KICKSTARTER APPLICATION

Starter development application

Abstract

This documentation describes how to setup and operate the application

Revision History

The following table records information regarding changes made to the project over time.

Version Number	Date	Author/Owner	Description of Change
1.0	09/13/2021	Guilherme Costa	Baseline Version
1.1	12/22/2021	Vitor Lima	Additional Sensor guide

Contents

Glossary

This section provides definition for the terms used in this documentation and also the system.

Device-Token: unique token of the device at TagoIO; used to send, delete or edit data stored at TagoIO.

Account-Token: high level token of the account; used to create devices, dashboards, actions, etc.

Network: resource entity from TagoIO that provides support for receiving data from an external network, such as Tektelic, Everynet, TTI, MQTT, HTTPs etc..

Connector: resource entity from TagoIO that provides decoding support for a specific sensor.

Connector ID: unique ID of the connector.

Authorization: unique token from TagoIO developers account to access devices. We recommend using it when trying to access devices from others TagoIO developer accounts.

Dictionary: a feature from TagoIO that allows multi-language support in your application. Accessible from the top right menu > Dictionary. Usually represented in the dashboards with the keyword #SLUG.TITLE#

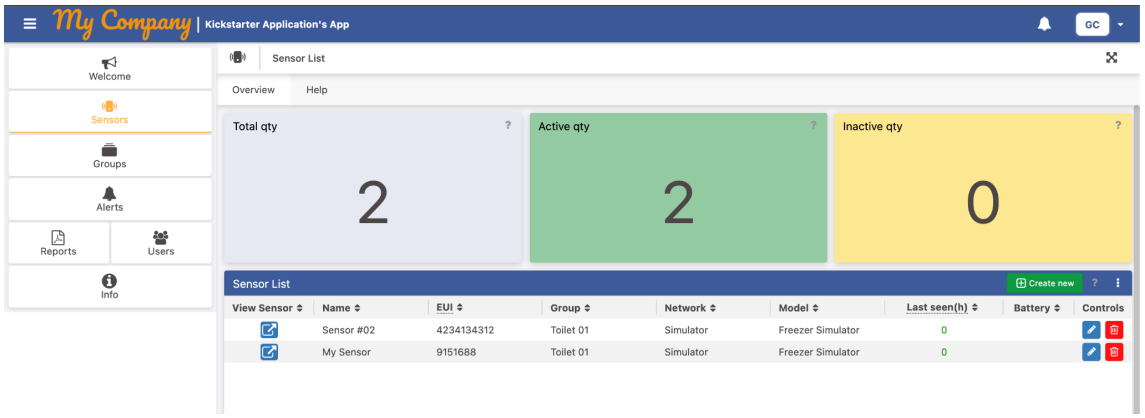
Tags: Tags are available in all resources of TagoIO, such as Devices, Dashboards, Access Policies, etc. It's composed of a key and a value.

Introduction

The purpose of this document is to describe how to operate the Kickstarter application.

The Kickstarter application is a combination of analysis, dashboards, actions and other features of TagoIO, that creates the correct environment for the application to run smoothly.

You can use the Kickstarter application to start exploring what TagoIO can do for you, and from this base develop and add your own features to it, or you can use it as a learning tool.



Features

In the Kickstarter application you will be able to use the following features:

Feature	Description
Organization Management	With an application administrator user, you will be able to create and manage different organizations, each one with their own sensors, users and alerts. One Organization doesn't have access to any information of a different organization.
Device Management	You will be able to create and give access to your customers to create sensors inside the application.
User Management	Each organization can have many users, being an Organization Admin or a Guest with different access levels.
Alert Management	Users can create alerts in the organization for each device or a group of devices.
Scheduled Reports	Users can set up scheduled reports in the Organization to be sent to their emails.
Plan Management	An Application Admin can create plans and set limits of SMS, Email and Data Retention for each organization.
Pin Marker Support	To pinpoint a sensor in an image file by using Groups.
Tracking Support	If the sensor can send geolocation, it will update the location of the sensor in a Map inside Groups.

What do I need to know beforehand

In order to take advantage of the documentation that we provided, you also need some knowledge about TagoIO Platform that is provided in TagoIO Documentation itself.

