimize or eliminate their RF interference to your 802.11 WLAN:

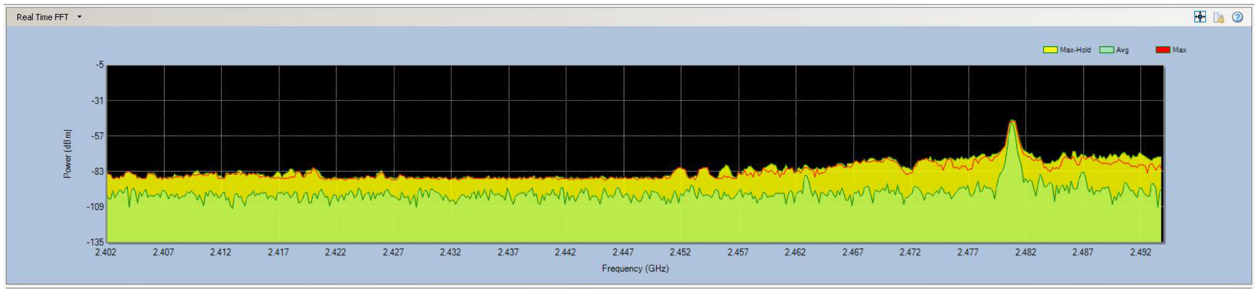
- If you have an 802.11a/b/g/n/ac/ax WLAN, avoid or stop using analog cordless phones on the same channel as your 802.11a/b/g/n/ac/ax APs. Instead try to set them on other non-overlapping channels.
- If you are using an 802.11b/g/n/ax WLAN, try to use 5.8-GHz or even old 900-MHz analog cordless phones which use different radio bands and channels.
- If you have an 802.11a/n/ac/ax WLAN, avoid or stop using 5.8-GHz cordless phones. Instead replace them with 2.4-GHz cordless phones.
- If you have an 802.11b/g/n/ax WLAN and 2.4-GHz analog cordless phones are a must, try to use those more expensive but less interfering ones which use Digital Spread Spectrum (DSS) technology that offer wider range, better security, with less interference.
- If optimal WLAN performance is not an issue, you may continue use your 2.4-/5.8-GHz cordless phones along with 802.11a/b/g/n/ac/ax WLANs but try to maximize the distance between WLAN APs and cordless phone bases to minimize RF interference between or among them.
- Consider upgrading your WLAN to 802.11ax standard, which not only provides better RF interference avoidance mechanisms but also offer greater throughput.

Baby Monitors

Wireless baby monitors (digital or analog) use radio frequencies to transmit their signals. These same radio frequencies are also used by wireless networks installed in the home environment. As a result, RF interference will occur when the two competing systems are operating in the same radio frequencies.

RF Spectrum Pattern

Most wireless baby monitors on the market today use the 2.4-GHz frequency, a bandwidth also used by the 802.11b/g/n/ax wireless network and many other wireless devices. The figure below shows the RF spectrum pattern of an analog baby monitor in the 2.4-GHz frequency band.



RF Spectrum Pattern of a Baby Monitor

AirMagnet Spectrum XT will detect FHSS, DSSS and Single Carrier models of baby monitors.

Impact on Wi-Fi Networks

Generally speaking, RF interference is not an issue when a baby monitor is not in use. However, when it is in operation, it could have a negative impact on an 802.11 network, especially when they are in close proximity. When the baby monitor is turned on, the device will compete for bandwidth with the wireless network that is using the same radio frequency, causing the wireless network to experience performance degradation as a result of RF interference, and vice versa. The impact is more obvious for web applications involving downloading files over the Internet or Voice over IP. The figure below shows the RF spectrum pattern of a wireless analog baby monitor using the 2.4-GHz frequency band.

Recommended Courses of Action

Once an interfering wireless baby monitor is successfully identified, you can take all or some of the following actions to minimize or eliminate the RF interference it causes to your 802.11 WLAN.

- Check the channels or frequencies used by your wireless network and wireless baby monitor to make sure that they are not competing on the same channel or frequency.
- Since most of the wireless baby monitors today operate in the 2.4-GHz frequency band, try to upgrade your wireless network to the 802.11ax standard.
- If you do not want to upgrade your wireless network, then try to get a wireless baby monitor that uses any radio frequency other than 2.4 GHz, such as 900 MHz.
- Since a baby monitor does not severely disrupt a wireless network unless the two are installed close together, try to place the wireless baby monitor and the wireless router as far apart as possible.

Digital Cordless Phones

Most digital cordless phones on the market today operate in either the 2.4-GHz or 5.8-GHz radio band, which happen to be the channel or frequencies used by 802.11a/b/g/n/ac/ax wireless LANs (WLANs). The problem is that the two are completely different systems that do not understand each other. As a result, radio signals from the two different systems will collide and cause mutual RF interference. This is especially the case when 2.4-GHz FHSS digital cordless phones are involved. Because they use FHSS modulation, their radio signals hop from one frequency to another across the entire 2.4-GHz band, in searching for the best channel or frequency to use. This hopping behavior will cause persistent RF interference to the 802.11b/g/n/ax WLAN in close proximity.   As a result, no matter which channel your WLAN use or switch to (Remember that there are only 3 non-overlapping channels in the 2.4-GHz radio band, that is, channels 1, 6, and 11), it is hard for 802.11b/g/n/ax APs to escape the RF interference caused by 2.4-GHz FHSS digital cordless phones. Such sources of interference can cause significant disruption in WLAN service and performance degradation.

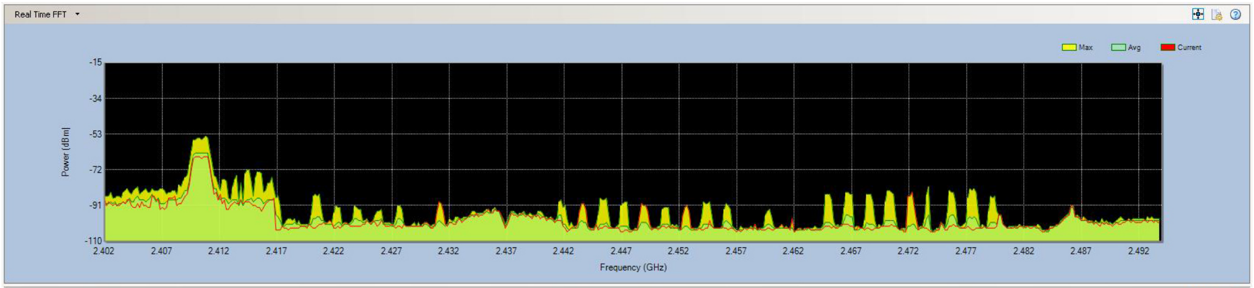
RF Spectrum Pattern

There are numerous digital cordless phones available on the market today. They are widely used in homes and businesses and are also a source of RF interference to the 802.11 WLAN.

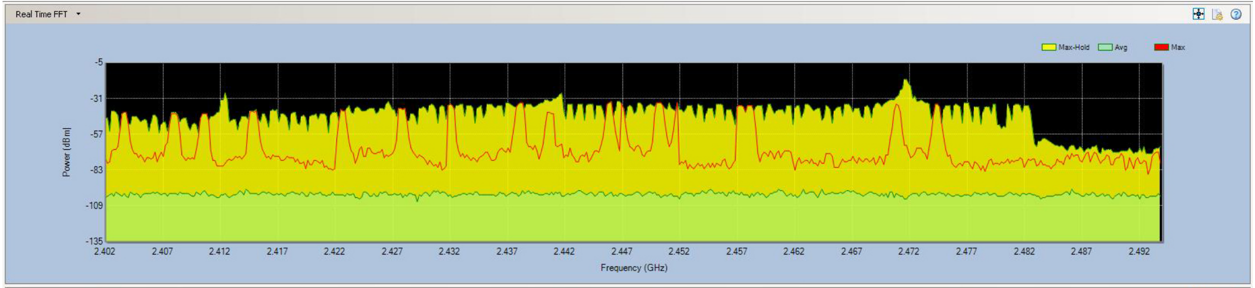
Below is a short list of digital cordless phones:

- Panasonic KX-TGA271 (2.4-GHz, FHSS)
- Panasonic KX-TG2700S (2.4-GHz, FHSS/DSS)
- Panasonic KX-TG5050 (5.8-GHz, DSS)
- AT&T 2355 (2.4-GHz)
- AT&T E5965C (5.8-GHz, FHSS/DSS)
- Uniden EX15660 (5.8-GHz)

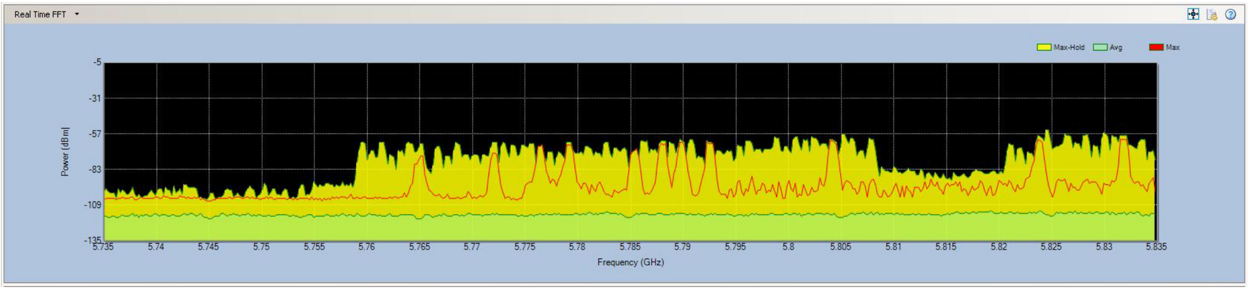
The figures below show the RF spectrum patterns of a 2.4-GHz DSS, 2.4-GHz FHSS, and 5.8-GHz FHSS digital cordless phone, respectively.



