Qeedji

User manual

SMT210

4.13.13 002G

Legal notice

SMT210 4.13.13 (002G_en)

Rights and Responsibilities

Product information

Product design and specifications are subject to change at any time and `Qeedji` reserves the right to modify them without notice. This includes the hardware, the embedded software and this manual, which should be considered as a general guide to the product. The accessories supplied with the product may differ slightly from those described in this manual, depending on the developments of the various suppliers.

Precautions for use

Please read and heed the following warnings before turning on the power: - installation and maintenance must be carried out by professionals. - do not use the device near water. - do not place anything on top of the device, including liquids (beverages) or flammable materials (fabrics, paper). - do not expose the device to direct sunlight, near a heat source, or in a place susceptible to dust, vibration or shock.

Warranty clauses

The `Qeedji` device is guaranteed against material and manufacturing defects for a certain duration. Check the device warranty duration value at the end of the document. These warranty conditions do not apply if the failure is the result of improper use of the device, inappropriate maintenance, unauthorized modification, operation in an unspecified environment (see operating precautions at the beginning of the manual) or if the device has been damaged by shock or fall, incorrect operation, improper connection, lightning, insufficient protection against heat, humidity or frost.

WEEE Directive

This symbol means that your appliance at the end of its service life must not be disposed of with household waste, but must be taken to a collection point for waste electrical and electronic equipment or returned to your dealer. Your action will protect the environment. In this context, a collection and recycling system has been set up by the European Union.

Table of contents

Part I

Description and installation

1.1 Introduction

This manual explains how to install and configure your SMT210 device.

Recommendations and warnings

This device is designed to be used indoor.

This device is intended to work with the power supply unit. This power supply unit must be connected to a mains socket conforming to standard NF C 15-100. If the AC power cable is damaged, it must be replaced. It is possible to order a power supply unit replacement by sending a request to the email address sales@qeedji.tech.

This device is a Class A device. In a residential environment, this device may cause radio interference. In this case, the user is asked to take appropriate measures.

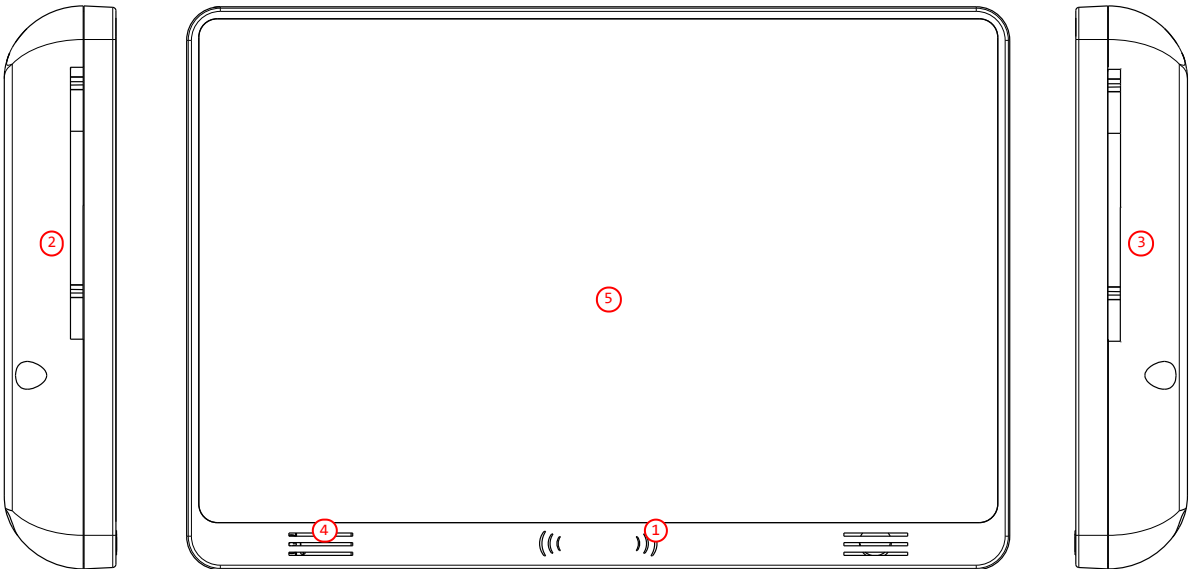
When powering the device from a PoE source, this PoE source must be "Limited Power Source" as defined in EN60950-1: 2006.

Content of the package

Items	Description	Quantity
Device	SMT210 device with Gekkota embedded.	1
Power supply unit	12 V power supply unit with cable of 1.2 m.	1
Labels	One on the cardboard packaging and another one at the back of the product. *Additional label can be present in case build-in options.*	2

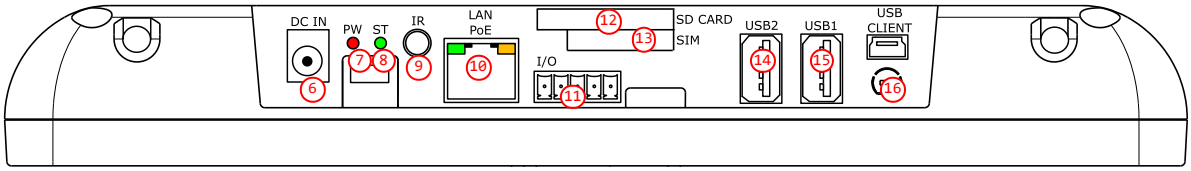
1.2 Getting started with the device

Front face and side face



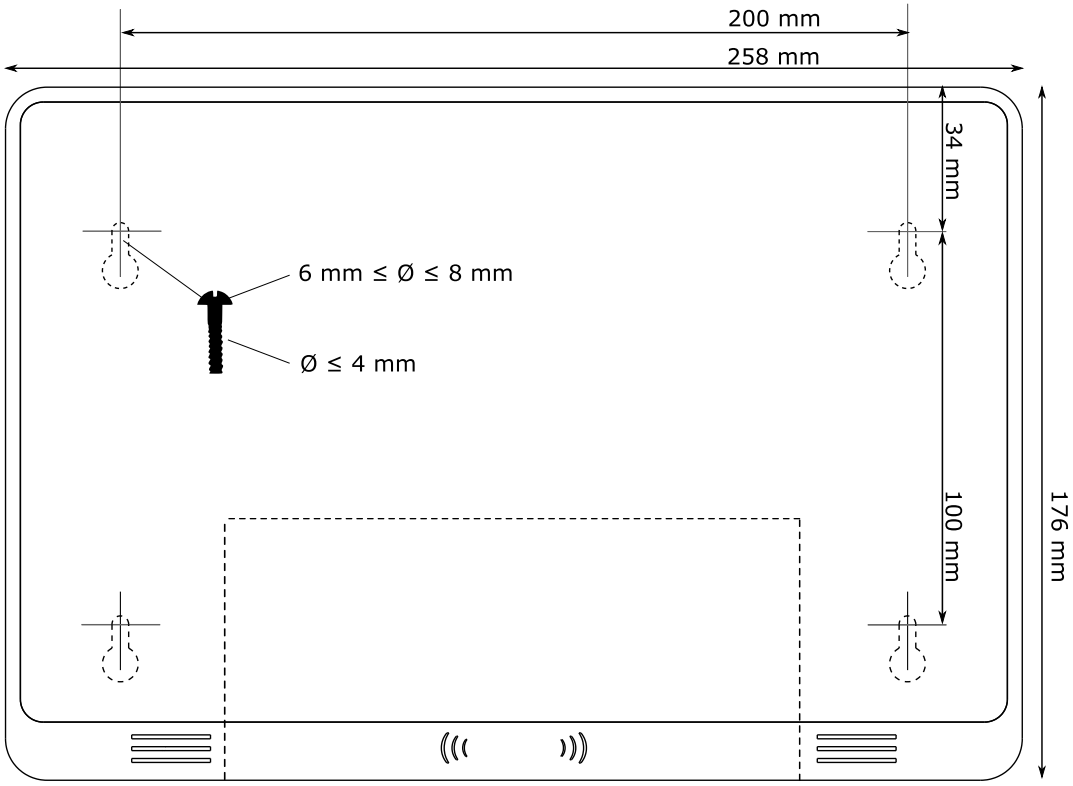
- (1) RFID tag sensor,
- (2) Left side LED,
- (3) Right side LED,
- (4) Built-in speaker,
- (5) Touch screen.

