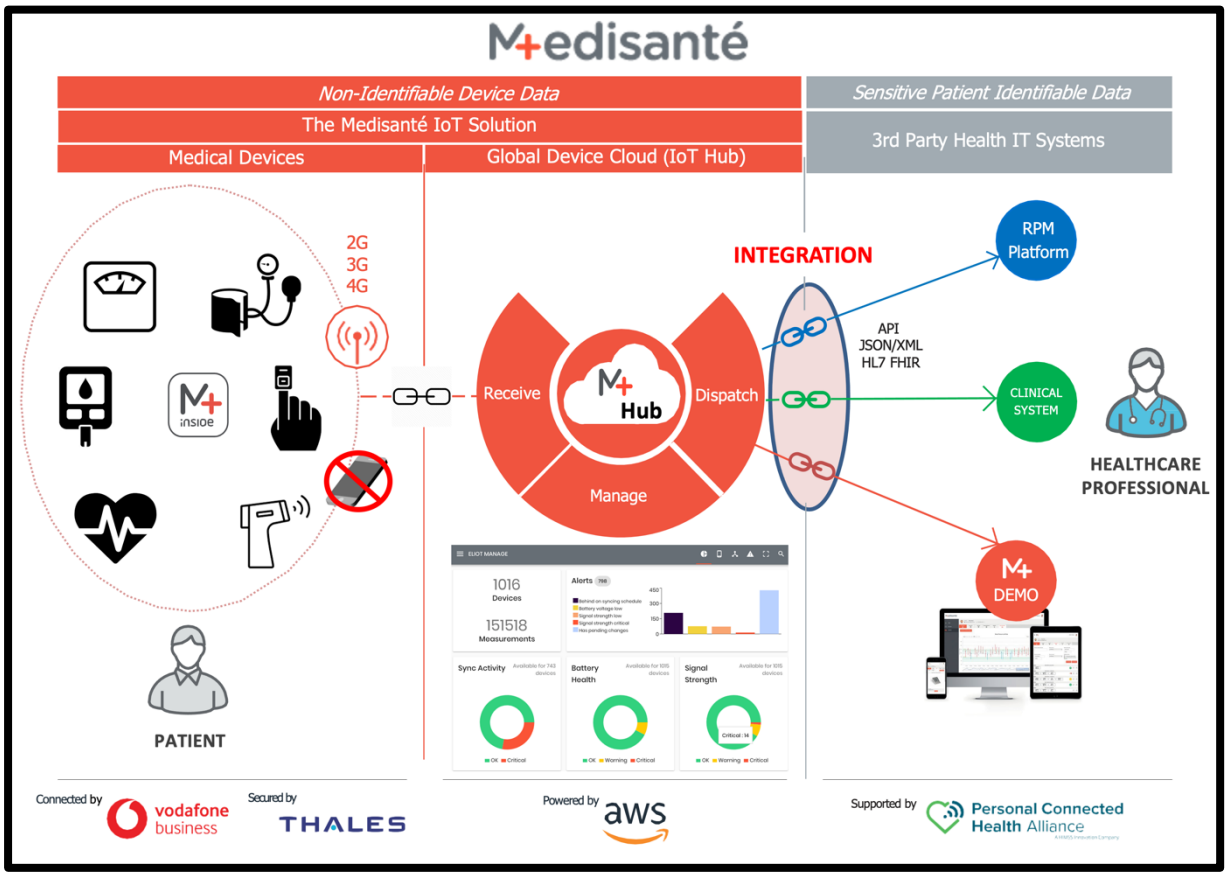
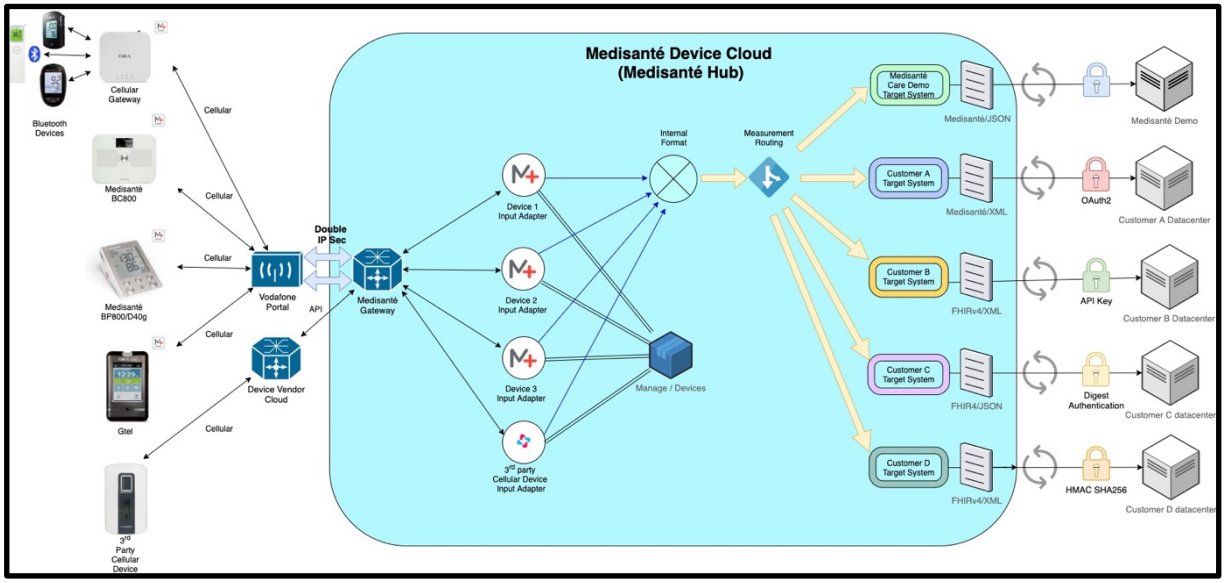
Medisanté (M+) Hub Integration Guide

Overview of Medisanté Medical IoT Infrastructure

Medisanté Device Cloud Hub is **pushing** device readings in *near* **real time** to the receiving clinical system/RPM platform





Prerequisites – Performed by Medisanté (For Customer information)

Pending the signature of the NDA and ahead of the integration planning, Medisanté will create the setup so that the described tasks under the "Integration" section below can be performed.

