



User Manual



This product complies with FCC radiation exposure limits set forth for an uncontrolled environment

Pursuant to FCC 15.21 of the FCC rules, changes not expressly approved by btwTAG Safety, LLC, might cause harmful interference and void the FCC authorization to operate this product.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any, interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an output on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.



Contents

Description	5
Getting Started	6
Signing in	6
Menu	7
Dashboard	7
Today Balance	9
Active Tags	9
Contacts Metrics	10
Real Time Areas	10
Real Time Gates	11
Last Activities	12
Latest Contact Events	12
Contact Events	12
Contact Tracing	14
People	15
Man-Tags	15
Device Configuration	16
Massive Configuration	19
Creating a Group	21
Employees	23
Environment	26
Areas	26
Gates	29
btwTAG Configuration	32
Single btwTAGs	32
Multiple btwTAGs	40
Programmer Mode	41
Live Configuration	41



Contact	43
Appendix I: APIs For OEM Platforms	44
Defining the Structure	44
STEP 1: Turn On and First Configuration.....	44
STEP 2: How to Handle Server-Side Calls	44
Tokens.....	46
Configuration Parameters.....	46
Changing Post-Registration Parameters	48
Sending the Contact Tracing	48
Answering the Call/Data	49
Appendix II: Device Specifications.....	51

Description

- The btwTAG (back-to-work tag) is a Confidential Workplace Contact Tracer and Social Distancing Reminder application.
- The device is equipped with a low power, high sensitivity transceiver that can detect messages from other sensors of the same type and estimate the distance between the sensors themselves with up to 20 cm (8 in.) of location accuracy. These "pings" are carried out in two ways: a BLE Bluetooth signal, and a 915 MHz frequency signal.
- During the application each sensor stores in memory a contact history with all other btwTAGs. btwTAGs send the stored data via Wi-Fi connection to a server at a preset time and/or when a Wi-Fi network is available. The data is displayed and managed in a Dashboard that serves also a configuration tool for the tags. No personal data resides in the system.
- The device independently alerts the user with light signal, acoustic warning and vibration when social distancing is not satisfied. The event is stored and ultimately uploaded to the Dashboard via Wi-Fi.
- The device is powered by a lithium battery, which is rechargeable through a micro USB connector. Battery life is determined by the frequency of data uploads.





Getting Started

Welcome “back to work”!

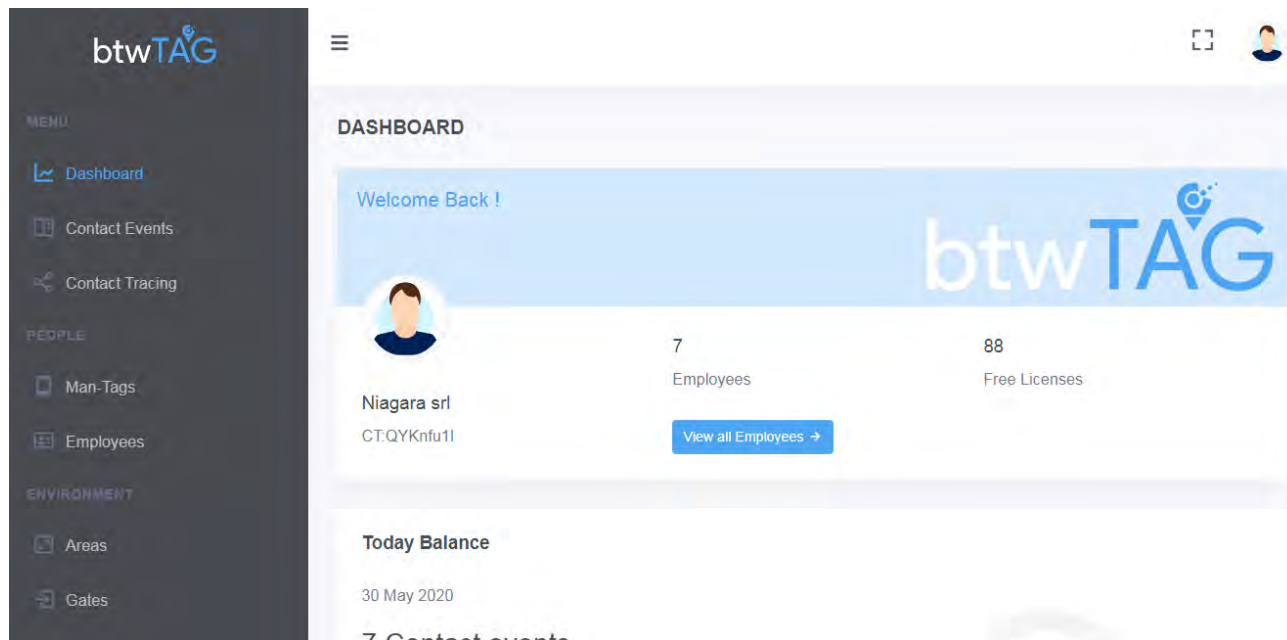
Signing in

A screenshot of the btwTAG login interface. At the top, it says "Welcome Back !" and "Sign in to continue to btwTag Dashboard." with the btwTAG logo. Below this are two input fields: "Email" and "Password". There is a checkbox labeled "Remember me" and a blue "Log In" button. At the bottom of the form, there is a link "Forgot your password?". Below the form, there is a link "Don't have an account ? Signup now".

Point your browser to www.btwTAG.com and click on the Sign In icon. A Dialog box will appear. Enter your email and password confirmed during the registration process.

Menu

Dashboard



The btwTAG Dashboard is designed to provide the end user with easy access to data and the tools with which to manage both the data and the devices themselves.

At the top of the dashboard there are:

- The Company Token
- Number of employees in system
- Free licenses (licenses yet to be paired with employees; the number will go down to zero)

The left sidebar shows the links to the contact data and devices. These will be discussed below. There is also a button to collapse the sidebar.

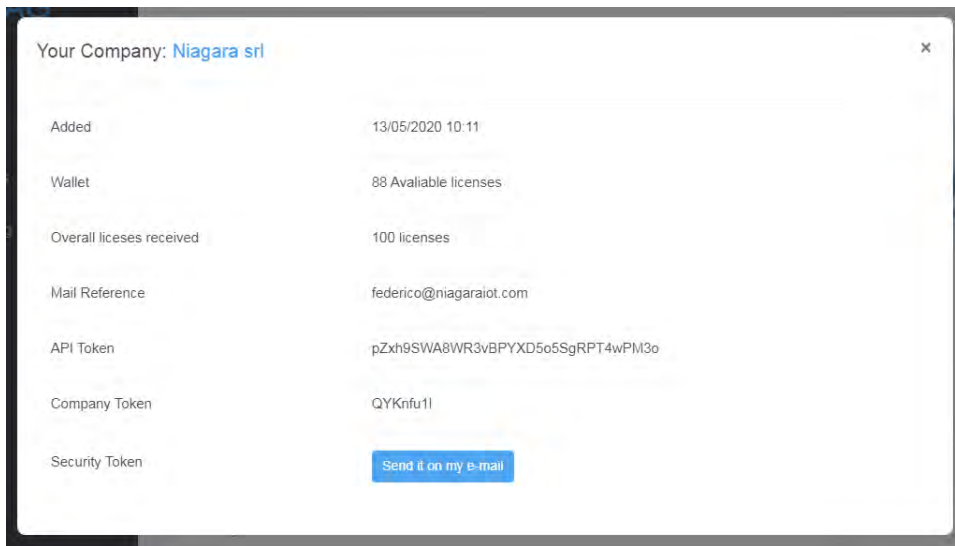
On the right side of the page is the image link to the company profile.