Bottom face

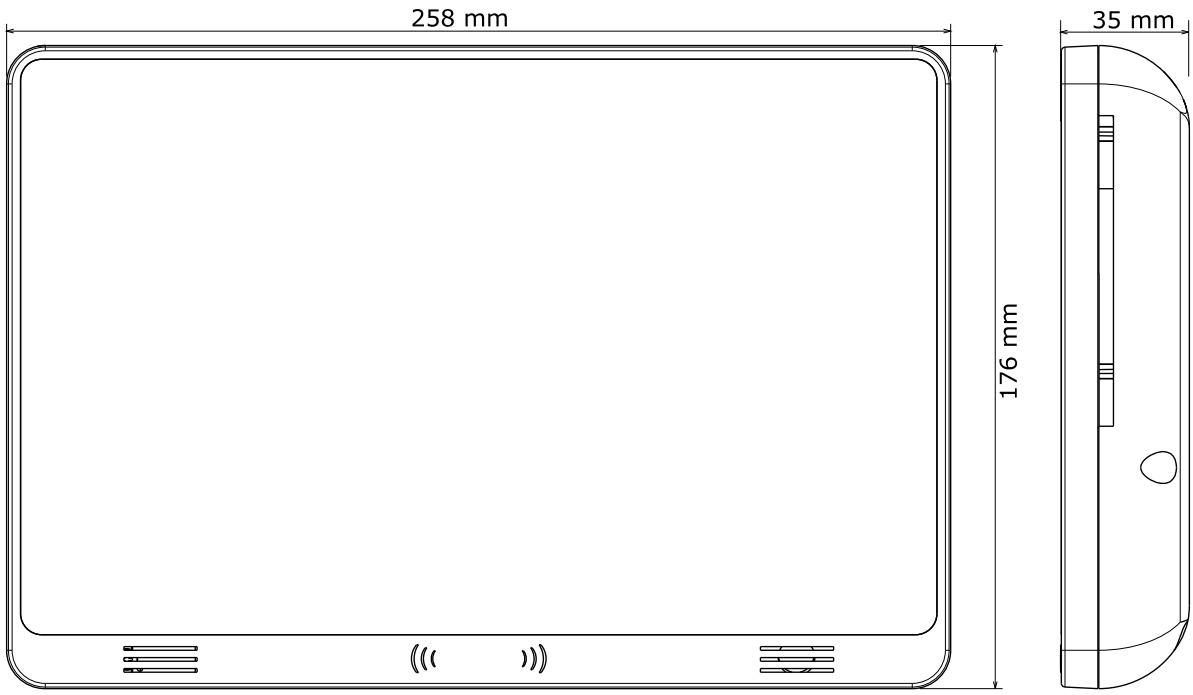


- (6) Power supply connector,
- (7) Power supply red LED,
- (8) Status green LED,
- (9) Jack 3.5 mm GPIO connector,
- (10) RJ45 LAN PoE connector,
- (11) Phoenix GPIO connector,
- (12) SD card connector,
- (13) SIM card (WWAN option) connector,
- (14) USB2 2.0 connector,
- (15) USB1 2.0 connector,
- (16) WWAN antenna location.

1.2.1 Device fixture



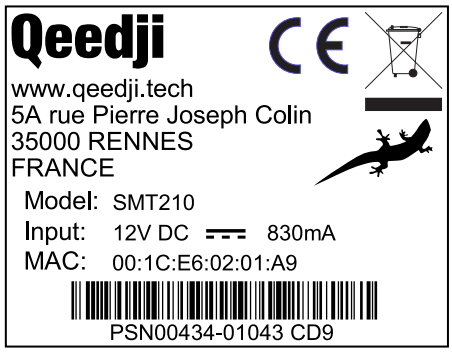
1.2.2 Device dimensions



1.2.3 Labelling

Product label

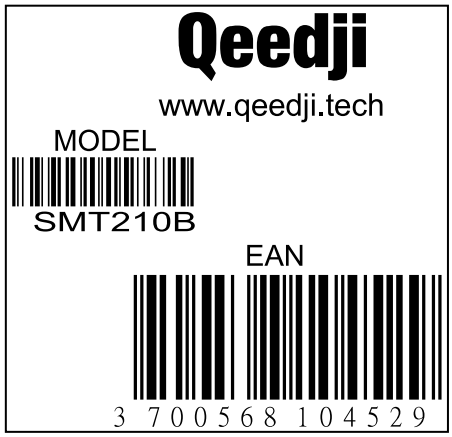
The model of the device, the power supply characteristics, the serial number (PSN) and the MAC address are written on a label stuck on the case.



Packingbox label

This is the label stuck also on the packingbox. It is showing information on:

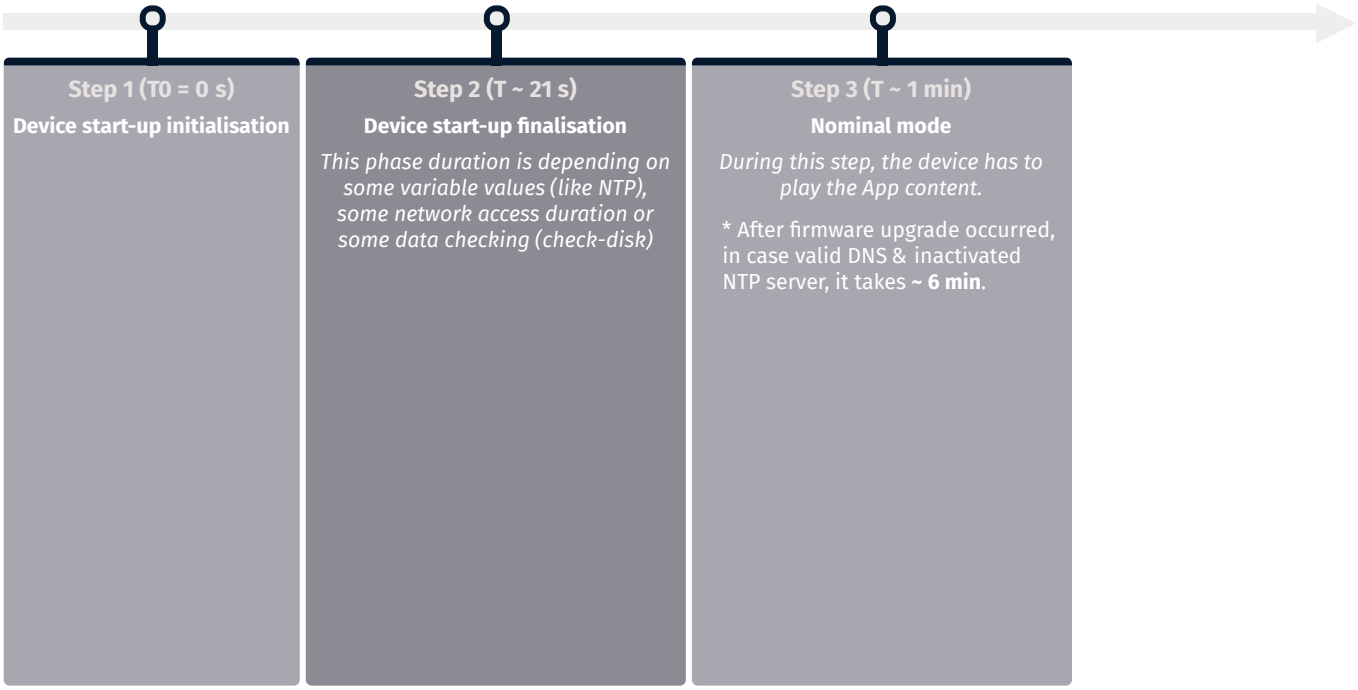
- the device model,
- the serial number (PSN).



Some additional labels may be present in case of built-in options.

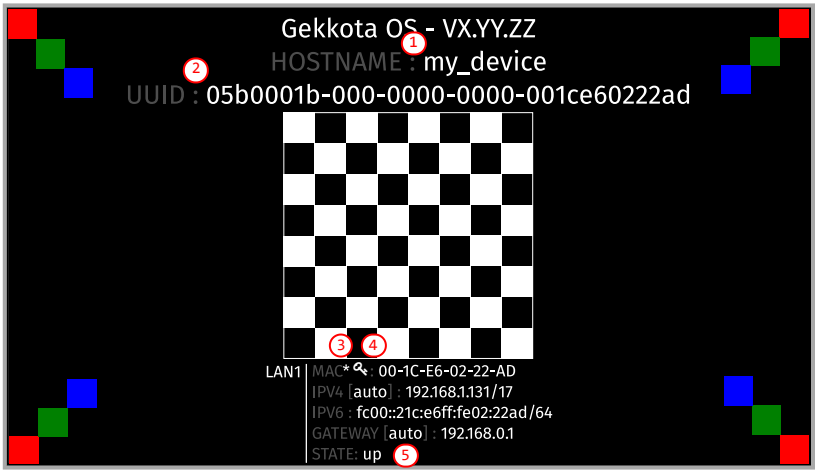
☛ *The serial number of the device could be requested in case of technical support.*

1.2.4 Device start-up step



1.2.5 Test card

At the factory, the device content set by default is the `Test Card`. The chart displays important information to assist in the device configuration:



> ☛ *The `*` star pictogram is showing the chosen identification method in the device. It can be `HOSTNAME` (1), `UUID` (2) or `MAC` (3). In the example, the star is showing the `MAC` identification method (default value).*
>
> ☛ *The key pictogram (4) is showing the MAC address value associated to the Gekkota license key.*
>
> ☛ *The `up` STATE (5) is meaning that the network interface currently showed is alive. If the STATE is `down`, the network interface is not alive.*

The `Test Card` can be inactivated by using the `Administration console` user interface.

1.3 LEDs behaviour

LED POWER behaviour (power on device)

State	Information
Red	**OK: Power supplied**
Off	**Error: Power supply issue** [1]

LED LAN behaviour (power on device)

State	Information
Off	There is no network traffic on the Ethernet connector.
Blinking	The blinking frequency is indicating the data rate on Ethernet connector.