Here is a list of topics that we expect you to already know before starting modifying the application:

- **Device, Buckets and Tokens Concept**: TagoIO applications only works by using all the three concepts mentioned. Learn more in How it works - TagoIO
- **Tags**: Tags are the most important feature related to Access and Permissions in TagoIO.
- **NodeJS and Running Analysis External**: Although not required for simple use of the application, it is required if you plan to do your own modifications. Learn more in Running Analysis as External using Node.JS - TagoIO
- **Payload Parser and Connectors**: TagoIO does support a lot of sensors, but you may be developing your own or just got a brand new sensor in hand. Adding support for sensors or even modifying sensor decoders is very important for any application. Learn more at In-depth guide to Payload Parser - How to - TagoIO Community.
- **Blueprint Dashboards**: You probably will want to change the looks of the dashboards, and the Blueprint dashboards are the most recommended feature for scalable applications. Take a look at the Blueprint Dashboard - TagoIO to learn how it works.
- **Dictionary and Multilanguage:** The application is made with multi language support in mind. You may want to use it or not, but it is best to know how it works so you don't get confused with existing dashboards. Learn in Using Dictionaries & Multi-language - TagoIO.
- **TagoRUN**: While you will access the application mostly by the developer's account, your users will access TagoRUN in order to use the application. You need to be able to apply your own branding and customization, learn more about it TagoRun - Branding and Deploying Applications - TagoIO.
- **Access Policies:** Access policies is a very important feature related to what users can see and access in your application. If you plan to modify that, you need to understand how this feature works: Defining Permissions - TagoIO.

Components

The following table contains all the components that must be imported to your account in order to run the application.

When looking at components, you will notice dashboard names in keywords. That is a feature from **Dictionary** of TagoIO, that we will explain better in the next section.

Resource type	Name	Description
Dashboard	#ADM.ADMIN#	Dashboard accessible to application admins to be able to create organizations.
Dashboard	#SEL.SENSOR_LIST#	Dashboard accessible by all users to see the sensor list of the application for a given organization.
Dashboard	#USERS.USERS#	Dashboard accessible by application admin and organization admin, that give access to user management of an organization.
Dashboard	#RPT.REPORT#	Dashboard accessible by all users to manage scheduled reports.
Dashboard	#ALC.ALERT_CENTRAL#	Dashboard accessible by all users to manage alerts of the application.
Dashboard	#GRO.GROUPS#	Dashboard accessible by all users to manage a group of devices.
Dashboard	#IMG.GROUP_VIEW#	Dashboard accessible by all users to view detailed information about a group of devices.
Dashboard	#HTD.HUMIDITY_TEMPERATURE_SENSOR_DASHBOARD#	Dashboard of a specific device type, in this case an example for the Browan Humidity/Temperature sensor.
Action (Schedule)	Data Retention Trigger	Action to trigger the Analysis Data Retention. Recommended to set to run each day.
Action (Schedule)	Device Status Updater	Action to trigger the analysis Device Status Updater. Recommended to set to run each minute.
Action (Variable)	Sensor Uplink Status	Action to trigger analysis Uplink Handler. Recommended to set to trigger on the **payload** variable.
Action (Variable)	Customer Alert	Automatically generated action to manage customer alerts, created from the Alert Central dashboard.
Access (Rule)	All	Give access to users on devices by matching tags org_id, user_org_id and site_id.
Access (Rule)	Admin	If a user has the tag **access** with value **admin**, it must have access to the entire application.

Access (Rule)	Guest	Give access to **device settings** and dashboards with **access tag** and **guest value**.
Access (Rule)	Organization Admin	Give access to **device settings** and dashboards with **access tag** and **orgadmin Value**
Device	Settings (Don't Remove)	Store common data of the application, used by all dashboards and users. Usually it is a HTTPS device without a decoder.
RUN (Email Template)	email_alert	Email template for alerts created by users.
RUN (Email Template)	checkin_alert	Email template for missed check in alerts of the application.
RUN (Email Template)	Password Recovery	Email template for when users try to recover their password.
RUN (Email Template)	user_register	Email template for when a new user is registered to the application.
Run (Sidebar)	Run Buttons	Run Buttons are expected for the user navigation between dashboards. If your dashboard is showing as a list for the user, make sure you set the configuration visible to false, option available on the "**more"** field of the dashboard. Some Run Buttons do have visibility options set, to only show up for users with specific levels of access.
Dictionary	Dictionary	Dictionary is available for multi-language support. You will notice dashboards and label fields with keys from Dictionary in all dashboards and scripts.

Application functionalities

This section will describe the main features of the application and which resource of TagoIO is being used.

1. Plan Management

In order to create Organizations, you must have at least one plan in the application.

Plans allows you to set up email, sms and data retention limits for a specific organization.
The Organization device, explained in the next section, will contain the name of the plan in its tags.

Tag Key	Tag Value	Description
plan	`Plan Name`	Tell analysis which plan the organization is using.

The following variables are also created in the settings device, in order to store the plan information and display on the Dynamic Table widget of the Plan Management dashboard.

Device	Variable	Description
Settings Device	plan_data	Value is the plan name and metadata parameter contains the email and sms limits.
Settings Device	plan_email_limit	Email limit to display in the Dynamic Table and enable editing feature. There is no other use.
Settings Device	plan_sms_limit	SMS limit to display in the Dynamic Table and enable editing feature. There is no other use.

Analysis are responsible for getting the Plan information and applying the defined limits.