The company profile shows the following:

- when the company started using the system
- the number of available licenses
- the number of licenses received
- the principal email address for the account (to be used in the validation process)

The profile also contains important information for access to your system using tokens. This includes:

- **Company Token:** The Company Token is used to configure a btwTAG
- **API Token:** The API Token is used to access the Middleware References
- **Security Token:** The Security Token is used to access the personal data on a separate secure server



How to get your company token:

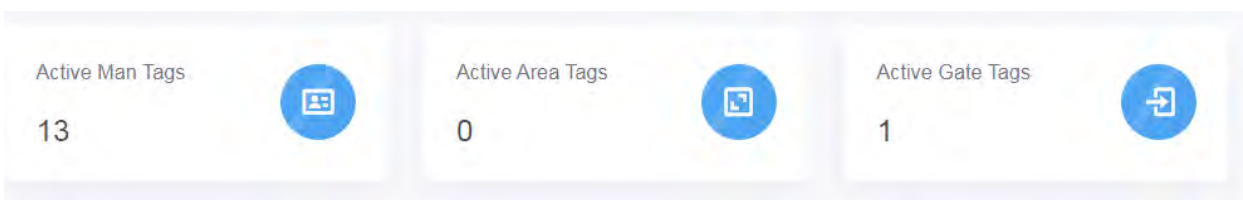
Today Balance

The first data display is Today Balance. It indicates the tally of contact events for the day and a six-day average. The display also shows how many active tags were generating the data.



Active Tags

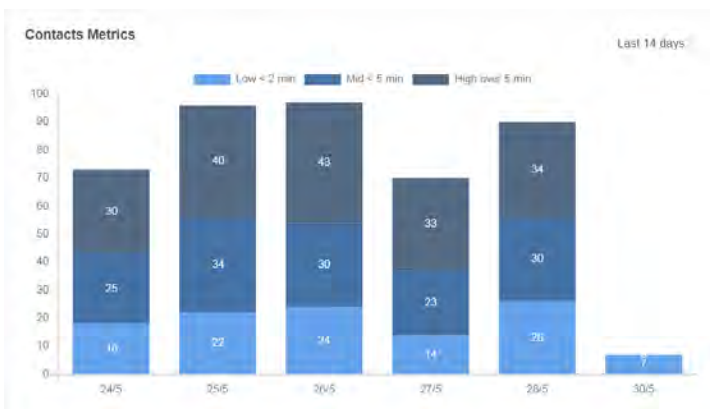
There are two types of active tags. First, all tags that are paired with an employee. Second, all tags that are not paired but act as beacons. Man Tags are all paired tags, and Area and Gate tags are all beacons. All active tags appear on the dashboard as below.



Contacts Metrics

The Contacts Metrics contain the last 14 days of data and is segmented by three time durations: less than 2 minutes; more than 2, but less than 5; more than 5.

Contact Metrics is a critical indicator: longer the contact, less healthy the situation. The goal is to keep contact events from happening, but when they happen, they become more serious with longer the time duration.



Need screen shot for last 14 days

Real Time Areas

Real Time Areas. All Active Area tags will be displayed here. Specific areas can be set to allow only a maximum of tags present at one moment. For example, a coffee room is set to maximum 20 tags. If that number is exceeded, a red bar is lit for that area. Under that number the bar will be green. When the number is being set, it will be yellow. A mail module is available to deliver real-time alerts for red lit areas.

Real Time Areas



0

Total Areas

[View More →](#)



Real Time Gates

Real Time Gates. All Active Gate tags will be displayed here. Like Area tags, the color of the number will change depending on the thresholds set by the Admin.

Real Time Gates



0

All Gates

[View More →](#)

Last Activities

An administrative aid to track recent admin activities such as the issuing of licenses.

Last Activities

13/05/2020 10:16 → 100 Licenses received

Latest Contact Events

The Latest Contact Events is a limited functioning spreadsheet that allows a ranking by the five fields: Origin, Target, Target Type, Duration, When. Click at the top of the column to activate the ranking.

Latest Contact Events

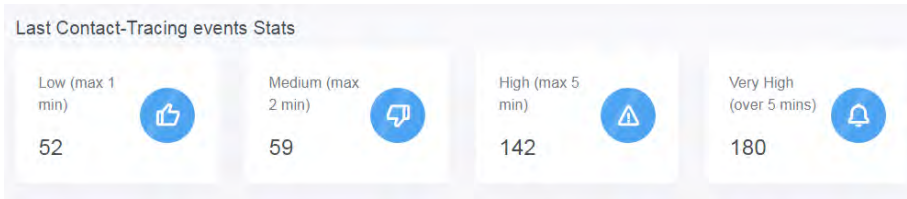
Origin	Target	Target Type	Duration	When
device01	device03	ManTag	High	24/05/2020 04:50
device01	device03	ManTag	Very High	24/05/2020 04:50
device01	device07	ManTag	Low	24/05/2020 04:50
device01	device07	ManTag	High	24/05/2020 04:50
device01	device05	ManTag	High	24/05/2020 04:50

TIP: Click at the top of the column to activate the ranking.

Each event has an Origin tag and a Target tag and type. Most important is the Duration of the contact which indicates the risk factor. Based on the same 14 day data as the contact metrics shot. The data time frame is customized for the user.

Contact Events

Clicking on the Content Events link on the left sidebar brings you to all contact events. At the top of the page are the Last Contact-Tracing events Stats.



Below that is the display for All Contact Events. These are the content event data:

- The device ID number
- The IDs of the devices that were within 6 feet of the tag
- The tag type
- The duration of the encounter
- The time of the encounter

In addition to the ranking function at the top of the columns, there is a search field.

All Contact Events

Search by Origin

Origin	Target	Target Type	Duration	Timestamp
ID- 00124B00204E171C	ID- 00124B00204E1789	Main Tag	Low	1590854524000
ID- 00124B00204E1769	ID- 00124B00204E171C	Main Tag	Medium	1590854318000
ID- 00124B00204E171C	ID- 00124B00204E1769	Main Tag	Medium	1590854315000
ID- 00124B00204E1769	ID- 00124B00204E1F17	Main Tag	Low	1590854290000

Contact Tracing

Clicking on the Contact Tracing link on the left sidebar brings you to the page where the end user can have access to names and surnames associated with the tags.

Type an Hardware Id OR an Employee Alias. To see names and surnames type also the Security Token

Device Hw-Id	Employee Alias	Security Token (Optional)
Hardware Id	Employee Alias	Security Token

Search

Center Zoom To Fit


With just the device hardware ID, the end user can view up to three levels of contact at the same time.

Type an Hardware Id OR an Employee Alias. To see names and surnames type also the Security Token

Device Hw-Id	Employee Alias	Security Token (Optional)
ID-00124B00204E1769	Employee Alias	Security Token

Search

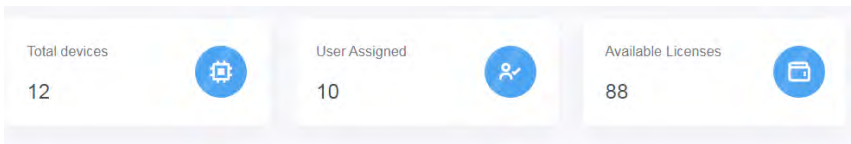
Center Zoom To Fit



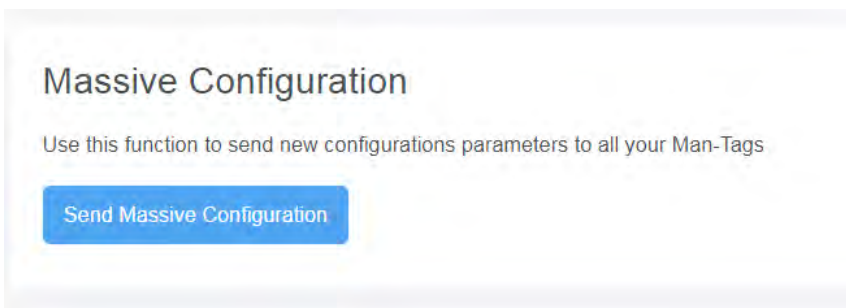
People

Man-Tags

Clicking on the Man-Tags link on the left sidebar brings you to the page where All Man Tags are displayed. This is also where the configuration of the Man-Tags for each employee occurs. The top of the page displays the total number of devices, those that are user assigned, and available licenses.



