



Location Services

Network Project Prerequisites

HID Location Services and Bluvision solutions require constant communications between the Beacon, BluFi Gateway, and the Cloud (called Bluzone). The Beacons are in constant communication with the BluFi, via BLE, providing location information and more. The BluFi's are in constant communication with the Bluzone Cloud service providing information on all the Beacons so the information can be captured, correlated, visualized, and stored. The communication between the beacon, BluFi, and Bluzone Cloud make up the overall solution.

This document discusses some of the main aspects of the network infrastructure that are necessary to install a productive system.

Table of Contents

Location Services	1
Getting Started.....	2
Description	2
How does it work.....	2
Network Preparation	3
BluFi Gateways	3
Heartbeat Testing.....	3
Configuration Requirements.....	3
Network Project Prerequisites.....	4
BluFi™ Enterprise WiFi	5
General Requirements.....	5
REQUIRED PORTS.....	5
Enterprise WiFi Requirements	5
SUPPORTED SECURITY TYPES.....	5
Testing.....	5

Getting Started

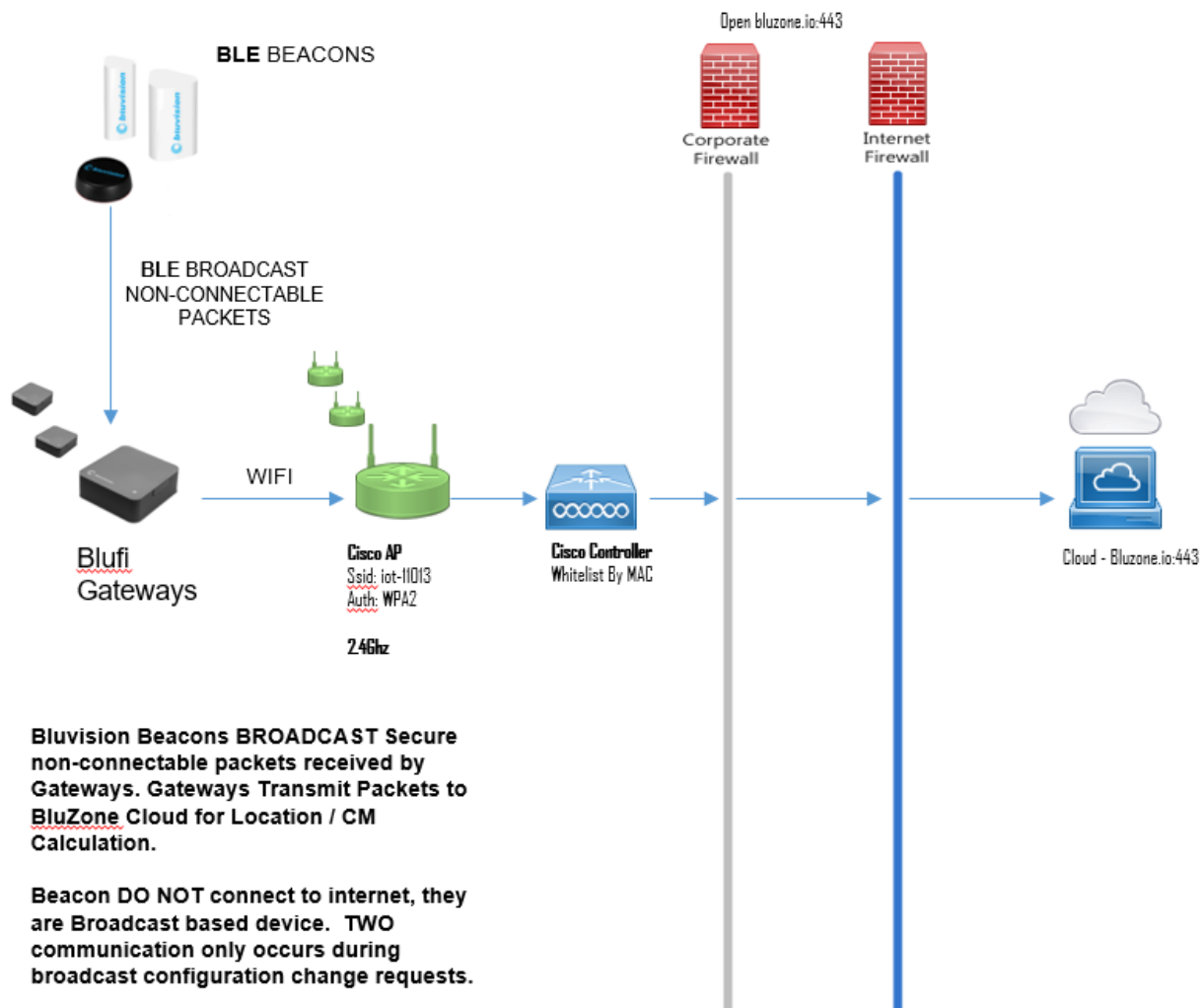
Description

HID Bluvision uses a combination of Bluetooth Low Energy (BLE) and a proprietary location engine to achieve high accuracy in asset tracking

How does it work

HID Bluvision beacons transmit a secure non-connectable BLE advertising packet that is received by Bluvision BLE to Wi-Fi Gateways called BluFi. BluFi gateways detect these non-connectable advertising packets that contain beacon telemetry and relay the information to HID Bluvision Bluzone Cloud via a SSL connection.

Sample - Network High Level Design



Network Preparation

BluFi Gateways

Minimal Hardware & Software Requirements:

- WLAN Standards: **802.11 g/n 2.4 GHz**
- Upload Speed: **1 Mbps “Sustained”**
- Access to Internet: (Domain) **bluzone.io** (Port) **443**
- Internet HTTP Proxy: **Disabled**
- Supported Authentication Protocols:

WEP	EAP PEAP1 PSK
WPA2	EAP PEAP1 TLS
EAP PEAP0 MSCHAPv2	EAP TLS
EAP PEAP0 PSK	EAP TTLS MSCHAPv2
EAP PEAP0 TLS	EAP TTLS PSK
EAP PEAP1 MSCHAPv2	EAP TTLS TLS

Heartbeat Testing

Has Customer successfully setup and provisioned a sample BluFi? [YES/NO]

Configuration Requirements

These devices will be preconfigured? [YES/NO]

- *If Pre-configured? Bluzone Template _____ will loaded.*

These devices will be custom labeled? [YES/NO]

- *If custom labeled? Use pattern _____.*

