BlueSleuth-Pro

BT + BLE Locator User Manual 1.9

Table Contents

Introduction

BlueSleuth-Pro is a handheld detector for locating BLE beacons, BT skimmers, hidden BLE personal tags and many other nearby BLE devices including wireless earbuds, smartphones, smartwatches, tablets and all kinds of wireless IoT (Internet of Things) devices. BlueSleuth-Pro detects hidden BLE personal trackers and tags including but not limited to Apple AirTag, Samsung SmartTags (1 and 2), Tile Trackers, Chipolo, eufy, AirCard and PebbleBee. There are many BLE tags with new ones announced regularly. If you need to detect a BLE tag not mentioned in this user manual, please contact support so that we can test and include new BLE tags in future firmware updates.

About Bluetooth and BLE

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the 2.4 GHz ISM band) from fixed and mobile devices, and building personal area networks (PANs). The Bluetooth protocol is active in over tens of billions of devices worldwide. Bluetooth technology, combined with a lower cost of entry, has enabled business cases for applications that were previously unthinkable.

BLE devices follow the Bluetooth standard. They manage their power by automatically powering up and down while remaining connected to the reader infrastructure (smart connectivity). Compared to previous versions, BLE enables 250% faster and more reliable over-the-air data transmission and 10x more packet capacity. The job of BLE is to drive the 'Internet of Things' (IoT), namely the thousands of smart, web connected devices – from fridges to toothbrushes – that are expected to enter our lives over the next decade.

Comparing Classic BT to BLE

Bluetooth and Bluetooth Low Energy (BLE) are two related but distinct wireless communication technologies. The main differences between Bluetooth and Bluetooth Low Energy are primarily related to power consumption, range, and use cases:

Power Consumption:

Bluetooth: Traditional Bluetooth (Classic Bluetooth) is designed for more data-intensive applications and typically consumes more power. It is suitable for continuous streaming of audio and other high-bandwidth applications.

Bluetooth Low Energy (BLE): BLE is optimized for low power consumption, making it ideal for devices that operate on coin cell batteries or other limited power sources. BLE is well-suited for applications where intermittent communication and energy efficiency are critical.

Range:

Bluetooth: Classic Bluetooth typically has a longer range compared to BLE. It can cover distances of up to 100 meters or more, depending on the class of the Bluetooth device.

Bluetooth Low Energy (BLE): BLE is designed for short-range communication, typically within a range of about 10 to 100 meters. This shorter range contributes to lower power consumption.

Data Transfer Rate:

Bluetooth: Classic Bluetooth supports higher data transfer rates, making it suitable for applications like audio streaming and file transfer.

Bluetooth Low Energy (BLE): BLE sacrifices data transfer rate for reduced power consumption. It is optimized for intermittent and small data transfers, making it suitable for applications like sensor data monitoring and tracking.

Connection Duration:

Bluetooth: Classic Bluetooth connections are designed for continuous and relatively high-throughput communication, which can result in more extended connection durations.

Bluetooth Low Energy (BLE): BLE is optimized for short bursts of data transmission with minimal connection time. Devices can establish connections quickly, transmit small amounts of data, and then disconnect to conserve power.

Use Cases:

Bluetooth: Classic Bluetooth is often used for applications that require continuous, high-bandwidth data transfer, such as audio streaming between devices like headphones and speakers.

Bluetooth Low Energy (BLE): BLE is commonly used in applications that prioritize energy efficiency and intermittent data transfer, such as fitness trackers, smartwatches, key finders, and other IoT (Internet of Things) devices.

Device Discovery:

Bluetooth: Classic Bluetooth uses inquiry and page procedures for device discovery, which can take longer and consume more power.

Bluetooth Low Energy (BLE): BLE utilizes an advertising mechanism for device discovery, allowing devices to be quickly discovered while keeping power consumption low.

Bluetooth and Bluetooth Low Energy are tailored to different sets of applications based on their power consumption, range, and data transfer characteristics. Classic Bluetooth is suitable for applications that require continuous data transfer, while Bluetooth Low Energy is designed for scenarios where energy efficiency is a primary consideration, making it well-suited for a wide range of IoT devices.

BLE Tag Technical Details

Bluetooth Low Energy (BLE) tracker tags, such as AirTag, Tile, Samsung Smart Tag, and Chipolo, are small devices designed to help users locate and track their personal belongings. These devices leverage Bluetooth Low Energy technology, a power-efficient version of the traditional Bluetooth wireless communication standard. Here's a technical overview of the key features and components commonly found in such tracker tags:

Bluetooth Low Energy (BLE) Technology:

Low Power Consumption: BLE is designed to minimize power consumption, making it suitable for battery-operated devices like tracker tags.

Short Range:

BLE has a relatively short range, typically around 100 meters, which is ideal for close-range tracking applications.

System Architecture:

Microcontroller Unit (MCU): Each tracker tag is equipped with a microcontroller unit responsible for managing the device's overall operation, including processing sensor data, handling Bluetooth communication, and managing power consumption.

Bluetooth Module:
This module enables the tracker tag to communicate with other devices, such as smartphones, using Bluetooth Low Energy.

Power Source:
Coin Cell Battery: Most tracker tags are powered by a coin cell battery, providing a compact and lightweight power source. The low power requirements of BLE contribute to the device's extended battery life.

Sensors:
Accelerometer: Many tracker tags incorporate an accelerometer to detect movement or changes in orientation. This information can be used to trigger actions, such as sending notifications to the user's smartphone when the tag is in motion.

Temperature Sensor:
Some tracker tags include temperature sensors to monitor the environmental conditions around the device.

Localization and Tracking:
Triangulation and Proximity Detection: Tracker tags use the signal strength of Bluetooth signals to estimate the distance between the tag and a user's smartphone. Triangulation algorithms can then be used to approximate the location of the tag. Proximity detection is also employed to alert users when they are getting closer to or moving away from their tagged items.

Mobile Applications:
Companion Apps: Users interact with tracker tags through companion mobile applications on their smartphones. These apps provide a user interface for configuring and managing multiple tags, as well as receiving alerts and locating tagged items.

Security:

Encryption and Authentication: BLE tracker tags implement security measures, such as encryption and authentication, to protect against unauthorized access and tracking.

Compatibility:

Cross-Platform Support: Tracker tags are typically designed to work with both iOS and Android devices, ensuring broad compatibility.

Cloud Integration:

Cloud Services: Some tracker tag ecosystems include cloud services that enable users to track their items beyond the range of Bluetooth connectivity. When another user's device detects a tracker tag, the location information can be anonymously relayed to the cloud, helping the owner locate their lost item.

BLE Vulnerabilities

Bluetooth Low Energy (BLE) devices are generally designed to be power-efficient and have a low impact on battery life, making them suitable for a wide range of applications, including wearable devices, health monitors, smart home devices, and more. While BLE devices are generally secure, there are potential threats and vulnerabilities associated with their use:

• Cyber Stalking & Tracking: Tiny BLE (Bluetooth Low Energy) tags are being placed in people’s vehicles, pockets, bags and other items on the move all the time. Mostly, these are harmless trackers but an increase in stalking, theft and even murder has resulted over the past few years and where tech companies have failed to respond, victims are looking for ways to fight back.

• Eavesdropping: BLE signals can be intercepted by unauthorized devices within range. If the communication between BLE devices is not properly encrypted, an attacker could eavesdrop on the data being transmitted.

• Man-in-the-Middle Attacks: Attackers might attempt to position themselves between two communicating BLE devices to intercept or manipulate the data being exchanged. This can lead to unauthorized access or data manipulation.

• Impersonation: An attacker could attempt to impersonate a legitimate BLE device to gain unauthorized access to a network or services. This could be a concern if proper authentication mechanisms are not implemented.

• Denial of Service (DoS): BLE devices can be susceptible to DoS attacks, where an attacker overwhelms the device with requests or interferes with its normal operation, leading to a loss of service.

• Bluejacking: This involves sending unsolicited messages or data to a Bluetooth-enabled device. While not a serious security threat, it can be used for harassment or annoyance.

• Exploiting Vulnerabilities in Implementations: Some BLE devices may have vulnerabilities in their software or firmware implementations. Attackers can exploit these vulnerabilities to gain unauthorized access or control over the device.

• Proximity-based Attacks: BLE devices often rely on the concept of proximity for pairing and communication. If an attacker can get within the communication range of the devices, they may be able to exploit vulnerabilities or launch attacks.

• Lack of Firmware Updates: If manufacturers do not provide firmware updates for their BLE devices, any security vulnerabilities discovered in the future may remain unpatched, leaving devices susceptible to exploitation.

To mitigate these threats, it's essential for device manufacturers and users to implement security best practices, such as encryption, authentication, and regular firmware updates. Users should also be cautious about pairing with unknown devices and ensure that their devices are configured securely. Additionally, the adoption of security standards and protocols can contribute to the overall security of Bluetooth Low Energy devices.

To keep your facility secure from potential Bluetooth threats we recommend regular security sweeps to detect and locate threats.

Unpacking Your Unit

BlueSleuth-Pro ships complete with the (1) BlueSleuth-Pro unit, (1) Li-Ion AA battery charger, (6) Li-Ion AA batteries, (1) USB Mini cable, (1) external SMA omni-directional antenna and (1) wideband direction finding antenna all inside a rugged Pelican transport case. The user manual is in digital format on www.bvsystems.com.

Battery Charging

BlueSleuth-Pro is powered by (3) AA Li-Ion rechargeable batteries. The unit ships with (6) of these batteries and a charger allowing users to charge batteries while operating BlueSleuth-Pro. Always use the supplied rechargeable batteries, charger and power adapter for consistent charging and runtimes. Take careful note of polarity by matching the + to the battery's polarity. Be sure to charge unit completely before updating firmware and follow instructions to download latest firmware from the support section at www.bvsystems.com. If you are experiencing technical issues with your BlueSleuth-Pro, contact support@bvsystems.com for further instructions and possible firmware updates as well.

Startup Screen

BlueSleuth-Pro has a physical power switch located on the top of the unit. Upon turning on that switch, users will immediately see this startup screen. The unit has already begun scanning the area for nearby BLE devices.

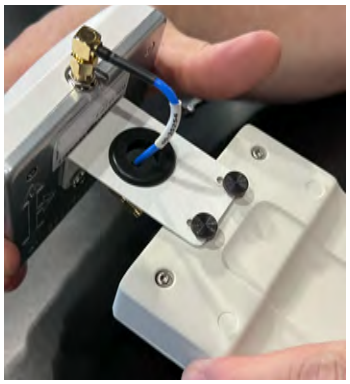
Unit Updates

BlueSleuth-Pro contains a Mini-USB port atop of the unit. This port allows for firmware updates via a BVS Windows PC firmware installer. Be sure to check with BVS support before updating your unit.

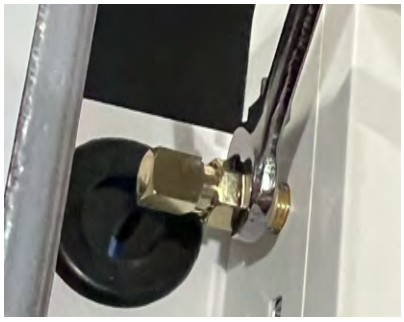
Setting Up Your Antennas

BlueSleuth-Pro supports both an omni-directional and wideband directional antenna system. We recommend you begin BLE/BT surveys with the omni-directional antenna to get a sense of all the surrounding BT/BLE device activity. Once you are ready to hone in on some specific devices or tags, remove the omni-directional antenna by unscrewing it from the SMA connector atop the unit.