Below that is the link to open the dialog box for Massive Configuration. SEE: [Device Configuration](#) below for more information.



All Man Tags are displayed in a searchable database with column ranking. The data displayed includes:

- Hardware ID
- User State
- Group
- Battery Level (e.g.: 5 days life with once-a-day data upload)
- Updated At

All Man Tags

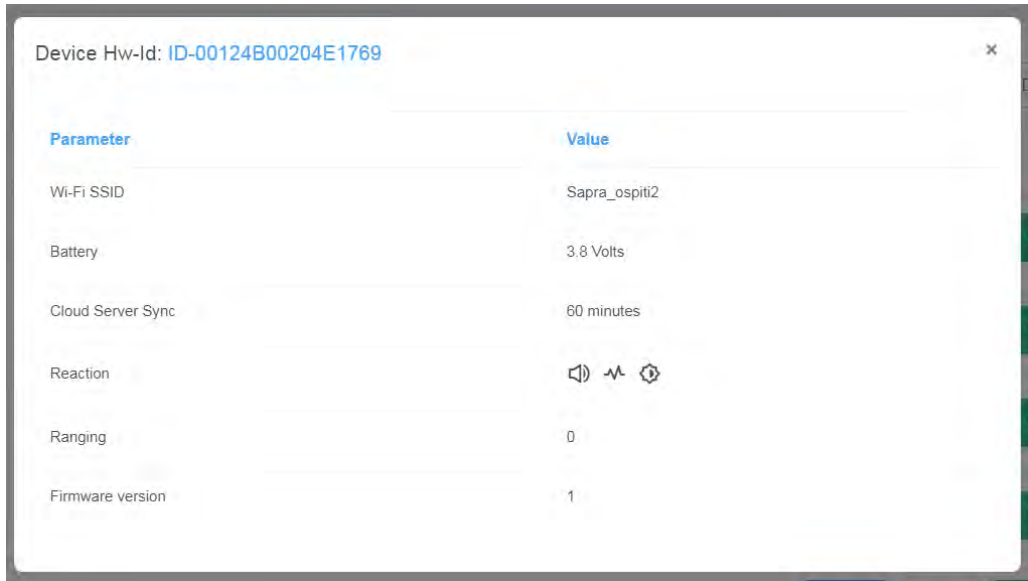
Hardware Id	User State	Group	Battery	Updated At
ID-00124B00204E1769	Unassigned	0	90%	02/06/2020 09:25

Device Configuration

The All Man Tags table also has the details for each hardware device which can be found by clicking on the Details button shown below.

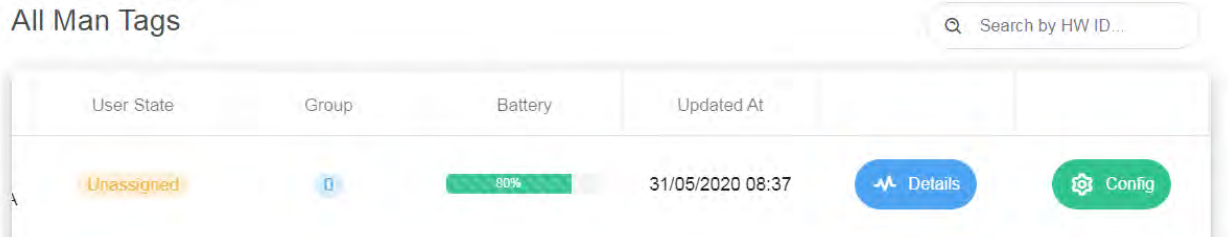
User State	Group	Battery	Updated At	
Unassigned	0	80%	31/05/2020 09:24	Details

This opens the device's hardware information.



The All Man Tags also has the link to open a dialog box for device configuration shown below.

All Man Tags



The Config Dialog allows configuration resets of the device parameters:

- Wi-Fi network (network ID and password)
- Cloud Synch Time (10-720 minutes – can be modified)
- Ranging Type (medium = 1 meter/high = 1.80 meter)
- Tag Reaction (audible, visible, vibrate: click each symbol to turn on/off tag reaction)
- Tag Type (Man-Tag, Area, Gate, Programmer)
- Turn On-Off

Parameter	Actual Value	Next Connection Changes	Set Config
Wi-Fi Network	None	None	<input type="text"/> <input type="button" value="Reset"/>
Wi-Fi Password	None	None	<input type="text"/> <input type="button" value="Reset"/>
Cloud Sync Time (minutes)	10	290	720 <input type="button" value="RESET"/>
Accuracy	High	None	<input type="button" value="Medium"/> <input type="button" value="High"/> <input type="button" value="RESET"/>
Reaction	<input type="button" value="On"/> <input type="button" value="Off"/>	<input type="button" value="On"/> <input type="button" value="Off"/>	<input type="button" value="On"/> <input type="button" value="Off"/> <input type="button" value="RESET"/>
Tag Type	None	None	<input type="button" value="None"/> <input type="button" value="None"/> <input type="button" value="None"/> <input type="button" value="None"/> <input type="button" value="RESET"/>
Turn On - Off	Off	None	<input type="button" value="On"/> <input type="button" value="RESET"/>

Note: The device will automatically perform an upload when the maximum 70 contact event limit is reached.

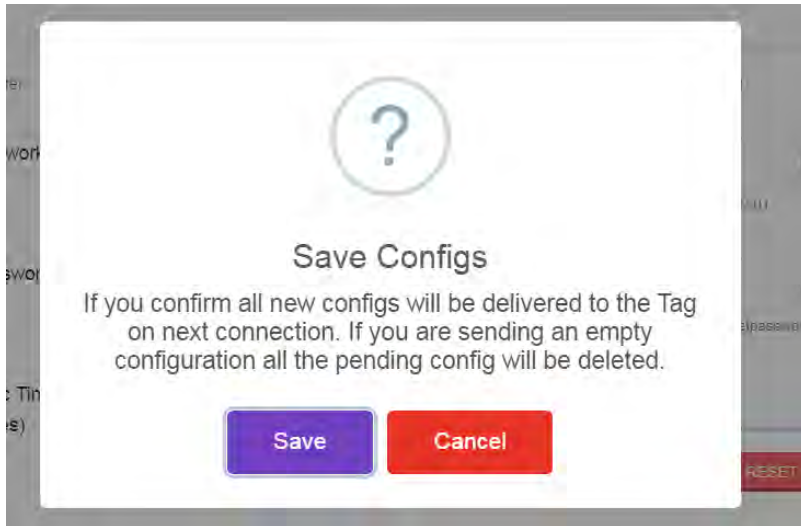
There are four columns: Parameters, Actual Value, Next Connection Changes, Set Config.

- Parameters: Six parameters and an off/reset option.
- The Actual Value is the current live setting of the device.
- The Next Connection Change is the new value to be loaded onto the device at the next tag synch (change upload when the tag synchs up with the cloud). Tag synchs can be scheduled on a regular basis. The NCC is yellow until the new changes are sent to the tag, wherein it will turn green. Red will indicate sent but off.
- Set Config: Change value and select reset.

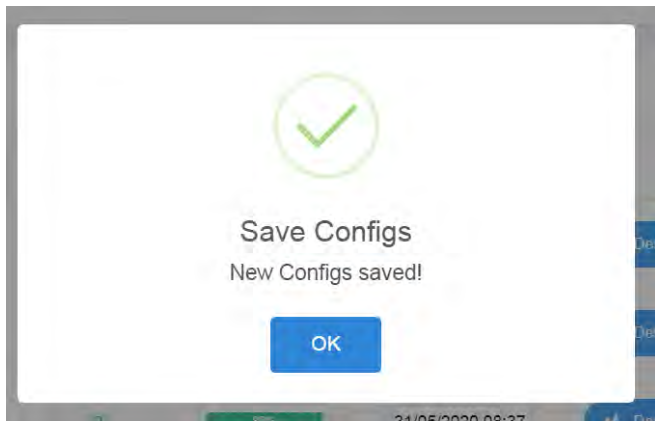
All changes need to be Saved to take effect as shown below.