Notes:

This BluFi version requires open internet access within 2.4 GHz wireless infrastructure with an outbound internet connection to bluzone.io:443 and NO HTTP PROXY. This BluFi utilizes the TI wireless chip that is NOT proxy aware/configurable. In preparation, these devices should be whitelisted by customer networking team.

Network Project Prerequisites

Below are prerequisites regarding the network and the connectivity to the cloud:

- Client will provide Project team with access to client’s Wi-Fi network and ensure good Wi-Fi network coverage of at least 2 Mbps in those areas where BluFi gateways are designated to be installed prior to installation date.
- Wi-Fi supports minimum download speeds of 2 Mbps. Wi-Fi supports minimum upload speeds of 2 Mbps.
- The wireless network configuration must allow automated and none-expiring login setup to allow BluFi’s continuous access to the Bluzone cloud. Wi-Fi network must operate over 801.11 g/n at the 2.4GHz frequency band.
- Wi-Fi is machine to machine (m2m) optimized that does not implement HTML sign-in.
- Client will be responsible to make available and maintain open outbound Port 443 for communication with the “cloud” (telnet bluzone.io:443 should work).
- Port UDP 123 must be open (NTP)
- Network SSID, username and password must be provided at least 7 days prior to equipment delivery date with access to the AWS hosted Bluzone cloud.
 - For projects including pre-provisioning of the network SSID, username and password must be provided at least 14 days in advance for this task to be completed before equipment ships to End User location. (Large orders will require this information eve
- Client will be responsible to make available power drops in designated installation points using Mini-USB or RJ45 PoE cable interfaces and any other physical install services of equipment which may require electrical or facility deployment.
- Best practices recommendation is for each access point to support no more than 25 – 30 mac address and no more than 20 - 25 BluFi gateways.
- Supported Protocols:

WEP	EAP PEAP1 PSK
WPA2	EAP PEAP1 TLS
EAP PEAP0 MSCHAPv2	EAP TLS
EAP PEAP0 PSK	EAP TTLS MSCHAPv2
EAP PEAP0 TLS	EAP TTLS PSK
EAP PEAP1 MSCHAPv2	EAP TTLS TLS

BluFi™ Enterprise WiFi

This section describes the operational requirements for setting up Bluvision BluFis with Enterprise Authentication. The section of “General Requirements” is common to all BluFi installations.