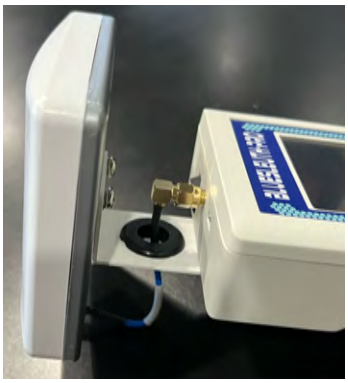
Connect the DF antenna bracket to the back of the unit and tighten the thumb screws.



Feed the antenna cable through the hole in the DF antenna bracket and hand-tighten it to the SMA connector. You may need to use a small end wrench to tighten it fully.

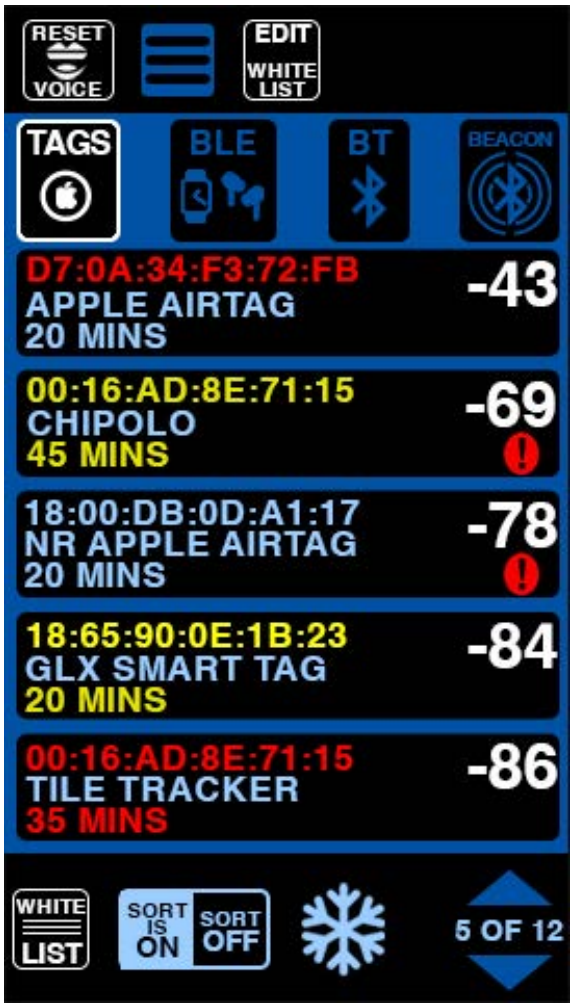


Your mounted DF antenna should look like this and you will see more directionality and slightly higher signal strength as you sweep areas with active devices. Be aware that devices you are pointing the DF antenna away from will appear further down the list with a lower signal strength.



Main Scanning List

From this Main Scanning List, users can view and filter all scanned devices.



RESET VOICE – Resets the voice alerts so that the strongest signal from each device type selected (TAGS, BLE, BT, BEACON) will trigger once again.

MAIN MENU – Takes users to the MAIN MENU allowing many settings to be altered.

EDIT WHITE LIST – Allows users to add and subtract devices from the WHITE LIST screen.

TAGS – This filter is adding only BLE tags to the scan list. BLE tags and trackers include AirTags, Tile, Samsung Galaxy SmartTags (versions 1 and 2), Eufy, Chipolo, Pebblebee, AirCard and more.

BLE DEVICES - This filter is only adds BLE devices to the scan list. BLE devices include wireless earbuds, smart watches, wearables, smartphones, tablets and more.

BT - This filter only adds Bluetooth devices to the scan list. Classic Bluetooth devices are not very common so this filter is used primarily to identify and locate Bluetooth skimmers hidden inside ATMs, gas pumps and retail POS card readers.

BEACON - This filter only adds BLE beacons to the scan list. BLE beacons are more commonly found in retail areas and indoor venues.

Depending upon the filter(s) selected by the user, this screen will list any combination of BLE devices, tags, beacons or BT skimmers detected from strongest (top) to weakest (bottom) in the list. An NR (Not Registered) AirTag is listed including its MAC address, manufacturer, signal strength in RSSI, duration of detection so far and spoofing indicator. In this list screen, all devices are scanned approximately every 5 seconds. Due to MAC spoofing and manufacturers' settings, some BLE devices and tags will shift frequently up and down the list and sometimes disappear altogether and some will take a little longer to be detected than others. MAC addresses associated with BLE tags are color-coded according to confidence that these devices are still nearby and active: blue MACs are detections with no confidence (yet), yellow MACs have some degree of confidence and red MACs indicate that the device or tag is nearby and active.

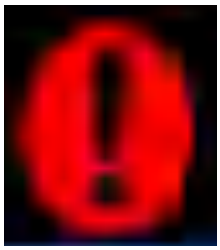
WHITE LIST – Select this button to view the current WHITE LIST of friendly, known devices. The user will automatically be taken to the corresponding white list for the scan mode currently engaged.

SORT LIST – This button has a toggle feature. When SORT IS ON, the listed BT and BLE devices will be sorted by RSSI value from strongest to weakest. When SORT IS OFF, BT and BLE devices appear in an order as they are received to populate the list.

FREEZE – Select this button to freeze the list as is. Users may scroll through multiple pages of frozen devices while in this mode. While activated, this icon will blink to remind the user that freeze is active.

PAGE NAVIGATION – Touch the UP or DOWN arrow to navigate between pages in this list. The maximum number of pages is 30.

MAC Spoofing



MAC address randomization is a process of generating MAC addresses that cannot be traced back to a specific device. MAC addresses are randomly generated and changed periodically, making it difficult for someone to track down a specific device. Many smartphones, Wi-Fi and BLE devices utilize MAC and Device ID spoofing to maintain user privacy. These spoofing randomizations usually occur about every 15 minutes (varies by manufacturer) but BlueSleuth-Pro can detect these changes and alert users to them. The red and black "!" next to any device ID indicates a likely MAC spoof. When this icon is displayed next to the MAC address in a list, it indicates that the MAC address has spoofed to something new. Attempts to isolate it from the list and enter the Single Device DF mode will be met by 4 beeps and denial of the DF function.

The frequency at which Bluetooth devices change their MAC addresses depends on the specific device and its configuration. In general, Bluetooth devices do not dynamically change their MAC addresses during normal operation. The MAC address is typically a unique identifier assigned to a device and remains constant throughout its lifetime.

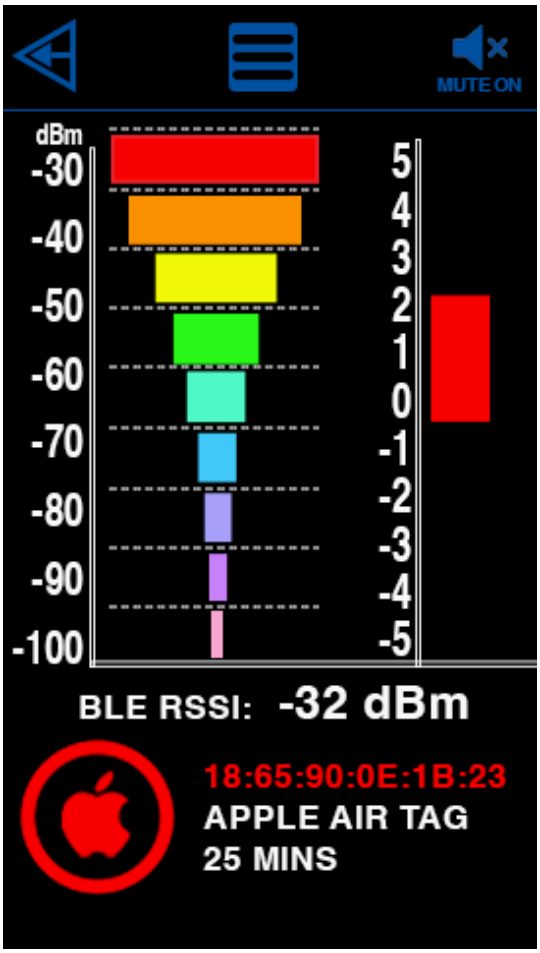
However, there are situations where a device might use temporary or randomized MAC addresses, particularly for privacy reasons. This practice is often seen in Wi-Fi and Bluetooth Low Energy (BLE) devices to enhance user privacy when scanning for nearby devices. For example, in BLE, devices can use a feature called "LE Privacy" that allows them to generate random MAC addresses periodically to avoid being tracked over time.

The specific mechanisms and policies for MAC address usage, including randomization, can vary between devices and manufacturers. Some devices may use randomized MAC addresses by default, while others may have this feature disabled. The use of randomized MAC addresses is often a configurable option in the device settings.

Unregistered Tags

If an 'NR' appears before the tag's name, the tag has not been registered yet. Normally, anyone tracking someone or something would need to have their tag registered in order to track it's whereabouts but most tags allow others to reset or unregister them if found. If a tag has power to it but has never been registered or re-registered, it can still be detected by BlueSleuth-Pro.

Single Device Scan



Once you have discovered the device or tag of interest in the main scanning list, select it to enter the Single Device Scan screen. This screen not only visually focuses on a single device but also scans just that device once every 1,2 or 5 seconds (adjustable in the MAIN MENU). Just like from the previous screen, the BLE device or tag by manufacturer is identified, the time that has elapsed since it was first detected, the MAC address and the signal strength. There are far too many BLE devices available to identify with new ones arriving all the time so BlueSleuth-Pro visually identifies (by name and product icon or shape) the most widely used BLE tags, but as new tags come to market, they will be included with future BlueSleuth-Pro updates. Users with specific needs or security applications should contact BVS sales and support direct for help. The duration of detection is a simple timer that starts incrementing the moment that the BLE device or tag is first detected. The only time this detection timer will reset is when the unit is powered off. This detection timer is useful for determining patterns and durations of device activity, but it does not necessarily provide real time BLE device status. It only serves as an indicator from initial detection. For real time detection of active BLE devices or tags, you must return to the Main Scanning List.

The direction finding scale operates displays a different color for each level (-30 dBm (strongest) and -100 dBm (weakest) signal strength) of signal strength as well as a more granular scale (right side) that correlates to the current signal strength. Five unique audio tones inform users if the signal strength is getting stronger or weaker so constant visual access to the touchscreen is not necessary:

-100 TO -76 dBm, IS FREQUENCY 440 HZ

-75 TO -60 dBm, IS FREQUENCY 587.33 HZ

-59 TO -50 dBm, IS FREQUENCY 783.99 HZ

-49 TO -40 dBm, IS FREQUENCY 1046.50 HZ

-39 TO -30 dBm, IS FREQUENCY 1396.91 HZ

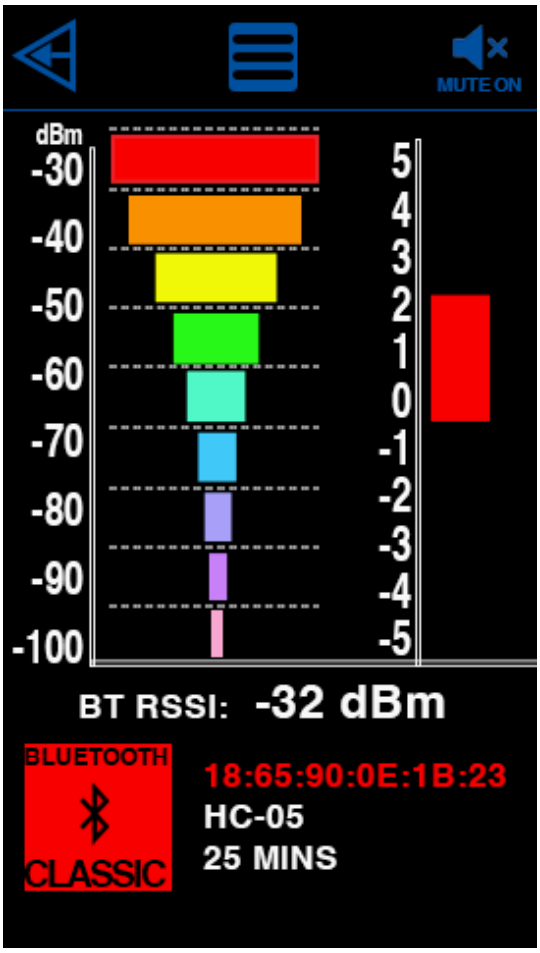
BACK ARROW – Touch this button in any screen to navigate back to the previous screen.