Parameter	Actual Value	Next Connection Changes	Set Config
Wi-Fi Network	None	None	<input type="text"/> <input type="button" value="Reset"/>
Wi-Fi Password	None	None	<input type="text"/> <input type="button" value="Reset"/>
Cloud Sync Time (minutes)	10	290	720 <input type="button" value="RESET"/>
Accuracy	High	None	<input type="button" value="Medium"/> <input type="button" value="High"/> <input type="button" value="RESET"/>
Reaction	<input type="button" value="On"/> <input type="button" value="Off"/>	<input type="button" value="On"/> <input type="button" value="Off"/>	<input type="button" value="On"/> <input type="button" value="Off"/> <input type="button" value="RESET"/>
Tag Type	None	None	<input type="button" value="None"/> <input type="button" value="None"/> <input type="button" value="None"/> <input type="button" value="None"/> <input type="button" value="RESET"/>
Turn On - Off	Off	None	<input type="button" value="On"/> <input type="button" value="RESET"/>

When you press Save you will be presented with a confirmation step.



This is followed with the confirmation.



The configuration will change at the next Wi-Fi update, or the user can lay the tag on a flat surface in a horizontal position and the tag will enter the sleep mode. When the tag is picked up, it will connect with the Wi-Fi and assume the new configuration.

Massive Configuration

There is also a Massive Configuration dialog box accessible from the Man-Tags page mentioned above. Click on the link to send a massive configuration.

Massive Configuration

Use this function to send new configurations parameters to all your Man-Tags

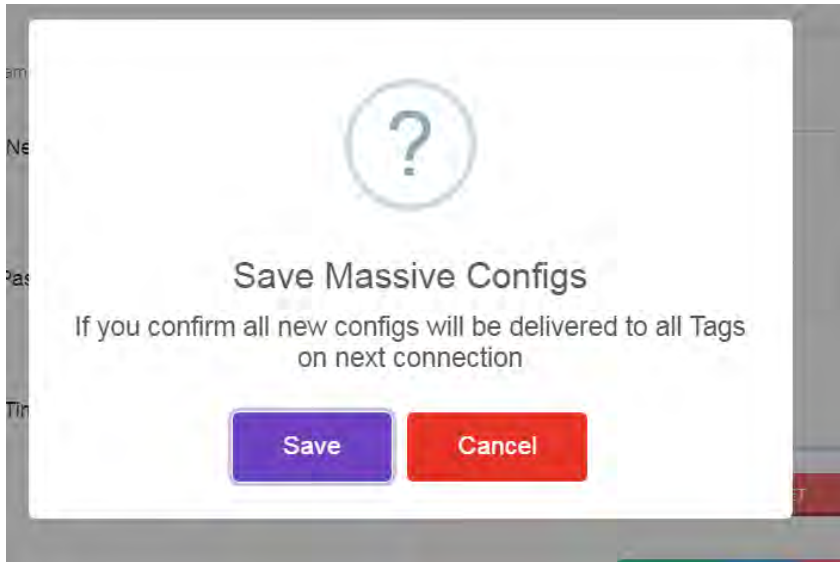
Send Massive Configuration

The link opens a configuration dialog box that is essentially identical to the configuration dialog described above for single tags. The difference is that the changes potentially apply to all devices.

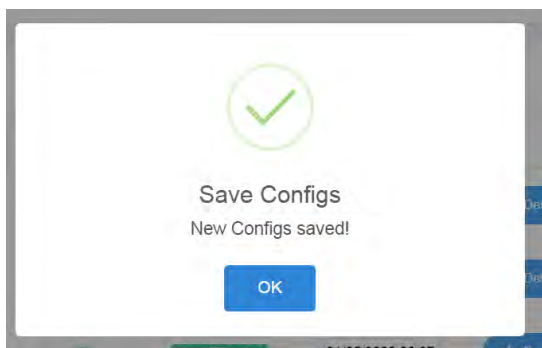
Massive Configuration Close Save

Parameter	Next Connection Changes	Set Config
Wi-Fi Network	Reset	<input type="text"/> Reset ex: Work-AP-01
Wi-Fi Password	Reset	<input type="text"/> Reset ex: mysecretpassword
Cloud Sync Time (minutes)	Reset	60 480 <input type="range"/> RESET

Click Save after the changes for the confirmation step.



This is followed with the confirmation.



The configuration will change at the next Wi-Fi update, or the user can lay the tag on a flat surface in a horizontal position and the tag will enter the sleep mode. When the tag is picked up, it will connect with the Wi-Fi and assume the new configuration.

Creating a Group

Select this first tag to be part of a group and click on Config.



This will open the Config dialog box. Scroll down to the tag type and click on Prog.

Tag Type

Man-Tag

None

Man

Area

Gate

Prog

The tag will turn into a programmer. Configure the device according to the requirement. Then the programmer card will be able to broadcast the new configuration to the other tags. The tags themselves will be reconfigured either when the tag uploads to the Wi-Fi, or when the tag is laid flat and allowed to reset (about 5 seconds) through sleep mode.

SEE: [btwTAG Configuration](#) below for the physical configuration to make clones of the devices.

The default Group value is zero. If two tags are close to each other and are both zero, they will collide and have a contact event. If two tags have the same group number that is not zero, they will not collide and have a contact event.

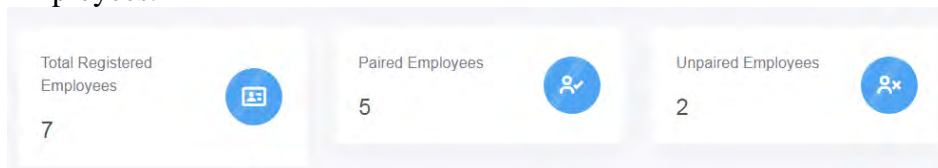
For example, if you have a museum and you assume that your visitors will be in groups of four people, then the first four tags are Group 1, and so on. (The maximum is 455 groups.) The Group 1 tags will not collide with each other but will collide with any other tag of another group other than Group 1.

All Man Tags				
Search by HW ID...				
Hardware Id	User State	Group	Battery	Updated At
ID-00124B00204E1769	Unassigned	0	80%	01/06/2020 13:24

Employees

Clicking on the Employees link on the left sidebar brings you to the page where employees can be added to the system and where all employees in the system are listed in a searchable data display.

The top of the page features current data for Total Registered Employees, Paired Employees, Unpaired Employees.



Below that is the dialog box to Add Employee to the system. Note that there is also the option to include the employee in a Team, which has certain advantages for managing departments within the company. It allows the sorting by Team when searching on the All Employees page.

The 'Add Employee' dialog box contains the following fields and buttons: 'First name' (text input), 'Last name' (text input), 'Alias' (text input), 'Team' (text input), and 'Team (optional)' (text input). There are two buttons at the top right: 'Upload CSV' and 'CSV Example'. An 'ADD' button is located at the bottom right.

There is a function to upload a CSV file with multiple employees at the same time with the Upload CSV button shown. It will open a search window to help you find your file.

A partial view of the 'Add Employee' dialog box showing the 'First name' and 'Last name' text input fields. The 'Upload CSV' and 'CSV Example' buttons are also visible at the top right.





A CSV example can be downloaded from the page.

Another partial view of the 'Add Employee' dialog box, showing the 'First name' and 'Last name' text input fields and the 'Upload CSV' and 'CSV Example' buttons at the top right.