1) Platforms environment, roles and responsibilities:

- Creation of an "Organization" (typically "Company Name") under which the integration setup will be implemented.
- Creation of an "Admin user" within the above Organization, with "System Admin" rights:
    - The "Admin user" is granted the following specific rights:
        - "Organization Manager": user creation/management, organization creation, "Device Manager" : webhook setup, device setup,
        - "User Manager" : user rights allocation.
        - More details on roles are available in the "Medisanté Software info" document in the Appendix Kit
    - The "Admin user" person needs to be communicated to Medisanté:
        - A valid email is required,
        - The person will then setup the credentials upon reception of an initial email
    - Once credentials are confirmed, the below integration steps are applicable

- Additional users can be created by the "Admin User"
    - Please check the Appendix A the procedure
    - Integration steps can only be performed by a user who has at least the "Device Manager" right in the Organisation

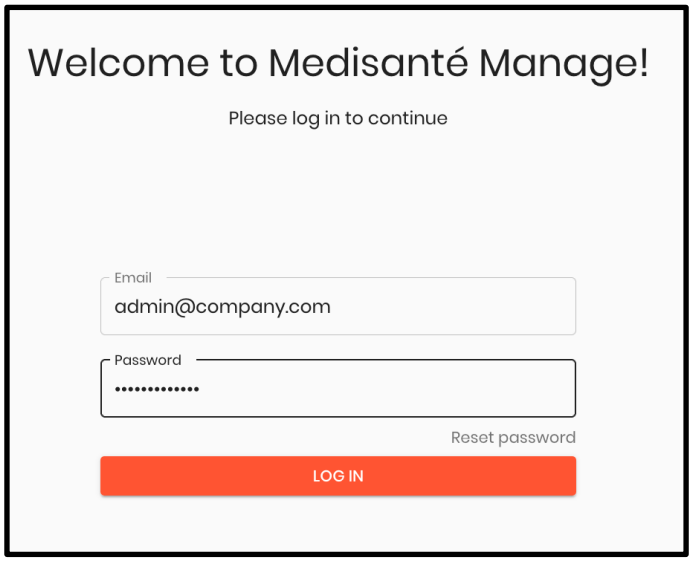
2) Medisanté web portals:

There are 2 portals for which access is required to perform the integration (More information available in the "Medisanté Software info" document). The same credentials apply to both.

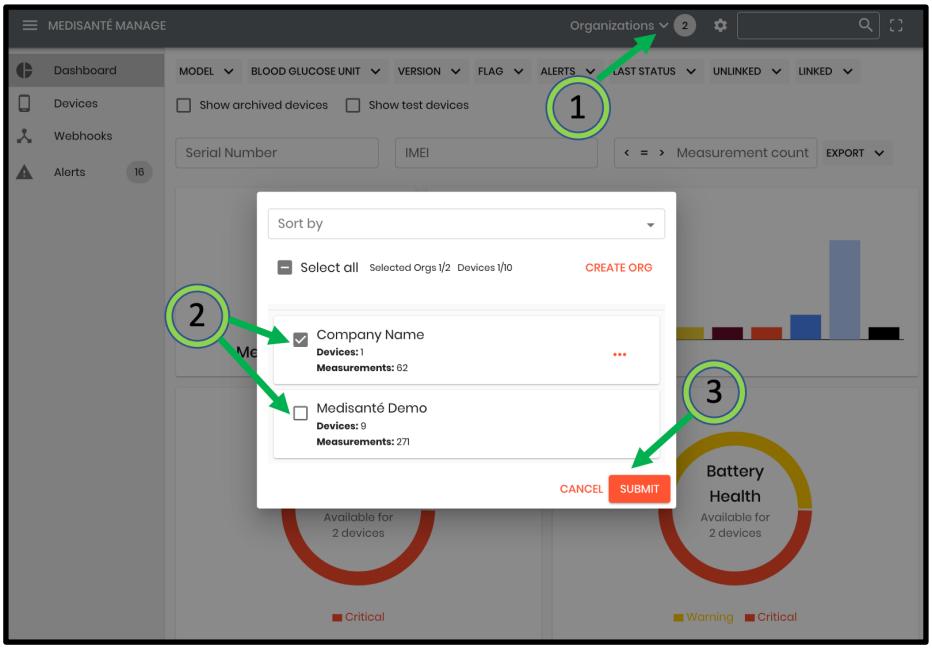
- "*Medisanté Manage*": platform for integration setup & ongoing device management
    - https://devices.medisante.net
- "*Medisanté Admin*": platform to manage organization's users and permissions
    - https://admin.medisante.net

INTEGRATION STEP 1
Create a Webhook

1) Log-in to "*Medisanté Manage*" with "Admin user" credentials : https://devices.medisante.net



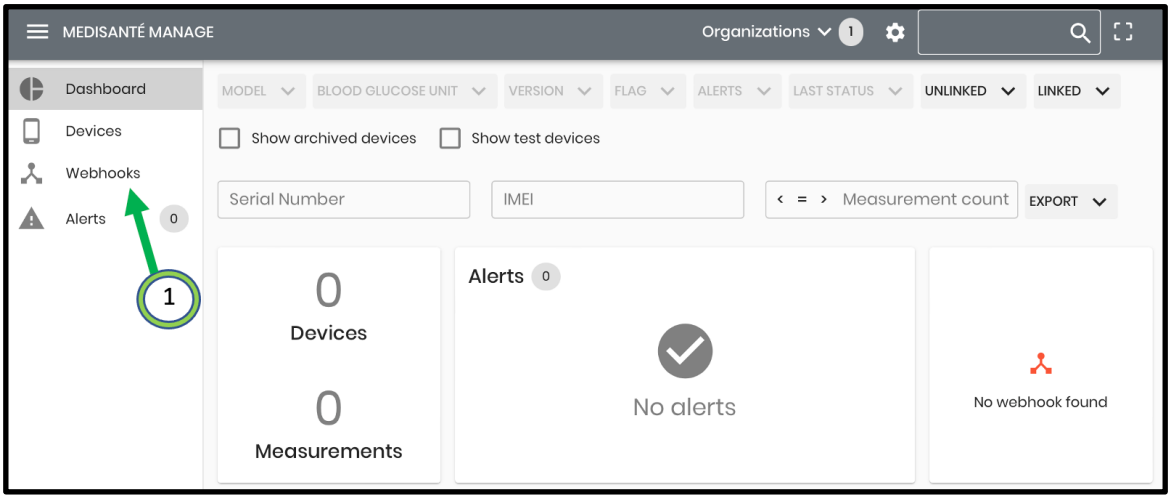
After login, the user operates by default within the "**Company Name**", unless it has been separately granted access to multiple organizations. In this particular case, select the right organization as shown in the picture below.