2. Organization Management

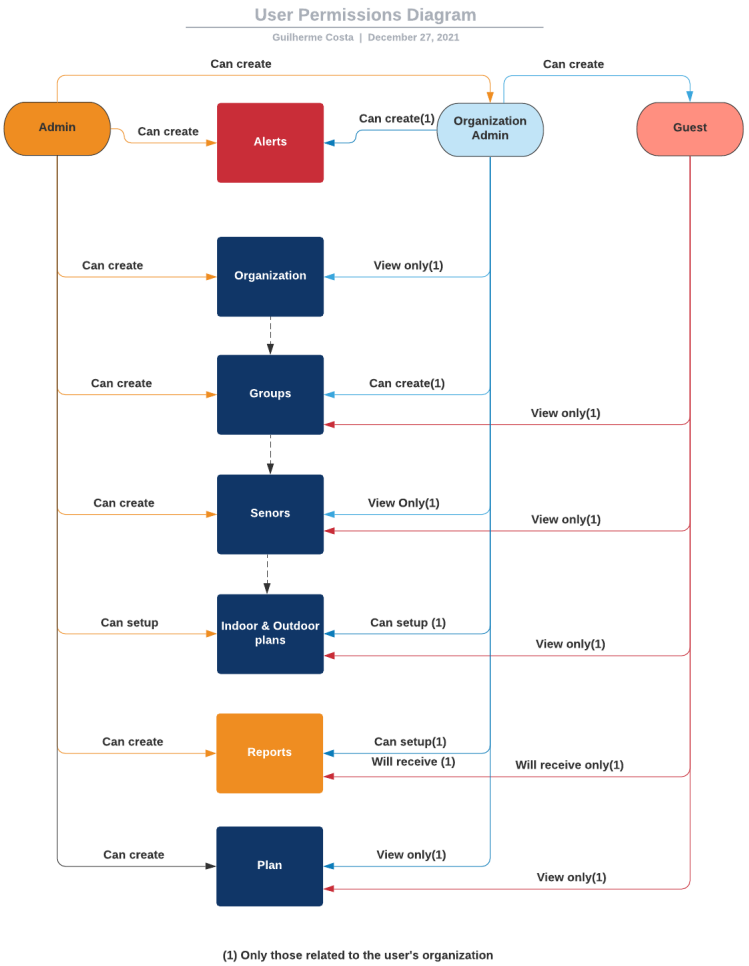
In order to use any functionality of the application, you must have an Organization.
Only administrators can create an organization.
If you do have Sign Up enabled, an organization will be created automatically when users register themselves in the application.

Organization ID

When Organizations are created, you will also have one **device** created for each one of them. This is a dummy device, created to store data specific to that organization, and also to set up Blueprint Dashboards to work with filtering options.

Through the application, you will also see the tag **organization_id**, which value is the ID of the mentioned organization device.

3. Access management



The access management makes use of both **Tags** on dashboards and devices, and the **Access Rules** of TagoIO, in order to provide which user has access to what.

You will find three types of users available for the Kickstarter application

- **Application Administrator**
  This role does have full access to the entire application and all organizations within. It can manage Plans and change the plans of the organizations. It's made for the owner of the application to use it without accessing the developer's account.

- **Organization Administrator**
  With this role, the user is able to access only your organization, add sensors, group the sensors, manage users, alerts and reports.

- **End User**
  The End User is a view-only role, which doesn't have write access to any of the resources of the application. With this role, the user is able to view sensors details, groupings and alerts, but can't create, edit or delete them.

The following tags are used for devices:

Tag Key	Tag Value	Description
access	admin	Give access to all dashboards and devices of the application.
organization_id	Organization Device ID	GIve access to the devices of an organization.
org_user_id	Organization Device ID	Give access to the devices of an organization, for guest users.
site_id	Group ID	Give access to devices inside of a group.

Dashboards that you plan to add to the application, or even if you want to change existing dashboards, must have the following tags:

Tag Key	Tag Value	Description
access	**admin** / **orgadmin** / **guest**	Allow users of specific level to be allowed to access the dashboard. You can have multiple tags of access with different values.

Devices that you plan to add to the application, or event if you want to change existing devices, must have the following tags:

Tag Key	Tag Value	Description
organization_id	Organization Device ID	Allow orgadmins to have access to the device. Also tell analysis that the device is related to the specified organization.
org_user_id	Organization Device ID	Allow guests to have access to the device.
site_id	Group ID	Relates the device with a group.

4. Alert Management

Alerts in the application make use of two analyses: Alert Handler and Alert Trigger.

It is also dependent on a dummy device, in the case of this application we use the **Organization Device** to store information regarding the alerts created, and it is also needed for the Dynamic Table in the Alert Management dashboard.

When anyone creates an alert using the application, the analysis actually creates an Action for the alert. The action contains all the rules needed, including **Action Unlock** trigger.