This is how the CSV file is formatted:

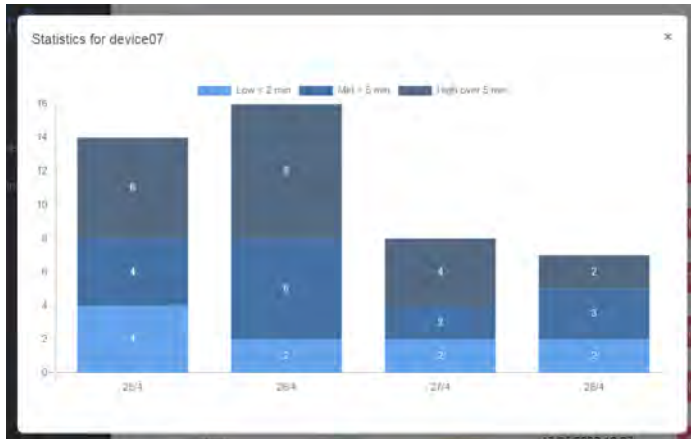
A1			
	A	B	C
1	alias;name;surname;team;;;		
2	User01;Name1;Surname1;;;		
3	User02;Name2;Surname2;;;		
4	User03;Name3;Surname3;;;		
5	User04;Name4;Surname4;;;		
6	User05;Name5;Surname5;;;		
7	User06;Name6;Surname6;;;		
8			

Scroll down the page and there is a data display for All Employees.

All Employees				
<input type="text" value="Search by Alias..."/>				
Employee Alias	Pairing State	Team	Updated At	
Griff	device07	No Team	13/05/2020 14:12	 
AB0001	device03	No Team	13/05/2020 14:13	 

Click of the Stats icon to see the contact statistics for the device:

All Employees				
<input type="text" value="Search by Alias..."/>				
Employee Alias	Pairing State	Team	Updated At	
Griff	device07	No Team	13/05/2020 14:12	 
AB0001	device03	No Team	13/05/2020 14:13	 

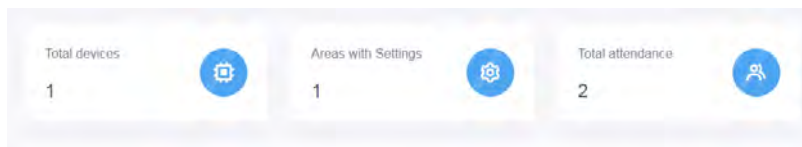


There will also be an unpairing function (TBA) that will allow the end-user to “unpair” the device from the employee or between visitors.

Environment

Areas

Areas can be tracked with a fixed device configured as an Area Tag. The dashboard shows total area tags, those tags with settings, and total attendance in the area. All Area Tags on the dashboard is the searchable database for Area Tags. Each Area Tag has a 6 to 8-meter radius. To configure, you go to the Man Tag page in the dashboard to configure the tag for Areas and Gates. All tags arrive on the system as Man Tag.



NOTE: There is no alarm when a Man Tag connects with an Area or Gate Tag.

Massive Configuration

Use this function to send new configurations parameters to all your Area-Tags

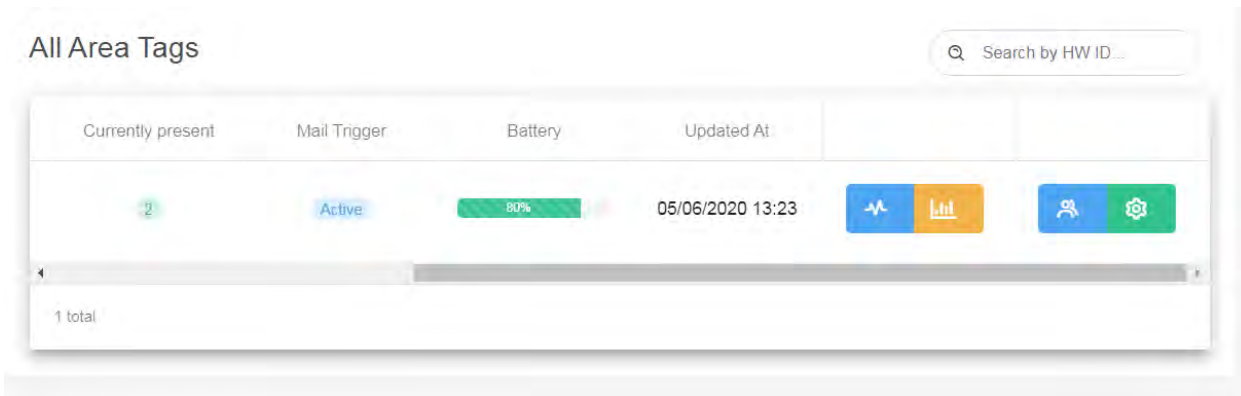
[Send Massive Configuration](#)


All Area Tags

Search by HW ID...

Hardware Id	Area Name	Area limit	Currently present	Mail Trigger
ID-00124B00204E1898	Dining Room	2	2	Active

1 total



Click on the  icon. This will open the Area Settings dialog box.

Area Settings ×

Whit this function you can set ID-00124B00204E1898 area parameters.

Area Name

Area name is available

Dining Room

Area Limit

0 2 16

Email Trigger

☒

a.griffiths@veracitygmbh.com

Close Save Settings

Use this dialog box to set area parameters for an Area Tag. The area limit can be set for the presence of Man Tags to a maximum of 16 per Area Tag. An email alarm trigger is also available for when the limits are exceeded.

The configuration will change at the next Wi-Fi update, or the user can lay the tag on a flat surface in a horizontal position and the tag will enter the sleep mode. When the tag is picked up, it will connect with the Wi-Fi and assume the new configuration.



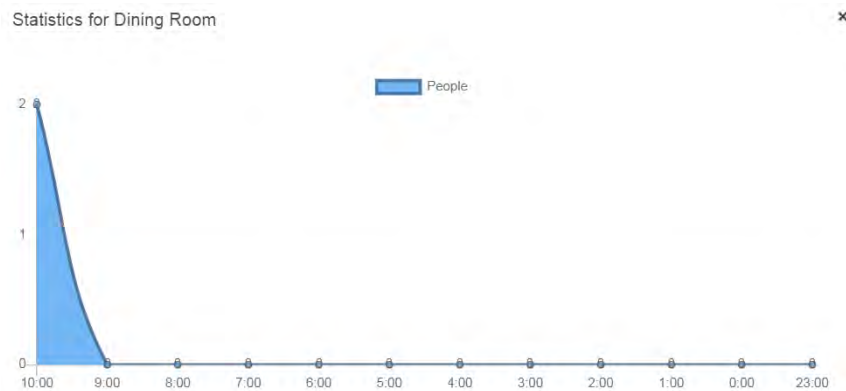
Click on this icon to open the device hardware ID.

Device Hw-Id: ID-00124B00204E1898

Parameter	Value
Wi-Fi SSID	Hiba
Battery	3.8 Volts
Cloud Server Sync	1 minutes
Accuracy	0
Firmware version	1




Click on this icon to view statistics for the area covered by this tag.



Scroll down to view the tags present in the area in real time.

Real Time Man-Tags in Dining Room area

Hardware ID	Wtag	Tag Type
ID-00124B00204E1AFA	Unconnected	Man-Tag
ID-00124B00204E1C78		Man-Tag

Click on this icon  to view the device configuration dialog box.

Device ID-00124B00204E1898 Configuration

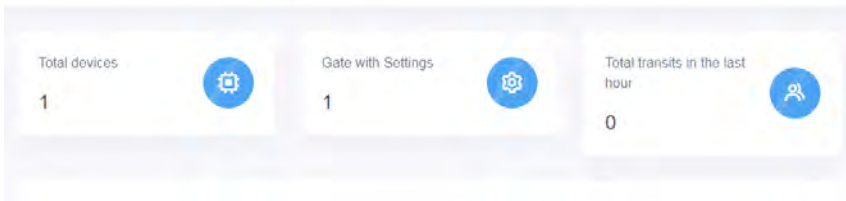
Close Save

Parameter	Actual Value	Next Connection Changes	Set Config
Wi-Fi Network	High	None	<input type="text"/> Reset <small>ss: Work-AP-01</small>
Wi-Fi Password		None	<input type="text"/> Reset <small>ss: mysecretpassword</small>
Cloud Sync Time (minutes)	5	None	60 — 240 <input type="range"/> RESET
Accuracy	High	None	Medium High RESE
Tag Type	Area-Tag	None	Man Area Gate Prog

Gates

Passages and egress/ingress areas can be tracked with a fixed device configured as a Gate Tag. The dashboard shows total gate tags, those tags with settings, and total attendance in the area. All Area Tags on the dashboard is the searchable database for Area Tags. Each Area Tag has a 6 to 8-meter radius. To configure, you go to the Man Tag page in the dashboard to configure the tag for Areas and Gates. All tags arrive on the system as Man Tag.