MUTE – Toggle this button to mute the “beep” volume on or off only for the direction finding screen.

It is important to note that the Single Device Scan screen only alerts users to activity for the current device shown and no other devices. That means that if another device or tag is detected while in this screen, you will not see nor get an alert to that new device. This screen also behaves a little like a Geiger counter. As you near closer to the device being scanned, the visual, color-coded signal strength generally increases as well as the vibrations (if you have them turned on in Alert Settings).

BT Classic Mode

When using Single Device mode to detect and locate a BT skimmer, operation can appear a little different due to the nature of BT classic compared with BLE. RSSI signal strength updates normally but if the signal strength suddenly goes all the way down to nothing (-120 dBm), it indicates that the user has either gone out of range or the BT device was possibly spoofed.



Detecting AirTags and Other Bluetooth Tracking Devices

When testing for the presence of Apple AirTags or similar Bluetooth tracking devices, it is important to understand how they communicate and why they may not always appear on a Bluetooth detection tool such as BlueSleuth-Pro or BlueSleuth-Lite.

An AirTag primarily relies on Bluetooth Low Energy (BLE) to broadcast short advertising packets. These packets are what scanning tools or unpaired devices can detect. However, once an AirTag has been paired to an iPhone, that phone establishes a secure BLE connection with the tag. While this connection is active, the AirTag no longer behaves like an “unknown” tag broadcasting to its surroundings. Instead, it enters a connected state and primarily communicates with its owner’s iPhone using encrypted BLE packets. Because of this, third-party tools like BlueSleuth-Pro or BlueSleuth-Lite will not detect the AirTag when the paired iPhone is nearby, since the tag is no longer advertising openly.

In addition to BLE, newer iPhones equipped with the U1 Ultra-Wideband (UWB) chip use UWB signals for precision ranging when the phone is close to the AirTag. If the owner’s phone is very close to the tag, UWB may replace or reduce the need for BLE advertising. This further decreases the likelihood of the AirTag being visible in a BlueSleuth-Pro or BlueSleuth-Lite scan.

For these reasons, when attempting to test or detect an AirTag using BlueSleuth-Pro or BlueSleuth-Lite, it is critical to isolate the tag from its paired phone. A good practice is to place the iPhone (or any phone that the AirTag is registered to) into Airplane Mode and to physically move it a sufficient distance away from the area being scanned (at least 20 feet away). It is also important to manually turn off Bluetooth, since Airplane Mode by itself does not disable Bluetooth, and the phone will continue to transmit and receive BLE signals if it is left on. In contrast, Airplane Mode will automatically disable the Ultra-Wideband (UWB) radio. By ensuring both Airplane Mode is active and Bluetooth is turned off, you prevent any direct BLE connections or UWB ranging from taking place. This in turn forces the AirTag to resume periodic BLE advertising. Once the AirTag is no longer “busy” communicating with its owner device, it will once again appear as an unrecognized BLE signal, which is what BlueSleuth-Pro or BlueSleuth-Lite is designed to detect.

In summary, BlueSleuth-Pro and BlueSleuth-Lite are optimized to identify tags that are unknown or hidden, not tags that are actively paired and communicating with their owner device. Therefore, when testing for AirTags or other tracking tags, always ensure that the paired phone is disabled (via Airplane Mode) and kept at a good distance away. This ensures that the AirTag is in its advertising state and can be properly detected during a scan.

Operator Procedure: Testing for AirTags Paired to Your Phone

• Identify the Owner Device

• Determine which iPhone (or other mobile phone) the AirTag is paired with.

• Disable Communication

• Place the paired phone into Airplane Mode to stop all BLE and UWB connections. (And shut off Bluetooth in addition)

Create Separation

• Physically move the paired phone away from the scan area.

• A separation of 10–15 feet (3–5 meters) or more is recommended to ensure UWB does not maintain communication.

Prepare the Detection Tool

• Launch BlueSleuth-Pro or BlueSleuth-Lite

• Ensure the tool is set to scan for unknown or hidden BLE devices.

Perform the Scan

• Begin scanning the area where the AirTag may be located.

• The tag should now appear as an unrecognized BLE signal, since it is no longer linked to its paired phone.

Verify Detection

• Repeat the scan from different positions in the area to confirm results.

• If the AirTag does not appear, double-check that the paired phone is fully disabled and sufficiently distant.

Once you have mastered locating a BLE tag you hid yourself, try locating one that someone else hid for you. Please remember that using an AirTag or any tracking device to monitor someone's location without their consent is illegal and a breach of privacy. It is crucial to respect others' privacy and use such devices responsibly and ethically.

Vehicles are often tracked and offer good hiding spaces if you want to practice searching. Here are a few tips:

Under the seats: BLE Tags are small and easily accessible, making them a common hiding spot.

Glove compartment: Easily accessible but also enclosed make it a popular hiding space.

Trunk: Popular choice for hiding tags because it offers additional hidden spaces such as under the spare tire.

Door storage pockets: Convenient space to hide small item especially if the pocket is already full of items.

Between seat cushions: The seam between bottom and back cushions fits any BLE tag nicely.

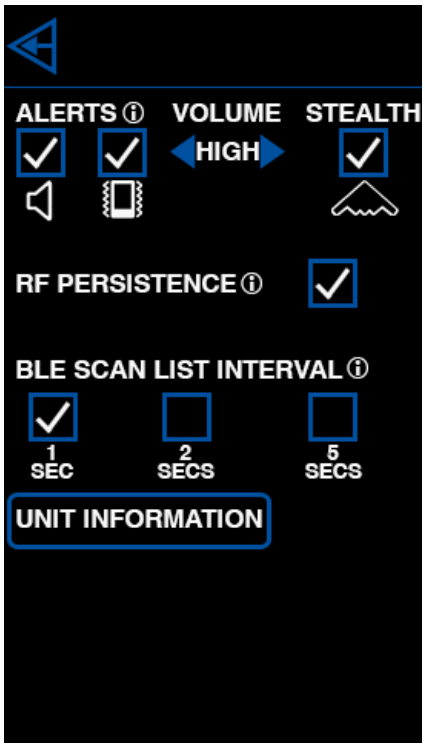
Cup holders: Sometimes the best hiding place is right in front of you or at least under your coffee cup.

Center console: Contains many compartments to hide many small items.

Floormat: Only takes a moment to place BLE tag under a mat and takes the same time to find one there too.

Outside vehicle: Too many possibilities to mention all of them but popular ones include inside gas cap, inside wheel well, under front/rear bumpers, behind license plate, inside front grill area, etc.

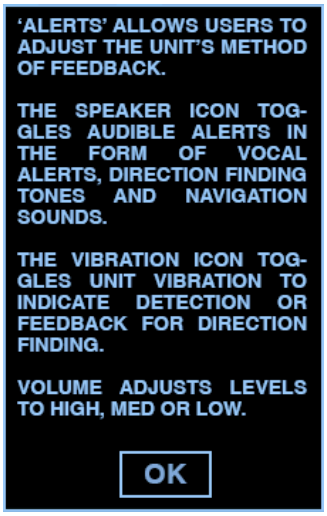
Main Options Menu



Choose the menu icon at the top of any screen to enter the Main Options Menu at any time. From this menu, users can adjust alert settings, scan settings and access unit information. Voice, tonal or vibrating alerts can all be toggled on or off. There is also a low, medium and high volume control for audio alerts. Tap the circle i (info icon) on the text it follows at any time for more information on that setting in the form of pop-up text. Stealth mode removes all audible beeping from the unit's speakers so that users can conduct more covert scans for hidden BLE devices.

AUDIO ALERTS are voice alerts that include BLE tags, BT skimmers, BLE devices and BLE beacons. When the user selects (filtering the list) one or any combination of these device types in the MAIN SCANNING LIST, voice alerts can be heard for each device type detected with the strongest signal strength. The primary voice AUDIO ALERTS are:

"AirTag Detected"
"Bluetooth Low Energy Detected"
"Skimmer Detected" (BT Classic)
"Beacon Detected"



Additional voice AUDIO ALERTS for wireless devices that pose a potential threat based upon their manufacturer are:

"ZTE Device Detected"
"Huawei Device Detected"
"Xiaomi Device Detected"

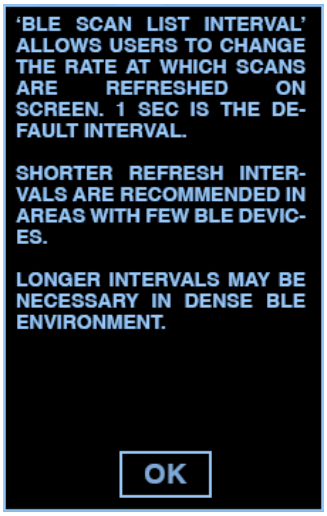
Additional voice AUDIO ALERTS for common BLE Tags or PEDs (Personal Electronic Devices) are:

"AirTag Detected"
"Tile Tracker Detected"
"Samsung Tracker Detected"
"PebbleBee Tracker Detected"
"Google Device Detected"

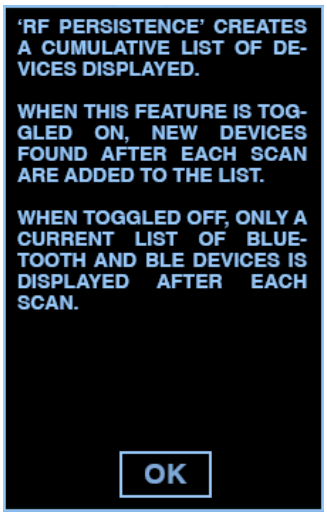
“FitBit Detected”

“Chipolo Detected”

BLE SCAN LIST INTERVAL allows users to change the rate at which scans are displayed. One second is the default interval with two and five second options as well. In environments with little activity, shorter intervals are recommended in order to achieve faster refreshes of BT and BLE device lists. In environments with lots of BT and BLE activity, longer intervals are recommended to display all nearby devices long enough to observe. If you wish to display a history of spoofed MAC addresses, you must select the 5 second option and the RF PERSISTENCE mode ON as well.



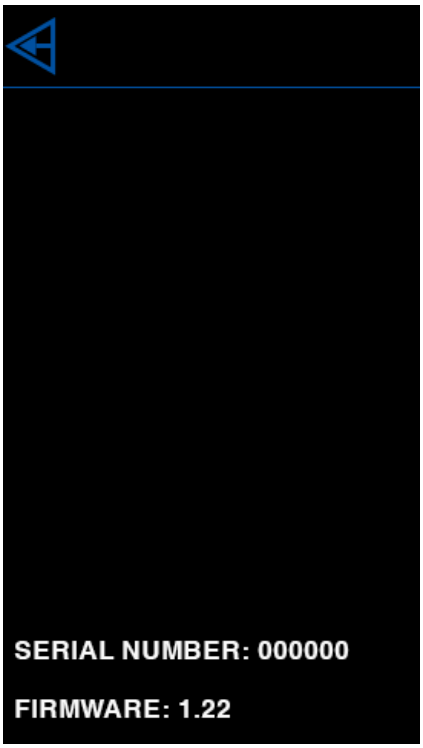
RF PERSISTENCE will help to identify some of the more elusive BLE devices and tags. BlueSleuth-Pro is capable of detecting many BLE devices and tags simultaneously but since the Main Scanning List can only display 5 devices on a screen page simultaneously, it can sometimes make it difficult to identify specific ones, especially if they broadcast intermittently. The general rule is to turn on RF Persistence when in areas with a lot of BLE devices and activity. RF Persistence does not change the rate or speed at which BLE devices and tags are scanned. It merely changes the rate at which they are removed from the list once they are no longer detected. To display a history of spoofed MAC addresses, you must select RF Persistence to ON.