RF Spectrum Pattern of a 2.4-GHz DSS Cordless Phone



RF Spectrum Pattern of a 2.4-GHz FHSS Digital Cordless Phone



RF Spectrum Pattern of a 5.8-GHz FHSS Digital Cordless Phone

Impact on 802.11 WLAN

Because the 2.4-GHz and 5-GHz radio bands are unlicensed (free to all), there are numerous 2.4-/5-GHz digital cordless phones by different manufacturers available on the market. They are widely used in homes and businesses where 802.11a/b/g/n/ac/ax WLANs are deployed. They have been recognized as a major source of RF interference for 802.11a/b/g/n/ac/ax WLANs. You may tackle these interfering 2.4-/5-GHz cordless phones by first identifying and locating them in your WLAN.

Recommended Courses of Action

Once interfering cordless phones are successfully located, you can take the following actions to minimize or eliminate their RF interference to your 802.11a/b/g/n/ac/ax WLAN:

- Do not waste your time switching AP channels, because RF signals from digital cordless phones spread over all channels or frequencies in the band they operate. Just adjusting AP channel is not the solution.
- If you have an 802.11b/g/n/ax WLAN, avoid or stop using 2.4-Ghz FHSS cordless phones. Instead replace them with 5.8-GHz or even old 900-MHz cordless phones which use different radio bands and channels.
- If you have an 802.11a/n/ac/ax WLAN, avoid or stop using 5-GHz cordless phones. Instead replace them with 2.4-GHz cordless phones.
- If you have an 802.11b/g/n/ax WLAN and 2.4-GHz cordless phones are a must, try to use those more expensive but less interfering ones which use Digital Spread Spectrum (DSS) technology that offer wider range, better security, with less interference.
- If optimal WLAN performance is not an issue, you may continue use your 2.4-/5-GHz cordless phones along with 802.11a/b/g/n/ac/ax WLANs but try to maximize the distance between APs and cordless phone bases to minimize their RF interference between each other.
- Consider upgrading your WLAN to 802.11ax standard, which not only provides better RF interference avoidance mechanisms but also offer greater throughput.

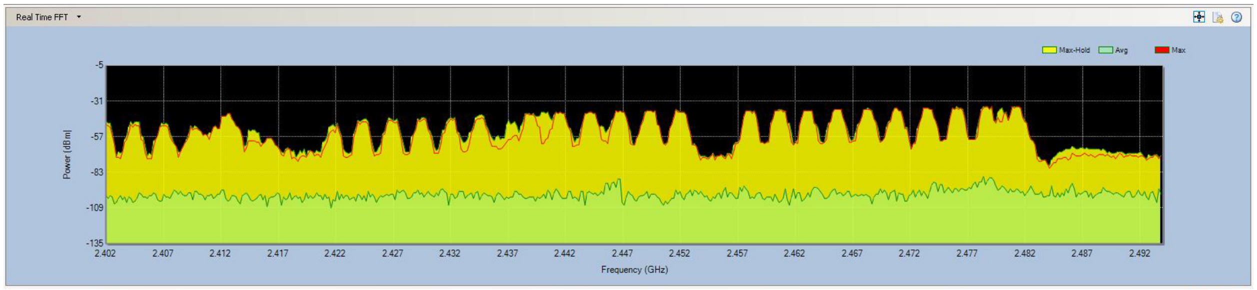
Digital Video Monitor

A digital video monitor is typically made up of three components: a video camera, a transmitter to send the signal, and a receiver to receive the signal. The system works in such a way that the wireless camera transmits video from the built-in transmitter to the receiver, which is connected to a display device (monitor) or a recording device.

Most digital video monitors operate on the 2.4-GHz frequency – an unlicensed radio band also used by 802.11b/g/n/ax WLANs, cordless phones, Bluetooth devices, and microwave ovens, and so on. Like the other non-WiFi devices operating in the 2.4-GHz frequency band, digital video monitor installed in close proximity of an 802.11b/g/n/ax WLAN can interfere with the normal operation of the WLAN. Unlike the other RF interfering devices operating in the 2.4-GHz band, radio signals from the transmitter of a digital video monitor can travel a relatively long range which varies from 200 to 700 feet (line of sight), depending on the physical conditions of the site. Typically, multiple cameras are needed in order to provide full, overlapping coverage of one site. To make matters worse, digital video monitors installed in homes and businesses are left on all the time. And so is the RF interference they cause to the 802.11 WLAN close to them.

RF Spectrum Pattern

Digital video monitors come in all shapes and sizes. They include wireless surveillance cameras, spy cameras, and so on. They are widely used in homes and businesses where the 802.11 WLAN is deployed. Their presence can cause serious performance issues in the WLAN. The figure below shows the RF spectrum pattern of a wireless camera using the 2.4-GHz frequency band.



RF Spectrum Pattern of a 2.4-GHz Digital Video Camera

Impact on 802.11b/g/n/ax WLAN

Because digital video monitors are widely used in homes and businesses where WLANs are deployed, radio signals from these devices have long been identified as a source of RF interference to 802.11b/g/n/ax WLANs in these settings. They can significantly slow down Internet applications such as Web file download and surfing.

Recommended Courses of Action

Once the interfering wireless security cameras are successfully identified, we recommend the following actions to minimize or eliminate the RF interference they cause to the 802.11 WLAN.

- If you are using an 802.11b/g/n/ax WLAN, avoid using 2.4-GHz digital video monitors. Instead, use 5.8-GHz video monitors that operate in the less crowded 5-GHz radio band. Or upgrade your WLAN to the 802.11ax standard which offers better interference avoidance.
- If you are using an 802.11a/n/ac/ax WLAN, avoid using 5.8-GHz digital video monitors.
- Check the operating channels on the digital video monitors, making sure that they do not overlap with the operating channels of the WiFi network.

Wireless Game Controllers

Wireless game controllers are handheld devices for gaming consoles without wires. Using wireless technology, wireless game controllers allow players to sit virtually anywhere (up to 30 feet away from the game console) in the room, making game play less restrictive.

For better coverage, most wireless game controllers operate on the 2.4-GHz frequency– an unlicensed radio band also used by 802.11b/g/n/ax WLANs, cordless phones, Bluetooth devices, and microwave ovens, and so on. Like the other non-Wi-Fi devices operating in the 2.4-GHz frequency band, wireless game controllers installed in close proximity of an 802.11b/g/n/ax WLAN can interfere with the normal operation of the WLAN.

Wireless game controllers are available for all major gaming consoles and computers. The following are some of the major brands:

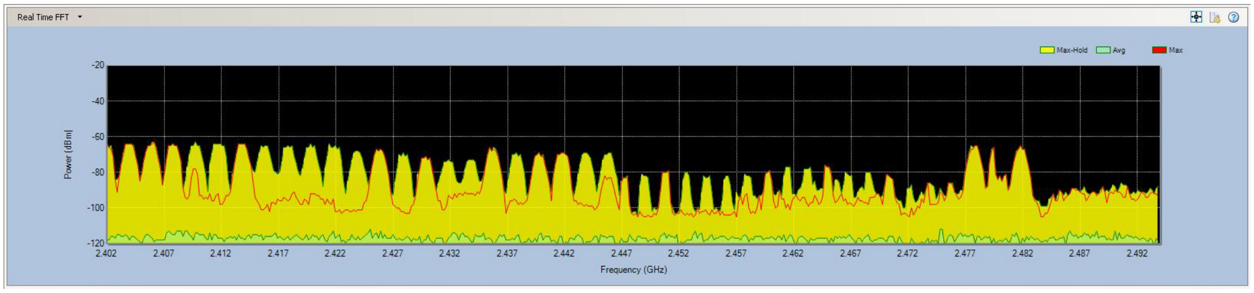
- Sony PlayStation® Wireless Game Controller
- Microsoft Xbox® Wireless Remote Controller

AirMagnet Spectrum XT will identify and list the following game controllers by their brand name: PlayStation and Xbox.

Note: Nintendo Wii, Sony Playstation 3, and newer gaming consoles are Bluetooth devices and will be detected as Bluetooth interferers. Playstation is a registered trademark of Sony Corporation.

RF Spectrum Pattern

Wireless game controllers come in all shapes and sizes. They are widely used in homes and even some businesses settings where the 802.11 WLAN is deployed. Their presence can cause serious performance issues in the WLAN. The figure below shows the RF spectrum pattern of a wireless game controller using the 2.4-GHz frequency band.



RF Spectrum Pattern of a 2.4-GHz Game Controller Transmitter

Impact on 802.11b/g/n/ax WLAN

Because wireless game controllers operate in the same radio frequency as the 802.11b/g/n/ax WLAN, radio signals from these devices have long been identified as a source of RF interference to 802.11b/g/n/ax WLANs in homes and businesses where they are used. They can significantly slow down Internet applications such as Web file download and surfing.

Recommended Courses of Action

Once the interfering wireless game controllers are successfully identified, take the following actions to minimize or eliminate the RF interference they cause to the 802.11 WLAN.

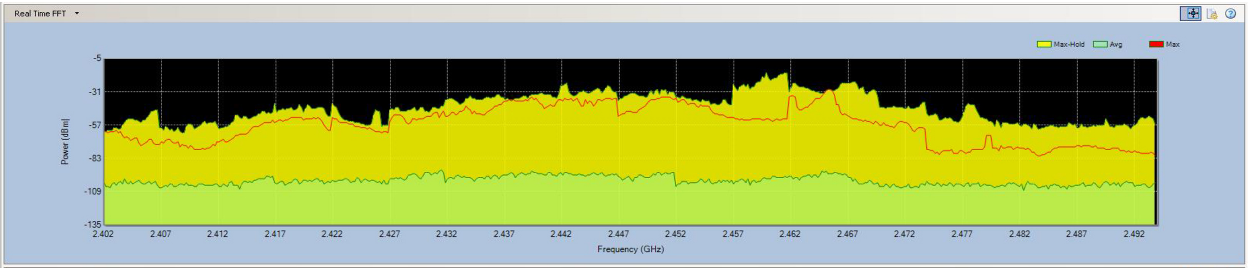
- Try to keep a "safe distance" between your 802.11b/g/n/ax AP and wireless game controller so as to keep interference to the minimum.
- Check the operating channels on the wireless game controller to make sure that they do not overlap with the operating channels of your 802.11b/g/n/ax network.
- If possible, consider upgrading your WLAN to the 802.11ax standard.