LED STATUS behaviour depending on device start-up steps

• Step 1: Device start-up initialisation

State	Information
Green: continuous	**OK**
Always Off	**Error: Power supply issue** [1]

• Step 2: Device start-up finalisation

State	Information
Off	**OK**. This step duration can be from several seconds to several minutes.
Green blinking: 1 second duration flash and periodicity every 2 seconds	**Error: Boot issue** [1]

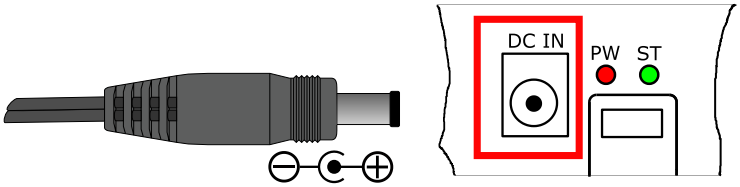
- **Step 3: Nominal mode**

State	Information
Green blinking: **1** very short flash (300 ms) spaced 4 seconds apart	**OK**
Green blinking: **2** very short and consecutive flashs (300 ms), spaced 4 seconds apart	**Warning: Fail Soft Mode Level 1** Frequent device reboot detected (for example 4 times in less than ½ hour) Message is displayed on screen «Fail Soft Mode: waiting for new content ». The instability has been caused probably by a content media not supported yet by system. Consequently, to prevent any further reboot, the content has been invalided. The message displayed on screen indicates that a new publication is needed to go ahead. [2]
Green blinking: **3** very short and consecutive flashs (300 ms) spaced 4 seconds apart	**Warning: Fail Soft Mode Level 2** Frequent device reboot detected (for example 4 times in less than ½ hour) Content is purged Message is displayed on screen «Fail Soft Mode: waiting for new content ». The instability has been caused probably by a content not supported yet by system or one user preference which has been modified. Consequently, to prevent any further reboot, the content has been invalidated and user preferences (saved before unexpected reboot) have been restored. The message displayed on screen indicates that a new publication is needed to go ahead. [2]
Green blinking: **4** very short and consecutive flashs (300 ms) spaced 4 seconds apart	**Warning: Check disk** The device has detected memory corruption on content storage. The media storage is being repaired. This repair step is called Check-Disk and its duration can be several minutes. During this step, a message “checking the file system of data partition in progress” is displayed on screen. [3]
Green blinking: **5** very short and consecutive flashs (300 ms) spaced 4 seconds apart	**Warning: errors on system partition** The user has to connect to device Web user interface, go to *Maintenance > Tools* menu, and click on the *Format* or *Repair* button to solve the problem. [3]
Green blinking: **6** very short and consecutive flashs (300 ms) spaced 4 seconds apart	**Warning: a firmware upgrade is pending** During this phase, no content is played on the device, **do not switch OFF the device.**
Green blinking: **7** very short and consecutive flashs (300 ms) spaced 4 seconds apart	**Error: write problem on the storage** For an unknown reason, your storage space isn't usable any more. [3]
Off	**Error**. [1]

[1] If the problem persists in despite of an appropriate power-supply, contact support@qeedji.tech.
[2] If the problem persists, it is recommended to find out the media not supported yet by the system and remove it from content.
[3] If the problem persists after a partition repairing, contact support@qeedji.tech.

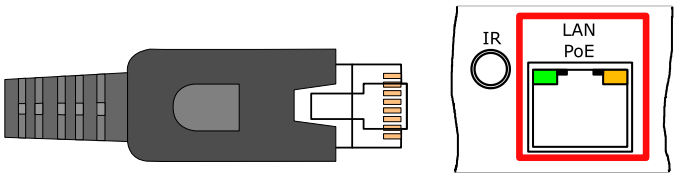
1.4 Connectors

Power supply connector (12 V DC - 1.2 A)

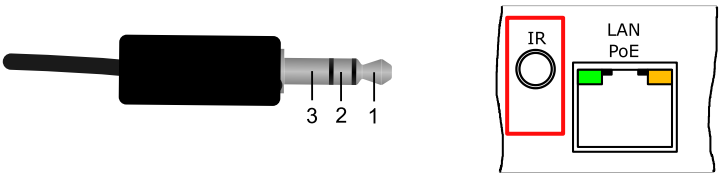


LAN connector

Ethernet RJ-45. 10/100 BaseT. It is recommended to use schielded calbe.



Jack 3.5 mm connector (GPIO4)



N°	Name	Write/ Read	Control
1	Voltage reference 3.3 V		
2	GPIO4	IN ou OUT	CPU/GPIO4
3	Ground		

GPIO4 Electrical features

	Vin min	Vin max	VOH min	VOH max	IOH max	VOL max	IOL max	VIH min	VIL max
GPIO4	-0.5 V	3.8 V	3.1 V (-20 µA)	5 V	-100 µA	0.6 V (2 mA)	5 mA	2.35 V	0.8 V

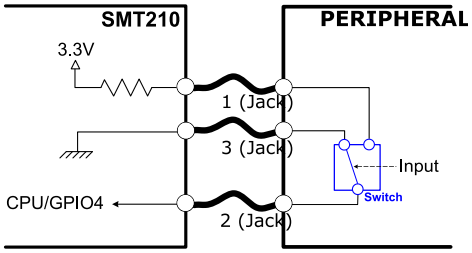
The pin 3.3 V must not be used as a power supply, but rather for voltage reference. A fuse (350 mA @ 20 °C) allows to cut the power in case current is more than 350 mA. Then the fuse can be manually re-armed. During board (re)starting, the defaut level for GPIO4 is 3.3 V

The GPIO4 has:

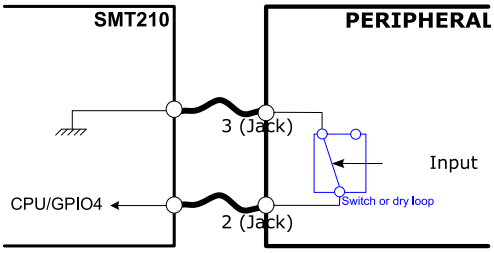
- one 4.7 KOhms pull-up to 3.3 V,
- one 182 KOhms pull-down to 0 V.

Principle schematics of several use case

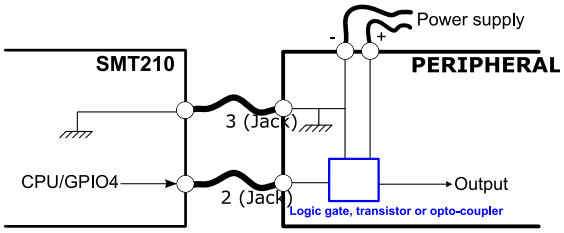
Three wires input configuration for GPIO4:



Two wires configuration for GPIO4:



Output configuration for GPIO4:



Jack 3.5 mm GPIO4 configuration

The GPIO configuration des GPIOs can be realized by editing some user preferences in the `Administration console` user interface or thanks to a configuration script.

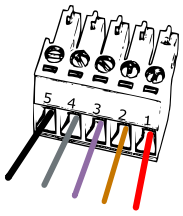
How to configure the Jack 3.5 mm connector:

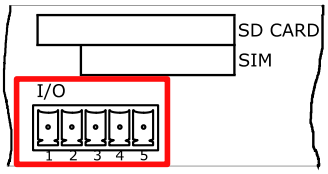
```
//Set Jack 3.5 mm mode infrared
if (aDirection == "disable")
{
    Services.prefs.setBoolPref("system.connector.jack35_1.1.io.uart_1.enabled", true);
}
else //Set Jack 3.5 mm mode GPIO
{
    Services.prefs.setBoolPref("system.connector.jack35_1.1.io.uart_1.enabled", false);
}

// Set the Jack 3.5 mm direction: input or output
if (aDirection == "out")
{
    Services.prefs.setBoolPref("innes.app-profile.gpio-input.jack35-gpio_1.jack35_1.*.authorized", false);
    Services.prefs.setBoolPref("innes.app-profile.gpio-output.jack35-gpio_1.jack35_1.*.authorized", true);
    Services.prefs.setBoolPref("system.connector.jack35_1.1.io.jack35-gpio_1.enabled", true);
}
else if (aDirection == "in")
{
    Services.prefs.setBoolPref("innes.app-profile.gpio-input.jack35-gpio_1.jack35_1.*.authorized", true);
    Services.prefs.setBoolPref("innes.app-profile.gpio-output.jack35-gpio_1.jack35_1.*.authorized", false);
    Services.prefs.setBoolPref("system.connector.jack35_1.1.io.jack35-gpio_1.enabled", true);
}
else if (aDirection == "disable")
{
    Services.prefs.setBoolPref("innes.app-profile.gpio-input.jack35-gpio_1.jack35_1.*.authorized", false);
    Services.prefs.setBoolPref("innes.app-profile.gpio-output.jack35-gpio_1.jack35_1.*.authorized", false);
    Services.prefs.setBoolPref("system.connector.jack35_1.1.io.jack35-gpio_1.enabled", false);
}
```

Phoenix connector

The Phoenix connector has 2 functions:

- the capability to drive with the GPIO1 an internal relay, allowing for example to open or close an electric door,
- the capability to drive a peripheral or get the state of another peripheral thank to the GPIO2 and GPIO3.





PIN N°	Name	Write/Read	Driving
1	Internal relay PIN1	OUT	CPU/GPIO1
2	Internal relay PIN2	OUT	CPU/GPIO1
3	GPIO2	IN or OUT	CPU/GPIO2
4	GPIO3	IN or OUT	CPU/GPIO3
5	Ground		

In case purchasing a male connector suitable for the peripheral, contact the provider WURTH and order the reference: `691 361 100 005` .

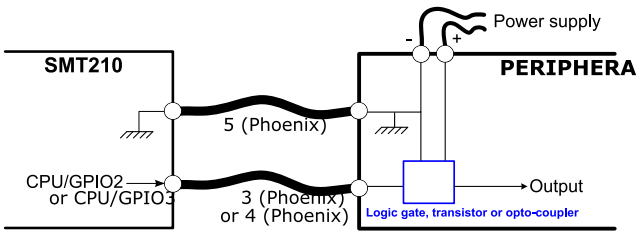
GPIO2/GPIO3 Electrical features

	Vin min	Vin max	VOH min	VOH max	IOH max	VOL max	IOL max	VIH min	VIL max
GPIO2	-0.5 V	6.5 V		5 V		0.4 V	10 mA	1.17 V	0.63 V
GPIO3	-0.5 V	6.5 V		5 V		0.4 V	10 mA	1.17 V	0.63 V

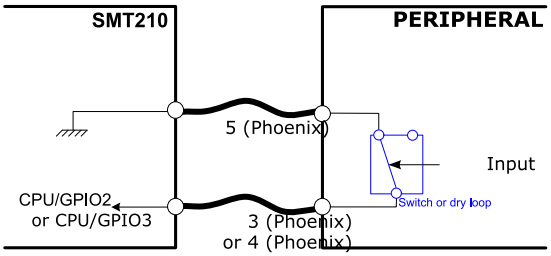
The GPIO2 et GPIO3 have a 10 KOhms pull-up to 5 V. After a device restart, the GPIO default voltage levels are 5 V.