UNIT INFORMATION displays all relevant info for that particular unit including serial number and firmware. Be sure to have this information handy if you are contacting BVS support for help.

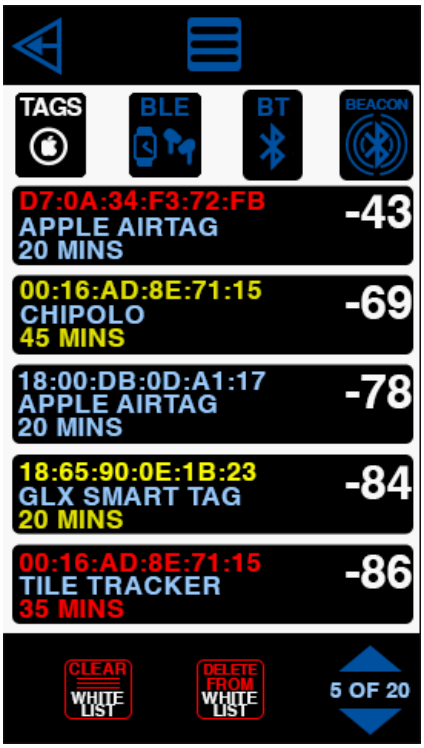
Unit Information

This screen displays your unit's unique serial number and current firmware version. Be sure to have this information handy if you are contacting BVS support for help.



White List

Each of the four scan modes in the BlueSleuth-Pro (Tags, BLE, BT and Beacon) has its own independent White List that can store up to 150 MAC addresses (5 per page x 30 pages). The White List button allows users to remove known/selected devices from the scan list. This feature allows users to spend more time identifying unknown and possibly dangerous rogue Tag, BLE, BT or Beacon devices instead of continually sorting through devices that have already been scanned and accounted for. Simply touch the White List button to activate this feature (the button will invert to a red color and blink to indicate activation). Next, touch each listed Bluetooth device in the scan list pages that you wish to white list. Every Bluetooth device you choose will disappear from the associated scan list and not return until the unit power is reset or until you choose to reset/edit any of the four white lists. Touch the White List button again when you are finished white listing devices.



To Edit any of the created White Lists, simply touch the "Edit White List" icon at the top of the display page for the scan mode that you are in. You will be automatically taken to the White List for that mode. When there, you will find two icons at the bottom of the display page which will read "Clear White List" and "Delete From White List". The "Clear White List" button will delete the entire White List at once. The "Delete From White List" will allow you to selectively delete particular MAC addresses from the White List while leaving the rest of the list intact. Depressing the "Delete From White List" button will invert the color of the button to red and also make it blink. While the button is in this state, click on any of the MAC addresses that you wish to clear from the White List. When finished, click on the "Delete From White List" button again. Those items that were individually removed from the White List during this operation will now rejoin the main scan pages where they were originally detected (if those devices are still present in your scan environment).

The "Edit White List" page also allows you to navigate to the four available White Lists (Tags, BLE, BT and Beacon) so that you can clear or edit them as explained in the paragraph above. Simply depress the corresponding button for Tags, BLE, BT or Beacon and you will be presented with the corresponding White List of MAC addresses for that mode. If no items were placed into the White List, the display area for listed devices will be blank.

Detectable BLE Tag List

This list changes (and new BLE tags introduced into the market) with more frequency than this user manual can be updated, so if you do not see your tag listed here, contact sales@bvsystems.com for the latest updates. If you need to detect a particular BLE tag not on the list, contact support@bvsystems.com and we can attempt an update to your unit's firmware to include that tag.

✔ Apple AirTag (registered and non-registered)

✔ Samsung Galaxy SmartTag (versions 1 and 2)

✔ Eufy Security SmartTrack Link

✔ Tile (Slim, Mate, Pro, Sticker, Sport)

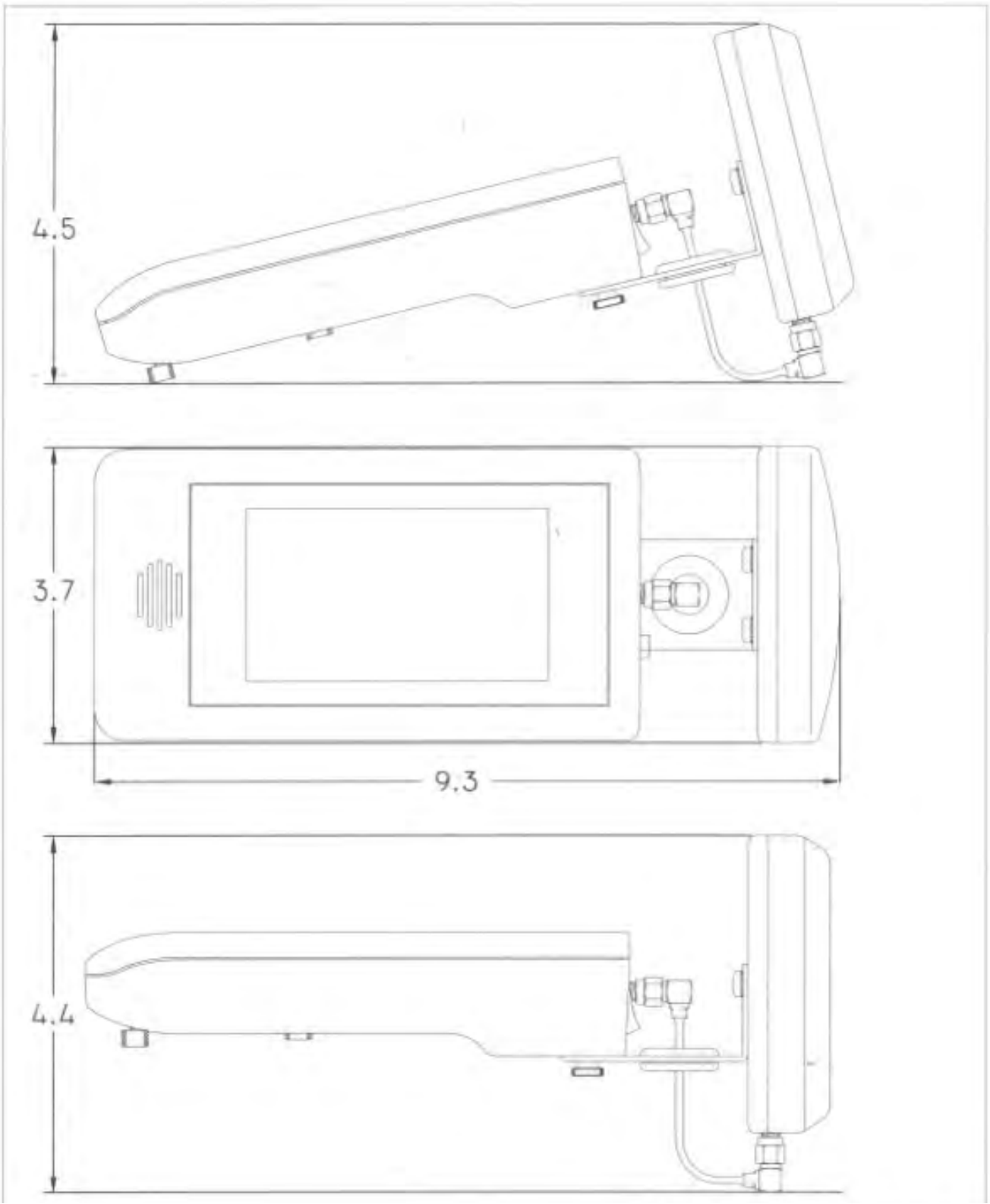
✔ AirCard

✔ Chipolo (generation 1 and 2)

✔ PebbleBee

✔ These lesser known tags simply identify as generic "Tag Detected"

BlueSleuth-Pro Unit Dimensions



W24-58-CP-9

M2M / WLAN

08/05/2015 v.A

Dual Band Directional Patch Antenna

High gain directional antenna

Covers 2.4 & 5GHz for WIFI/WLAN

Ideal WIFI coverage extender for large rooms, car parks & warehouses

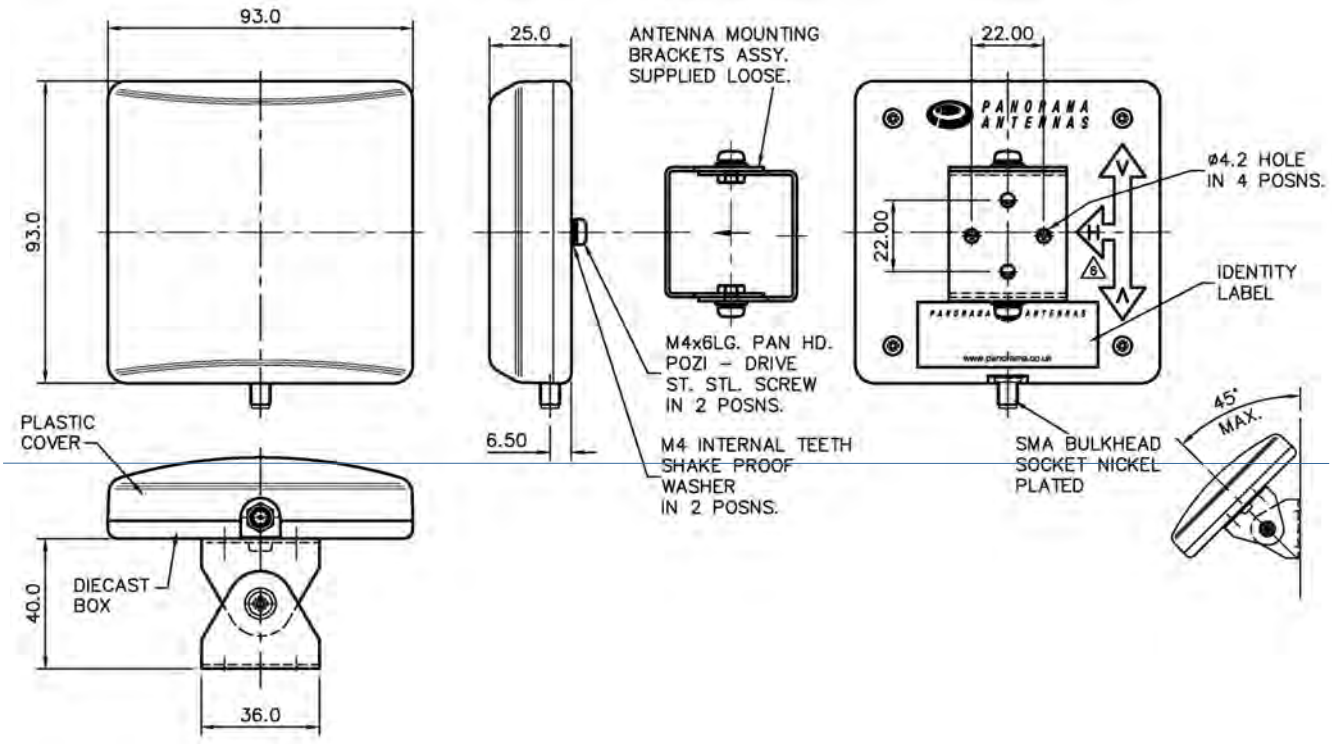
The Panorama client patch antenna is a directional wall or mast mounted antenna covering 2.4 & 5GHz for WIFI / WLAN applications.

This antenna is ideal for point to point communications or can be used to cover a wide area thanks to its relatively wide beamwidth in the horizontal and vertical planes. Several of these antennas can be used to provide cost effective sectored coverage.