The dashboard displays total devices, Gates with Settings, and Total transits in the last hour.



There is the Massive Configuration send button.

Massive Configuration

Use this function to send new configurations parameters to all your Gate-Tags.

[Send Massive Configuration](#)





All Gates Tags is the searchable database for gate tags.

All Gate Tags

Hardware Id	Gate Name	Last hour	Battery	Updated At
ID-00124B00204E21EB	Dining Room	0	100%	06/06/2020 16:54

1 total

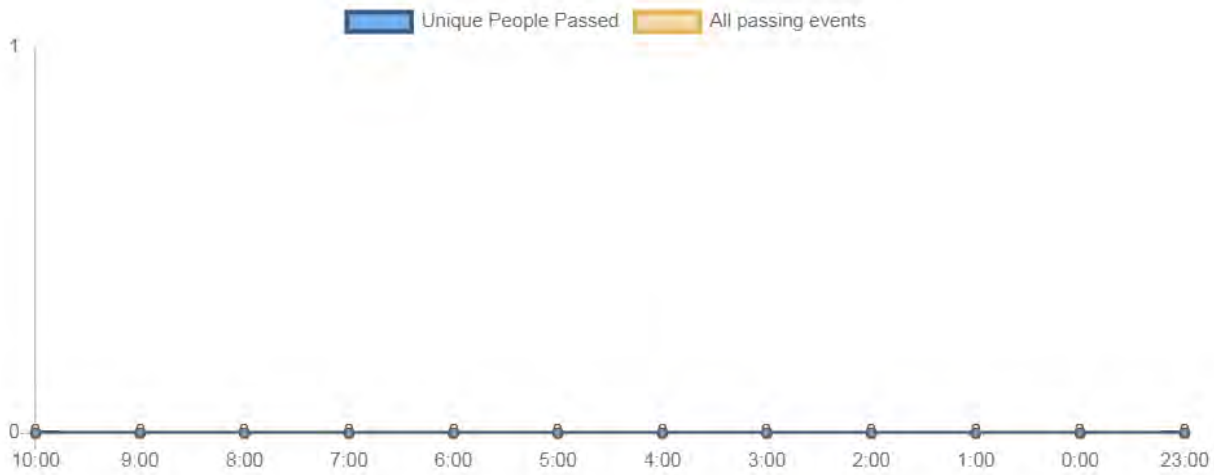
All Gate Tags


Last hour	Battery	Updated At	
0	100%	06/06/2020 16:54	   

1 total

Click on this icon  to view statistics.

Statistics for Dining Room



Click on this icon  to view or change Gate Settings.

Gate Settings

Whit this function you can set ID-00124B00204E21EB gate parameters.

Gate Name

Gate name is available.

Dining Room

Close

Save Settings



btwTAG Configuration

Single btwTAGs

General properties and features of the tags:

Specs here?

3 color LED light

Green rapid flashing: battery charging

Green constant: battery fully charged

Green flashing every 10 seconds when worn: device in operation

Red rapid flashing: Alarm and contact

Blue rapid flashing: Searching for network; configuration change

When device is laid flat, after 10 seconds, the device will go into sleep mode. One blue flash/one short beep indicates sleep mode.

When device is picked up, there is a single flash of blue, then green flash every 10 seconds (normal operation)

Tag during contact event: There are 3 alarms audible LED vibrate. Alarm can be customized.

Audible: three beeps then stop. 10 second later another 3 beeps if still in target area. Every 10 second until the tag is out of contact.

Vibration: same

Light: Continuous red

Max 70 contact events

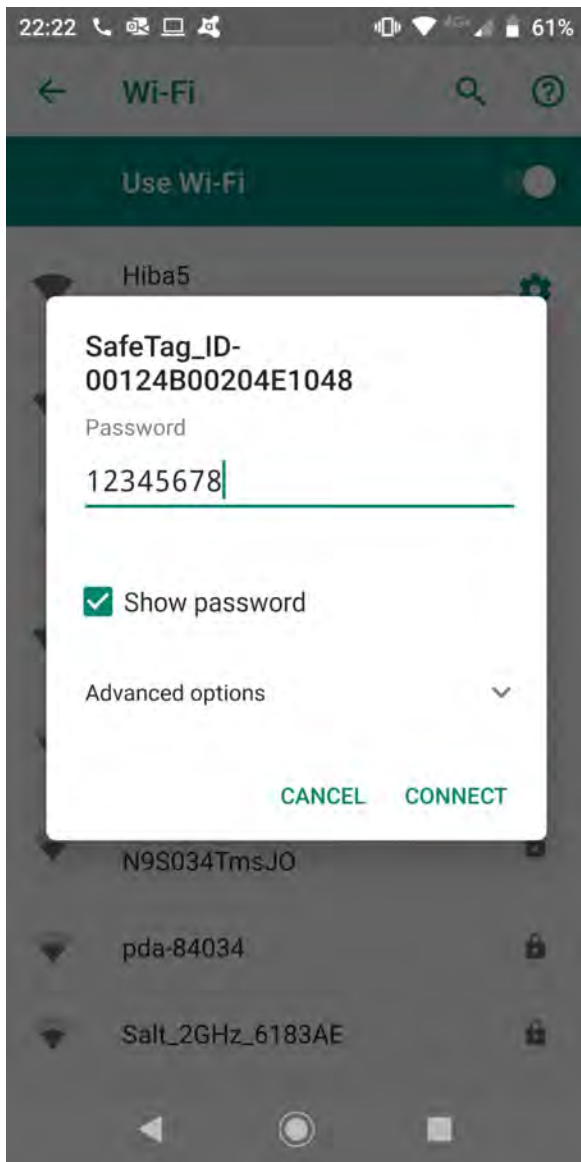
Uploads: 3-20 second after with Wi-Fi connected depending on signal strength.

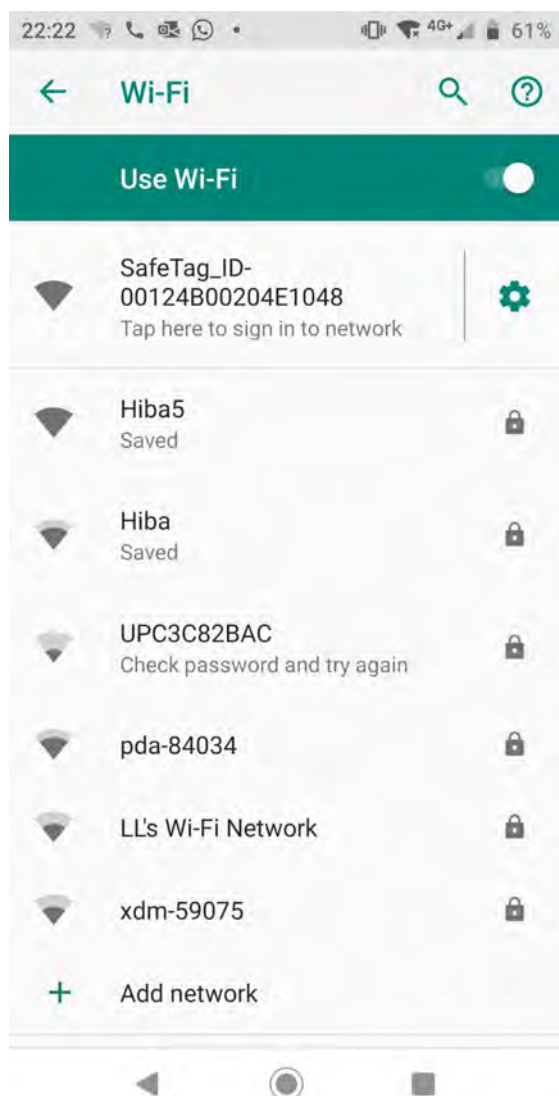


Here are the steps to configuring a single btwTAG:




- Connect the btwTAG to the power supply
- Open a PC with Wi-Fi and connect to the btwTAGXXXX network
- Open a browser and point to 192.168.0.1/config
- Enter the name of the Wi-Fi network that the btwTAG will use to send data to the server
- Enter your network password
- Enter the Company Token


















22:24


4G+

60%


Sign in to SafeTag_ID-00124B0...