Several use case schematics

Output configuration for the GPIO2 or GPIO3:



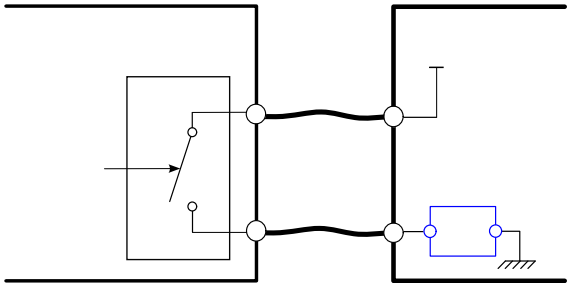
Two wires input configuration for GPIO2 or GPIO3:



Internal relay driving with the GPIO1

To drive the relay, the GPIO1 has to be configured in OUT mode (Write). After a device restart, the GPIO1 default voltage level GPIO1 is 0 (relay is opened). A logic level **1** on the GPIO1 allows to close the relay. Once the relay is closed, the PIN1 and the PIN2 of the relay are connected. The relay can support 1 A max under 24 VCC. . The logic level **0** on the GPIO1 allows to open the relay. The PIN1 and PIN2 can be switched.

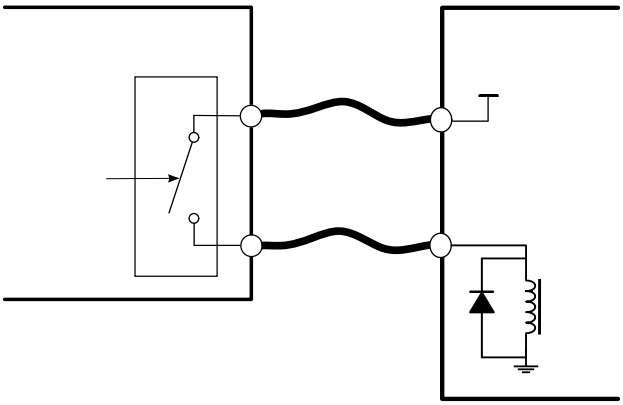
Relay usage schematics



Application when using a strike

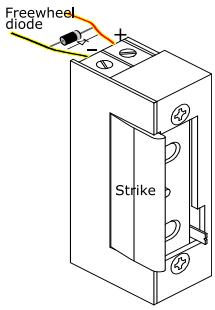
In case the device SMT210 has to drive a strike for an electric door, it is highly recommended to check, before any use, that an additional **freewhell diode** is really installed with the strike. Please refer to the strike User manual. If no **frewheel diode** is mounted on the electrical system of the strike when using for the first time, the user acts to deliberatly degrade the SMT210 device which is not warrantied in this case.

- electrical system example:



*The only **freewheel diode** (D1), mounted in parallel of the strike (L1), ensure the electric protection against the huge over-voltage which can degrade, when the relay is opening, a part of the SMT210 device.*

- example of electrical system with a strike and its freewheel diode:



It is recommended to plug the freewheel diode very close to the strike.

Phoenix connector GPIOs configuration

The GPIOs configuration can be done by editing the user preferences in the device Web user interface or with a configuration script. The part related to the GPIO configuration is explained below:

```
// Set Phoenix direction: input or output
if (aDirection == "out")
{
    Services.prefs.setBoolPref("innes.app-profile.gpio-input.phoenix-gpio_1.phoenix_1." + aPort + ".authorized", false);
    Services.prefs.setBoolPref("innes.app-profile.gpio-output.phoenix-gpio_1.phoenix_1." + aPort + ".authorized", true);
    Services.prefs.setBoolPref("system.connector.phoenix_1." + aPort + ".io.phoenix-gpio_1.enabled", true);
}
else if (aDirection == "in")
{
    Services.prefs.setBoolPref("innes.app-profile.gpio-input.phoenix-gpio_1.phoenix_1." + aPort + ".authorized", true);
    Services.prefs.setBoolPref("innes.app-profile.gpio-output.phoenix-gpio_1.phoenix_1." + aPort + ".authorized", false);
    Services.prefs.setBoolPref("system.connector.phoenix_1." + aPort + ".io.phoenix-gpio_1.enabled", true);
}
else if (aDirection == "disable")
{
    Services.prefs.setBoolPref("innes.app-profile.gpio-input.phoenix-gpio_1.phoenix_1." + aPort + ".authorized", false);
    Services.prefs.setBoolPref("innes.app-profile.gpio-output.phoenix-gpio_1.phoenix_1." + aPort + ".authorized", false);
    Services.prefs.setBoolPref("system.connector.phoenix_1." + aPort + ".io.phoenix-gpio_1.enabled", false);
}
```

Part II

Applicative user interface

2.1 Applicative user interface

The SMT210 device has a Web user interface that can be accessed with a Web browser. The supported Web browsers are: `Google Chrome`, `Mozilla Firefox`, `MS-Edge (Chromium)`.

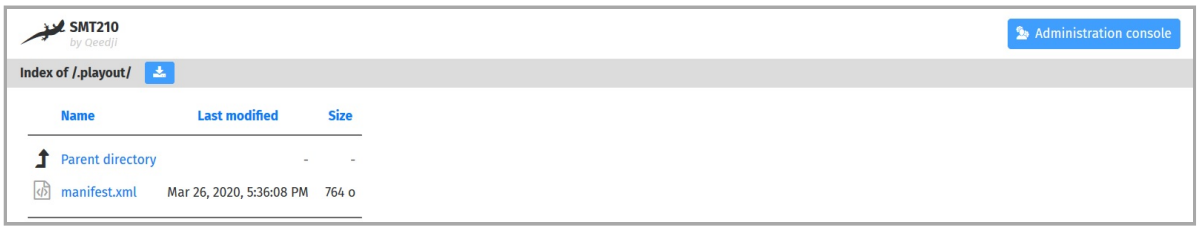
It is available from the URL: `http://<device_IP_addr>/`.

By default, the login credentials for the device Web user interface are:

- login: `admin`,
- password: `admin`.

The URL falls automatically into the applicative user interface: `http://<device_IP_addr>/.playout/`. This pane allows to watch the App content:

product = smt210



WebDAV directories
Clicking on the parent directory provides access to the root of the device's WebDAV server, which provides access to directories, among other things:

- `.playlog/` : location to store data for mediametry,
- `.resources/` : location to store the resources of the device Web user interface,
- `.software/` : location to store `.frm` middleware for updates,
- `.status/` : location to store the device status file `status.xml`,
- `.upnp/` : location to store `device.xml` device status for UPnP detection,
- `.assets/` : location to store some of the resources of the device Web user interface,
- `.playout/` : location to store the App when deployed on the device,
- `.log/` : location to store the application logs, when they are activated.

Part III

Administration console user interface

3.1 Administration console user interface

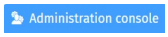
The SMT210 device has a Web user interface that can be accessed with a Web browser. The supported Web browsers are: `Google Chrome`, `Mozilla Firefox`, `MS-Edge` and `MS-Edge (Chromium)`.

It is available from the URL: `http://<device_IP_addr>/`.

By default, the login credentials for the device Web user interface are:

- login: `admin`,
- password: `admin`.

The URL falls automatically into the applicative user interface[1]. At the top right corner, click on the `Administration Console` button.



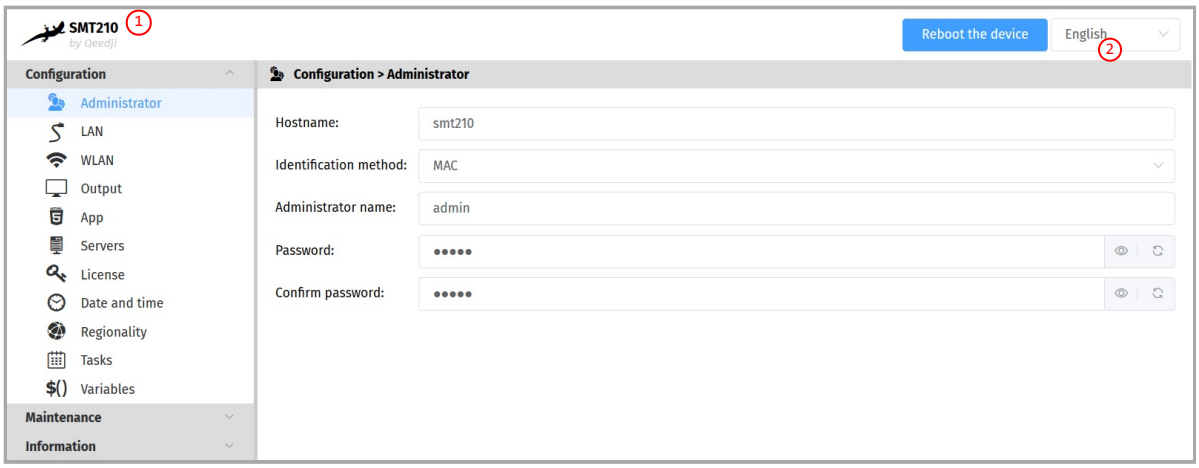
[1] *For further information, refer to the chapter § Applicative user interface.*

With the button at the top right corner (1), choose the language in which your device Web user interface needs to be displayed. The supported languages are:

- *English*,
- *Spanish*,
- *German*,
- *French*.

> ⚠ It is desirable that your device SMT210 device is on time. When possible, do synchronize it with an NTP server.

This is the `Administration console` user interface.



> ⚠ After you have changed and saved all your settings in the different panes, be sure to perform a device restart by clicking on the `Reboot the device` (2) button so that your changes are fully reflected.

Click on the device logo (1) at the left top corner to return to the applicative user interface.

⚠ If the device does not respond to its IP address, either the device power supply is unplugged, or the Ethernet cable is not connected, or the network configuration is not properly adjusted. To solve the problem, if your computer and local network supports IPV6, connect an Ethernet cable on the device and connect to the device Web user interface with its IPV6 address, which can be found on the test pattern displayed on the screen.