The antenna is supplied with a 90 degree adjustable wall / mast mount angle bracket to give optimal mounting flexibility.

Ideal to infill network coverage black spots or to provide a consistent connection for subscriber terminals the W24-58-CP-9 is a cost effective solution to network coverage issues.

Technical Drawing



PANORAMA ANTENNAS

Panorama Antennas Ltd

Frogmore, London, SW18 1HF, United Kingdom

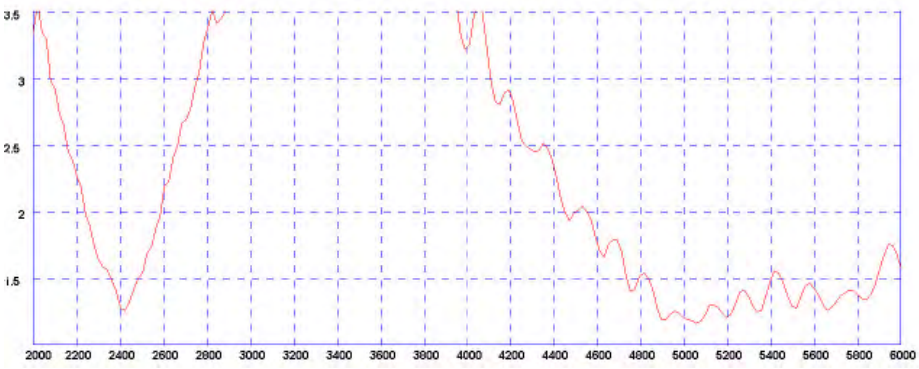
T: +44 (0)20 8877 4444

F: +44 (0)20 8877 4477

E: sales@panorama-antennas.com

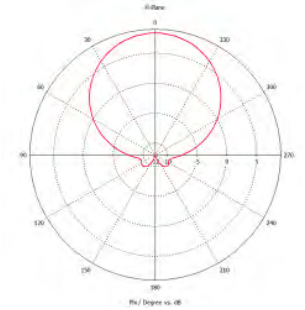
www.panorama-antennas.com

Typical VSWR

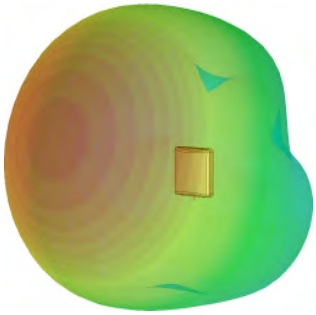


*VSWR measured in free space without additional cable

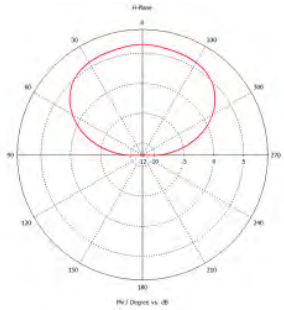
Typical H-Plane (2400MHz)



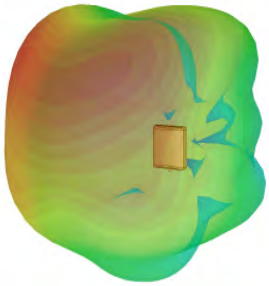
Typical 3D Plot (2400MHz)



Typical H-Plane (5400MHz)



Typical 3D Plot (5400MHz)



Part No.		
		W24-58-CP-9
Electrical Data		
Frequency Range (MHz)		2400-2485 /4900-6000
Operational Band		2.4GHz/5GHz WLAN
VSWR		≤ 2:1
Peak Gain: Isotropic		9dBi
Pattern		Directional
3dB Beamwidth	Azimuth 2.4GHz	60°
	Azimuth 5GHz	90°
Polarisation		Vertical
Impedance		50Ω
Max Input Power (W)		50
Mechanical Data		
Dimensions (mm)	Height	93 (3.66”)
	Width	93 (3.66”)
	Depth	25 (0.98”)
Operating Temp (°C)		-30° / +70°C (-22° / +158°C)
Material		Geloy PC/ASA & die cast aluminium
Colour		Signal White
Mounting Data		
Fixing		Wall mount or Mast mount
Environmental Specification		
Wind Load / Resistance		11N at 150km/h
Radome Flammability		UL94 V0 - Halogen Free
Connector Data		
Termination		SMA socket

ANT-DB1-LCD-ccc

Data Sheet

Product Description

The Linx LCD Dipole Antenna is a superior solution for users searching for best-in-class performance for WLAN devices using Dual-Band WiFi (802.11ac, 802.11n, 802.11ax) or U-NII applications.

With a compact package and low price, the LCD's high peak gain and superior efficiency make it an excellent option for high volume, cost sensitive applications.

Dipole design means that no additional ground plane is required.

Features

- Excellent performance
- Dual-band
- Very low VSWR
- Omni-directional pattern
- Tilt and swivel base
- Standard SMA or Part 15 compliant RP-SMA connector

Ordering Information

ANT-DB1-LCD-RPS (with RP-SMA connector)
ANT-DB1-LCD-SMA (with SMA connector)

Electrical Specifications

Parameter			
Recommended Frequency Range	2.4GHz WIFI	U-NII	5.8GHz WIFI/ U-NII-3 Band
	2.4 – 2.5GHz	5.125 – 5.725GHz	5.725 – 5.875GHz
VSWR	<2:1	<2:1	<2:1
Peak Gain (max in the band)	2.8dBi	4.5dBi	2.92dBi
Average Gain (typical)	–0.6dBi	–1.5dBi	–2.2dBi
Efficiency (typical)	85%	70%	65%
Polarization	Linear		
Radiation	Omni-Directional		
Max Power	10W		
Wavelength	1/2-wave		
Impedance	50-ohms		
Connection	SMA Plug (Male) or RPS (Reverse Polarity Male)		
Weight	7.4g (0.26oz.)		
Operating Temperature Range	–40°C to +80°C		

Measurements taken on a 100 x 100mm ground plane, mounted on the edge, bent 90°.

Revised 10/18/2018

Product Dimensions

Dipole antennas, ground planes and additional orientations

Since it is not always possible to provide an adequate ground plane, dipole antennas like the LCD are designed with a built-in ground plane, so an external ground plane is not required for the antenna to radiate properly.

Linx knows how our customers most frequently use our antennas in theirs designs, typically mounted to enclosures, conductive or non-conductive, so we tested our LCD antenna in 2 different configurations: straight, without ground (free space), and edge of a ground plane bent at 90°.

Straight, without ground

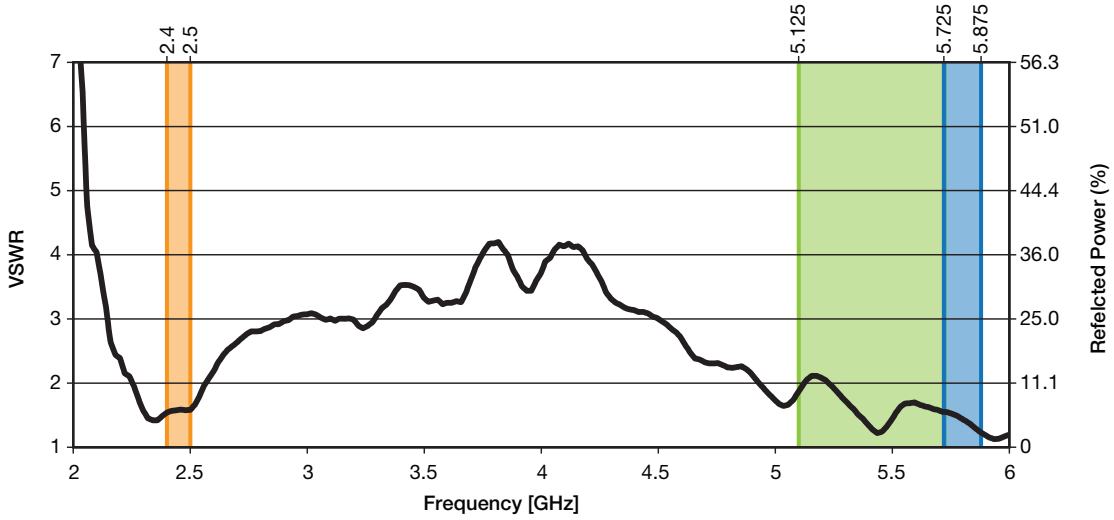
Bent 90°, on edge of ground

Linx tested the LCD dipole antenna to ensure excellent radiation behavior and minimize the risk to the customer when implementing a new design, regardless of complexity.

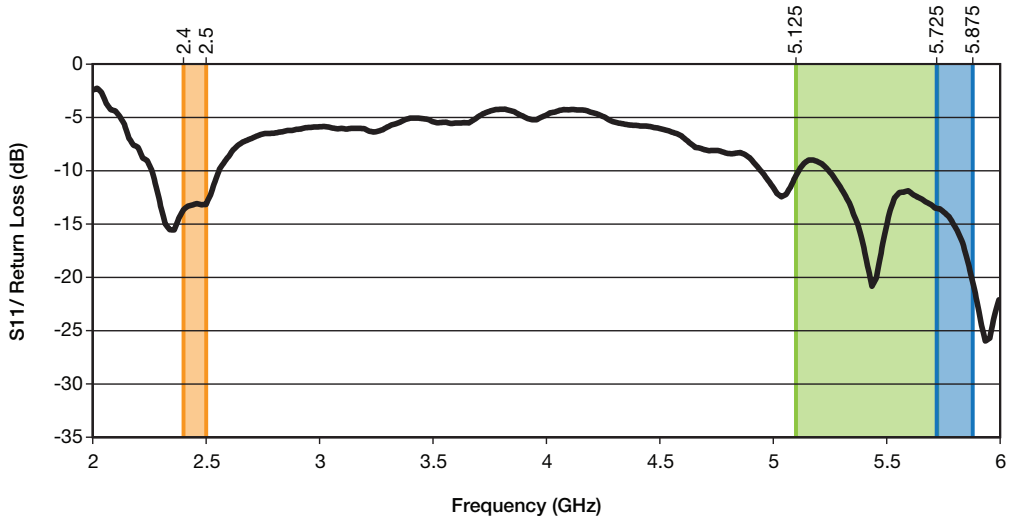
Additionally, there are many other configurations with which our LCD antenna will have similar performance to the Bent 90°, on edge of ground, with minimal difference, as shown below.