General Requirements

BluFis must have access to Bluzone Cloud. BluFis connect to Bluzone using HTTPS (secure web socket wss://) and require port 443. BluFis also require access to NTP servers on port 123;

REQUIRED PORTS

- 123 (NTP) - 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org, 3.pool.ntp.org
- 443 (wss/https) - bluzone.io (dynamic IP address)

Enterprise WiFi Requirements

There are several ways to configure an enterprise WiFi. In most cases, one would expect to have a certificate of the access point, a username and a password. The certificate must be in .PEM or .DER format.

If the certificate does not include a root CA (which is very common), then the user should unselect the checkbox for “Verify Certificate” in the Bluzone BluFi Template configuration screen. This lets the BluFi use the certificate without trying to validate the root certificate.

The most commonly used enterprise security type in Bluzone is **EAP_PEAP0_MSCHAPv2**

SUPPORTED SECURITY TYPES

- EAP_PEAP0_MSCHAPv2
- EAP_PEAP0_PSK
- EAP_PEAP0_TLS
- EAP_PEAP1_MSCHAPv2
- EAP_PEAP1_PSK
- EAP_PEAP1_TLS
- EAP_TLS
- EAP_TTLS_MSCHAPv2
- EAP_TTLS_PSK
- EAP_TTLS_TLS

Testing

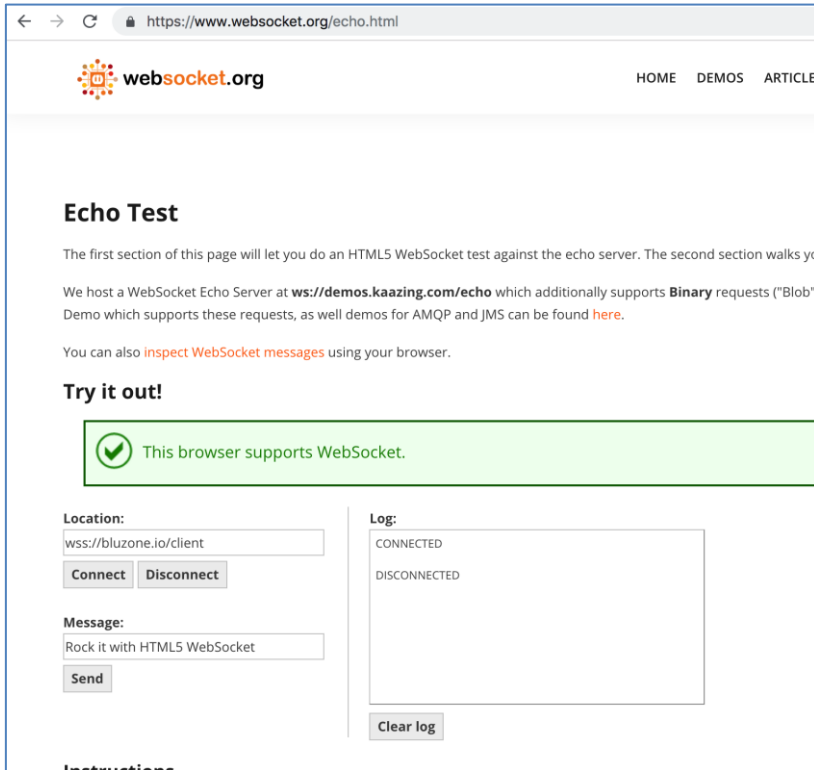
The goal is to get a BluFi connected to the customer’s WiFi network using with an enterprise security. It may be helpful to first get a laptop computer connected using the credentials provided by the customer.

Once connected to the Internet, it may be helpful to verify that the enterprise network allows outbound traffic to Bluzone via a websocket. There is a helpful online tool that can be used to perform this test.

<https://www.websocket.org/echo.html>

Open the above URL in a browser and enter: `wss://bluzone.io/client` into the “Location” field and click “Connect”. If you see “CONNECTED” show up in the “Log” window, then you can be reasonably sure that a BluFi will be able to connect to Bluzone.