Microwave Ovens

Most microwave ovens used in homes and businesses today operate in the 2.45-GHz frequency, which is roughly the frequency of Channel 9 in an 802.11b/g/n/ax WLAN. When a microwave oven is operating, the radio waves emitted from the radio antenna inside the oven are mostly confined within the oven's case, with only a small amount leaking out sometimes, especially with old ovens. To an 802.11b/g/n/ax WLAN operating within close proximity, the radio waves that leak out of the microwave oven are a source of RF interference that may cause serious performance issues. This is because the interfering radio signals leaking out of the microwave oven will cause WiFi station to hold off transmission until the airwave is clear, causing network delay in the process. Furthermore, interfering RF signals do not follow the rules of the 802.11 protocols and are rather unpredictable: they can come and go at any time, disrupting normal communications between 802.11 devices in the WLAN. Study found that a microwave oven operating within ten feet of an 802.11b/g/n/ax access point (AP) could cause a 75% drop in network throughput on Channel 9 (2.45 GHz frequency). Significant drop in throughput was also observed on adjacent channels such as Channels 8, 10, and 11. The impact was more severe near the edges of the AP's coverage area.

RF Spectrum Pattern

The figure below shows the RF spectrum pattern of radio signal from a microwave oven.



RF Spectrum Pattern of a Microwave Oven

Impact on 802.11b/g/n/ax WLAN

Because microwave ovens are widely used in homes and businesses where WLANs are deployed, radio signals leaking out of an operating microwave oven have long been identified as a source of RF interference to 802.11b/g/n/ax WLANs in these settings. They can significantly slow down basic Internet applications such as Web file download and surfing. In the worst cases, they can knock out the network connection completely.

Recommended Courses of Action

Once the interfering microwave oven is successfully located, take the following actions to minimize or eliminate the RF interference it causes to the 802.11 WLAN:

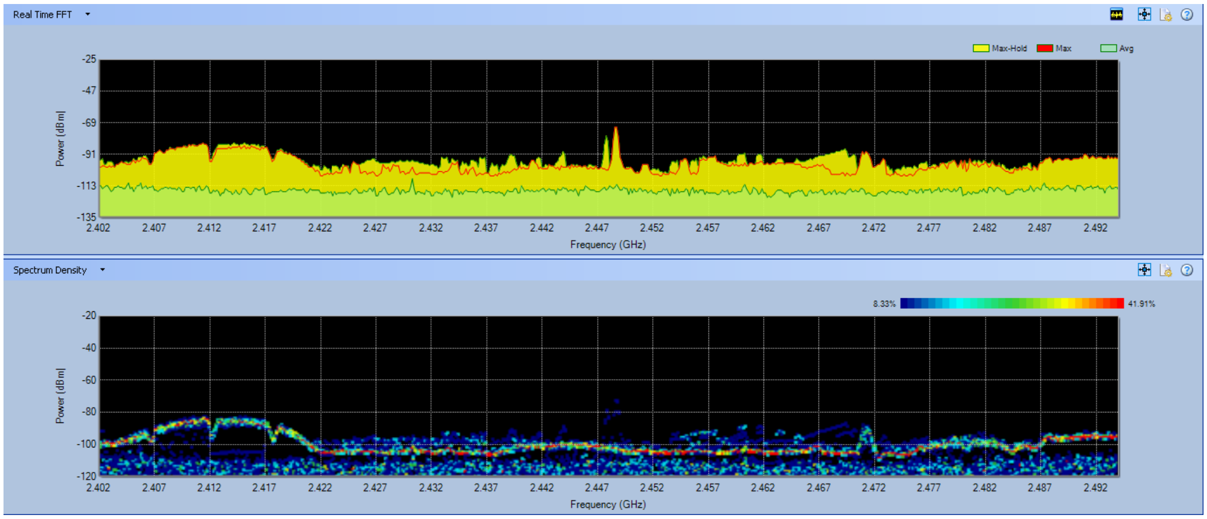
- Avoid using 802.11b/g/n/ax WLAN near a microwave oven.
- When actively using WLAN applications (for example, downloading files, video-conferencing, searching the Internet), make sure to keep a “safe” distance (at least 10 feet away) from an operating microwave oven. The farther away you are from the microwave oven, the less the interference.
- Find out the center frequency (which may vary depending on make, brand, or model) of a microwave oven from its label, and try to steer your WLAN away from it.
- Upgrade your WLAN to 802.11ac/ax, which will not only avoid RF interference from microwave ovens operating in the crowded 2.4-GHz band but also offer greater throughput.

Motion Detector

Motion detectors are devices that use a variety of methods to determine if a body of a significant size is moving through an area, usually as part of a security or energy management system. While most models use in infrared detection system, some newer models incorporate a microwave detection system. In some models, this microwave detection system transmits on a narrow band of frequency in the 2.4-GHz band. While only active at times of motion detection, in areas of high pedestrian traffic, or areas of high WLAN traffic, these devices present the possibility of disrupting WLAN traffic if the transmitting frequency of the device corresponds with the channel the WLAN is operating on.

RF Spectrum Pattern

Below is a sample of what the spectrum pattern for what a Motion Detector would look like in a relatively noiseless 2.4GHz spectrum.



Spectrum Pattern for a Motion Detector

Impact on 802.11b/g/n/ax WLAN

The impact on 802.11 networks depends on the amount of pedestrian traffic near the motion detector.

- Because this technology only transmits a signal when the correct parameters for motion detection are met, in areas of low pedestrian traffic, the impact on a WLAN network will be low. The device may cause intermittent interference only if it is transmitting on a frequency within the channel width of a WLAN AP, and only if it is significantly close enough to the WLAN network to have an impact.
- If the motion detector is in an area of high pedestrian traffic, is on a frequency within the channel width of the WLAN AP, and if it is significantly close enough to interfere with the WLAN, this device type can have a significant impact on a WLAN, behaving almost as a Narrow-band Jammer would.

Recommended Courses of Action

• If possible, change the channel that your WLAN is operating on to one that is unaffected by the Motion Detector.

• You may consider changing from the 2.4GHz band to one of the 5GHz bands, as these bands will not be affected by the Motion Detector.

• If you have to use your Motion Detectors along with 2.4GHz WLANs, try to maximize the distance between APs and Motion Detectors to minimize their RF interference.

Non-Bluetooth Wireless Mouse

Since the 2.4-GHz and 5-GHz wireless spectrums are unregulated, companies are allowed to use those bands for more than just WLAN traffic. In response to some of the concerns about the interference between WLAN and Bluetooth networks, or between WLAN and continuous transmitter technologies like some cordless phones, some companies have developed technologies that allow their devices to operate in a way that minimizes the impact on WLAN networks. With the ability to find a frequency with the least amount of WLAN traffic in the 2.4-GHz spectrum, non-bluetooth wireless mice minimize their impact on the WLAN network.

RF Spectrum Pattern

Currently the only devices detected for this device type are made by Logitech. This is based on the new Logitech Advanced 2.4 GHz wireless technology. Some of the models that ship with this technology include the following:

- Marathon Mouse M705
- Marathon Mouse M310
- Anywhere Mouse MX™
- Wireless Mouse M510
- Wireless Mouse M305
- Performance Mouse MX™
- Wireless Mouse M505
- MX™ 1100 Cordless Laser Mouse
- VX Nano Cordless Laser Mouse
- MX Air™ Rechargeable Cordless Air Mouse

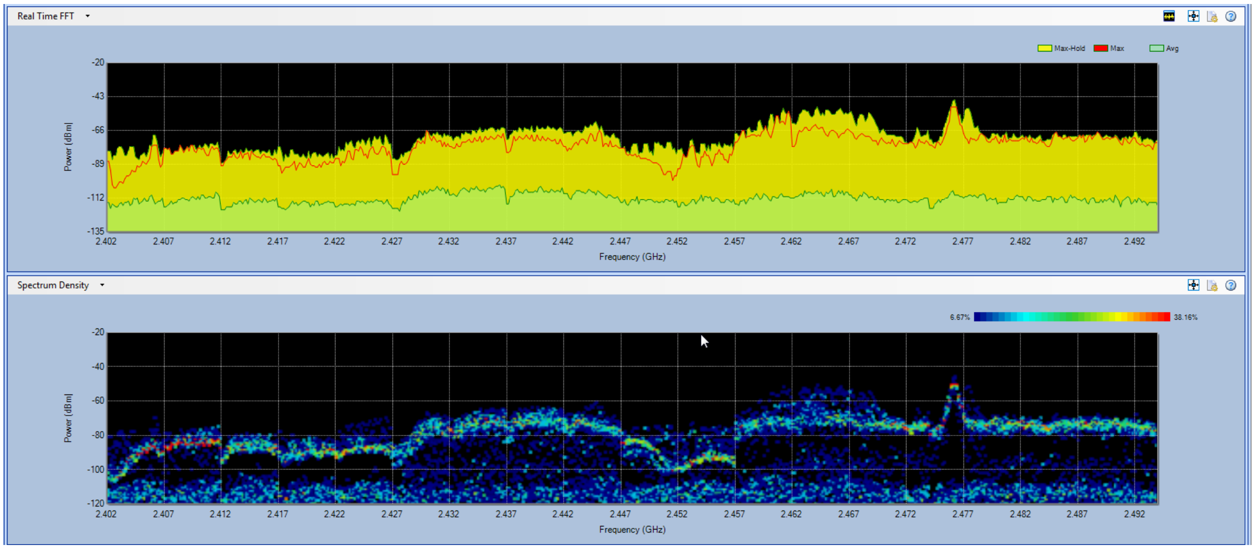
In particular, Logitech advanced 2.4 GHz wireless technology hops at 250 times/sec and supports bi-directional data transmission with error correction to maintain a reliable RF link. And Logitech's architecture automatically pairs your peripheral to the provided transceiver that is attached to your computer, while avoiding conflicts with other devices. In other words, when you use a Logitech peripheral with advanced 2.4 GHz technology, you can be certain that when you move your mouse or type on your keyboard, your commands will be carried out instantaneously.