192.168.0.1

btwTAG

Hiba	 78%
xdm-59075	 48%
LL's Wi-Fi Network	 48%
Salt_2GHz_6183AE	 32%
pda-84034	 30%
DIRECT-CYDESKTOP-N9S034TmsJO	
UPC Wi-Free	 26%  28%
UPC3C82BAC	 24%

save



22:26 4G+ 59%

Sign in to SafeTag_ID-00124B0...
192.168.0.1

SAPRA
electronica

btwTAG

Hiba	78%
LL's Wi-Fi Network	52%
xdm-59075	44%
Salt_2GHz_6183AE	30%
pda-84034	28%
DIRECT-CYDESKTOP-N9S034TmsJO	28%
UPC Wi-Free	12%

Password123!

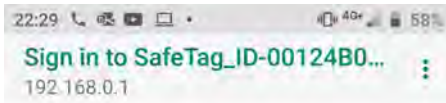
password

DRXK4gfl

<https://us-central1-btwtag.cloudfunctions.net>

save

[Scan](#)



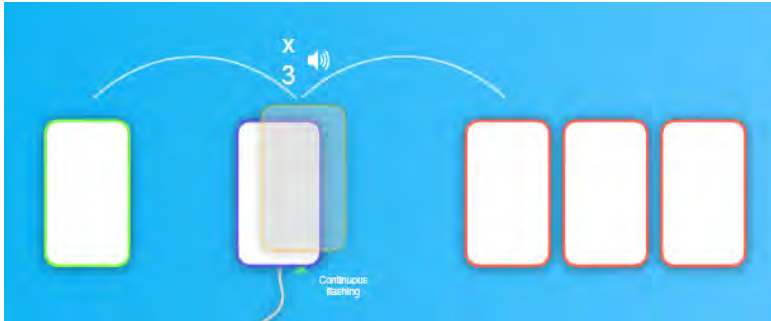
Credentials Saved
Trying to connect Weredad to network.
If it fails reconnect to AP to try again



Multiple btwTAGs

Here are the steps to configuring multiple btwTAGs:

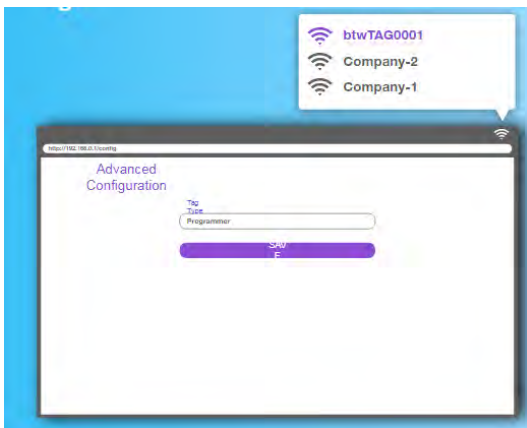
- Set up a btwTAG only as per previous instructions
- Reopen the configuration web page and go down to the "Advanced Configuration" section
- Select the "Tag Type" drop-down and select "Programmer" and press "Save".
- The Led Tag will start blinking fast and continuously.
- Take an unconfigured btwTAG, attach it to the power supply, and place it on top of the Tag Programmer for a few seconds.
- The Tag you placed when you received the setup will emit 3 quick beeps.
- Repeat the "support" operation with all the Tags you want to configure.



Programmer Mode

How to select the "Programmer" mode:

- Connect the btwTAG to your power supply
- Open a PC with Wi-Fi and connect to the btwTAGXXXXX network
- Open a browser with 192.168.0.1/config
- Go to the "Advanced Setup" section
- Select the type "Programmer" in the "Tag Type" field
- Press "Save"



Live Configuration

How to change the configuration when the btwTAG is operating:

- Go to the Dashboard
- Enter the "Man Tags" section

- Press the "Config" button of the Tag you want to Configure (use slide tool to find button at right on screen)
- Find the device by searching the HW ID in the Configuration page.
- Enter the new parameters and press "Save"

All Man Tags

Group	Battery	Updated At		
0	100%	30/05/2020 12:03	Details	Config



Contact

1730 Park Street
Naperville, IL. 60563
USA
info@btwtag.com

Appendix I: APIs For OEM Platforms

This documentation (Version: Draft V1.4) allows developers to build a server for exchanging data with OEM-based btwTAGs.

Defining the Structure

btwTAGs communicate with the server using 2 Rest API calls of type Post. The device inside it is configured with a standard endpoint. btwTAG cloud: to take advantage of the device in the btwTAG version OEM will need to change this parameter.

The two POST calls are:

1. /add , is the first call that makes the device to register with the server.
2. /date, are all subsequent calls in which the device will communicate all the application data and any new parameters of configuration.

...

STEP 1: Turn On and First Configuration

1. Turn on the btwTAG and connect it to the power supply. When the btwTAG is connected to the power supply will enter 5 minutes. This mode sets the btwTAG Host and exposes a configuration web page.
2. Use a PC, scan nearby Wi-Fi networks, and connect to the "btwTAGXXXXXX" network where the x correspond to the serial number of the device.
3. Once connected, open a Browser and go to the 192.168.0.1/config
4. Within the page there will be two areas:
The first allows the quick configuration and then entering SSID and Password Wi-Fi network that the Tag will use to reach the server and the company token (explained below);
The second allows advanced configuration.
5. Fill in the quick configuration fields by entering the value companydiTest as company_token.
6. Proceed to the advanced section and replace the value of the endpoint parameter with the address of the API server. This value it can be both a local server (ex: <http://192.168.0.99:3000>, both a masked endpoint e.g.: <http://192.168.0.99/api>, is an endpoint cloud https e.g.: https://mio_cloud.com:3000). The important is that the server exposes the two calls / add and / data of type POST. It is therefore possible to set the end point also for versioning of the API ex: https://mio_cloud.com/tag/api/v1 will be the tag ad append the route / add and / data to the endpoint.
7. When you have compiled this parameter, press the Save key. The Tag at this point it will restart, detach it from the power so that entering its main function.

STEP 2: How to Handle Server-Side Calls

As described in the introduction, the btwTAG will perform a first recording call. In this call, you will expose all your data and configuration parameters and will wait for a response confirm that contains a security token. Let's go into detail call:

/add - First Configuration Call

Type: POST

url: https://endpoint/add

header: { 'Content-Type': 'application/json', 'Accept':
'application/json', 'token': token-primitivo }

body: payload (json)

PAYLOAD (JSON):

```
{  
  dev: { hw : string,  
          ct : string,  
          bt : float },
```

```
  cfg: [  
    { param: 'sy', value: int },  
    { param: 'pi', value: int },  
    { param: 'wi', value: string },  
    { param: 'rg', value: int },  
    { param: 'rc', value: [int, int, int] },  
    { param: 'ty', value: int },  
    { param: 'wr', value: [int, int] },  
    { param: 'wt', value: [int, int] },  
    { param: 'ar', value: [int, int] },  
    { param: 'at', value: [int, int] },  
    { param: 'tx', value: int },  
    { param: 'ch', value: int },  
    { param: 'fr', value: int },  
    { param: 'fw', value: string },  
  ],
```

```
  mtc: []  
}
```

Positive response expected from the Device:

Registration complete:

201 - payload (JSON) { new_token: 'token' }



Tokens

The btwTAGs Firmware contains a token-primitive, this token will be placed in the header of the /add call, it will be the job of the server return an object (JSON) in the response within which to insert the key new_token and as a value a new alphanumeric token of 8 figures that the btwTAG will encapsulate in the header of subsequent calls to /date type.