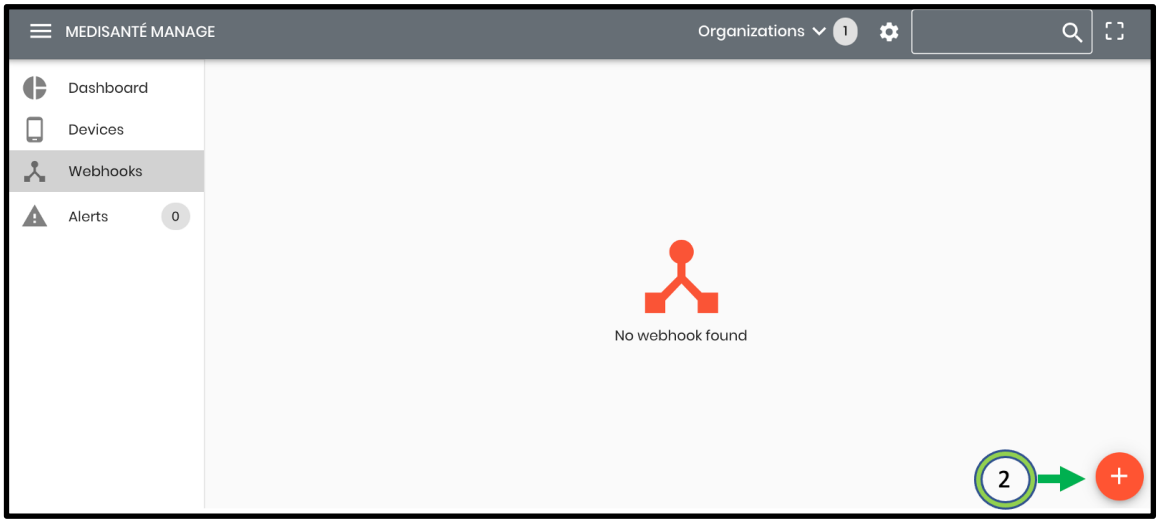


2) Webhook creation:

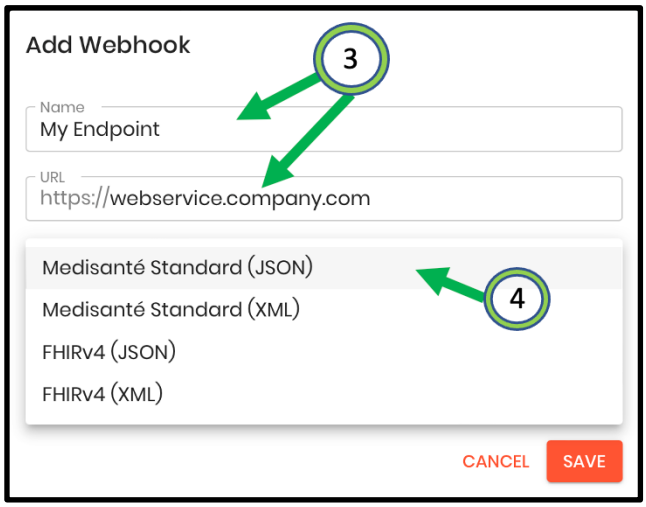
- Requirement :
  - An "*https endpoint*" / your application proxy, should be up and running.
  - NB : we are offering a ready to use "https endpoint" in case you are looking for a fast path implementation. Please contact us in this case

- Below, the webhook we will create is "My Endpoint"

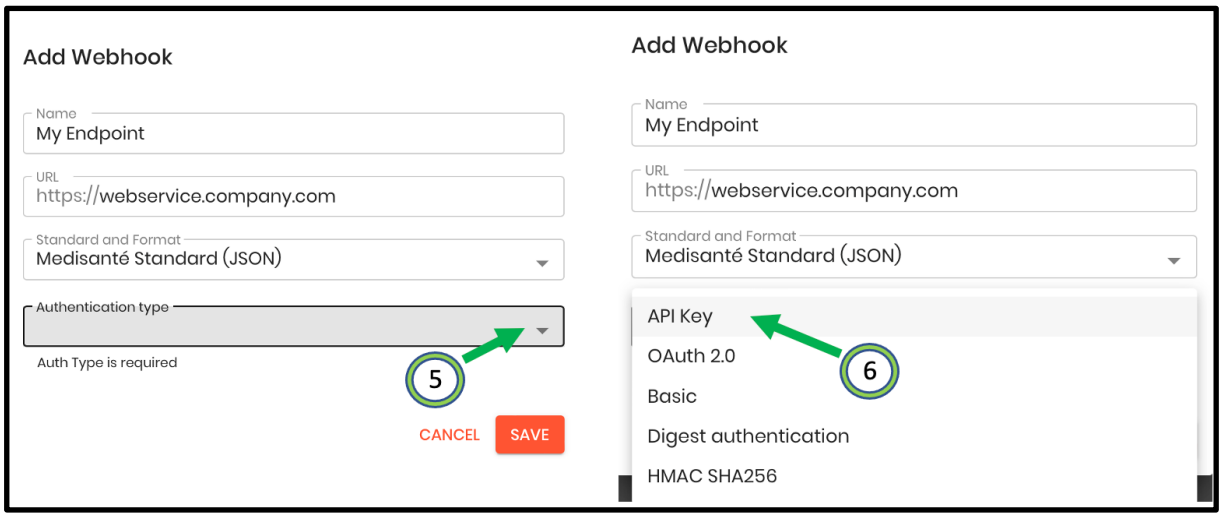


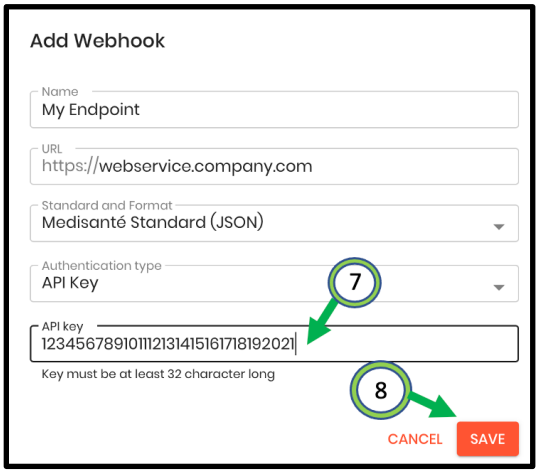


- Enter the name of the webhook (“My Endpoint) and enter its URL (provided by your development team)



- Select desired Standard/Format:
  - Supported ones are :
    - Medisanté Standard/JSON, Medisanté Standard/XML
    - FHIRv4/JSON and FHIRv4/XML
  - Samples files are provided in the integration kit for all physical devices qualified at the time of the release of this kit
- Select the preferred authentication type. Available options are:
  - API Key
  - OAuth2.0 (Client Credentials/Authorization code/JWT bearer)
  - Basic
  - Digest Authentication
  - HMAC SHA256
  - (Client Side TLS is also available, please get in touch with us to implement this)