The script setup Tags in the action created as well, containing important information:

Tag Key	Tag Value	Description
organization_id	Organization Device ID	Organization which the alert belongs to
site_id	Group ID	Group the alert belongs to, if it is a Group Alert.
send_to	User Ids (comma separated)	ID of users that must receive the notification if the action triggers.
action_type	notification_run,email,sms	Alert types selected by the user when the alert was created.
device_id	Device ID	One or more pair of this tag for each device that trigger this action.

5. Sensor List

The Sensor List, or summary of sensors, is an important dashboard where users can see all their devices inside the Organization.

As mentioned before the dashboard uses the Device List widget, and the application uses two layers to setup the devices that show up in the list:

- Devices are filtered by the Access Rules being applied to the user. Which means that users can't see any device that isn't covered by their Access Policies.
- The Device List widget filtering rules. Which you can see by editing the widget in the dashboard.

As expected, the Application does take care of all the tags and access policies for us, but this is important information if you plan to change the dashboard or which device users can see.

Device Summary Columns

The Application uses the columns to display a summary of information about the devices, such as *Battery level* and *Last Check In* information, you will notice that all this information comes from the **Configuration Parameter** of the device.

In order for that information to be available in the Configuration Parameter, the application uses an Analysis called **Device Updater**, which is responsible for reading the last information sent by each device, and updating the information in the Configuration Parameters. Which means if you want to have additional columns, you need to update the mentioned script to include new parameters.

6. Groups of Sensors

In order to group sensors we took a very straightforward approach that also give us a lot of freedom when adding new features that do make use of this feature.

First you create a group, and the application creates a **Group Device** - HTTPs, no decoder - and uses the Device ID as an Identifier for the group. The device created is important, cause when grouping data from different sensors we will need to store it in there.

Group ID

Second, when you attach devices to the group, what the application does is add a new tag to the device:

Tag Key	Tag Value	Description
group_id	Group Device ID	Group which the device is included to.

The **group_id** Tag is used on:

- Access Rules, when we want to filter the devices the users have access based on a Group.
- Analysis, when it needs to take action in all devices of a Group, it filters the devices using the group_id tag.
- Since the value of group_id is the device ID of the group, we can easily use it to find the Device of the group in any situation.

7. Reports

In order to change reports you will need to know, at least, HTML and Javascript code languages, as any change to the report is very dependent on those skills.

The reports are generated by an Analysis. The code can use an HTML file and replace keywords inside the file, or in some cases the Analysis will generate an entire HTML file, as it happens for most tables. The good part is that you can actually use Javascript libraries to generate charts and graphs.

Developer - Administrator User

You will need to manually create users that you expect to have administrator access, which means, full access to all functionalities of the application and all organizations.

If you just set up the application now, you may want to create an Administrator user to start using it.

1. Adding Administrators

Take the following steps if you want to add an administrator to the application.

- Access your developer account at https://admin.tago.io
- Click on the **Users** button.
- Press **+ Add user** button.
- Fill up all fields accordingly.
- Go to the **Tags** tab.
- Add the tag key **access** with value **admin**.
- Create the user. It should have full access to the application.

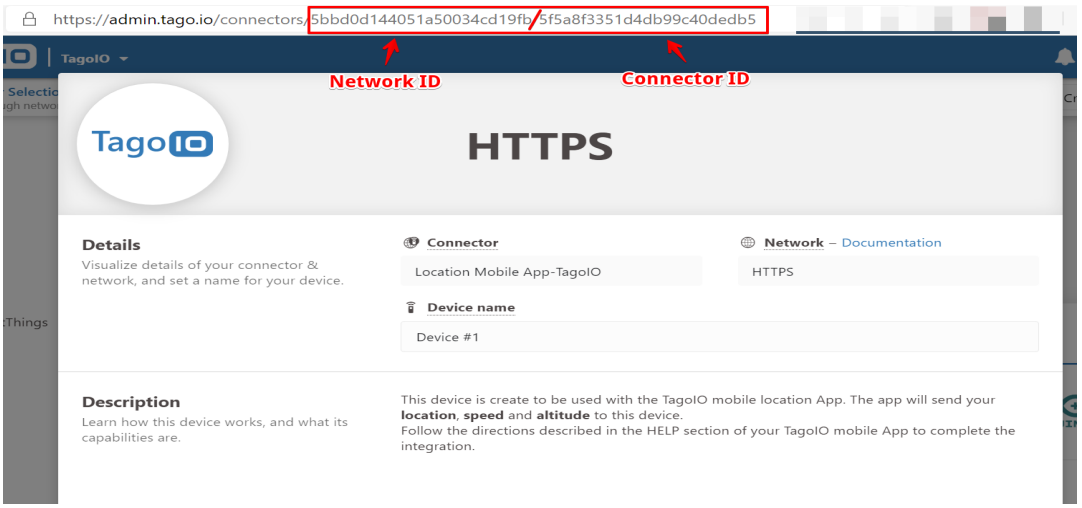
Developer - Sensor Support

There are two main steps you are required to do when adding support in the application for a new sensor. You need to create a dashboard for the sensor, and also to add the connector ID to the Input form in the dashboard for creating new sensors.