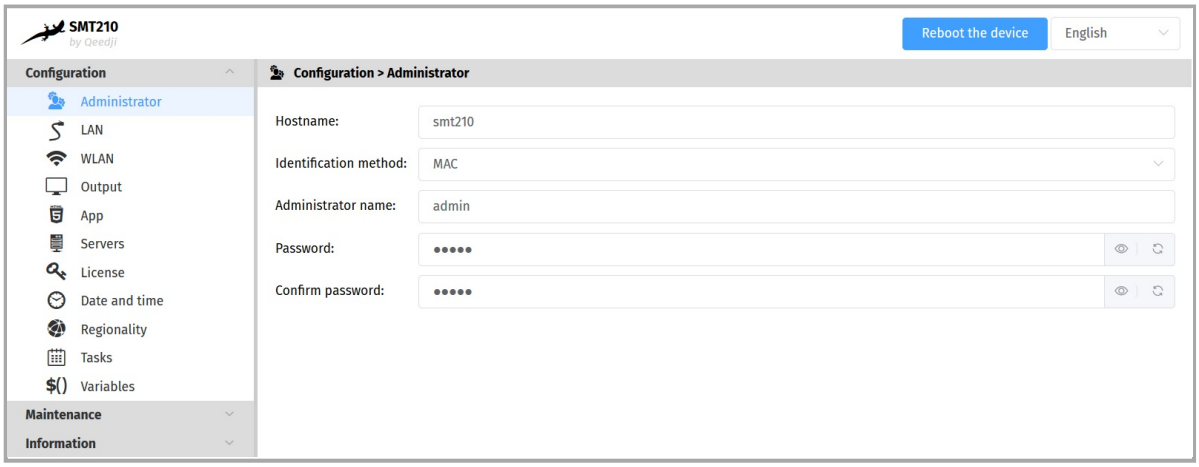
```
For example, for the MAC address value: ``00-1c-e6-02-1e-45`,
In a Web browser, enter the URL: http://[fc00::21c:e6ff:fe02:1e45]/.admin/
```

> To obtain the application note reminding some notions about IPV6 configuration, refer to the appropriate application note on the Qeedji Web site.

3.1.1 Configuration > Administrator

In the `Configuration` pane, select the **Administrator** menu to change:

- the `Hostname`,
- the login credentials:
  - `Administrator name`,
  - `Password`,
- the device identification method:
  - `MAC` (default),
  - `Hostname`,
  - `UUID`.

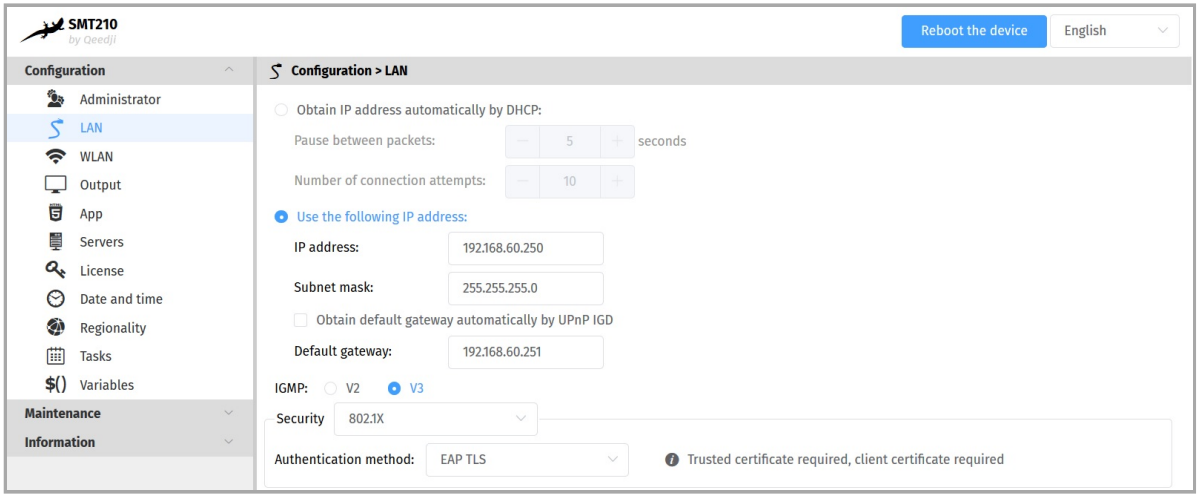


For security reasons, it may be useful to change the login credentials to access to the device's Web user interface. Please keep these login credentials in a safe place afterwards.

> ☛ *The same login credentials are used to access to the WebDAV server.*
>
> ☛ *It is recommended that you enter one unique `Hostname` value for each device. In case several SMT210 devices are located in different buildings or geographical locations, we recommend that you enter hostname values with information about the building and the location (e.g. `Hall-RD-Paris-1`).*

3.1.2 Configuration > LAN

In the `Configuration` pane, select the **LAN** menu to set up the network configuration of the `LAN` interface of your device.



If your device is not located in a secure network, select:

- security: *None*.

If your device is located and properly declared in a secure network, select `802.1X`, then select an `802.1X` authentication method supported by your RADIUS server:

- security: *802.1x*.

> ☛ *In the context of a secure network, your device must be first declared in your dedicated RADIUS server with a user `login` / `password`. Given that the login credentials used by Qeedji devices for all the 802.1X authentication methods are the LAN MAC address value of the SMT210 device, any new Qeedji device entry must be registered in your RADIUS server with these specific values with the format `aabbccddeeff` / `aabbccddeeff` for a MAC address AA-BB-CC-DD-EE-FF. Some `identification methods` may require you add a `trusted certificate`, used by your RADIUS server and/or a `client certificate`, generated with the MAC address of your device, the radius users credentials and the trusted certificate of the RADIUS server; For further information, please contact your IT department.*
>
> ☛ *When using a 802.1X certificate with an expiration date, in case your device is not on time or when the expiration date has expired, the device is not able to access to the network anymore. To work around, you have to insert one USB stick containing a specific configuration script to set either a new certificate or update the device date and time.*

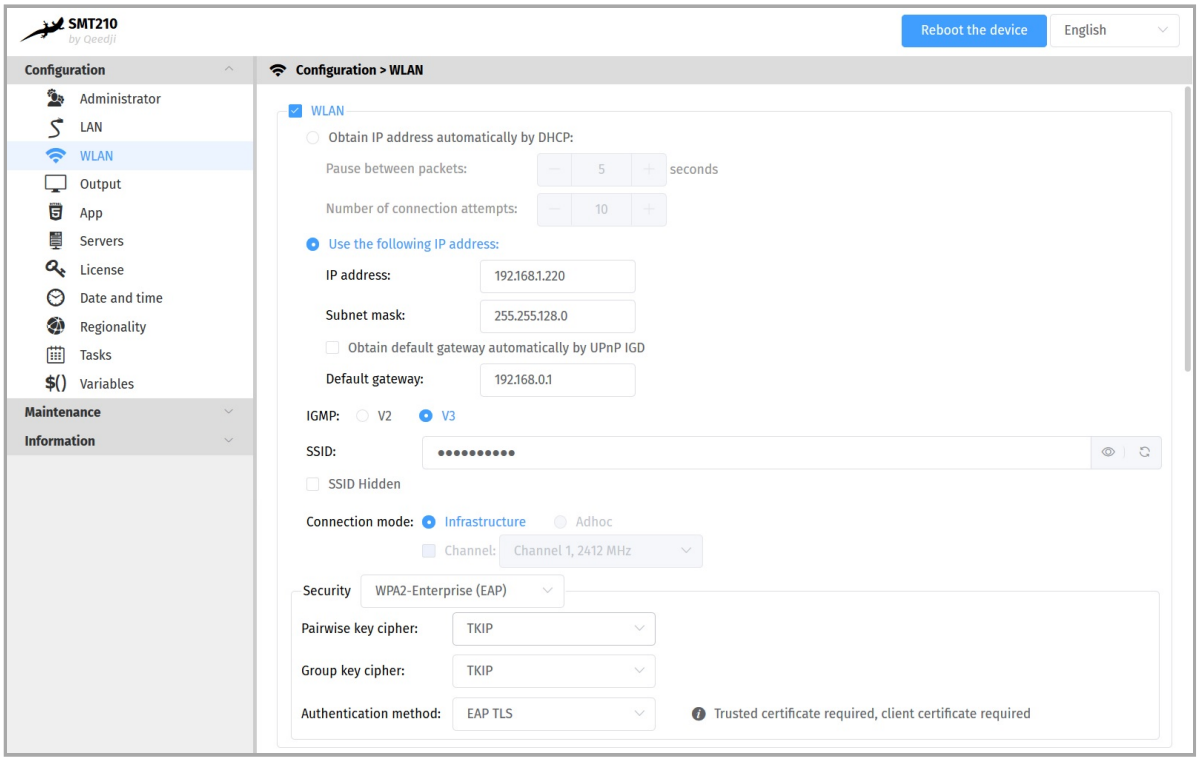
> ☛ *The device supports the UPnP and can be for example detected in the local network environment of your computer.*

> ☛ *By default, the device is configured with DHCP activated. In case the DHCP server is not available, after the DHCP timeout, the device ends up using the static IP address whose default value is 192.168.0.2 when it has not been changed yet by the end user. It is recommended to set an appropriate IP address, netmask and gateway if this case would happen.*

3.1.3 Configuration > WLAN

From the `Configuration` pane, select the **WLAN** menu to set up the network configuration of the `WLAN` interface on your device.