NOTE: One still needs to determine if port 123 is open for NTP.



The screenshot shows a web browser window at `https://www.websocket.org/echo.html`. The page title is "Echo Test" and it features a navigation menu with "HOME", "DEMOS", and "ARTICLES". The main content area includes an "Echo Test" section with introductory text and a "Try it out!" section. A green notification box with a checkmark icon states "This browser supports WebSocket." Below this, the "Location:" field contains `wss://bluzone.io/client` and the "Message:" field contains `Rock it with HTML5 WebSocket`. The "Log:" window displays the status `CONNECTED`. Buttons for "Connect", "Disconnect", "Send", and "Clear log" are visible.

Network Considerations

BluVision devices are deployed within enterprise grade wireless infrastructures with strict network compliance guidelines. Therefore, these devices may be presented with the following obstacles to connectivity and successful provisioning:

- **Wi-Fi Spectrum Compatibility** – BluFi Requires 2.4 GHz and IS NOT compatible with 5 GHz
- **MAC ADDRESS White Listing** – Wireless network may require BluFi's Wi-Fi Mac Address be explicitly added to approved devices table.
- **Firewall** – BluFi's require open internet access to bluzone.io via port 443 to successfully connect and provision device.
- **HTTP Proxy** – A HTTP proxy may be to route/monitor all outbound internet traffic. Customer networking team will need to whitelist BluFi devices to BYPASS proxy provided direct access to bluzone.io:443
- **Certificate Authentication** – Customer is attempting to use an improperly formatted and-or signed certificate. Compatible formats are .pem and .der
- **No DHCP** - BluFi Gateway will fail to provision when host network requires static IP address and DHCP services are not enabled. Resolution, setup segmented VLAN with DHCP.
- **Slow DHCP** – BluFi Gateway may fail to provision using a mobile device when host network has slow issuance of IP addresses via DHCP. If time to acquire IP address lease exceeds 30-60 seconds, mobile application will exceed timeout and return failure response. However, BluFi may succeed if left plugged in and successfully gets assigned IP address.
- **Slow or Unstable Wi-Fi Network** – BluFi may have connectivity issues on overloaded or poor signal Wi-Fi infrastructures. BluFi gateways require a **minimum** of 2 Mbps “sustained” upload speed to successfully transmit beacon telemetry.
- **BluFi Excessive Reconnects** – BluFi gateway installed in location that is too far from Wi-Fi access point, within area that contains a RF barrier (Metal), and-or within a Wi-Fi zone with too many overlapping access points.
- **Network throttling** – BluFi Gateway has been installed on cellular based internet access point with assigned upload speed and-or connection limits. Customer may have issues when data plans exceeds subscription levels.
- **Captive Portal** – Host network requires the use of web page based acceptance of terms and conditions to approve access to internet. (Used in Hotels). BluFi gates are NOT compatible with captive portals.

Prior to arrival on site for installation and configuration network connectivity should be done with test BluFi to verify portal access. This step must also be completed prior to pre-provisioning at the factory.

Technical Services Overview

Bluvision Devices with Bluzone Configuration and Settings

- Bluvision intent is to delivered all Devices both Beacons and BluFi pre-provisioned and ready for deployment.
- Professional Services will be onsite to oversee installation and training.
- Pre-configuration of the Bluzone account to meet customer requirements.
- Onsite meetings with end-users to adjust final configuration settings and testing.

Bluzone – Key settings

- Best BluFi is/isn't considered the core setting for this installation?
- Geofences will be placed to Encompass key Parking areas as defined in the layouts.
- Geofences will also be placed around Key transit areas as stated in the layouts.
- Establish Geofenced areas in Bluzone.
- Onsite and remote review and adjustment of settings by Bluvision Staff.

Meetings, Reviews

Bluvision will conduct meetings to review the project scope, objectives, milestones, and deliverables.

- Change Order Process established as soon as possible after the project start date.
- Regularly scheduled daily Deployment Meetings.
- Regularly scheduled weekly status conference call.
- Parties will establish a standard Review and Sign Off process.
- Set dates for final testing, Project Sign on and Closure of Project.

To submit pre-provisioning data for BluFis and beacons download [this form](#), fill it out and submit it to sales@bluvision.com