Antenna straight on non-conductive surface/ Free space

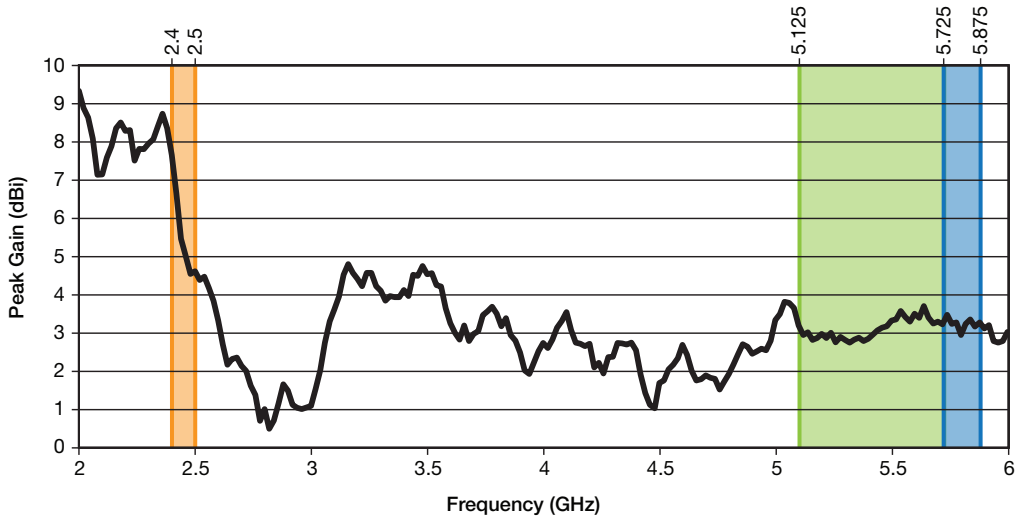
VSWR



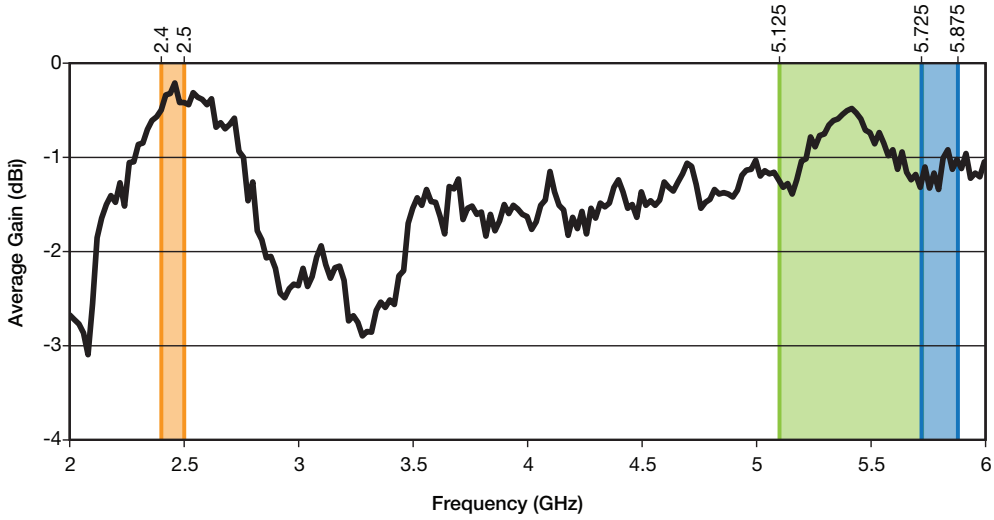
Return Loss



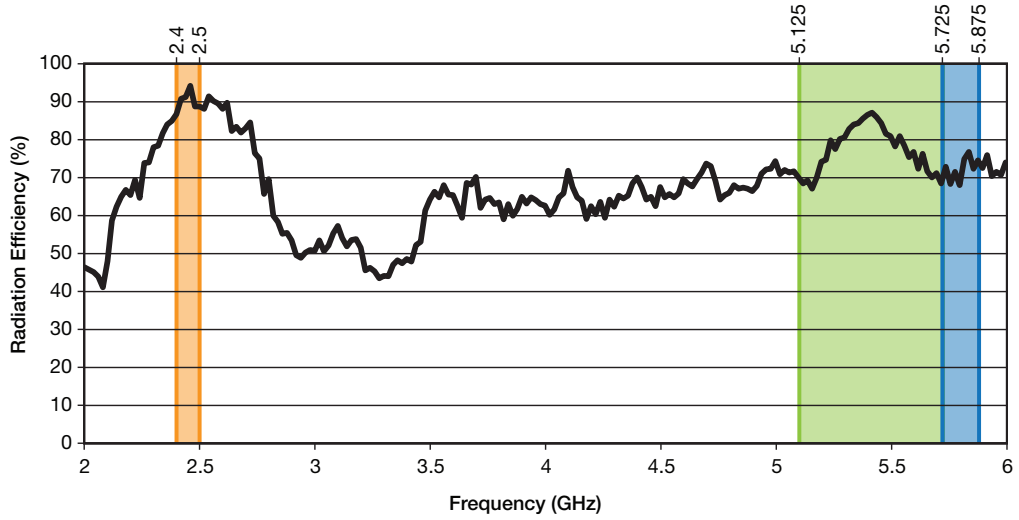
Peak Gain



Average Gain



Radiation Efficiency



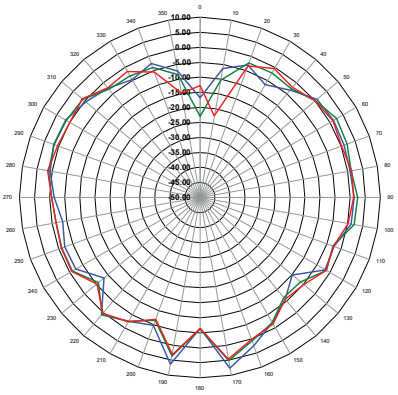
Antenna straight on non-conductive surface/ Free space