Logitech's proprietary wireless protocol is used together with a high-performance RF transceiver. This is a highly integrated, single-chip transceiver that operates in the 2.4 GHz ISM band and is ideally suited for the most demanding applications. In addition to the technical features described above, this technology also provides the lowest-power RF solution on the market today, translating into significantly longer battery life.

Feature	**Logitech Advanced 2.4GHz Wireless Technology**	**Bluetooth**
Range	10 m	10-100 m

Bandwidth	2Mbps bursts	1-3 Mbps bursts
Latency at reconnection	<90 ms	.5-2 seconds
Interference resistance	Best	Best
Battery life	Best	Good
Report rate	125 rpt/s or faster	80 rpt/s
USB interface	FS	FS

Below is a sample of what the spectrum pattern for a Non-Bluetooth Wireless Mouse would look like in a relatively noiseless 2.4GHz spectrum.



Impact on 802.11 WLAN

Since this technology is designed to minimize its interference with WLANs, the impact of having a few of these devices in the spectrum should be low. If there are no frequencies that have low levels of WLAN traffic, the device will choose the least used frequency, which may cause minor disruptions to the WLAN.

Recommended Courses of Action

• Ensure that the WLAN network is operating on non-overlapping channels like 1, 6, and 11. This will maximize the number of frequencies with little to no WLAN traffic on them.

• If multiple devices of this type exist in the spectrum, begin removing devices until the interference clears up.

• If you have to use your non-Bluetooth wireless mice along with 802.11b/g/n/ax WLANs, try to maximize the distance between APs and wireless mice to minimize their RF interference between each other.

• Consider upgrading your WLAN to 802.11ax standard, which not only provides better RF interference avoidance mechanisms but also offer greater throughput

Possible Interferer

Given the fact that the WLAN is operating in an environment crowded with numerous non-Wi-Fi devices and that the RF spectrum patterns from some of the non-Wi-Fi devices are not that easy to tell from one another at the first glance, sometimes it could be difficult for the application to recognize or categorize an RF signal it has detected. That’s why AirMagnet Spectrum XT uses Possible Interferer as category of devices it is able to detect.

The Possible Interferer classifier is based on the non-Wi-Fi channel utilization data that the application has collected in a given period of time. It averages the data for each channel over the last 5 scans. If the average non-WLAN channel utilization data is above a threshold, currently sent around 20% (of the time), then a Possible Interferer detection is declared. This is done to make sure the application reports an interfering device whose category cannot be determined for the time being.

When a known interferer is seen, it is usually classified and reported before it can be declared a Possible Interferer. However, if it does take a while for a classifier to detect a known interferer, then a Possible Interferer is declared instead, before the known interferer is declared. However, if something started as a Possible Interferer is later classified as a known interferer as more data becomes available, it will then be declared as a known interferer. The moment that happens, then the Possible Interfere message is cancelled or stopped.

Impact on 802.11a/n/ac/ax WLAN

All interferers in the WLAN environment, whether known or unknown, can interfere with the operation of the WLAN, consuming network bandwidth, causing traffic congestion, and degrading network performance.

Recommended Courses of Action

The WLAN shares the same airwave with numerous non-Wi-Fi devices, which may cause interference to the networks. To ensure the normal operation of the WLAN, it is important to constantly monitor the RF environment in network for sources of RF interference and take immediate action to mitigate, avoid, or eliminate them.

Radar

The 5-GHz band is an Unlicensed National Information Infrastructure (UNII) band, which is divided into several segments, each being designated for a specific use. The UNII-2 (5.25 GHz~5.35 GHz) and UNII-2 extended (5.47 GHz~5.725 GHz) bands used to be set aside exclusively for military and weather radar systems. When the FCC decided to open these bands up for Wi-Fi network, its ruling came with an important caveat: Dynamic Frequency Selection version 2, or DFS2, compliance.

DFS is a mechanism that tells the transmitter to dynamically listen for radar signals in the airwave and automatically switch to another channel if a radar signal is detected. The mechanism is designed to protect the incumbent military and weather radar systems from the RF interference from 802.11a/n/ac/ax devices in their vicinity. With DFS2, the transmitter on a Wi-Fi device will continuously listen for radar signals, both before and during transmission. If a radar signal is detected on a channel, it will either vacate that channel or flag it as unavailable.

DFS2 is a must-have on 802.11a/n/ac/ax APs in order for 802.11a/n/ac/ax network systems to co-exist with military and weather radar systems. According to the latest FCC ruling, all Wi-Fi devices operating in the UNII-2 and UNII-2 extended bands are required to support DFS, to detect and automatically switch channels to prevent WLAN operations from interfering with military or weather radar systems. The mandate became effective on July 20, 2007 in the US and Canada. A similar mandate became effective on April 1, 2008 in the EU.

Since then, in April 2009 new EN 301 893 v1.5.1 requirements also called DFS-3 Compliance have also been enforced for 802.11 APs operating in Europe.

AirMagnet Spectrum XT can detect all 5 types of radar waveforms as described in "FCC Memorandum Opinion and Order 06-96", bins 1-5 and radars as specified in the ETSI specification EN 301 893 v1.5.1.

Impact on 802.11a/n/ac/ax WLAN

Since the 802.11a/n/ac/ax wireless network shares the same radio frequency bands/channels with military and weather radar systems, the FCC regulation and requirements on DFS/DFS2/DFS3 undoubtedly puts some serious challenge to the operation of the 802.11a/n/ac/ax wireless network. Care must be taken to ensure that WLAN operation will not interfere with or disrupt the normal operation of radar systems.

Recommended Courses of Action

Based on FCC regulations, take the following actions on the part of the 802.11a/n/ac/ax wireless network in order to minimize or eliminate its potential interference with military and/or weather radar systems:

- Make sure all 802.11a/n/ac/ax devices that are operating on your WLAN are DFS2 or 3-certified.
- If you have uncertified 802.11a/n/ac/ax devices on your network, make sure that the UNII-2 and UNII-3 bands/channels are blocked.

- If you have 802.11a/n/ac/ax devices that were manufactured prior to July 20, 2007 (US), then check with the vendors for possible firmware upgrade. The same goes for DFS3 requirements in Europe.

RF and Narrowband Jammers

A jammer is any device which serves the purpose to flood a frequency or range of frequencies with un-modulated Radio Frequency (RF) noise. Depending on the power of the device, the range of the jamming effect can be over a small or large area, though most handheld devices have an operational radius of 10 to 15 meters. The types of jammers fall into two main categories: narrow-band and wide-band. Narrow-band jammers usually affect less than 5 MHz at a time, while wide-band jammers have the ability to disrupt an entire band of WLAN traffic. Wireless jammers can be used to disrupt Wi-Fi, WLAN, or Bluetooth networks in the 2.4-2.5GHz frequency range. Jammers can also serve a positive purpose, allowing users to cut off Wi-Fi connections in targeted areas of a WLAN and prevent leaking out sensitive data.

- **RF Jammer:** Designed to block Wi-Fi/WLAN/Bluetooth networks, which work on 2.4GHz. It could help you cut off WiFi connections in targeted areas of a WLAN and prevent leaking out sensitive data.

- **Narrowband Jammer:** Designed to block Wi-Fi/WLAN/Bluetooth networks for a specific area of the screen on a 2.4GHz frequency. It could help to cut off Wi-Fi connections in targeted areas of a WLAN and prevent leaking out sensitive data. Refer to the figures below.

RF Spectrum Pattern

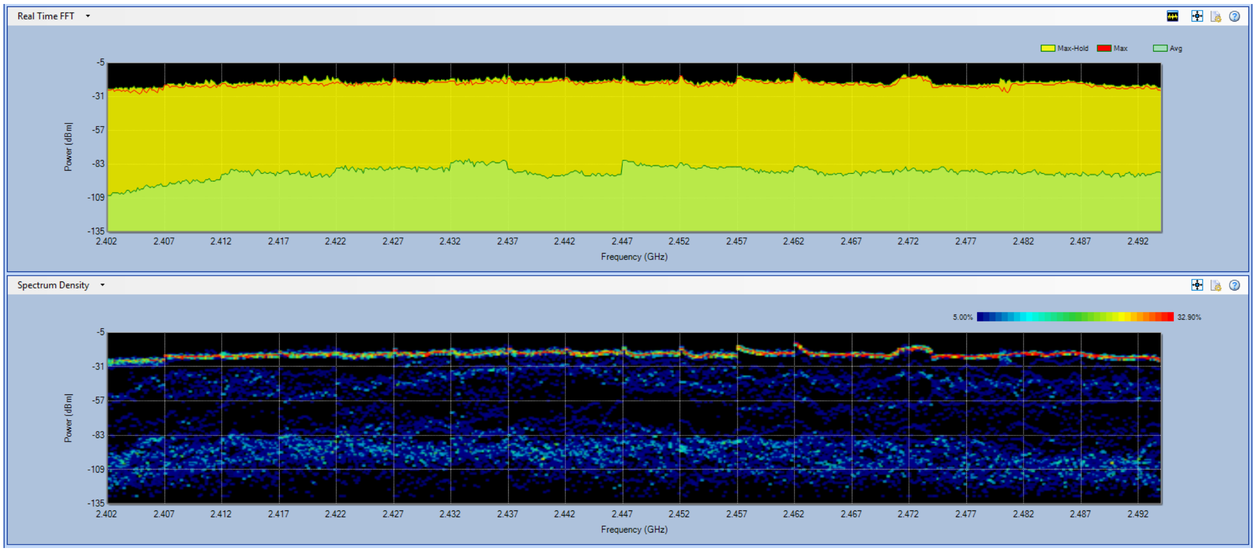
RF Jammers operate in the 2.410~2.480 GHz frequency range. Their radio signals can transmit in a 15 feet radius with output power of 7 dB.