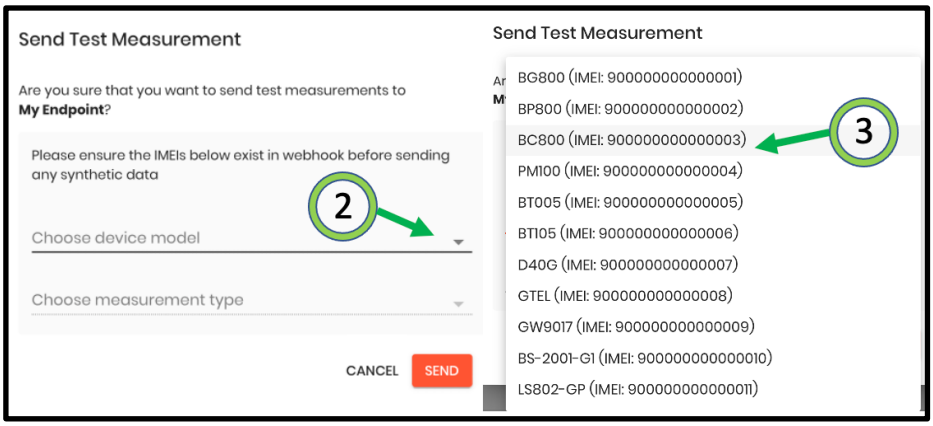




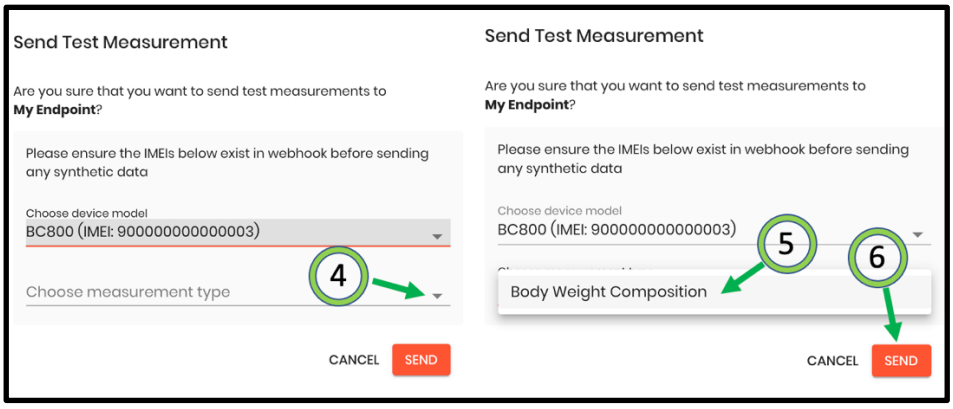
- Congratulations! The webhook is now created.

INTEGRATION STEP 2 :
Test the Webhook ("My Endpoint") with virtual device data

- This step enables to check if your target application effectively receives data – without having a physical device in hand.
- We offer the capability of sending synthetic measurements to Webhooks from a set of *virtual* devices - that mimic data sent from physical devices. You therefore do NOT need to have physical devices in hand to perform that step.
- Follow the steps below to test your webhook "My Endpoint"

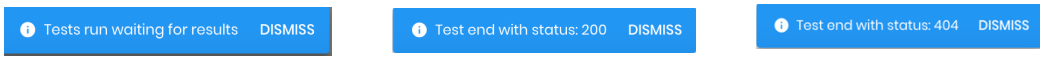


- The device types available in the dropdown list continuously expands over time



Synthetic Data is sent using "My Endpoint" alongside with IMEI numbers that emulate real devices.

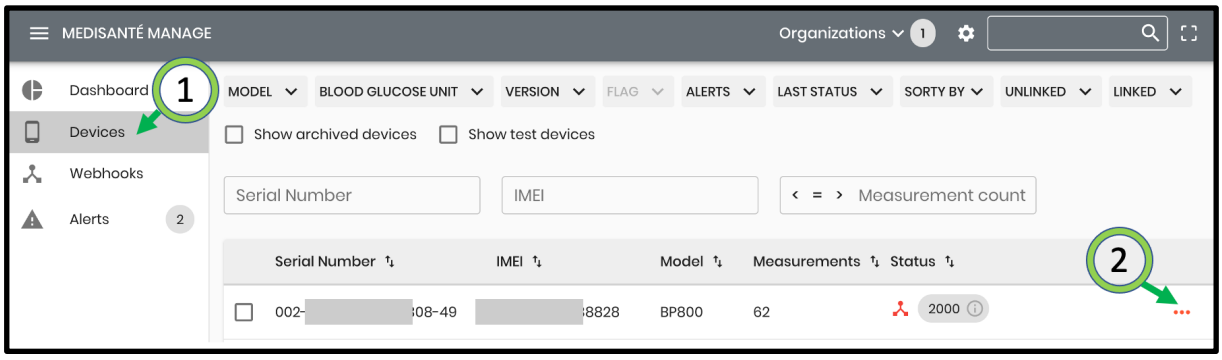
The system returns a status code after a few moments. If successful, it should be "2XX".



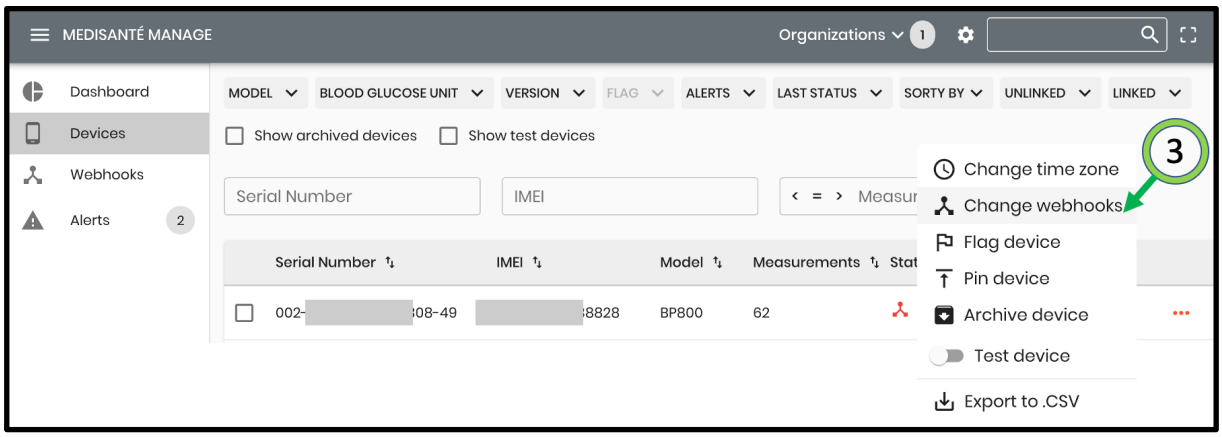
Please consult the document "Target System status code" in the kit for more details.