> ☛ *The `WLAN` menu is only displayed when the `WLAN` option is supported by your device.*



- `Connection mode` :
  - `Infrastructure` : Allows to establish a WIFI connection between your device and a WIFI router:
    - `Security` :
      - *None*,
      - *WEP*,
      - *WPA-Personal (PSK)*,
      - *WPA2-Personal (PSK)*,
      - *WPA-Enterprise (EAP)*,
      - *WPA2-Enterprise (EAP)*.
  - `Adhoc` : Allows to establish a direct WIFI connection between your device and e.g. your computer, without using a router.
    - `Security` :
      - *None*,
      - *WEP*.

The `SSID Hidden` option tells to the device whether or not the SSID value is broadcasted over the network by your WIFI router. It also allows to deduce the subset of `pair key encryption` and `group key encryption` modes supported.

The maximum lengths for WLAN crypto keys are:

- for `WEP` key:
  - 26 hexadecimal characters max.
- for `WPA-Personal (PSK)` and `WPA2-Personal (PSK)` keys:
  - 63 ASCII characters max.

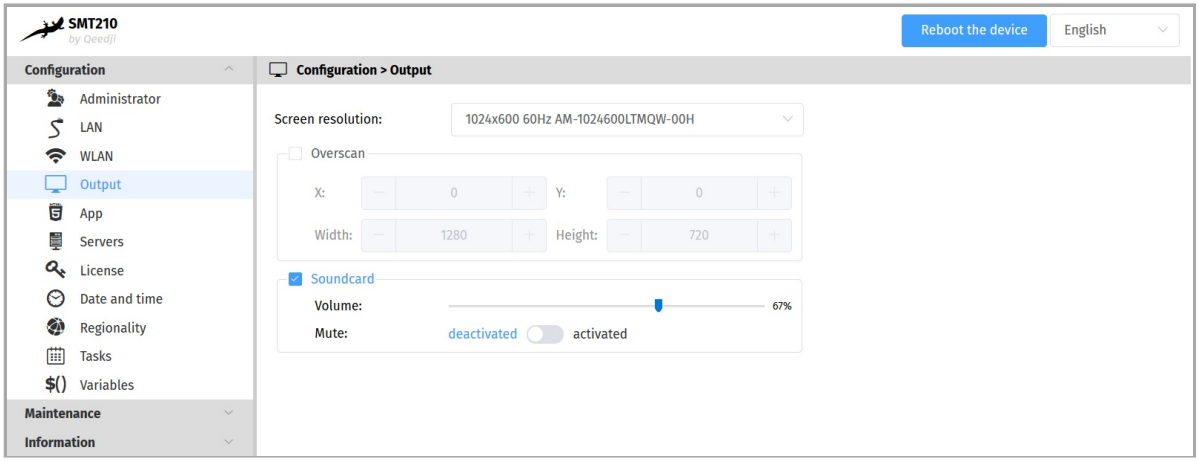
> ☛ *`TKIP` pair (or group) key encryption is not supported if the router is in `IEEE 802.11n` mode.*
>
> ☛ *Some computer OS version may not support `Adhoc` connection. For further information, contact your IT department.*
>
> ☛ *Selecting the WPA-Enterprise (EAP) or WPA-Enterprise (EAP) security implies that your device is located in a secure network, and therefore connects to a properly configured WIFI router with a dedicated RADIUS server.
>
> ☛ *In the context of a secure network, your device must be first declared in your dedicated RADIUS server with a user `login` / `password`. Given that the login credentials used by Qeedji devices for all the 802.1X authentication methods are the LAN MAC address value of the SMT210 device, any new Qeedji device entry must be registered in your RADIUS server with these specific values with the format `aabbccddeeff` / `aabbccddeeff` for a MAC address AA-BB-CC-DD-EE-FF. Some `identification methods` may require you add a `trusted certificate`, used by your RADIUS server and/or a `client certificate`, generated with the MAC address of your device, the radius users credentials and the trusted certificate of the RADIUS server; For further information, please contact your IT department.*

The `WLAN` interface is not checked by default.

> ☛ *In WLAN configuration, it is recommended that the device has a daily device reboot task.*

3.1.4 Configuration > Output

From the `Configuration` pane, select the **Output** menu to configure the audio output of the device, among other things.



- `Screen resolution` : *1024x600 60Hz AM1024600LTMQW-00H*.
- `Overscan` :
  - `X` : horizontal origin of the viewport in pixel,
  - `Y` : vertical origin of the viewport in pixel,
  - `Width` : width of the viewport in pixel,
  - `Height` : height of the viewport in pixel.
- `Sound card` option: allows to enable or disable the sound card:
  - `Volume` : *0..100%*,
  - option `Mute` : *on* (mute) or *off* (mute on).

> Some screen, due to their construction, have been designed with an overscan, which means that the edges of your broadcast content on your device may not be visible on your screen even when choosing the right optimal resolution for your screen. To alleviate this problem, use the overscan on your `Qeedji` device to slightly reduce the width and height of your viewport. While doing so, it is recommended to display the test pattern of the device.
>
> ⚠ When using the overscan, for a good configuration of your device, please make sure that your screen is not in `Wall`, `Mozaic` or `Tile` mode.

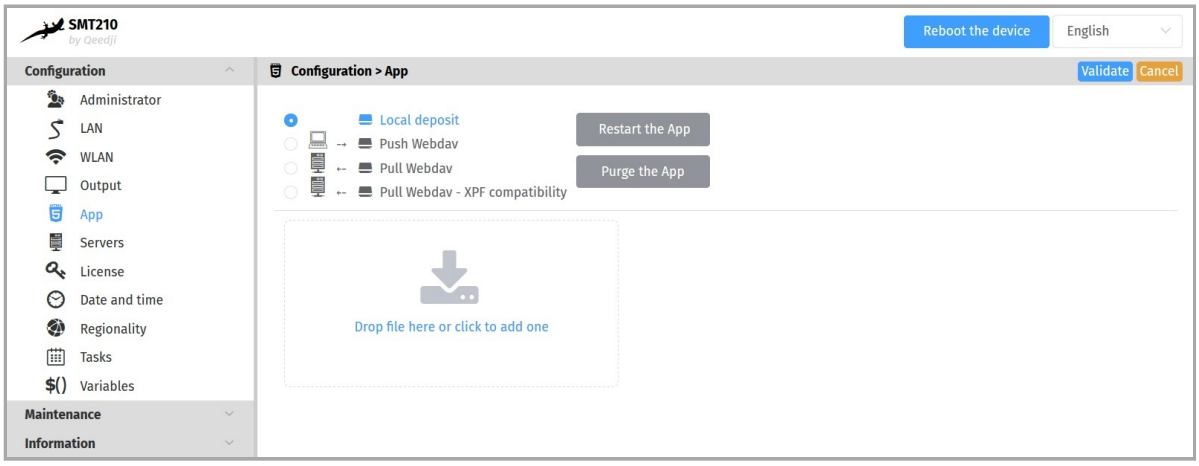
3.1.5 Configuration > App

From the `Configuration` pane, select the **App** menu to select how the App must be loaded.

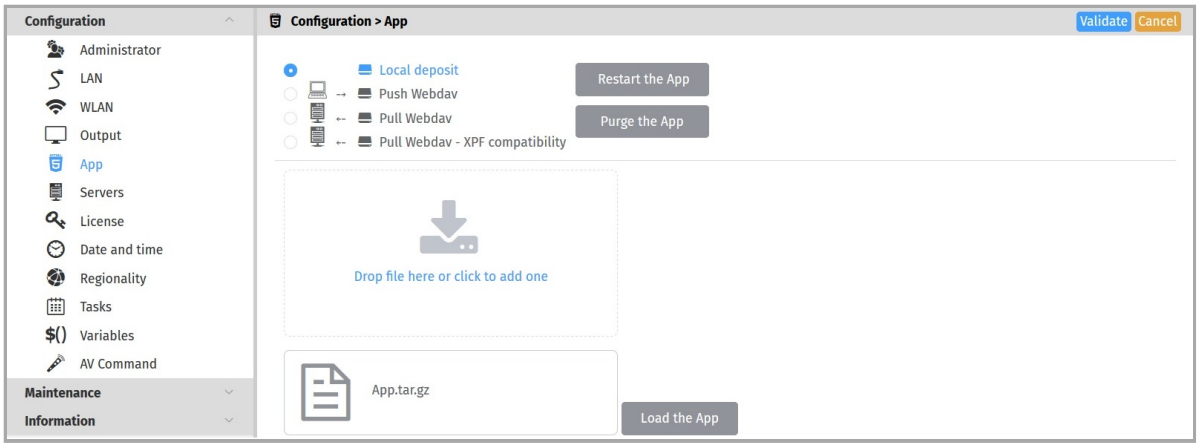
For each mode, you can use the `Purge the App` or `Restart the App` buttons at any time to remove the `App` from the device or restart it, respectively.

> ☛ *The `Restart App` or `Purge the App` cannot work when `Test card` is activated.*
>
> ☛ *In order to restart an `App`, the `App` must be first loaded on the device.*

- `Local deposit` : Allows to load an App from the device Web user interface and play its content immediately.



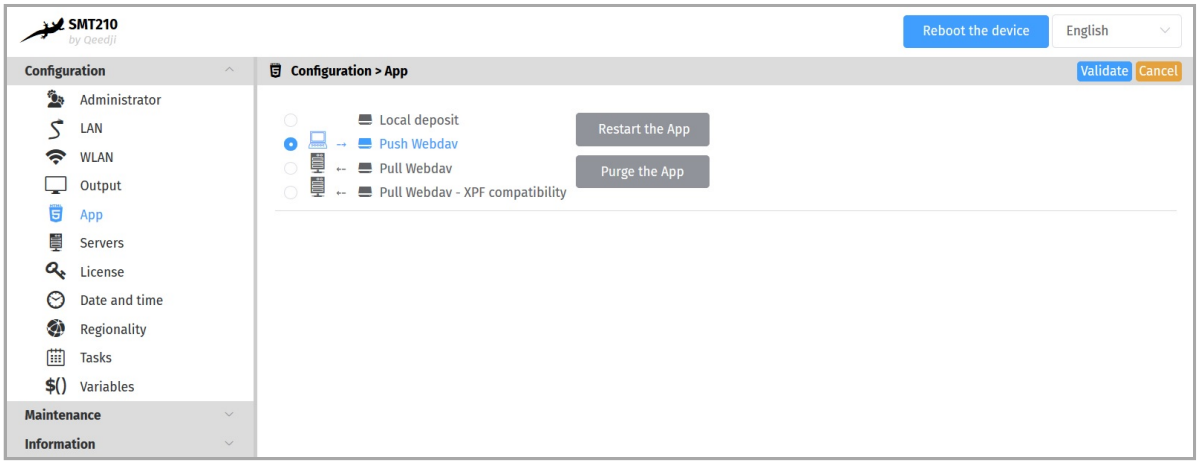
Use the `Drop file here` box or click to add one to drop your `App`.