Listed below are a couple known jammer-type devices:

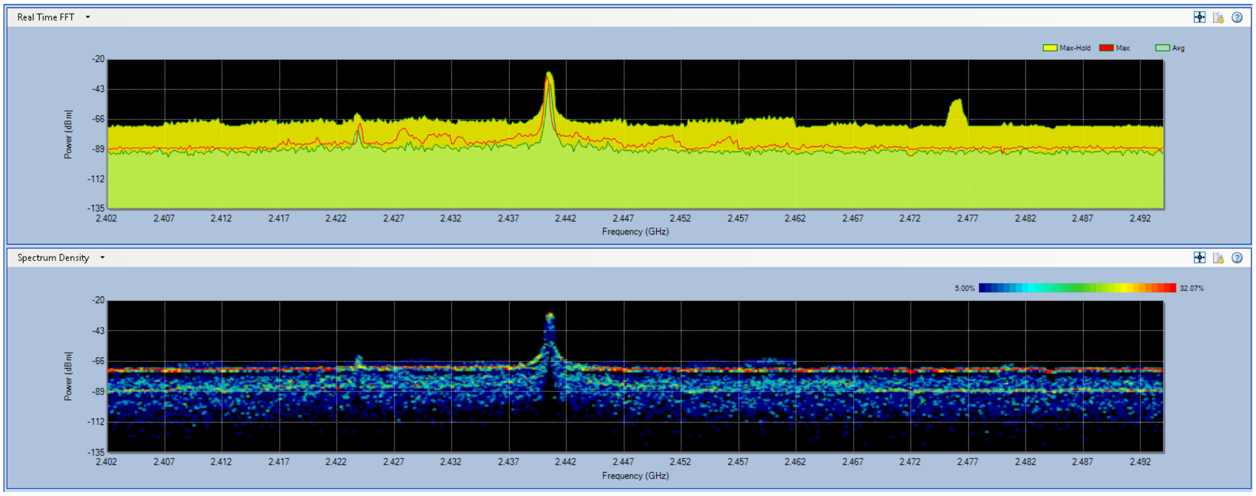
- Proxim PSG-1

- LS 2.4GHz Wireless Jammer

Below is an example of what the spectrum pattern for what a wide-band jammer would look like in a relatively noiseless 2.4GHz spectrum.



RF Spectrum Pattern of an RF Jammer



RF Spectrum Pattern of a Narrowband Jammer

Impact on Wi-Fi on Wi-Fi Networks

Wi-Fi jammers are designed to protect important working area and avoid leakage of sensitive data by blocking Wi-Fi networks. Since it works in the 2.4 GHz frequency band and channels, this type of device can be a good "defensive" tools against data leakage over wireless network, but can also be a "double-edged sword". Anyone could use it to disrupt the operation of a wireless network. Because of its compact design, it can be hidden in a pocket or briefcase or elsewhere and can be carried around and deployed at any location of a network without being discovered.

Recommended Courses of Action

Since RF Jammers operate in the same 2.4-GHz frequency band as 802.11b/g/n/ax networks do, take the following actions in order to minimize or eliminate their interference to 802.11b/g/n/ax WLANs:

- Monitor your WLAN on a regular basis to make sure that no RF Jammer is causing interference to your WLAN.

- Conduct regular WLAN site RF surveys to determine the proper location and use of RF Jammers, if they are necessary.

RF Signal Generator

A device that generates repeating or non-repeating RF signals. An example of this type of device is the AirHorn Channel-Signal Generator. This USB PC-based product aids users in testing Wi-Fi antennas, RF shields and wireless networks. It is a radio frquency (RF) signal generator that covers the 2.4 and 5 GHz ISM bands and was designed for microwave and RF applications. AirHorn transmits stable and accurate RF signals for each of the Wi-Fi channels, and is ideal for research and development for antenna design. AirHorn can be used for rapid evaluation of receiver performance.

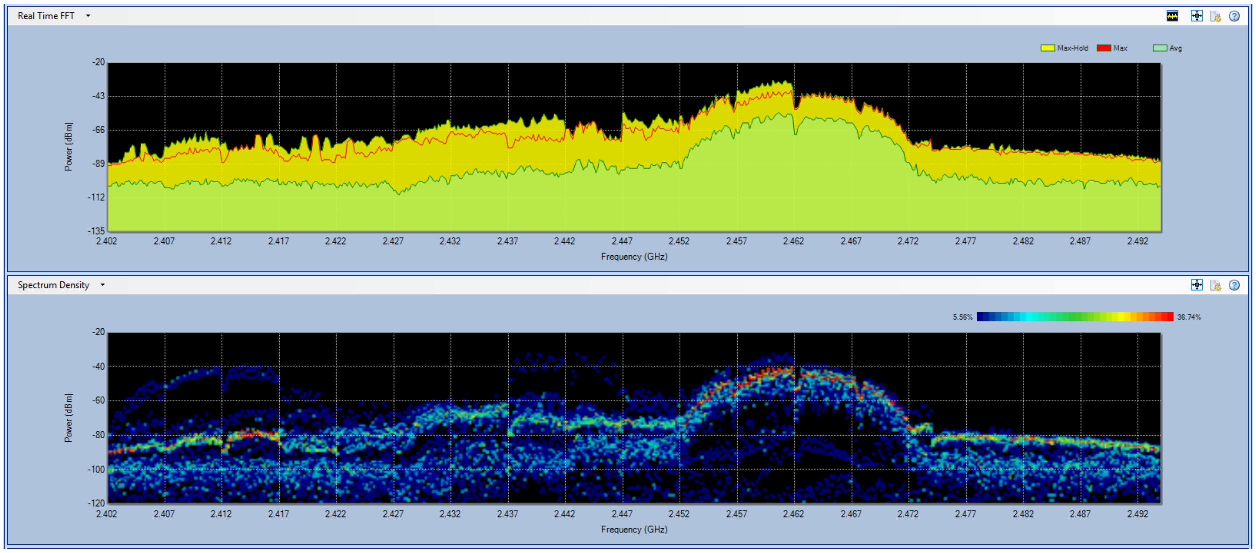
RF Spectrum Pattern

AirHORN Channel-Signal Generator is a proprietary hardware/software solution sold by Nuts About Nets. Only the devices in this product category will show up as this device type.

Below is an example of what the spectrum pattern for what an AirHORN Channel-Signal Generator would look like in a relatively noiseless 2.4GHz spectrum.

Impact on 802.11 WLAN

Used incorrectly, the AirHORN Channel-Signal Generator can create a signal that will essentially block all Wi-Fi and WLAN traffic across a 2.4 or 5 GHz ISM band, until it is either turned off or switched to a different channel.



Recommended Courses of Action

Use the following recommended actions to minimize or eliminate their interference to 802.11a/b/g/n/ac/ax WLANs:

- Monitor your WLAN on a regular basis to make sure that no RF signal generator is causing unintended interference to your WLAN.
- Conduct regular WLAN site RF surveys to determine the proper location and use of RF Signal Generators, if they are necessary.
- If it is necessary to use the RF Signal Generator, only use it on channels that do not overlap with the channels used by your WLAN.
- If optimal WLAN performance is not an issue, you may continue use your RF Signal Generator along with your WLANs, and try to maximize the distance between APs and RF Signal Generator to minimize their RF interference.

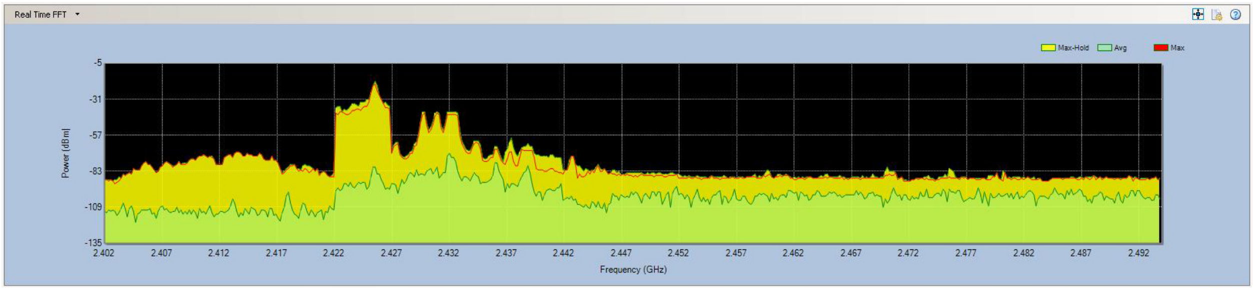
Wireless Cameras

A wireless security camera is typically made up of three components: a camera, a transmitter to send the signal, and a receiver to receive the signal. The system works in such a way that the wireless camera transmits video from the built-in transmitter to the receiver, which is connected to a monitor or a recording device.

Most wireless cameras operate on the 2.4-GHz frequency – an unlicensed radio band also used by 802.11b/g/n/ax WLANs, cordless phones, Bluetooth devices, and microwave ovens, and so on. Like the other non-Wi-Fi devices operating in the 2.4-GHz frequency band, wireless security cameras installed in close proximity of an 802.11b/g/n/ax WLAN can interfere with the normal operation the WLAN. Unlike the other RF interfering devices operating in the 2.4-GHz band, radio signals from the transmitter of a wireless security camera can travel a relatively long range which varies from 200 to 700 feet (line of sight), depending on the physical conditions of the site. Typically, multiple cameras are needed in order to provide full, overlapping coverage of one site. To make matters worse, wireless security cameras installed in homes and businesses are left on all the time. And so is the RF interference they cause to the 802.11 WLAN close to them.

RF Spectrum Pattern

Wireless cameras come in all shapes and sizes. They include wireless surveillance cameras, spy cameras, and so on. They are widely used in homes and businesses where the 802.11 WLAN is deployed. Their presence can cause serious performance issues in the WLAN. The figure below shows the RF spectrum pattern of a wireless camera using the 2.4-GHz frequency band.