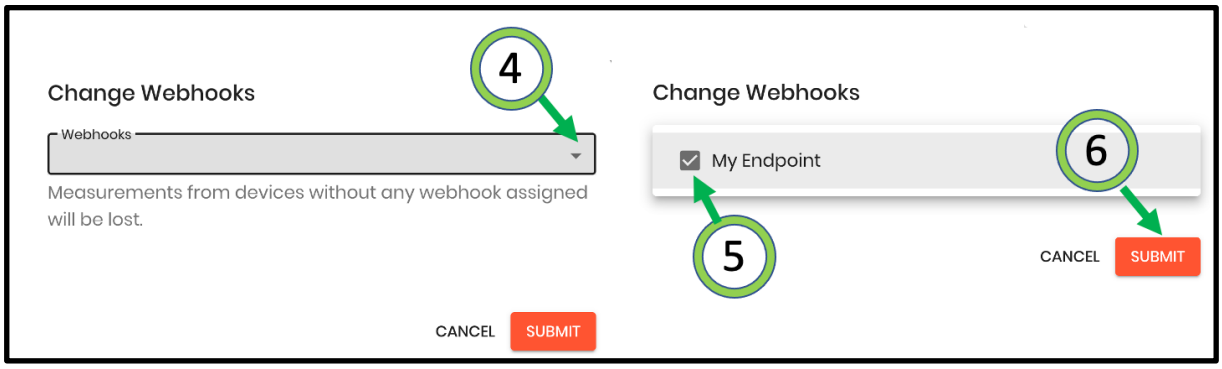
INTEGRATION STEP 3 :
Test the Webhook ("My Endpoint") with physical devices

- This step is possible if you have received a device from Medisanté and you want to send data from this device to your application. It's a "real life test".
- That device has been allocated to your organization: it's visible in the "Medisanté Manage" portal.
- In this example, one physical device will be configured to send data to your webhook "My Endpoint".
- A device without a webhook (i.e. without destination for its data) has the following icon
- Select the device in "Medisanté Manage"



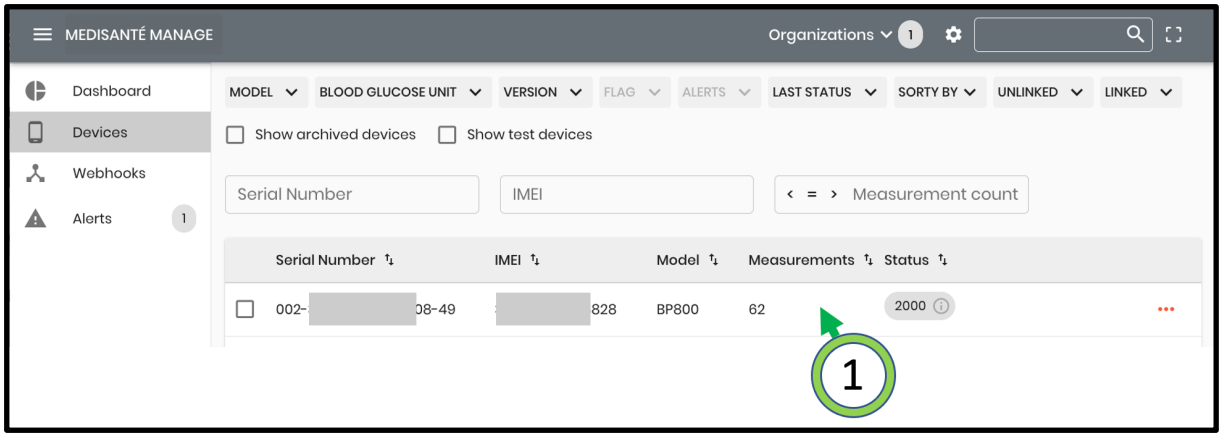
The "...." menu items list depends on the device type and firmware version

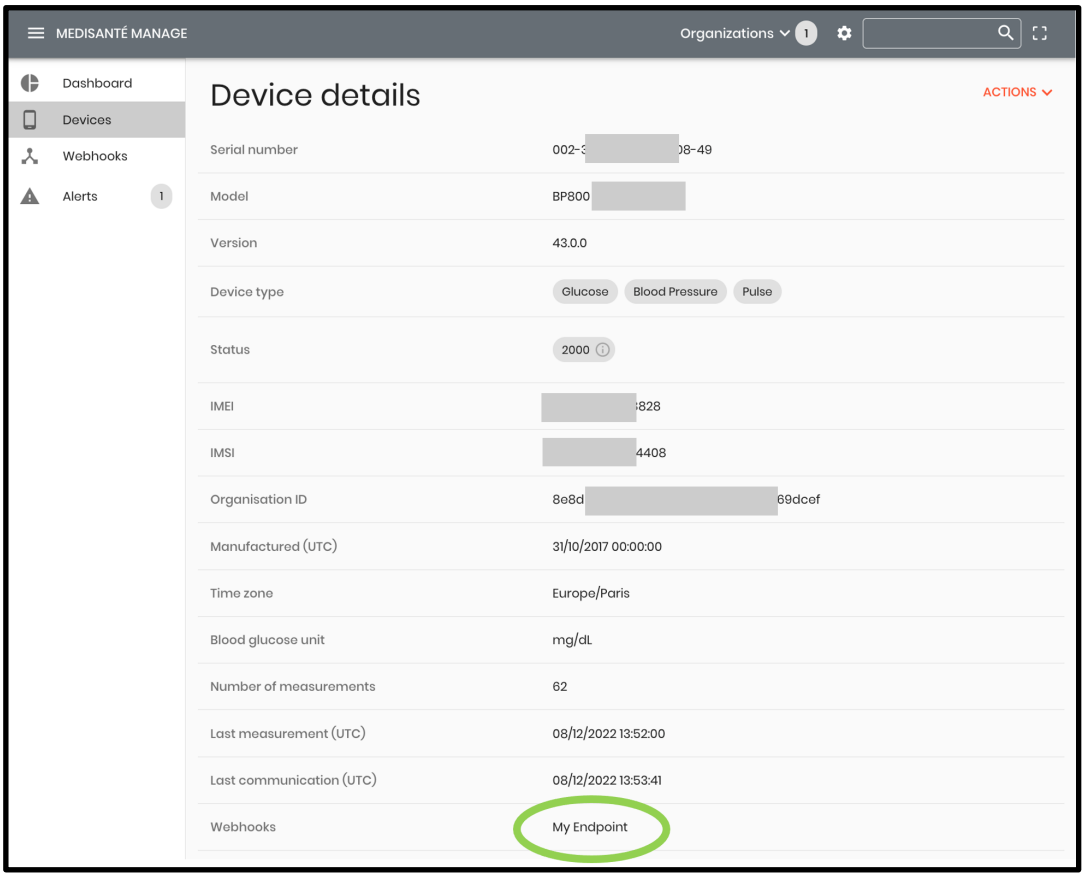




The device is now configured to sending any measurements to "My Endpoint" webhook.
You can check it how described below.

NB : Devices can send data to multiple webhooks at the same time.





Well done !!