XZ-Plane Gain

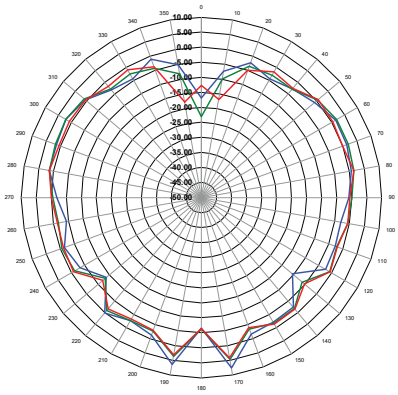
YZ-Plane Gain

XY-Plane Gain

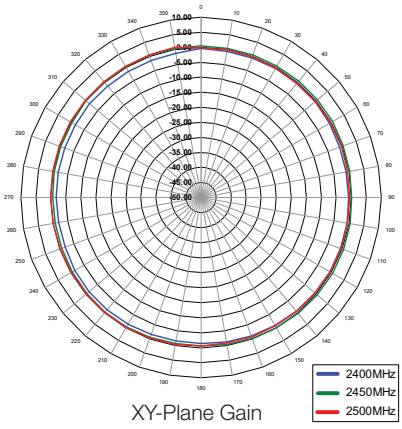
2400 - 2500MHz



XZ-Plane Gain

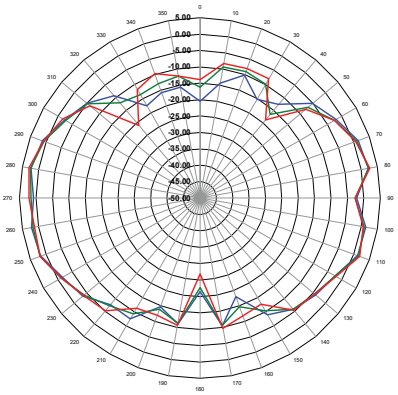


YZ-Plane Gain

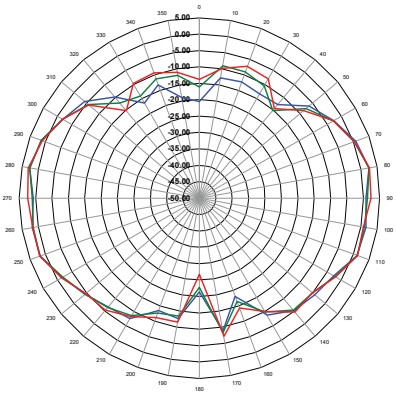


XY-Plane Gain

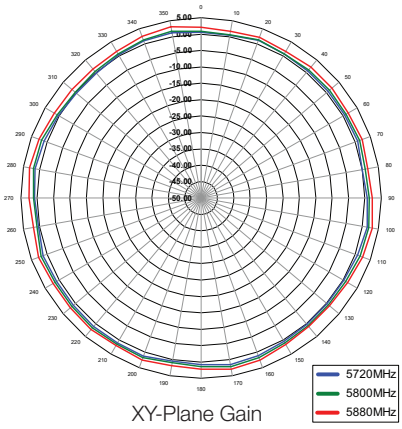
5720 - 5880MHz



XZ-Plane Gain



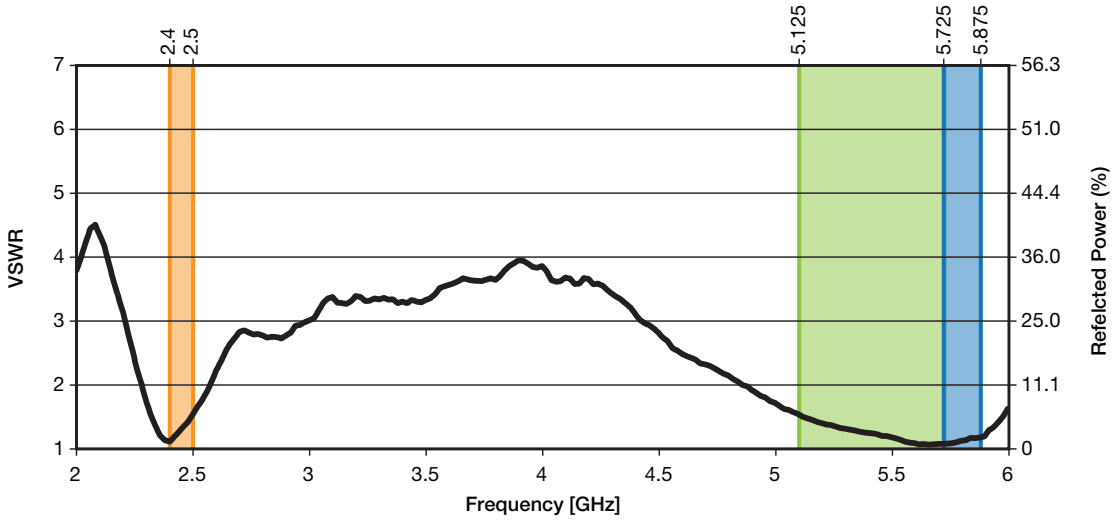
YZ-Plane Gain



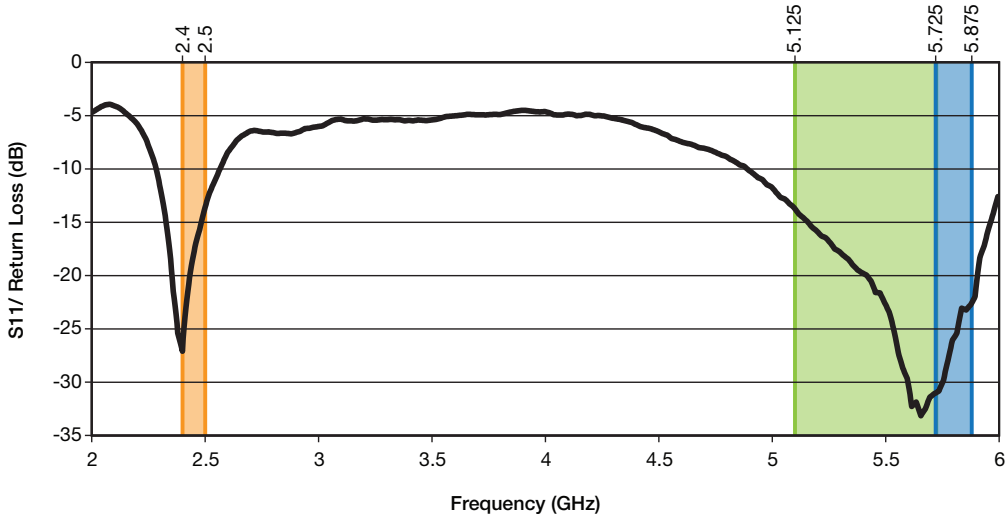
XY-Plane Gain

Edge of the Ground Plane, Bent 90°

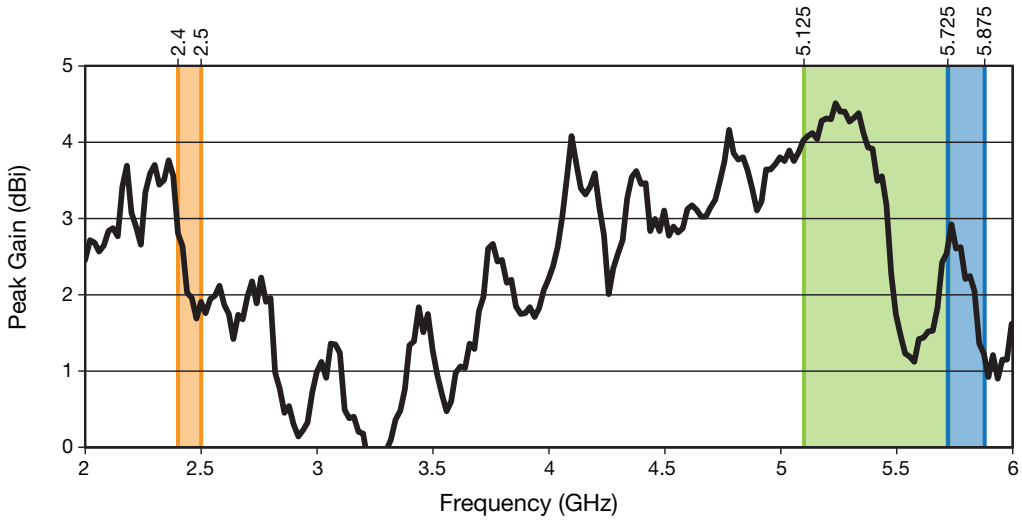
VSWR



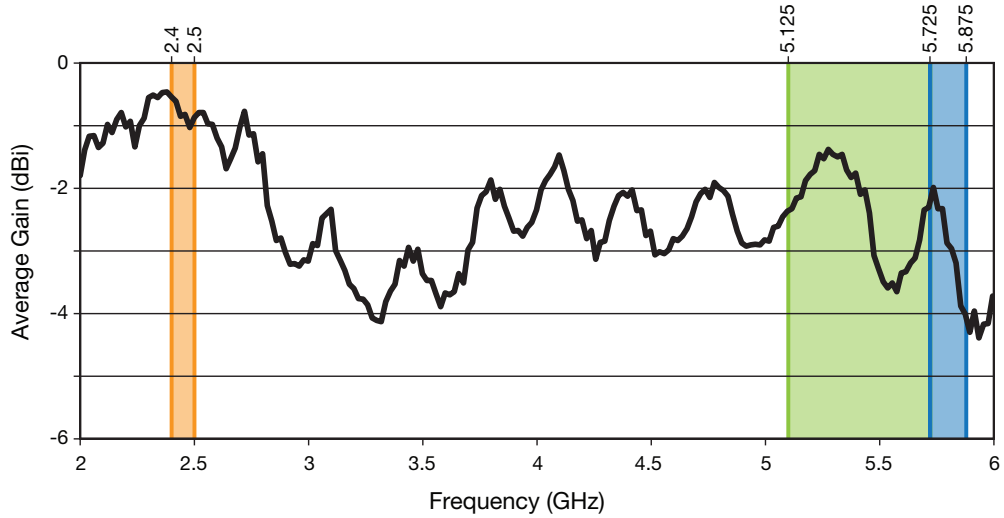
Return Loss



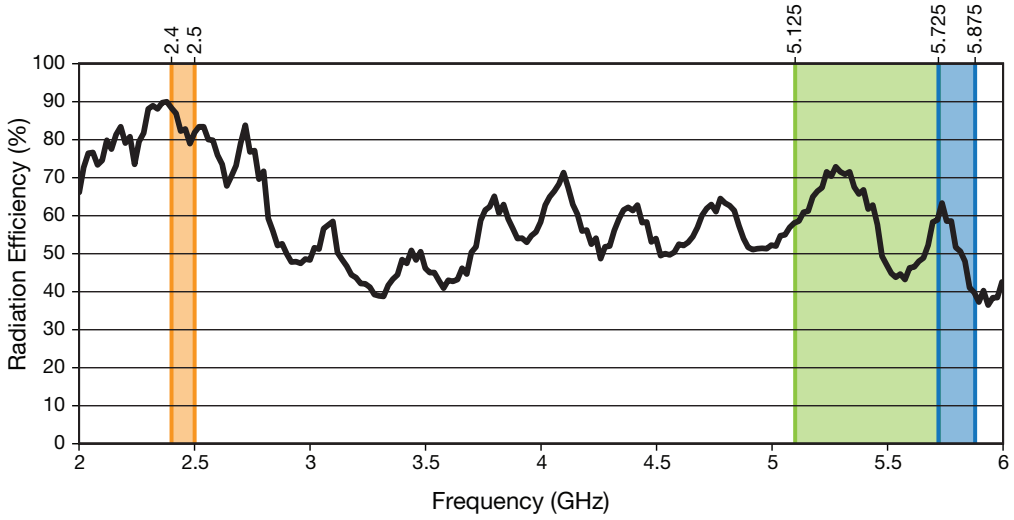
Peak Gain



Average Gain



Radiation Efficiency



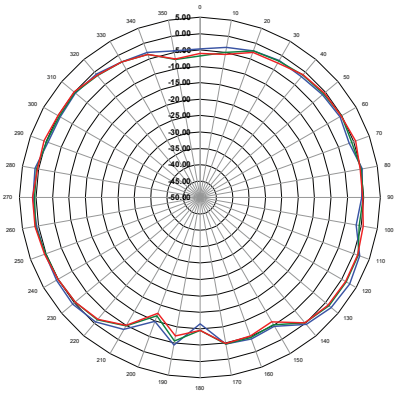
Gain Plots - Edge of Plane, Bent 90°

XZ-Plane Gain

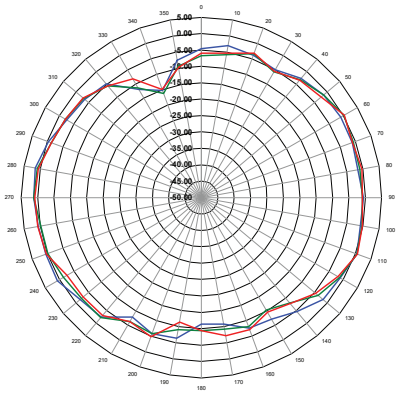
YZ-Plane Gain

XY-Plane Gain

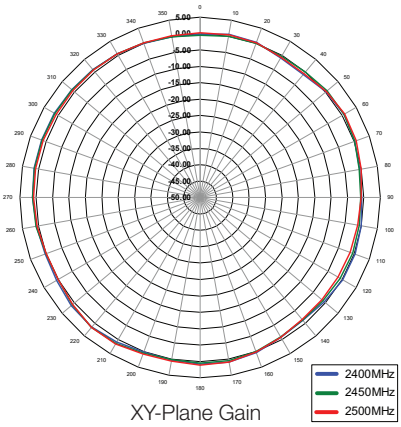
2400 - 2500MHz



XZ-Plane Gain

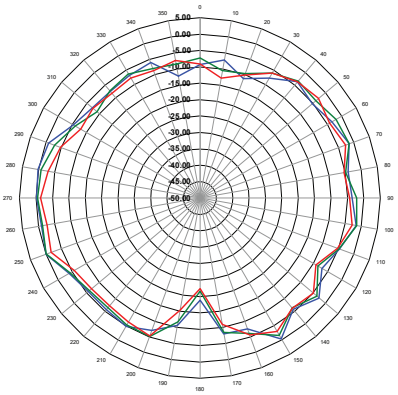


YZ-Plane Gain

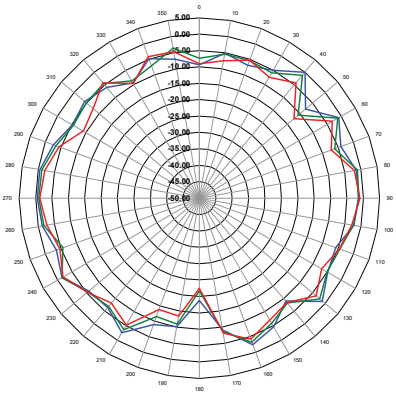


XY-Plane Gain

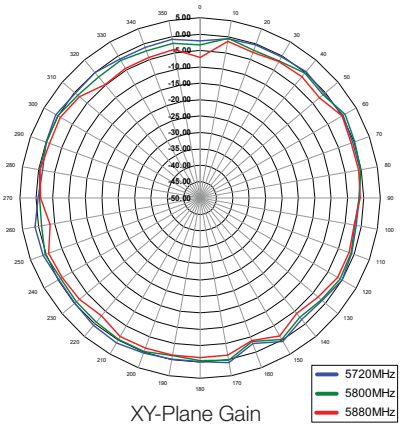
5720 - 5880MHz



XZ-Plane Gain



YZ-Plane Gain



XY-Plane Gain

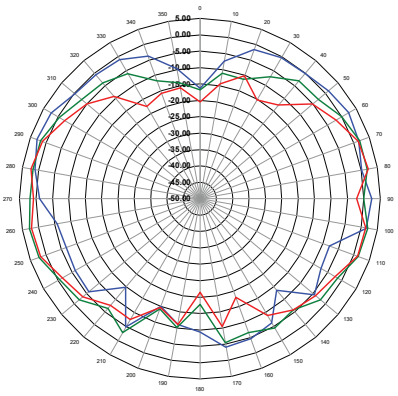
Performance in the U-NII Band - Antenna straight on non-conductive surface/ Free space

XZ-Plane Gain

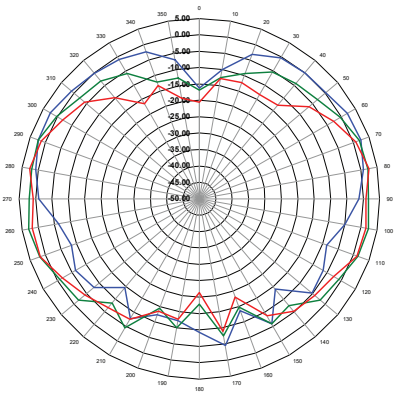
YZ-Plane Gain

XY-Plane Gain

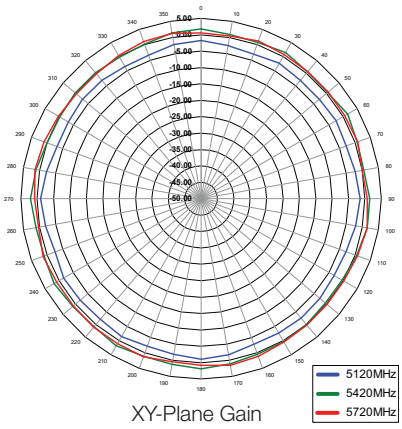
5120 - 5720MHz



XZ-Plane Gain

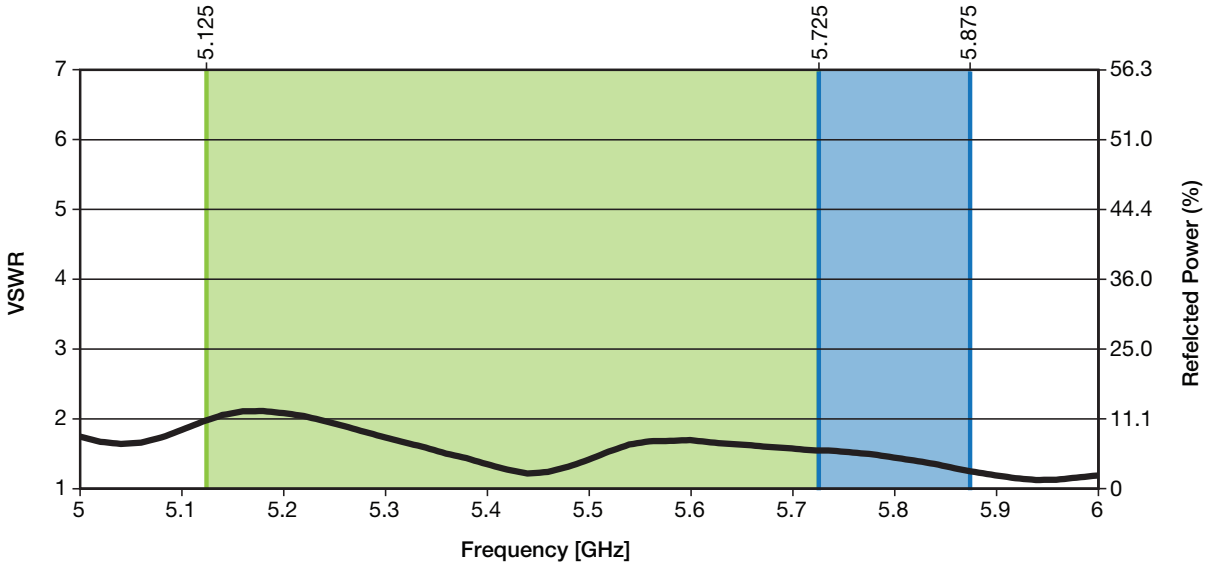


YZ-Plane Gain



XY-Plane Gain

VSWR



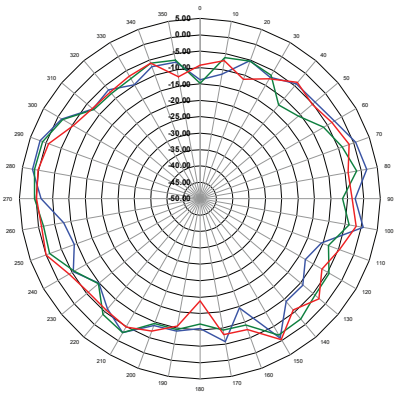
Performance in the U-NII Band - Edge of the Ground Plane, Bent 90°