RF Spectrum Pattern of a Wireless Security Camera

Impact on 802.11b/g/n/ax WLAN

Because wireless cameras are widely used in homes and businesses where WLANs are deployed, radio signals from these devices have long been identified as a source of RF interference to 802.11b/g/n/ax WLANs in these settings. They can significantly slow down Internet applications such as Web file download and surfing.

Recommended Courses of Action

Once the interfering wireless security cameras are successfully identified, perform the following actions to minimize or eliminate the RF interference they cause to the 802.11 WLAN.

- If you are using an 802.11b/g/n/ax WLAN, avoid using 2.4-GHz wireless cameras. Instead, use 5.8-GHz wireless cameras that operate in the licensed, less crowded 5-GHz radio band. Or upgrade your WLAN to the 802.11ax standard which offers better interference avoidance.
- If you are using an 802.11a/n/ac/ax WLAN, avoid using 5.8-GHz wireless cameras.
- Check the operating channels on the wireless cameras, making sure that they do not overlap with the operating channels of the Wi-Fi network.

ZigBee Devices

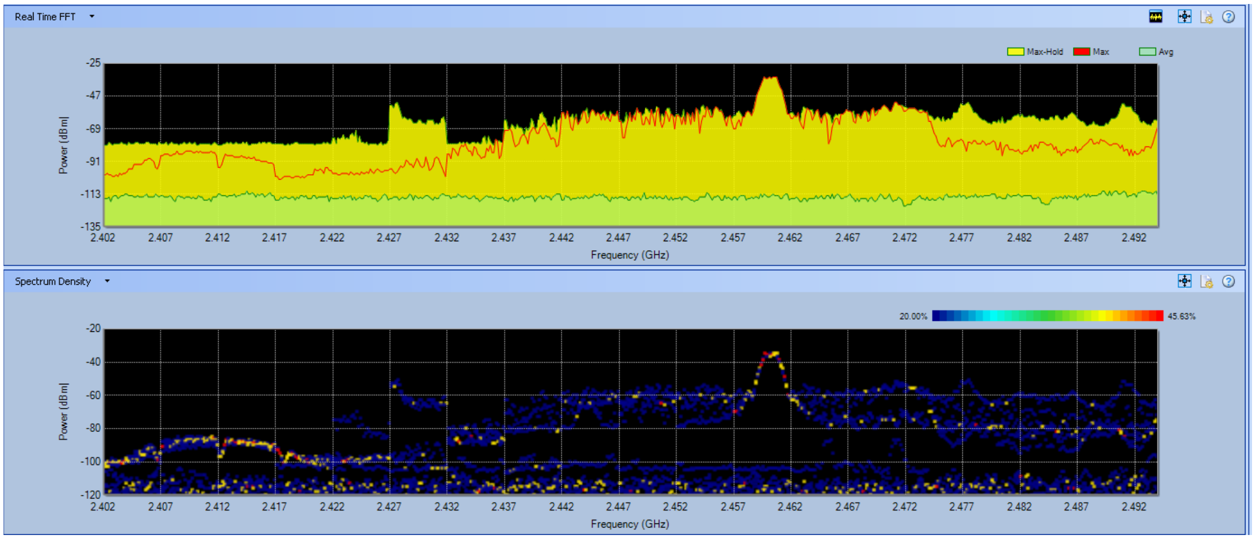
ZigBee is a low-cost, low-power, and short-range wireless mesh networking standard based on the IEEE 802.15.4 specifications. ZigBee devices can operate in the 860-MHz, 915-MHz, or 2.4-GHz band using DSSS modulation. First ratified in 2005, billions of dollars have been invested in ZigBee technology and ZigBee-based devices have now found their way into homes and businesses. Typical applications include:

- **Home Entertainment and Control** – Audio/video systems, smart lighting, temperature control.
- **Safety and Security Monitoring** – Sensors (access, water, and power), smoke detectors, smart appliances.
- **Commercial Property Management** – Access control, lighting, energy monitoring, HVAC.

- **Industrial Automation** – Process and device control, asset/energy/environmental management.

RF Spectrum Pattern

For network administrators, it is the 2.4-GHz Zigbee devices that cause concern because they use the same radio frequencies as the 802.11b/g/n/ax wireless networks do. 2.4-GHz ZigBee devices can operate on one of 16 non-overlapping channels (11 in North America) that are 3 MHz wide and 5 MHz apart. Generally a ZigBee mesh network uses only one channel. Once set up, it stays on that channel until it is changed manually. ZigBee radios use very low transmit power (typically -3dBm or 0.5mW) and receive sensitivity (between -80dBm and -100dBm depending on radio). Their maximum bit transfer rate is 250 Kbps. Even though the size and length of ZigBee data packets vary, their target applications are of low duty cycle and low power consumption. Because of this, the ZigBee network does not have as much traffic in comparison to an 802.11b/g/n/ax network.



RF Spectrum Pattern of a ZigBee Device

Impact on Wi-Fi Networks

Given the fact that a 2.4-GHz ZigBee network operates on a fixed 3 MHz of bandwidth in the 2.4-GHz band, the chance of collision between a ZigBee device and an 802.11b/g/n/ax device depends on the channels on which they operate. If the channels overlap, the chances are high. Otherwise, the chances are very low.

Recommended Courses of Action

Once a ZigBee network or devices are identified, take the following actions to minimize or eliminate the potential RF interference that they may cause to the Wi-Fi network:

- Try to set your ZigBee network to a non-overlapping channel not used by an 802.11b/g/n/ax network.

- Try to keep ZigBee devices physically away from Wi-Fi devices to minimize the chances of interaction.

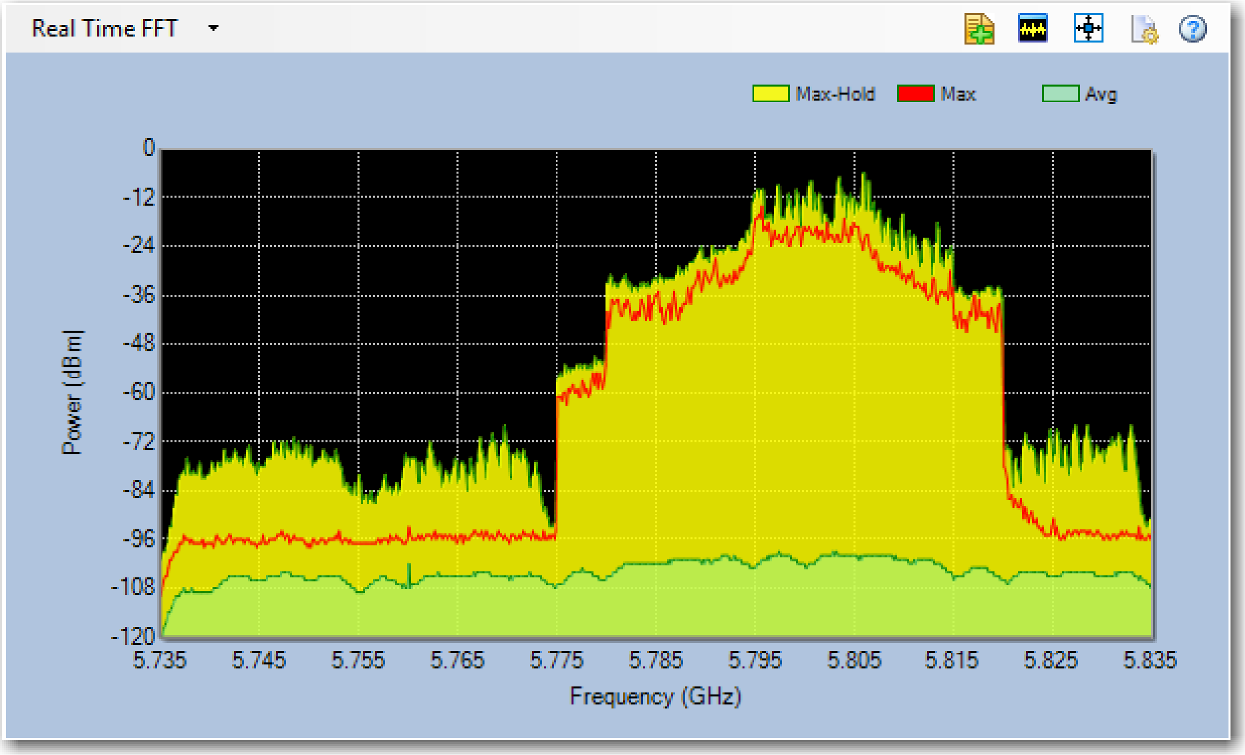
Canopy Devices

A typical Canopy setup consists of a cluster of up to 6 co-located standard access points (APs), each with a 60 degree horizontal beamwidth antenna, to achieve a 360-degree coverage. The most commonly used APs are available in 120-, 180-, or 360-degree models for site-based coverage, thus decreasing the number of APs needed on a tower. Also included would be one or more backhauls or otherwise out-of-band links (to carry data to/from other network occasions) and a Cluster Management Module (CMM) to provide power and synchronization to each Canopy AP or Backhaul Module (BM).

Customers of the system receive service through subscriber modules (SM) aimed towards the AP. The SMs should be mounted on the highest point of a building to get a reliable connection; otherwise, Fresnel zone obstruction will weaken the signal. Under ideal operating conditions, the system can communicate over distances of 3.5 to 15 miles (5.6 to 24.1 km) depending on the frequency using equipment with integrated antennas. Network operators can opt to install reflector dishes or Stinger antennas or to use Canopy models that accept external antennas at one or both ends of the link to increase coverage distance. 1

RF Spectrum Pattern

Canopy devices operate in 2.4 GHz, 5.2 GHz, 5.4 GHz, and 5.7 GHz. In general, the 900 MHz version is more effective for use in outlying areas because of its ability to penetrate trees. However, it requires careful installation because of the easy propagation of interference on that band. 1



Impact on 802.11a/b/g/n/ac/ax WLAN

Radio signals from canopy devices can be a source of RF interference to 802.11a/b/g/n/ac/ax WLANs. They can significantly slow down Internet applications such as Web file download and surfing.