You can now test real life scenario and receive data from Medisanté physical devices in your system

NOTES : Customization of the environment can be done in several ways

- Addendum 1 : Additional user creation
- Addendum 2 : Device settings configuration
- Addendum 3 : Bluetooth to cellular gateway configuration
- Addendum 4 : Using the API

Addendum 1-4 are available at the end of this document

IMPORTANT

On the receiving application side, integration also requires the design of a module that maps Device IDs to patient IDs:

- The target system receives device data alongside with the device ID
  (e.g. “80.3 kg” coming from IMEI : xxxxxxxxxxxx)
- There is a requirement for the target application to build and maintain a “mapping table” between Patient Id ←→ Device Id, to associate the received data with the patient in the target application.
  - Some of our partners have for example used a bar-code reader to associate device with patients on the clinical application side

Integration Kit Content

The following documents are available in the “Integration kit”:

- Access Security
- Clinical Coding Dictionary
- Data Integrity
- Data Retention Policy-GDPR
- Role Based Access
- Software Info v3
- Software Q&A Sheet
- Target System Status Codes
- Undelivered Measurement Error Handling
- Webhook Info
- Sample Data Files (Medisanté & HL7/FHIRv4 formats, JSON & XML encapsulation)

Additional Technical information

- Medisanté provides a HTTPS push-based method of delivery for measurements
- Its RESTful API can also be queried for pull-based delivery of device metrics and services
- Delivery of messages is expected to be in near real time
- TLS and IPSec are used to protect data in transit
- AES-256 encryption is used to protect our data at rest (stored data)
- Medisanté’s exposed API uses oAuth2
- For pushing devices readings, Medisanté support API keys and TLS client certificates
- An API key has to be set to authenticate us (any measurement should contain this key in the X-Api-Key header)
- Data retention policy is described in appendix
- User Roles are described in appendix

Addendum 1
Additional User Creation

In the standard process, the **Admin User** is the primary user with the responsibility of implementing the integration.

However, this user can be assisted by others within the same organization.

For this purpose, **Admin User** has the possibility to create additional users, and assign them roles.

Such new organization members may require access to:

- "*Medisanté Admin*": to create/edit/view users,
- "*Medisanté Manage*": to edit/view device parameters.

NB : The Appendix document "Role Based Access" explains all the available roles in details.

To allow users device access (through "*Medisanté Manage*"), **Admin User** can assign them one of the following roles:

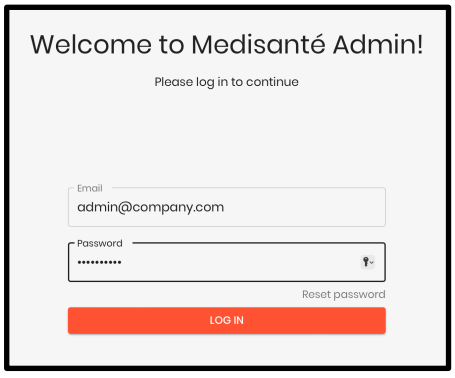
- Device Manager (Read/Write),
- Device Viewer (Read)

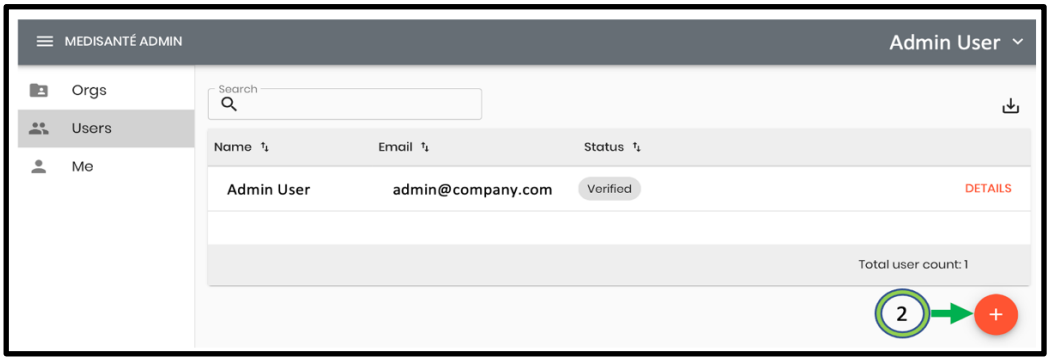
To give user configuration rights (through "*Medisanté Admin*"), **Admin User** can assign them one of the following roles:

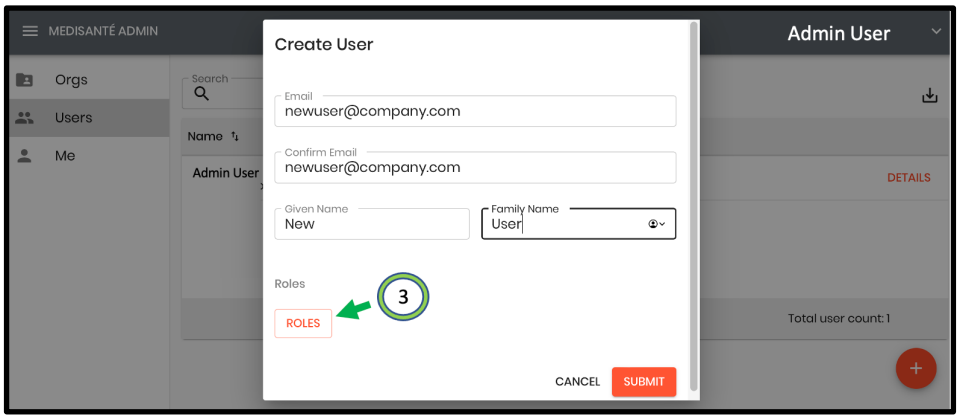
- User Manager (Read/Write),
- User Viewer (Read)

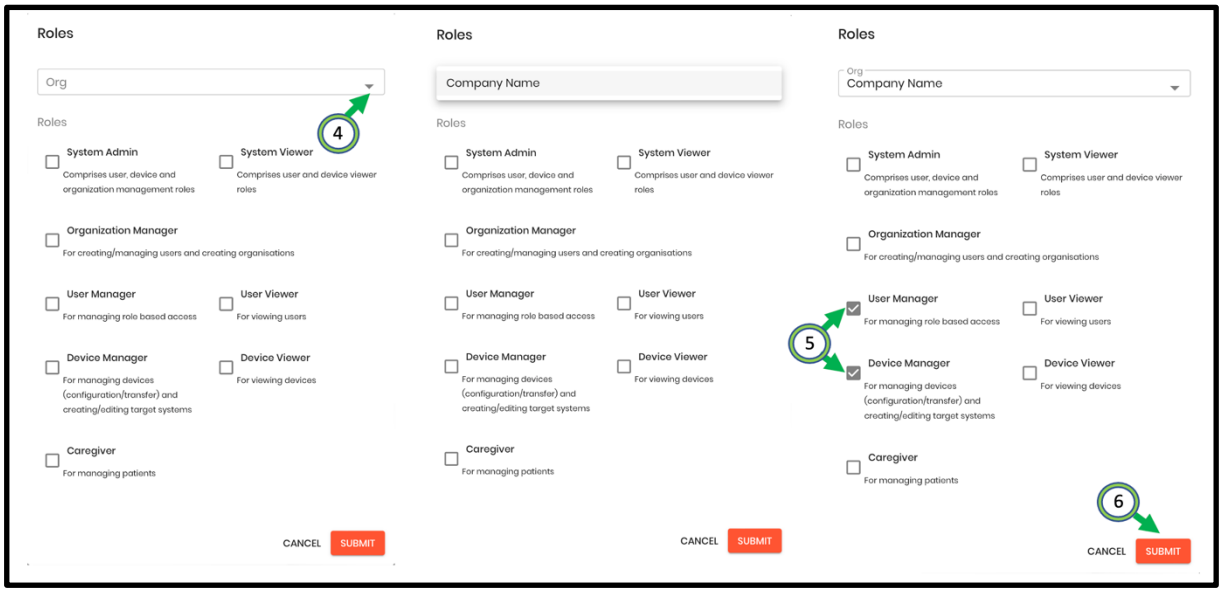
Below is an example of **Admin User** creating a "**New user"** User within the Organization, with User Manager & Device Manager roles