XZ-Plane Gain

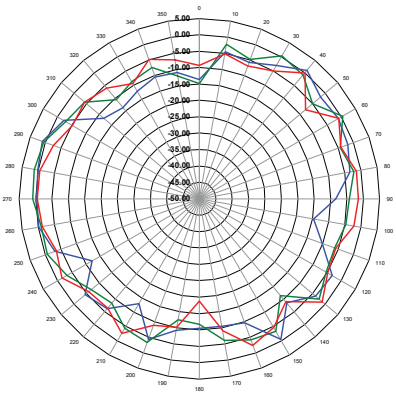
YZ-Plane Gain

XY-Plane Gain

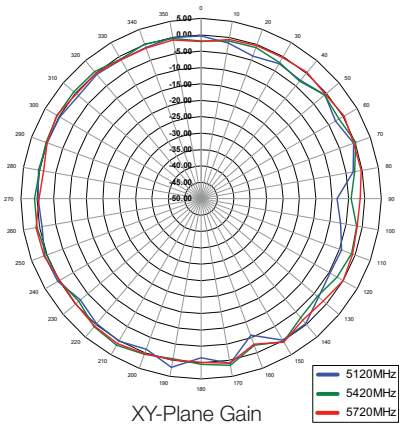
5120 - 5720MHz



XZ-Plane Gain

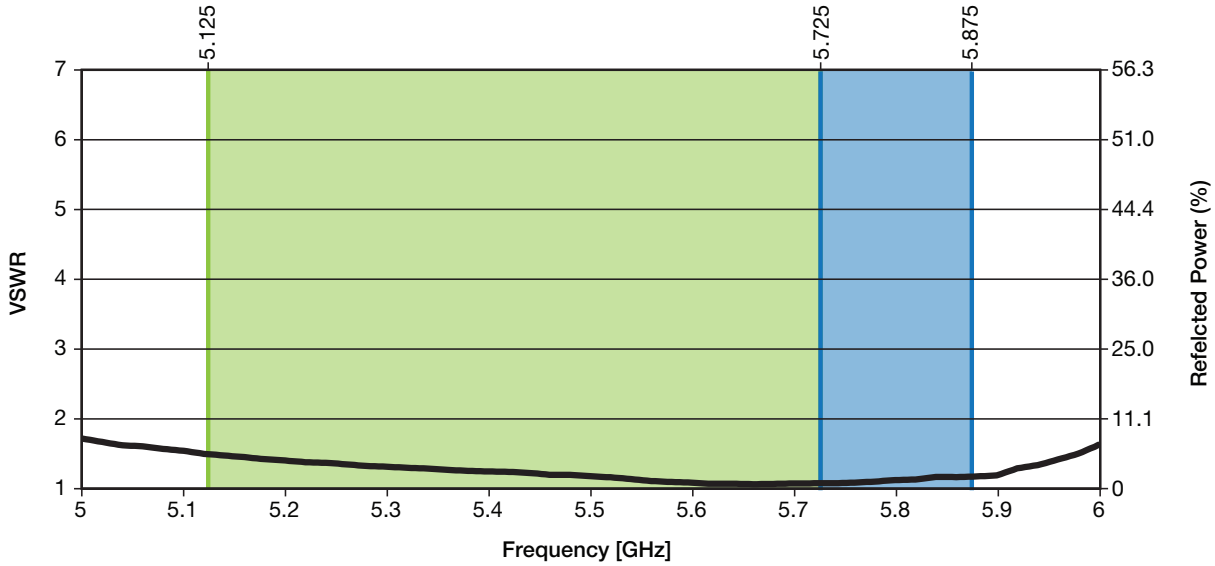


YZ-Plane Gain



XY-Plane Gain

VSWR



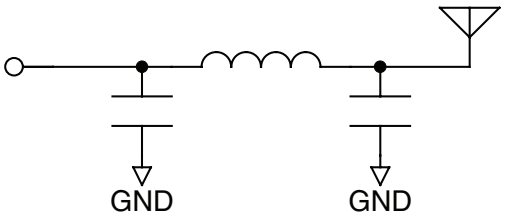
Matching Network

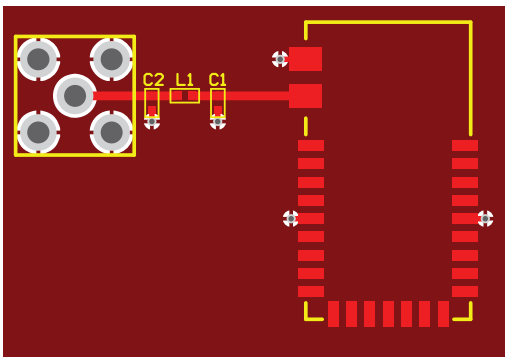
Linx tests all our antennas in ideal scenarios where effects from conductive surfaces, non-conductive surfaces or human proximity issues are eliminated. As a designer, you do not have much control over the environment your product will be used in.

Linx has always worked closely with our customers, and we know what the primary concerns and pitfalls are for designers and how to prepare for them. Whether you are designing for a monopole or a dipole antenna, or an external or even an embedded surface mount antenna, the most common question is, “Why isn’t my design working?”, and frequently it turns out the design needed a matching network.

As your product design progresses, the chances for proximity effect increases as other components are added. Some components can act like ground planes, if they have large conductive surface areas, and can cause interference. This interference is called proximity effect, which can cause a downward shift in the center frequency of the circuit, depending on how strong the effects are. Proximity effect is commonly caused by components like pc boards, batteries, motors, sensors, actuators and even non-conductive enclosures like radomes. Interference can also occur from human proximity, like when using a hand-held mobile device.

Although our dipole antennas have been designed to minimize these effects, we strongly recommend the use of a matching network, so you can ensure that you retain optimum signal levels. A matching network is a circuit that balances the impedance and ensures there is minimum reflected energy coming back from the antenna. This enables the integrator to optimize the performance in a specific band or to level performance across all bands. The most common matching network design is called a Pi circuit, placed between the antenna and the radio; it is a simple circuit of two capacitors to ground on either side of a series inductor.





The values can be selected to electrically tune the antenna. It does take test equipment, such as a network analyzer, to get this right though. Often a design ends up having little or no proximity effect, eliminating the need to retune the matching section. In these cases, the matching section can have a zero ohm resistor in place of the Inductor, leaving the other two shunt components un-populated.

The values of the matching components are determined experimentally on the product’s board. Since there are many variables that play into the antenna’s final performance, it is very difficult to predict what it will do on any specific design. It is best to design in the matching network, see what the antenna does on the prototype and then dial the performance in with the network components. Not all of the components may be needed on a particular design, so they do not need to be populated in production; but it is a good idea to have the component pads on the board in case they are needed. The components should be placed close to the antenna connection. The component pads should be placed on the 50-ohm line between the radio and the antenna.

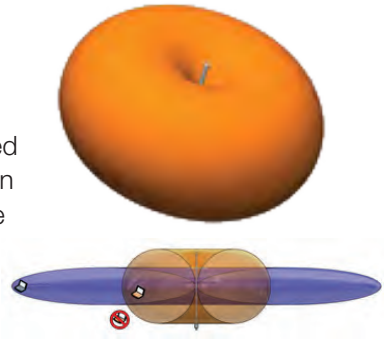
Linx Technologies offers a service to help customers tune our antennas to their circuit boards. Please contact Linx for more details.

About Gain Plots

The true measure of the effectiveness of an antenna in any given application is determined by the gain and radiation pattern measurement. For antennas gain is typically measured relative to a perfect (isotropic) radiator having the same source power as the antenna under test, the units of gain in this case will be decibels isotropic (dBi). The radiation pattern is a graphical representation of signal strength measured at fixed distance from the antenna.

Gain when applied to antennas is a measure of how the antenna radiates and focuses energy into free space. Much like a flashlight focuses light from a bulb in a specific direction, antennas focus RF energy into specific directions. Gain in this sense refers to an increase in energy in one direction over others.

It should also be understood that gain is not "free", gain above 0dBi in one direction means that there must be less gain in another direction. Pictorially this can be pictured as shown in the figures to the right. The orange pattern represents the radiation pattern for a perfect dipole antenna, which is shaped like a donut. The pattern for an omnidirectional antenna with gain is shown in blue. The gain antenna is able to work with a device located further from the center along the axis of the pattern, but not with devices closer to the center when they are off the axis – the donut has been squished.



Gain is also related to the overall physical size of the antenna, as well as surrounding materials. As the geometry of the antenna is reduced below the effective wavelength (considered an electrically small antenna) the gain decreases. Also, the relative distance between an electrically small antenna and its associated ground impacts antenna gain.

What is VSWR?

The Voltage Standing Wave Ratio (VSWR) is a measurement of how well an antenna is matched to a source impedance, typically 50-ohms. It is calculated by measuring the voltage wave that is headed toward the load versus the voltage wave that is reflected back from the load. A perfect match has a VSWR of 1:1. The higher the first number, the worse the match, and the more inefficient the system. Since a perfect match cannot ever be obtained, some benchmark for performance needs to be set. In the case of antenna VSWR, this is usually 2:1. At this point, 88.9% of the energy sent to the antenna by the transmitter is radiated into free space and 11.1% is either reflected back into the source or lost as heat on the structure of the antenna. In the other direction, 88.9% of the energy recovered by the antenna is transferred into the receiver. As a side note, since the ":1" is always implied, many data sheets will remove it and just display the first number.

How to Read a VSWR Graph

VSWR is usually displayed graphically versus frequency. The lowest point on the graph is the antenna's operational center frequency. In most cases, this is different than the designed center frequency due to fabrication tolerances. The VSWR at that point denotes how close to 50-ohms the antenna gets. Linx specifies the recommended bandwidth as the range where the typical antenna VSWR is less than 2:1.

159 Ort Lane, Merlin, OR 97532
Phone: +1 541 471 6256
Fax: +1 541 471 6251
www.linxtechnologies.com

Thank you for your purchase, we look forward to supporting you and your team.

Customer Support

Berkeley Varitronics Systems, Inc.
Liberty Corporate Park
255 Liberty Street
Metuchen, NJ 08840

8:00 AM to 6:00 PM EST
Toll Free: 888-737-4287
Phone: 732-548-3737
Fax: 732-548-3404

24/7 (expect a reply within one day)
email: support@bvsystems.com
www.bvsystems.com