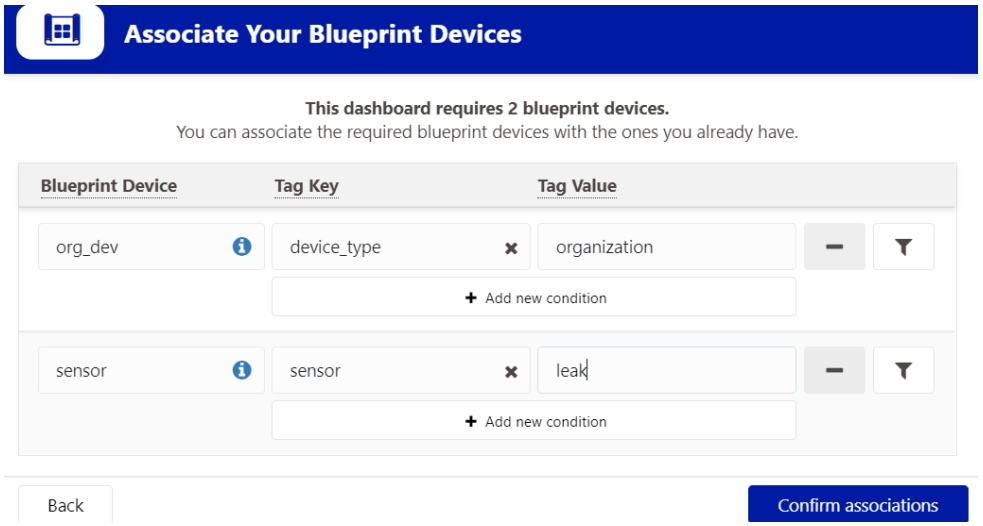
1. Adding new sensor dashboard

Take this step first to create the dashboard for the sensor you're adding to the application.

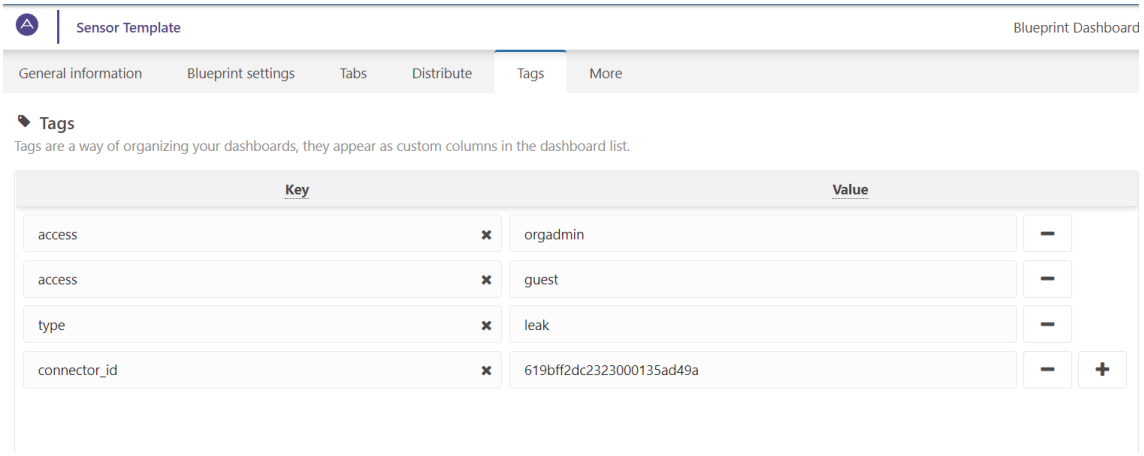
- Get the Connector ID. You can do that by going to Devices > + Add Device, in your developer account. By selecting the network and the sensor you want to add, you should notice the ID of the connector in the TagoIO URL:



- Install the dashboard template from the link: https://admin.tago.io/template/619bffeb706f560011d8dbf9. It will have all the tags and blueprint settings you need for the sensor.
- When adding the template, enter a **Type** for your sensor, it can be any name of your choice, just make sure it is unique within the application. An example is **water leak** for leak sensors.



- Make sure you have the following tags in your dashboard. Enter the edit mode of the sensor and press the engine icon to access the Tags. You should have something like this:
  - **Tag key:** access; **Tag Value:** orgadmin
  - **Tag key:** access; **Tag Value:** guest
  - **Tag key:** connector_id; **Tag Value:** type the connector ID you copied in the first step.