Recommended Courses of Action

Once the interfering device is successfully identified, take the following actions to minimize or eliminate the RF interference they cause to the 802.11 WLAN.

Try to set your network to a non-overlapping channel not used by the canopy device.

Source: http://en.wikipedia.org/wiki/Motorola_Canopy

Frequency-Hopping Spread Spectrum devices

When the IEEE 802.11 Specification was first ratified, there were two data transmission strategies included: direct-sequence spread spectrum (DSSS) and frequency-hopping spread spectrum (FHSS). It was found that, in order to support both strategies, two separate, incompatible sets of transmission technology would have to be developed and maintained. In lieu of this fact, and that 802.11b (which supported DSSS) was more reliable than FHSS, the FHSS strategy was discarded.

When using FHSS, the transmitter shifts the central frequency of a signal several times a second, with each hop taking place in a pseudo-random pattern that both the transmitter and receiver know. In the United States, the FCC mandated at least 75 unique frequencies needed to be used, with a maximum dwell time on each frequency of no more than 400 milliseconds. Limited to speeds of only 1 and 2 Mbps, it was found that not only were FHSS and DSSS incompatible from a communication standpoint, but the FHSS transmissions also interfere with the DSSS communication stream.

RF Spectrum Pattern

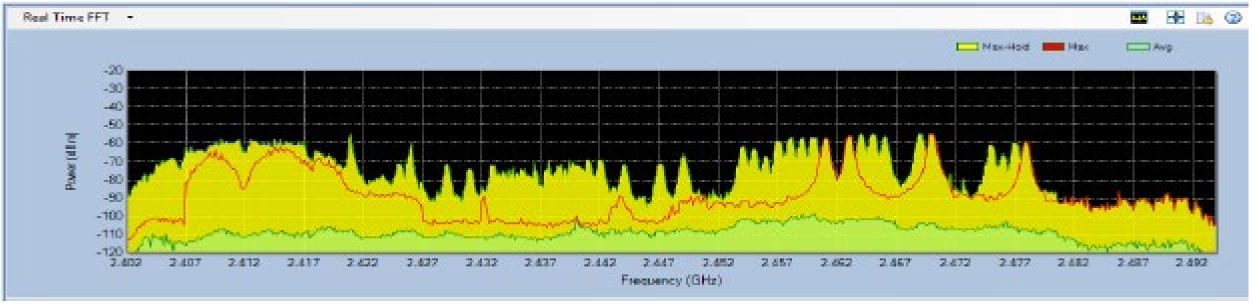
While never officially recognized as a ratified 802.11 transmission strategy, there were manufacturers that produced devices with limited interoperability for commercial applications, like Point-of-Sale solutions.

Below is a short list of manufacturers of 802.11 FHSS devices:

- Alvarion
- BreezeCom
- Digital/Cabletron
- Lucent
- Netwave Technologies
- Symbol Technologies
- Proxim Wireless

The figure below shows the RF spectrum pattern of a 2.4GHz 802.11FHSS device.

Frequency-Hopping Spread Spectrum Device



Impact on 802.11 WLAN

802.11FHSS devices can have a significant to severe impact on your WLAN. Because these devices hop across the entire band in a semi-random pattern, no 802.11 channel is considered safe from these devices. The actual impact of the 802.11FHSS on your WLAN will depend on the range between the devices, the relative signal levels, and amount of data being transmitted by each network.

Recommended Courses of Action

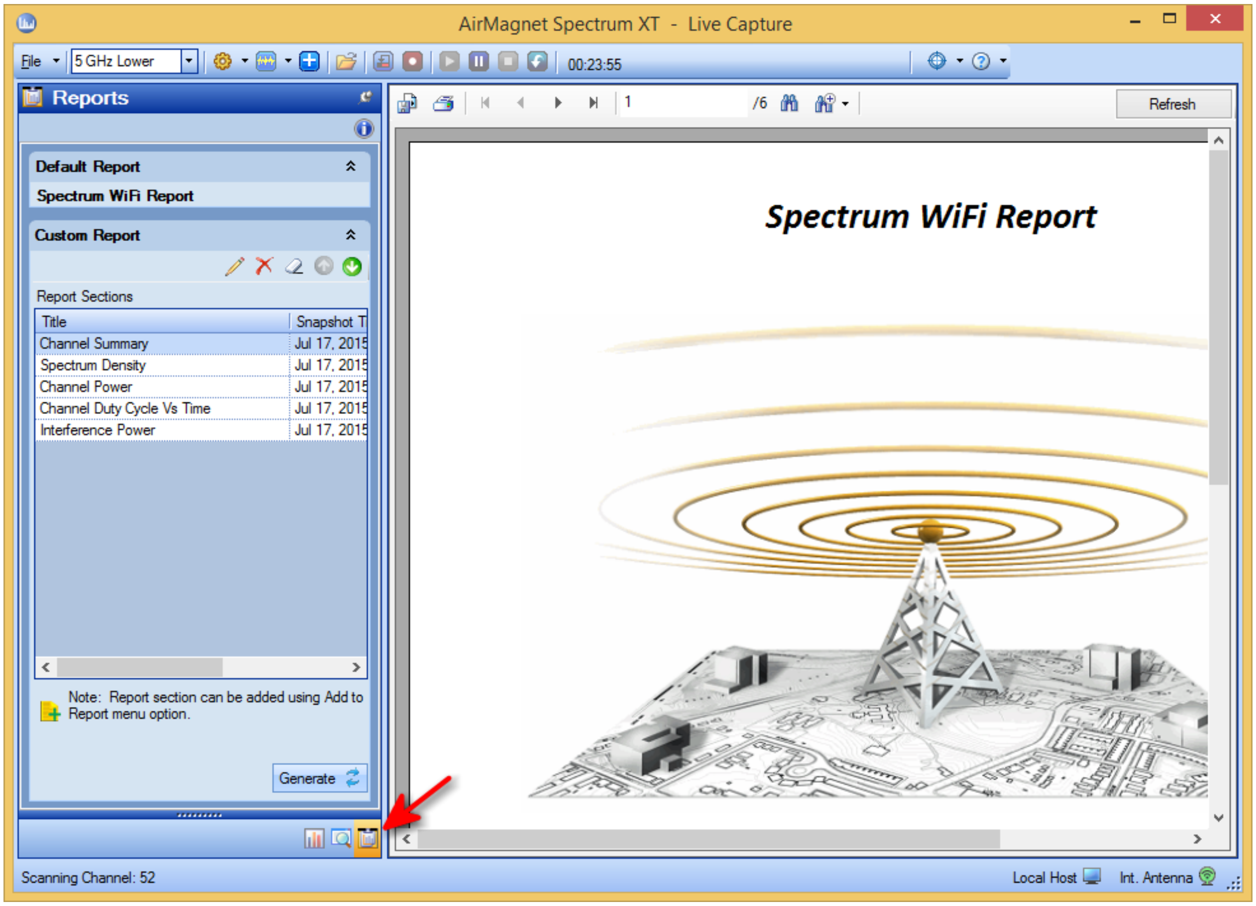
Once interfering FHSS devices are successfully located, take the following actions to minimize or eliminate their RF interference to your 802.11a/b/g/n/ac/ax WLAN:

- Do not waste your time switching AP channels, because RF signals from FHSS devices spread over all channels or frequencies in the band they operate. Simply adjusting AP channel is not the solution.
- If you have an 802.11b/g/n/ax WLAN, avoid or stop using 2.4-Ghz FHSS devices. Instead replace them with 5.8-GHz or even old 900-MHz FHSS devices, which use different radio bands and channels.
- If you have an 802.11a/n/ac/ax WLAN, avoid or stop using 5-GHz FHSS devices. Instead replace them with 2.4-GHz FHSS devices.
- If you have an 802.11b/g/n/ax WLAN and 2.4-GHz FHSS devices are a must, try to use those more expensive but less interfering ones which use Digital Spread Spectrum (DSS) technology that offer wider range, better security, with less interference.
- If optimal WLAN performance is not an issue, you may continue use your 2.4-/5-GHz FHSS devices along with 802.11a/b/g/n/ac/ax WLANs but try to maximize the distance between APs and FHSS devices to minimize their RF interference between each other.
- Consider upgrading your WLAN to 802.11ax standard, which not only provides better RF interference avoidance mechanisms but also offer greater throughput.

Spectrum WiFi Reports

Opening the Reports Page

Spectrum XT comes with a Reports page that enables you to create reports using data it captures. You can open the Reports page by clicking the **Reports** button (📋) at the bottom of the screen, as illustrated in this *image*.



Title	Snapshot T
Channel Summary	Jul 17, 2015
Spectrum Density	Jul 17, 2015
Channel Power	Jul 17, 2015
Channel Duty Cycle Vs Time	Jul 17, 2015
Interference Power	Jul 17, 2015

Note: Report section can be added using Add to Report menu option.

As seen on the screen, the Reports page has two panels: left and right. The left panel contains tools for generating reports; the right panel displays the report you've generated,

The following sections are the main topis related to the Reports page:

- Default Reports vs. Custom Reports
- Tools on the Reports Page
- Creating a Cover Page
- Generating a Default Report
- Creating a Custom Report

Tools on Reports Page

The Reports page comes with many tools for creating, viewing, and sharing reports using data captured in Spectrum XT. The table below highlights these tools and provides basic instructions on how to use them.

Tool Icon	Description
ⓘ	Opens the Report Cover Page Information dialog where you can create a report cover page.
Spectrum WiFi Report	Click this to generate a default report, which contains spectrum and Wi-Fi data the application captures at the time you click this button.
✏	Opens the Report Section dialog where you can edit the selected report section. Refer to Modifying a Report Section.
✗	Deletes the selected report component.
⌫	Clears all report components in the Custom Report panel.
⬆	Moves the selected report component upward.
⬇	Moves the selected report component downward.
Generate ⇄	Generates a custom report.
💾	Opens the Export Report dialog so that you can export the current report in any of the following file format: ▪ Crystal Report (*.*rpt*) ▪ Adobe Acrobat (*.*pdf*) ▪ Microsoft Excel 97-2000 (*.*xls*) ▪ Microsoft Excel 97-2000 - Data Only (*.*xls*) ▪ Microsoft Word (*.*doc*) ▪ Microsoft Word - Editable (*.*rtf*) ▪ Rich Text Format (*.*rtf*)
🖨	Opens the Print dialog so that you can print the current report.