Note: Of course, you can return to all Tags the same new token; for security reasons we encourage you to use a unique token for each Tag.

The server (for example) will need to receive the /add call:

1. verify that the primitive token is present and is correct
2. verify that the payload contains the device key with the hw_id (unique serial of the device) and possibly the company_token (that is, an identifier of the ecosystem in which it will operate).
3. Save the Tag and all its parameters to a database and generate a 8-digit alphanumeric token.
4. Return the JSON (as per snippet) as a response within the to insert the new token.
5. From this moment on, the Tag will always only send type /data and in the header of these will encapsulate the token generated received in the response to the /add call.

...

Before we see the /data call let's see what the parameters that the Tag sends to the first recording.

Configuration Parameters

The btwTAG has several configuration parameters. tend to be used by the standard user because could go to change the functioning of radio frequency and then the performance of contact-tracing, however one person properly trained can achieve ad hoc performance by modifying them.

Let's see the list of parameters

param:'hw': Unique hardware identifier of the tag

ex: ID-00124B001BCA3C37

param:'ct': company token

Identification of the company in which it is used

param:'bt': battery level

param:'sy': sync time with the server

It is the time window (in minutes) at the end of which the tag will turn on the Wi-Fi and try to send the data to the Server.

param:'pi': broadcast message time.

This is the frequency (in seconds) of the message's sending time broadcast of "presence" that other Tags "listen" to determine the contact.

NOTE: The tag automatically sends data to the server whenever it has filled the event memory available on the device regardless of scheduled times.

param:'wi', : ssid wifi network to connect to

param:'wp', : wifi network password to connect to

nb: Password is the only parameter that is not sent in the array of parameters "config" of the /add type call

param:'ct': ecosystem identifier/place/company in where the tag operates, is manually inserted into the quick configuration

param:'end': btwTAG cloud endpoint default

param:'rg': 0 - Close Proximity, 1 - Normal Proximity It is the type of ranging (more or less stringent) that the to determine a contact.

param:'rc': [0,0,0] : [Beep,Vibration,Led] 1st yes 0-no

It's the kind of reaction that the tag will adopt when it finds in contact with another tag, build the array based on the preferences, if put at [0,0,0] the tag will record the contacts but it won't ring, it won't vibrate, it won't flash, vice versa if set to [1,1,1] will perform all reactions.

param:'ty': 0 = ManTag, 1 = GateTag , 2 = AreaTag, 3 = Programmer
Type of Tag between person, gap, area and programmer.

param:'wr': [rssi for ranging 0,rssi for ranging 1]

Value of rssi above which (attention is a number negative) the tag is considered to be in the warning area for the two Close Proximity (Normal Proximity).

Example [-60,-90]

If the tag, in Close proximity mode, hears a broadcast message of another tag whose value of rssi is greater than -60 (and therefore closer to 0) will consider at a warning distance.

param:'wt': [time for ranging 0,time for ranging 1]

Like the distance, this value indicates the time (in seconds) beyond which the warning distance is considered a warning event.

Note: Warning events will cause reaction to run for a short moment (warning) but will not be saved.

param:'ar': [rssi for ranging 0,rssi for ranging 1]

param:'at': [time for ranging 0,time for ranging 1]

Like the warning, we have the parameters of rssi and time also for the alert. The alert, unlike the warning, performs reaction until the contact stops and the event is saved and then forwarded to the Server.

param:'tx': tx power (min:0,max:14,def:0)

Power of TX Rf message broadcast to RF Sub-G

param:'ch': channel (min:0,max:9,def:0)

Sub-G Frequency Communication Channel note: All communication devices must coexist on the same frequency and on the same channel

param:'fr': 0 -868Mhz, 1 th 915Mhz (def:0)

Frequency at which the Tag should operate

note: 915Mhz is only for the US, 868Mhz for EU

param:'fw': realease fw

...

Changing Post-Registration Parameters

To change a Tag configuration parameter after registration there are 2 methods:

1. Connect the Tag to power, connect using Wi-Fi, open the configuration web page and edit the parameters. This will cause the Tag in its next /data call will insert the modified parameters and their parameters into the array to the config key. new value. This will make it possible for server-side to be able to display the parameter changes made manually.
2. Send new configuration parameters from the server by entering them in the response to the /data type call.

Sending the Contact Tracing

The tag if the "sync_time" sync time has expired or is it close to filling the capacity of the memory-events will call the server /data route.

The payload of the "contact-tracing" message is identical to the Recording.

/data - contact-tracing message

Type: POST

url: https://endpoint/data

header: {'Content-Type':'application/json','Accept':
'application/json','token': token-generated}

body:payload (json)

Payload:

```
{  
  dev:{ hw: string,  
        ct: string,  
        bt: float },
```



```
cfg:[],  
mtc:[]  
}
```

The config array can contain objects equal to those used in the registration phase:

```
... ..config:[{p:string,v: new_value}]
```

where p corresponds to the parameter (ex: ar,at,wr,wt ect)

where v corresponds to the value (ex: int,string,[int,int], etc.)

The match array can contain objects by following the following schema:

```
... match:[{ dv: string, ti: number, ty: int, d: number - }]
```

where dv corresponds to the hw of the intercepted device

where you match unix time timestamp

where ty corresponds to the ty of the intercepted tag

where d is the duration of the contact in seconds

Positive response expected from the Device:

Saving the data successfully:

201 - payload (JSON received_configs)

```
new_configs:null/[objects]'
```

First, it should be noted that in the header to the token key, the Tag will no longer insert the token-primitive as in the /add call but will encapsulate the token-generated and obtained in the call response /add.

If you have changed the parameters manually from Wi-Fi connection the Tag will hang an object to the "cfg" array for each changed parameter.

If you have made contact between tags, the device will hang the device key "mtc" as many objects as were the registered contacts.

The contact object shows the hw of the device with which you have found in the alert zone, the timestamp (unix time), the duration of the type of tag that was detected (ManTag,AreaTag,GateTag).

In the "dev" section, the tag will enter its identification data (hw/company_token) and battery level.

Answering the Call/Data

The Tag to type /data call waits for a constructed response according to the schema of the snippet.

1. At the key `received_configs`, it will expect "true" if you have sent in the request for manually obtained configurations Wi-Fi, if it is returned "false" it will try to send parameters back to the server.
2. At the key `new_configs`, it will expect null, if != from null will cycle the array expecting objects constructed according to the `cfg`. (`p:string`, `v:newvalue`)

The Server will then call the /data type (for example) and perform:

1. Check for header tokens, and that it is correct with generated after registration.
2. Check for `hw` and `company_token` (`ct`), retrieve the tag record from database.
3. Check for new configurations set serverside.
4. Check for new configurations in the payload of the and save them to the database.
5. Check for contacts in the call payload and save them to databases.
6. Respond with flags to true if new config is received from the ex step 4, encapsulate the new configs if you need ex point

Appendix II: Device Specifications

Dimensions	48.6x93x15 mm
Rechargeable battery	Lithium 1000mAh
Charging	Micro-USB port
Material	ABS (UL94HB) and Silicone
Operating Temperature	-10 °C / +60 °C
Led	X1
RF	BLE (4.2) 2.4Ghz
RF	Wi-Fi 2.4Ghz 802.11a/b/g/n
RF	Sub-G 915 MHz 802.15.4
Certifications	CE / RoHS