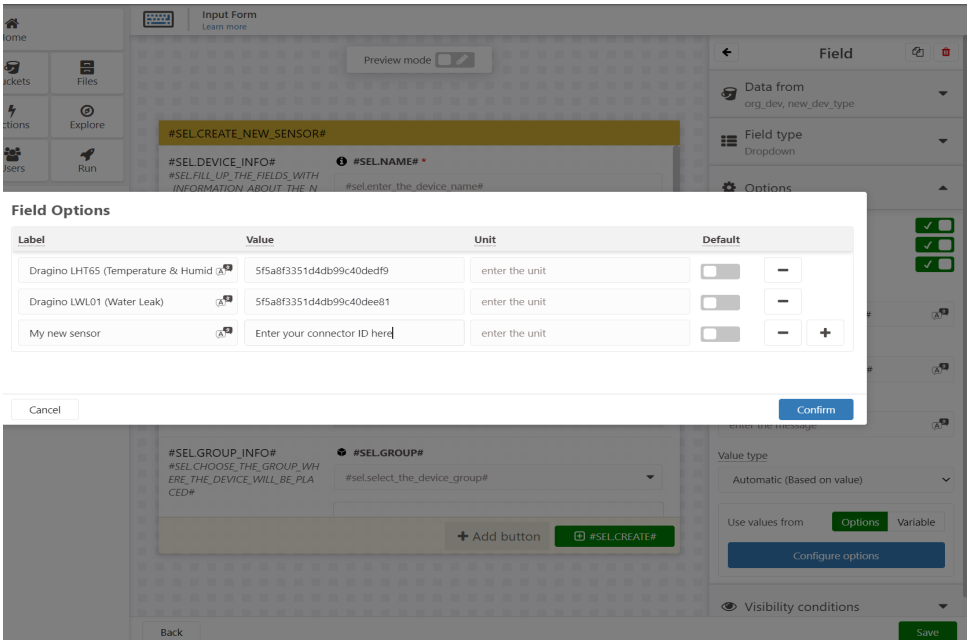


- Add and edit widgets. Make sure you select the **sensor** BP device on the widgets. The template already has some widgets that you can easily edit. If you see any name with #, it is a keyword from the dictionary of your account. You can freely erase it if needed, or add it to your dictionary for multi-language support.
- Still inside the dashboard configuration, click in the **More** table and turn off the visible switch, so it will not show up the dashboard constantly in the sidebar for the users.

2. Adding new sensor to Input Form

This is the second step that will make the sensor available to select when creating a new sensor through the Sensor Input Form dashboard.

- Access your dashboard list by accessing: https://admin.tago.io/dashboards.
- Access the dashboard with name **#SEL.SENSOR_LIST#**, which should contain the button to add a sensor to the application.
- Enter the edit mode by clicking in the pencil in the top corner of the dashboard.
- Go to the **Hidden** named tab that will show up when you enter the edit mode.
- You should now see the widget from the Input Form. Click in the three dots of the widget and then **Edit.**
- Click in the **#SEL.TYPE#** field to start editing it, then click in the **Configure Options** that will show up in the left sidebar.
- Now you should see all the sensors supported by the application. Press the **+** button to add a new entry, then enter a name for your sensor and the value must be the **Connector ID**. If you don't have it, check the previous section to see how to get the ID.



- Press Save and you're done.