Then click on the `Load App` button. When the file disappears from the interface, the App is loaded and starts automatically.

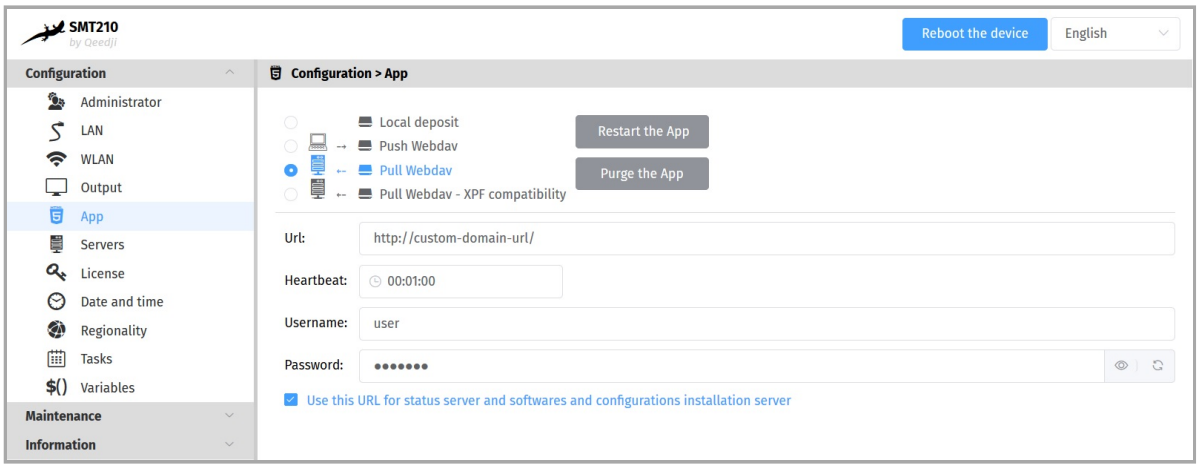
> ☛ *The development of App is reserved for advanced users with software development skills. The content of the App must contain at least these 2 files `manifest.xml` and `player.html`. Then archive your App in one of the supported formats: `*tar.gz, *.zip, *.tar, *.tgz`. App examples are available at github SDK-G4 API (PDF example). For further information, contact support@qeedji.tech.*

- `Push WebDAV` : Configure the device to receive an App coming from any WebDAV client or from any compatible software suite. Once the App is loaded, it starts immediately.



> ☛ *To find out which software suites are capable of publishing an App on `Qeedji` devices, contact support@qeedji.tech.*

- `Pull WebDAV` : allows to configure the device so that it can regularly load or update an App from a remote WebDAV server. Once the App is loaded, it starts immediately.

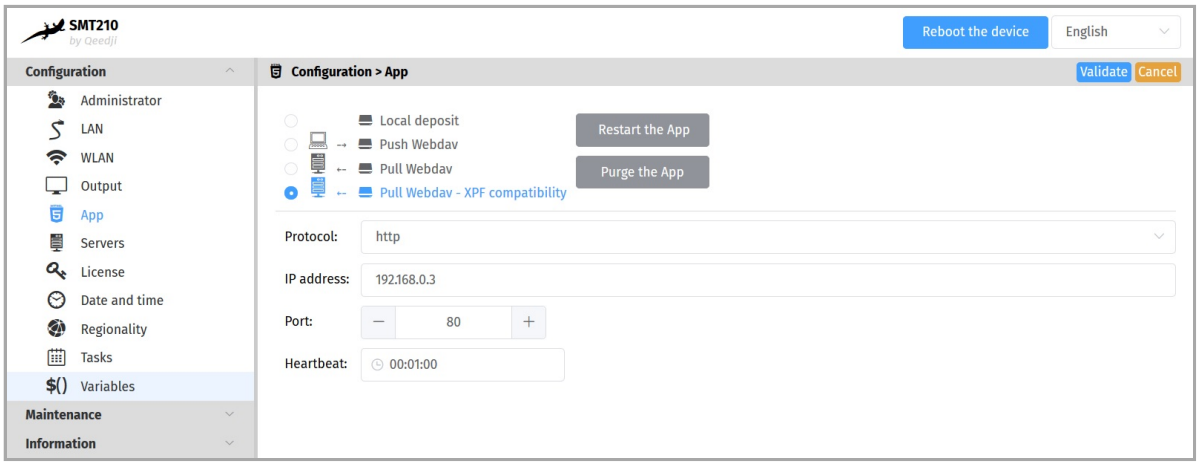


Fill in the fields below correctly:

- `URL` : URL of the remote server's WebDAV frontal. For example: `URL` : http://domain:8080/.directory/
- `Username/Password` : login credential to access to the remote server's WebDAV frontal.
- `Heartbeat` : in *HH:MM:SS* format, time period to connect to the remote server (default: 1 minute).
- option: `Use this URL for the status server and the software and configuration installation server` :
  - if enabled, this option allows, based on the defined URL, to automatically set the URLs of the remote servers for:
    - firmware upgrade and configuration scripts distribution:
      - `URL` + `.setup/` suffix,
    - the diffusion of the device status:
      - `URL` + `.devices-status/` suffix.
  - if disabled, this allows to set specific remote server URLs.

> ☛ *The user preference `innes.app-profile.addon-manager.*.*.*.http-downloader.validity-calendar` allows to store the content of an ICAL file defining the validity range for triggering firmware upgrade and configuration scripts.*
>
> ☛ *The user preference `innes.app-profile.manifest-downloader:g3.*.*.*.validity-calendar` allows to store the content of an ICAL file defining the validity range for device content updates.*
>
> ☛ *The user preference `innes.launcher.status.validity-calendar` allows to store the content of an ICAL file defining the validity range for the diffusion of the device status (status.xml).*
>
> ☛ *To find out which software suites are able to publish on a remote server, an App supporting `Qeedji` devices, contact support@qeedji.tech.*

- `Pull WebDAV - XPF Compatibility` : allows to configure the device so that it can regularly retrieve XPF content from a remote WebDAV server and transform it into an App. Once the App is generated, its content is immediately played.



> ☛ *The user preference `innes.app-profile.manifest-downloader:g2.*.*.*.validity-calendar` allows to store the content of an ICAL file defining the validity range for content updates of devices in `Pull WebDAV - XPF compatibility` mode.*

Fill in the fields below correctly:

- `Protocol` : *http* or *https*,
- `IP address` : IP address of the remote server (XPF compatibility),
- `Port` : port used by the remote server (XPF compatible),
- `Heartbeat` : in *HH:MM:SS* format, time period to connect to the remote server (default: 1 minute).