⏮ ◀ ▶ ⏭	The buttons (from left to right) allow you to ▪ Jump to the first page (of the current report) ▪ Move to the previous page ▪ Move to the next page ▪ Jump to the last page
🔍	Opens the Find Text dialog so that you can do a text search through the current report.
🔍 ▾	Opens the **Zoom** list menu with options for zooming in and out the current page of a report.
Refresh	Updates the default report with fresh data the application captures. **Note:** This feature only works for default reports. It has no effect on custom reports.

Default Report vs. Custom Report

Spectrum XT allows you to create both default and custom reports, depending on the way the reports are generated.

- **Default Report** - A default report contains immediate data Spectrum XT captures the moment the report is generated. In addition, all parts (report sections) in a default report are presented in a default sequence set in the system.
- **Custom Report** - A custom report is one that contains data you select from among the report sections under Default Report. The report sections are the snapshots of data you take using the **Add to Report** button (➕) on the Spectrum-WiFi Summary page. When creating a custom report, you can choose the report sections to be included, modify their descriptions, and set the sequence they are presented in the report.

Creating a Cover Page

Spectrum XT allows you to add a unique cover page to every report you generate. This feature comes in handy when sharing and archiving reports. It makes it easier to find the right report among the collection of reports you may accumulate over time.

Before you start to generate a report (wether it's a default report or custom report), you should create a cover page using the following steps:

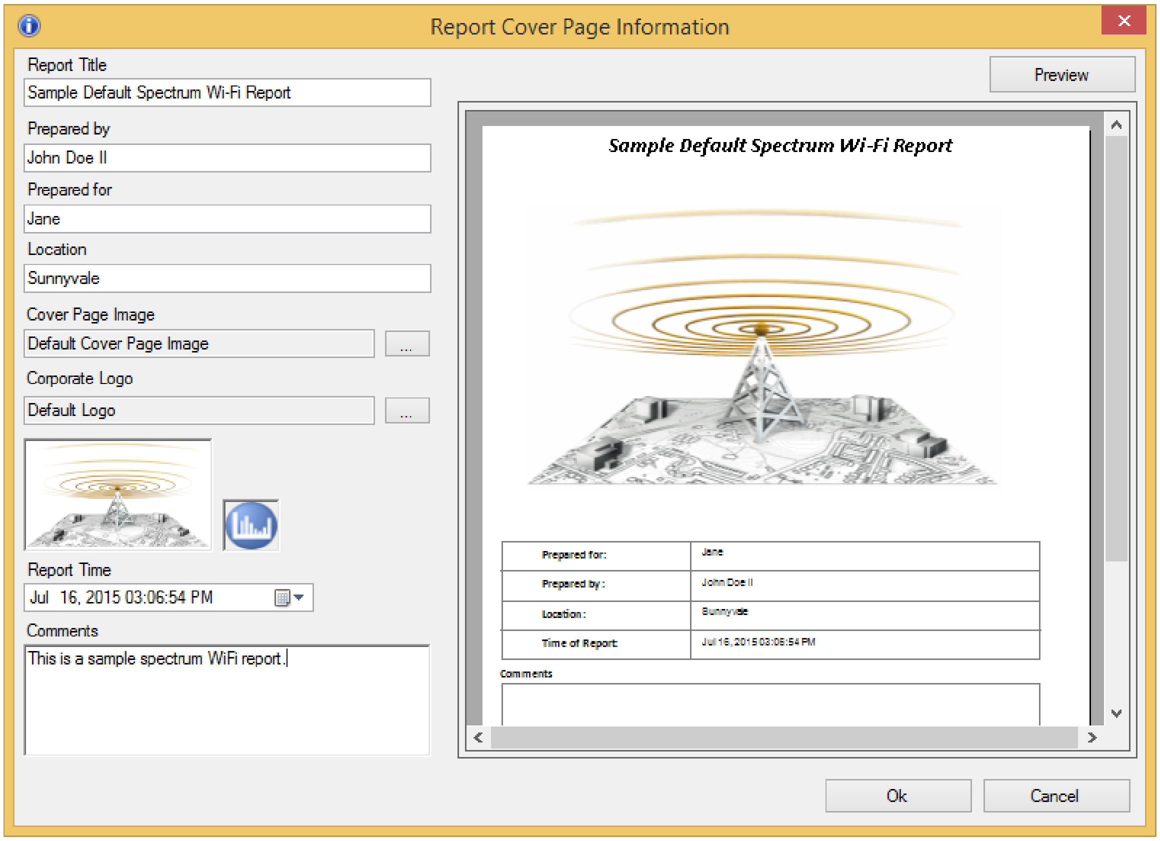
1. Click the **Report Information** button (ℹ) to open the Report Cover Page Information dialog.

2. In the dialog, make the desired entries and/or selections.

3. Click **Review** to review the cover page.

4. When you are satisfied with what you see in the Review Panel, click **OK.**

5. (Optional) Click *here* to see a sample report cover page configuration.



Report Cover Page Information

Report Title: Sample Default Spectrum Wi-Fi Report

Prepared by: John Doe II

Prepared for: Jane

Location: Sunnyvale

Cover Page Image: Default Cover Page Image

Corporate Logo: Default Logo

Report Time: Jul 16, 2015 03:06:54 PM

Comments: This is a sample spectrum WiFi report.

Sample Default Spectrum Wi-Fi Report

Prepared for:	Jane
Prepared by :	John Doe II
Location :	Sunnyvale
Time of Report:	Jul 16, 2015 03:06:54 PM

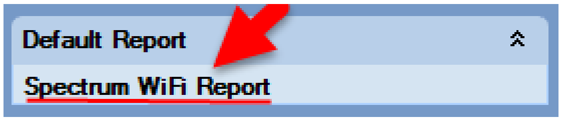
Comments

Generating a Default Report

A default report contains whatever data Spectrum XT has captured when you generate it. You can create a default report using the following steps:

1. Click the **Report Information** button (ⓘ)to create a cover page for the report.

2. Under **Default Report,** click the **Spectrum WiFi Report**. Refer to the image below.



Note: The default report automatically opens in the right panel of the page when it has been generated.

Creating a Custom Report

A custom report is one that contains report sections you select on the Reports page. The report sections are snapshots of data that are taken when you click ➕ (**Add to Report)** on the Spectrum - WiFi Summary page. You can find this button on every spectrum and Wi-Fi graph as well as the Channel Summary section of that page. Refer to Capturing Data as Report Sections.

When you click the button, Spectrum XT takes a snapshot of the data at that moment in time. At the same time, the Report Section dialog pops up, prompting you to add the snapshot as a report section. All snapshots you take will end up in the Custom Report section of the Reports page.

To create a custom report:

1. From the Reports page, click the **Report Informatio**n button (ⓘ) to create a cover page. Refer to Creating a Cover Page.

2. In the Custom Report section, do the following:

   - To edit a report section, select it and click ✎ (**Edit selected report section**). In the Report Section dialog, make the desired changes and click **Update.**

   - To exclude a report section from the report, select it and click ✗ (**Remove selected report item**). When the confirmation message pops up, click **Yes.**

   - To clear all report sections from the Reports page, click ⌫ (**Clear all report items**). When the confirmation message pops up, click **Yes.**

   - To move a report section up, select it and click ↑ (**Move selected section up**).

   - To move a report section down, select it and click ↓ (**Move selected section down**).

3. When all is set, click **Generate.**

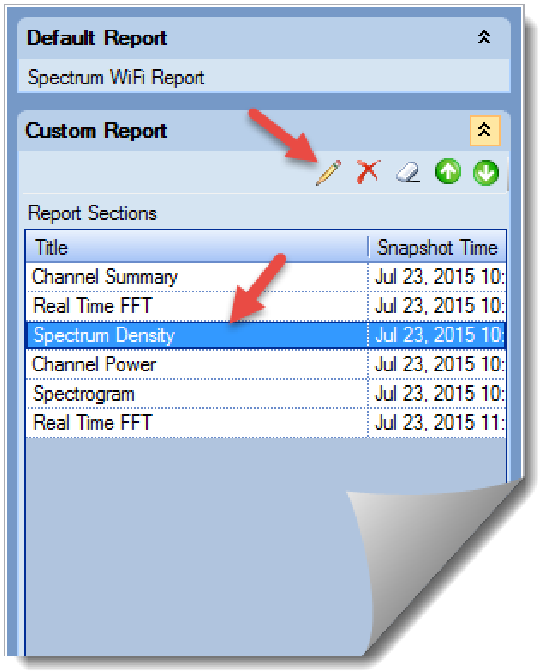
Modifying a Report Section

When you click (**Add to Report**) on the Spectrum - WiFi Summary page, Spectrum XT captures the data at the moment as a report section. At the same time, the Report Section dialog pops up. If you like to, you can rename the title of the section and add a brief description in the spaces provided before clicking the **Add** button at the bottom of the dialog.

When compiling a custom report, you are still able to make changes to the title and/or the description from the same Report Section dialog.

To modify a report section:

1. In the Custom Report section of the Reports page, highlight the report section and then click (**Edit selected report section**). Refer to the illustration below.



Title	Snapshot Time
Channel Summary	Jul 23, 2015 10:
Real Time FFT	Jul 23, 2015 10:
Spectrum Density	Jul 23, 2015 10:
Channel Power	Jul 23, 2015 10:
Spectrogram	Jul 23, 2015 10:
Real Time FFT	Jul 23, 2015 11:

2. In the Report Section dialog, do either or both of the following (if you want to):
   - Highlight the section title and type a new title over it.
   - Enter a brief description (if the field is empty) or modify the existing description (if the field is already populated)
3. Click **Update** at the button of the dialog.