Developer - Adding new alerts

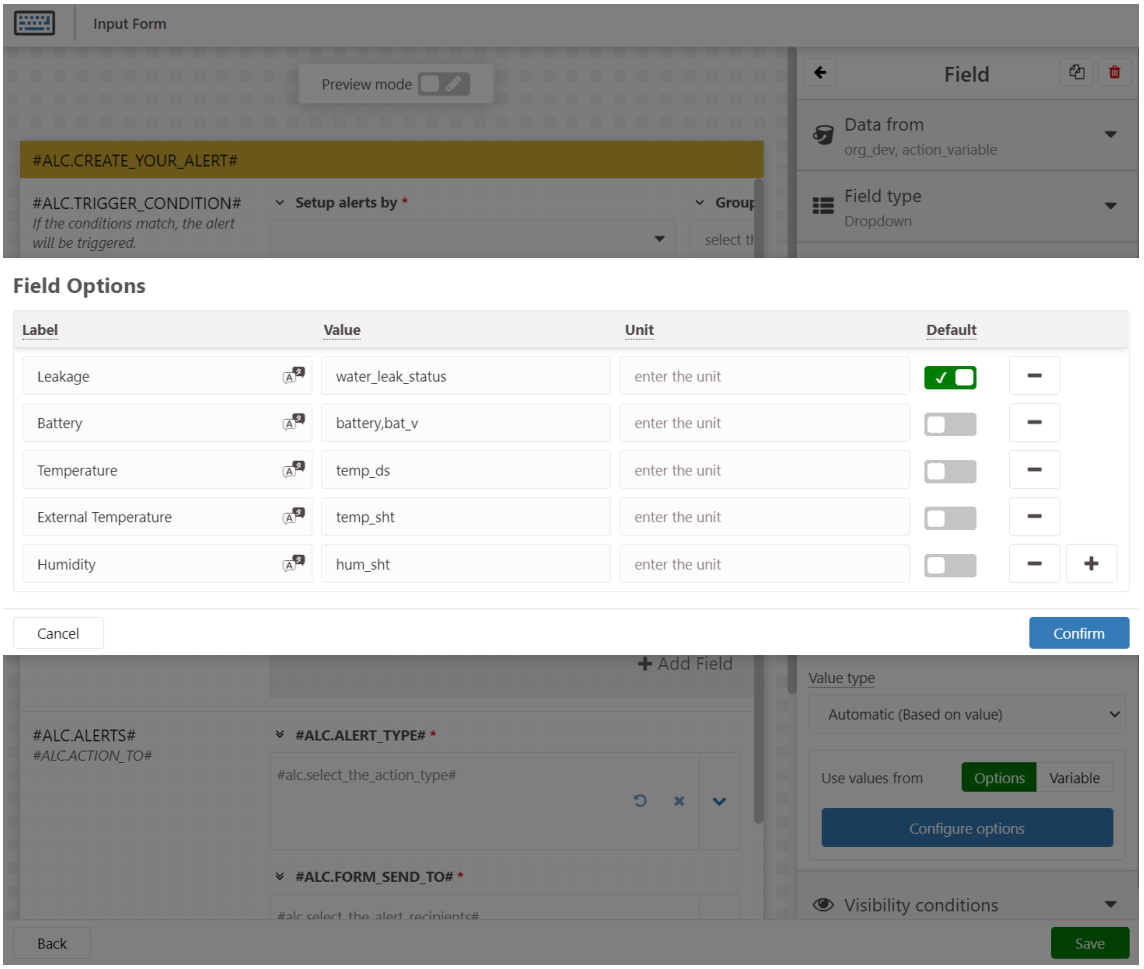
The goal of this section of the documentation is to describe how to change the alerts behaviour in the application.

1. Add/Edit variables options for alerts.

- Access your dashboard list by accessing: https://admin.tago.io/dashboards.
- Access the dashboard with name **#ALC.ALERT_CENTRAL#**, which is the dashboard with all the alerts.
- Enter the edit mode by clicking in the pencil in the top corner of the dashboard.
- Go to the **Hidden** named tab that will show up when you enter the edit mode.
- You should now see the widget from the Input Form. Click in the three dots of the widget and then **Edit.**
- Click in the **#SEL.TYPE#** or **Type** field to start editing it, then click in the **Configure Options** that will show up in the left sidebar.
- Press the **+** Button and add a label and the variable of your sensor that you want the alert to work with.

You can check all the variables available in your sensor if you add one to the application and go to the Device's Bucket through the developer's account.

- Press save.
- Now you must repeat the same steps for the List in the **List** tab. Edit the widgets, click in the variable column - usually the second one -,, go to **Edit Options** and then **Configure Options** and add the variables.



2. Add different alerts behaviours

If there is a need to add an additional way to set up alerts, that can be only done by editing the source code of the application, so there is no way to provide documentation here.

Please take the in-code documentation available inside the code of alerts in order to get orientations on how to change the existing alerts behaviour.

Developer - Adding new type of user

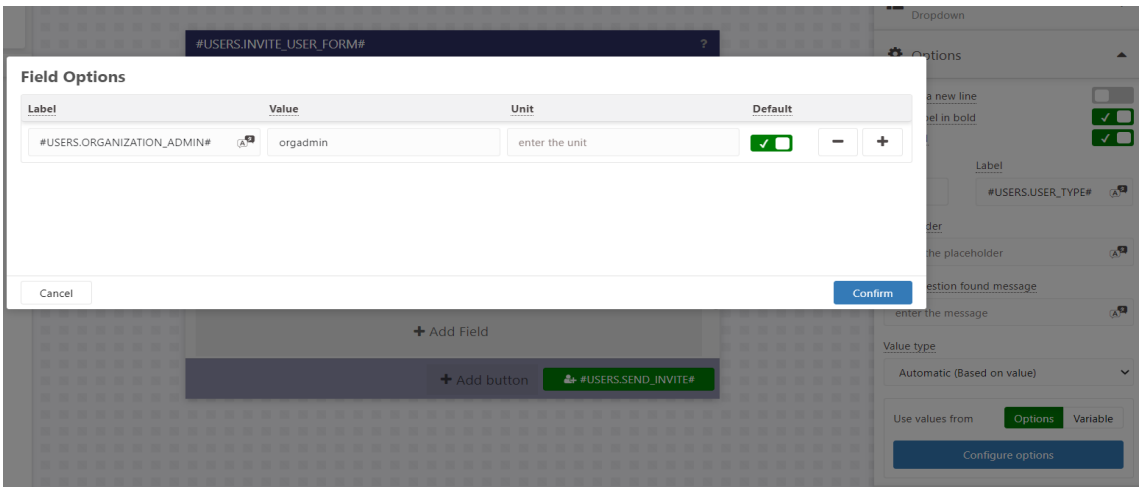
Actually, there aren't any scripts that are dependent on the user access level. The way we set the user access management in this application is by just giving them access to a dashboard and device or not.