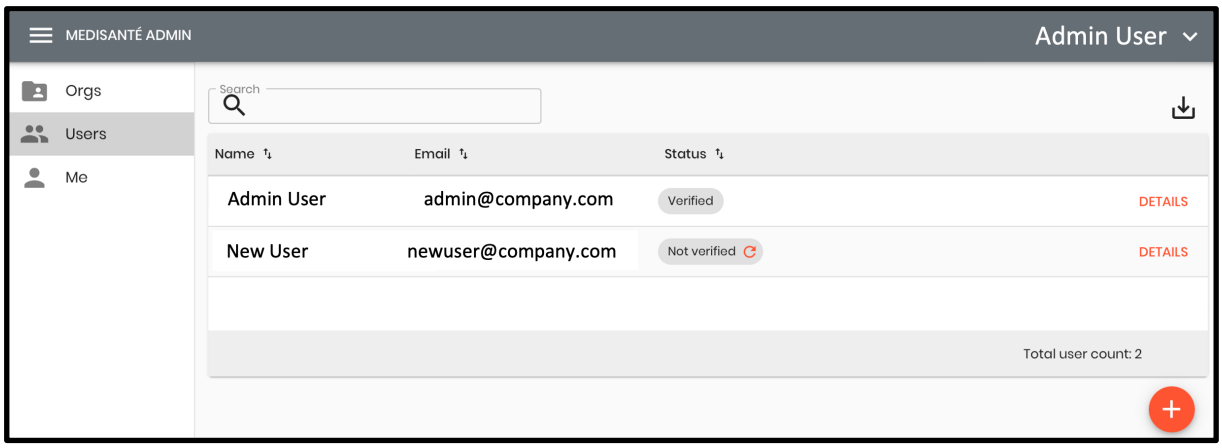
- Log in "Medisanté Admin" (https://admin.medisante.net) as **Admin User** :




MEDISANTÉ ADMIN
Admin User
Orgs
Users
Me
Search
Name
Email
Status
Admin User
admin@company.com
Verified
DETAILS
Total user count: 1
2


MEDISANTÉ ADMIN
Admin User
Create User
Email
newuser@company.com
Confirm Email
newuser@company.com
Given Name
New
Family Name
User
Roles
ROLES
3
CANCEL
SUBMIT


Roles
Org
Company Name
System Admin
Comprises user, device and organization management roles
System Viewer
Comprises user and device viewer roles
Organization Manager
For creating/managing users and creating organisations
User Manager
For managing role based access
User Viewer
For viewing users
Device Manager
For managing devices (configuration/transfer) and creating/editing target systems
Device Viewer
For viewing devices
Caregiver
For managing patients
4
5
6
CANCEL
SUBMIT


MEDISANTÉ ADMIN
Admin User
Orgs
Users
Me
Search
Name
Email
Status
Admin User
admin@company.com
Verified
DETAILS
New User
newuser@company.com
Not verified
DETAILS
Total user count: 2

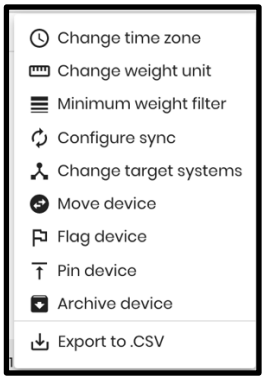
The newly created user will receive credentials via email in order to finalize the setup.
Once done, the access to "*Medisanté Admin*" and/or "*Medisanté Manage*" will be granted

NB: Assigned Roles can be changed/removed by any user having "User manager" rights within the organization

Addendum 2
Configure device settings

It is possible to configure pull-based device metrics preferences in "Medisanté Manage", as per your requirements.

Available actions and parameters depend on the type of device and firmware version. The example below is for a V2.4 BC800 (weight scale):



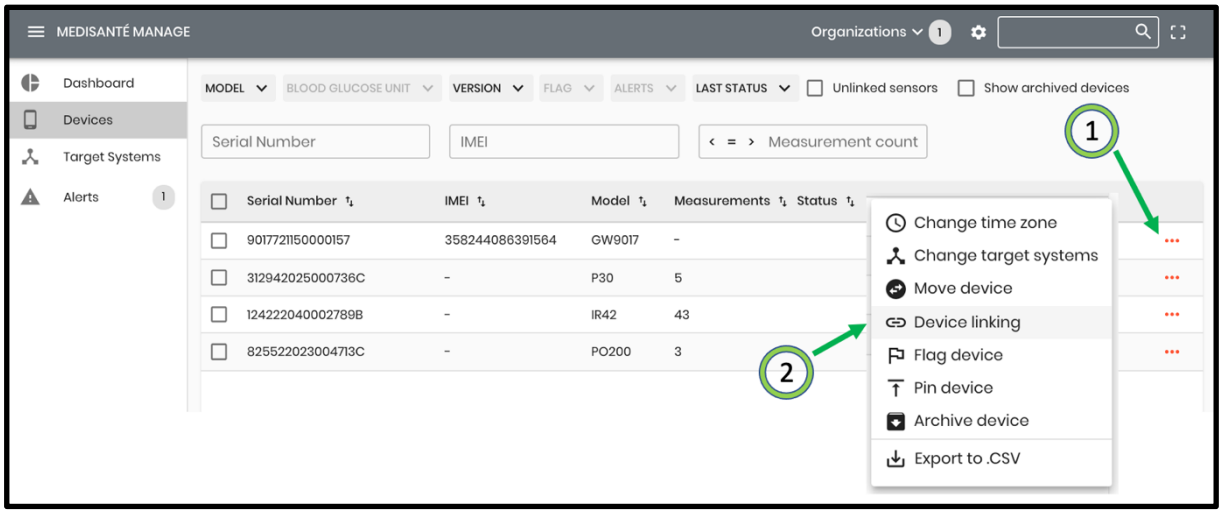
- "Change Time Zone" : Set up display time based on geographical location
- "Change Weight Unit" : Switch weight scale unit from lb/kg/stone.
- "Minimum Weight Filter" : Set up a filter value (between 0kg and 40kg) below which weights will not be processed
- "Configure Sync" : Enable periodical sync'up with Medisanté Hub (both measurement and device data), irrespective of weight scale effective usage.
- "Change Webhook" : Add/modify target systems to which the current device sends data
- "Move Device" : Move device from one organization to another (requires privileges on both Orgs)
- "Flag Device" : Toggle Lost/Stolen or Faulty/Damaged flag on the device
- "Pin Device" : Mark the device for future attention
- "Archive Device" : Hide current device from being displayed on the device list of the Organization (can be seen back when crossing the "Show archived device" box of the UI)
- "Export to .CSV" : Exports the attributes of the current selected items into a CSV file for future reuse.