That said, you can play around with new types of users as much as you want by just changing the **Access** policies of your developer's account. If you go there now, you should notice the **All Users access policy**, which automatically gives correct access by using **tag match** with the **access** tag.

Other tags are used in order to give access to devices. For this architecture, we give access to all devices to an user of the application. The reason is that there is no API route from TagoIO that allows an user to use a device if it's not being used by a dashboard. But you can add more security layers if you want to.

If you need a step by step:

1. Go to your dashboard list by accessing https://admin.tago.io/dashboards
2. Access the #USERS.USERS# dashboard.
3. Click on the pencil button to start editing the dashboard.
4. Go to the **Hidden** tab and edit the Input widget with title **Invite User**.
5. Click in the **#USERS.USER_TYPE#** field.
6. Click in the **Configure Options** in the sidebar.
7. Press the **+** button and enter a Label name for the user, and a value to be used in the **access** tag.
8. **Confirm** and **Save** your changes.



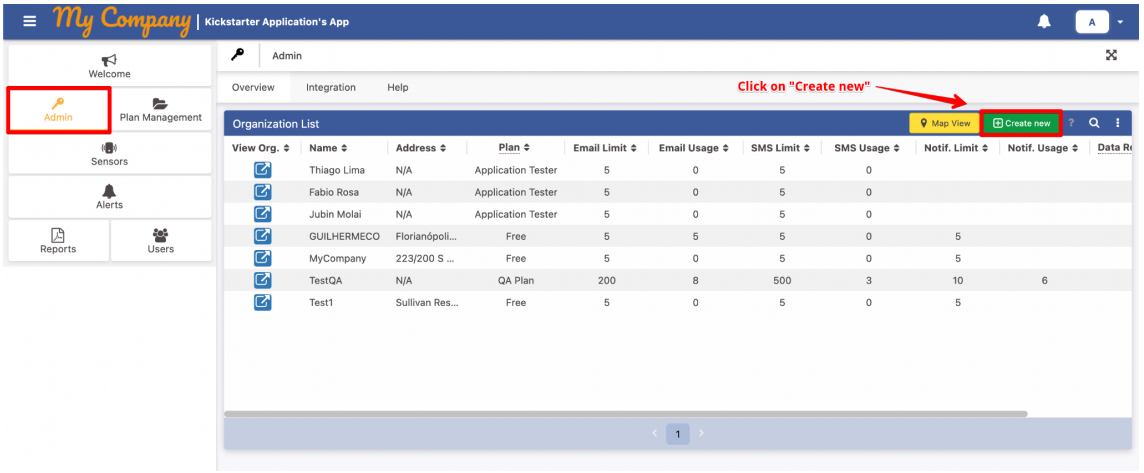
9. Go to the dashboards you want this type of user to have access to, and add a new tag **access** with the same value you entered in the previous steps.
10. Go to **RUN** then **Sidebar** and add the same tags to the visibility of the buttons that already exist for the dashboards you want them to see the buttons.

Application Administrator – Basic walk-through

This is a basic walkthrough to using the application as an administrator. Most dashboards do have a **Help** tab available explaining its functionality.

1. Grant access to a new end user

- At the “Admin” landing view page, click on “Create new” at the “Organization List” table.



- Fill in the required information.
- After creating an organization, an authorization token will be generated.
- You will now need to invite a user and address to that organization. Click the “Users” button on the sidebar, at “Users List” table click “Invite User”.
- Fill in the required information.
- An email should be sent to the user’s email with an invitation. That invitation will include the application’s URL and their new access credentials.

2. Removing an Organization and all its users.

Warning: all user’s data will be lost, including (user’s credentials, groups and sensors)

- At the “Admin” landing view page, at the “Organization List” table, find the organization which you wish to remove.
- Click on the red bin icon.

- After confirming, all data related to the user will be deleted.

3. Creating sensors to an end user

- In order to create a new sensor, an end user organization should be created. If the end user doesn't have an organization see "1. Grant access to a new end user".
- Click the "Sensors" button on the sidebar.
- At "Sensor List table", click "Create new".
- Fill in the required information.
- After creating, the sensor should be able to receive information. (Make sure the user's authorization token is set correctly at the network service).