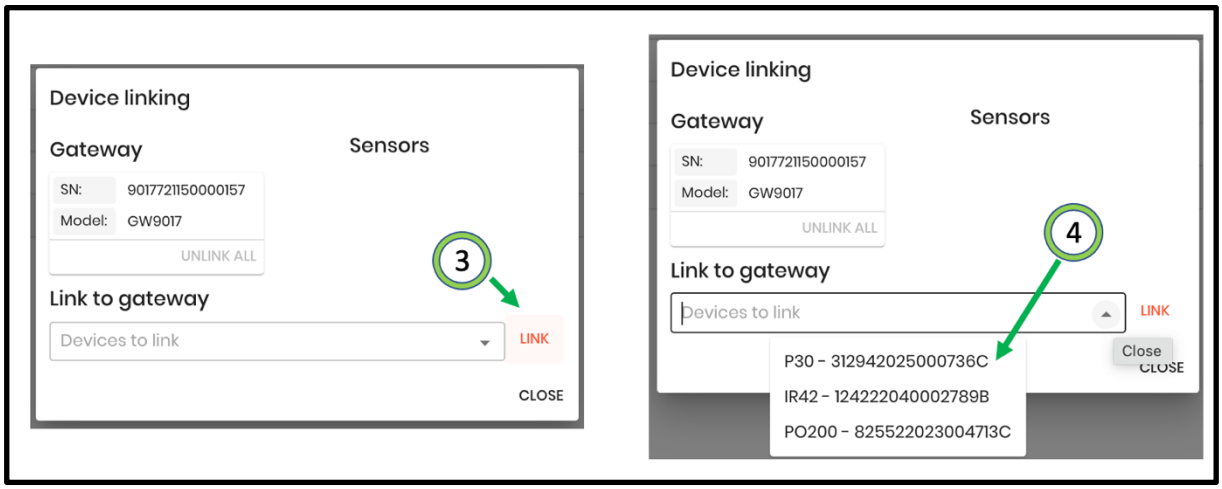
Addendum 3
Bluetooth to cellular gateway configuration

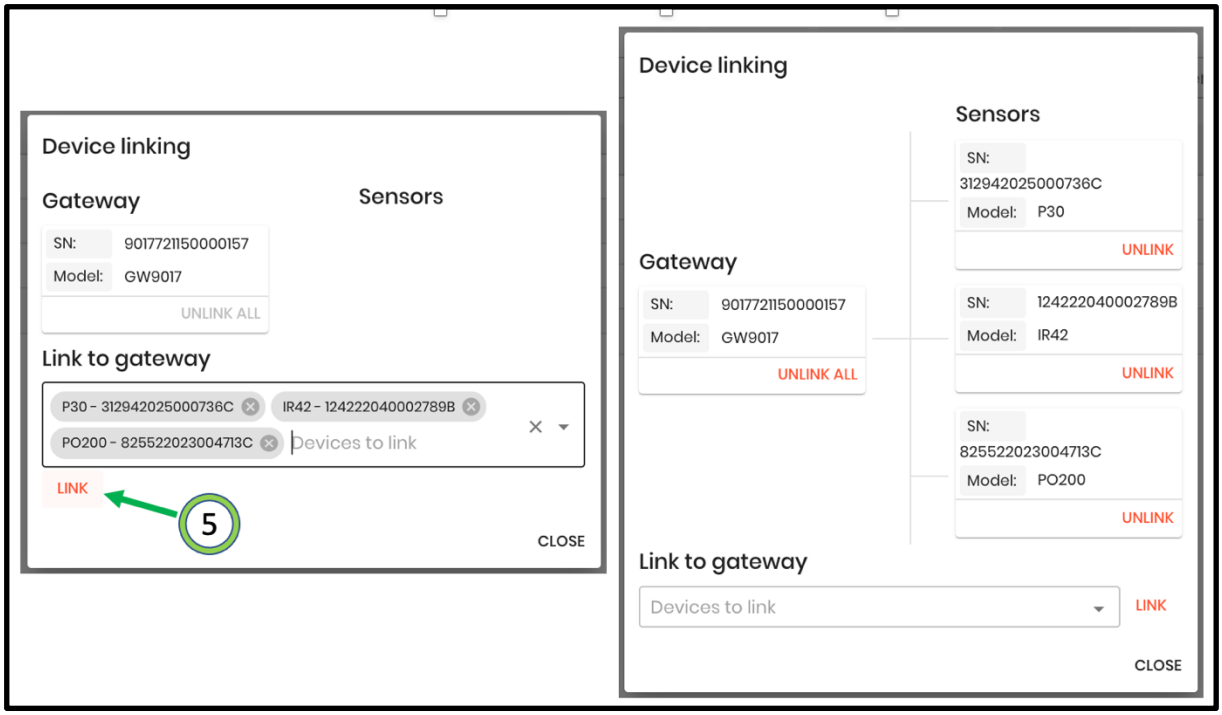
Medisanté is also offering an alternative to cellular enabled devices, while still relying on cellular technology to upload the data.

It is now possible to use qualified Bluetooth devices, that automatically connect to a “Bluetooth to Cellular” gateway (ForA/M+ GW9017)

This requires a few configuration steps detailed below, using “*Medisanté Manage*”, by a user who has “Device Manager” rights







Addendum 4
API Usage

Beside integration for medical device readings delivery, we have a documented REST API (available at https://api-docs.medisante.net/ accessible to users with "System Admin" role) that can be leveraged for example to gather technical device readings such as battery level and signal strength. These parameters are of interest to biological technicians.

The API can also be used to configure the platform from an external application: manage the user and organization database, change the device measurement unit (weightscale), the time zone & where measurements are routed...

These configuration changes are done today via our web portals: "*Medisanté Manage*" & "*Medisanté Admin*".