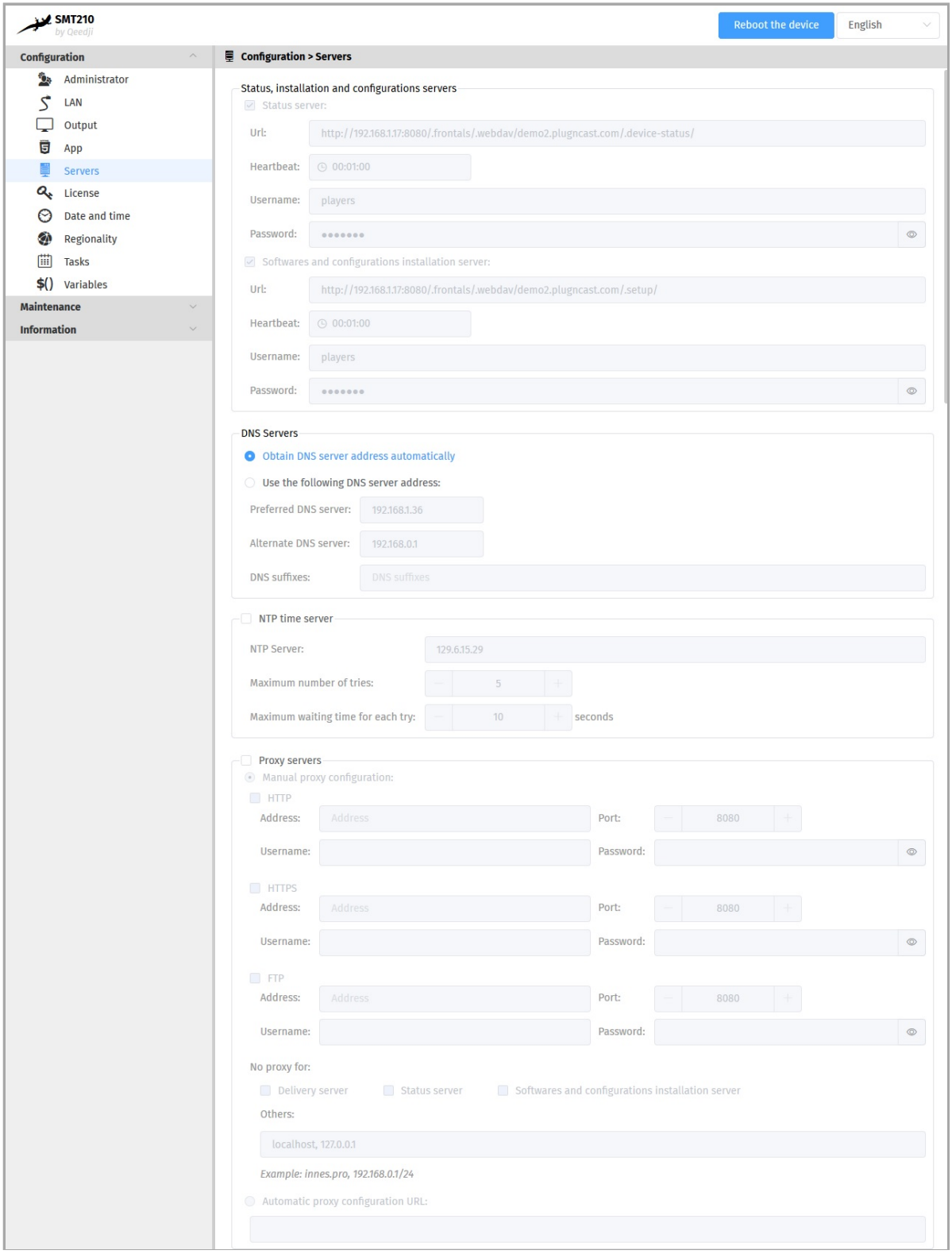
App supported

The device can support for example *Room booking* App. With this App, the SMT210 device can book, validate or delete meeting room reservations. Connected to an LDAP server, the user has to first authenticate itself with an NFC badge. For further information, contact support@qeedji.tech.

The device can support also for example App coming from `Qeedji PowerPoint publisher for media players`. Once this PowerPoint Add-on is installed on your computer, it allows to publish a PowerPoint presentation on some of your media players. For further information, refer to the chapter § Appendix: Qeedji PowerPoint publisher For Media Players

3.1.6 Configuration > Servers

In the `Configuration` pane, select the **Servers** menu to define the configuration of the servers peripheral to your device.



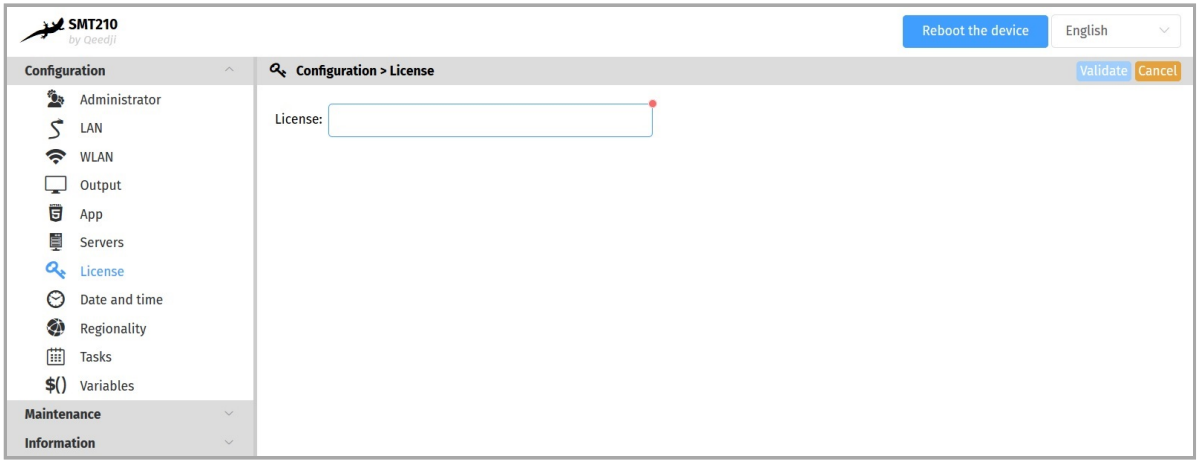
- status, software installation and configuration servers.
  - `Status server` :
    - `URL` : URL of the remote server's WebDAV frontend for the broadcast of the `.device-status/status.xml` device status file. For example: http://domain:8080/.directory/
    - `Username/password` : login and password for the remote server's WebDAV frontend connection.
    - `Heartbeat` : in *HH:MM:SS* format, period duration of the connection to the remote server (default: 1 minute).
  - `Software installation and configuration servers` :
    - `URL` : URL of the remote server's WebDAV frontend for hosting update software and configuration scripts. For example: ```http://domain:8080/.directory/````
    - `Username/password` : login and password for the remote server's WebDAV frontend.
    - `Heartbeat` : in *HH:MM:SS* format, period duration of the connection to the remote server (default: 1 minute).
- `DNS servers` ,
- `NTP Time Servers` : allows to set a time server in order the device is always on time [1],

- `Proxy server`.

[1] If your device does not have access to the Internet, it is possible to turn an MS-Windows computer into a NTP server. For further information, contact your IT department.

3.1.7 Configuration > License

In the `Configuration` pane, select the **License** menu to view your device license number.

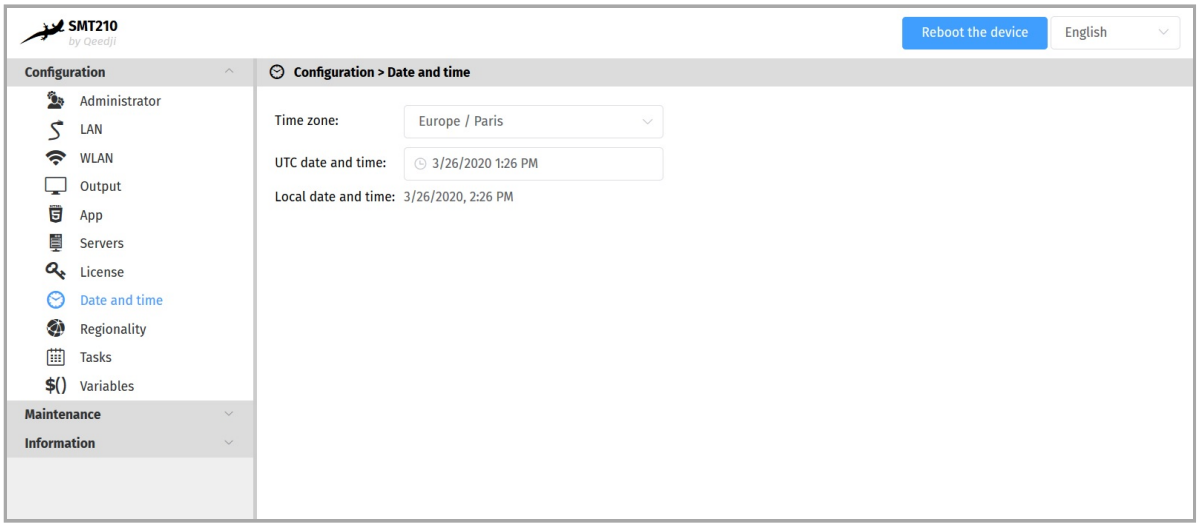


This license number is registered at the factory when the device is ordered. It is then sent to you by e-mail. If it has disappeared due to a handling error or after formatting your device, an error message indicating that the license is invalid will appear on your screen. In this case, please re-enter the license for your device.

3.1.8 Configuration > Date and time

From the `Configuration` pane, select the **Date and Time** menu to check the time configuration:

- timezone,
- system date of your device (day and time).

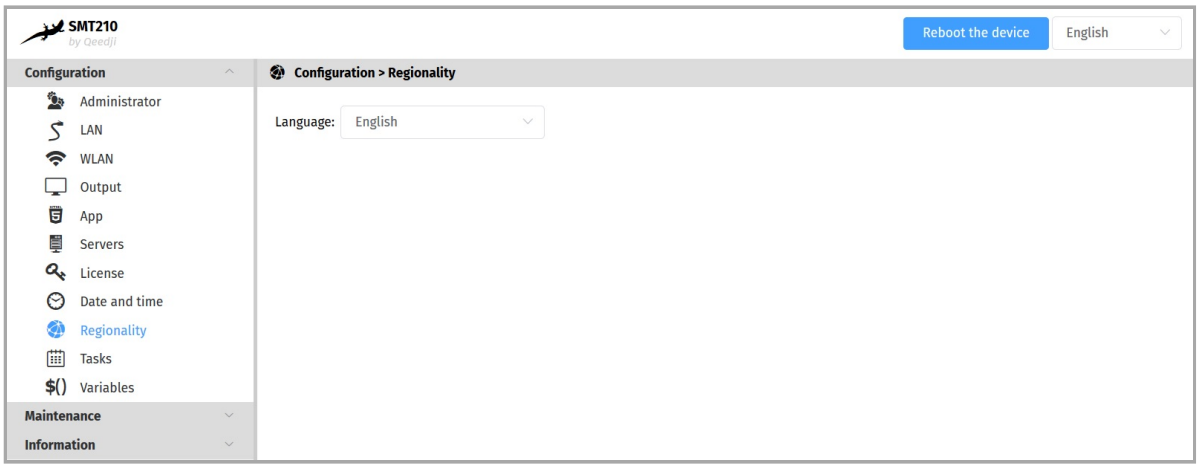


To update the date and time of your device, click on the `UTC Date and Time` value and then click on the `Now` button.

> ☛ *Resetting the time involves a restart of the device immediately. If you have several configuration settings to change, it is advisable to adjust the date and time at last.*
>
> ☛ *It is advised that your device is on time. If your device is connected to the Internet, it is advised to synchronize the date and time on a Web NTP server. For further information, refer to the chapter § Configuration > Servers.*

3.1.9 Configuration > Regionality

From the `Configuration` pane, select the **Regionality** menu to choose the language in which information messages or error messages related to the device need be displayed.



The supported languages are:

- *English*,
- *Spanish*,
- *German*,
- *French*.

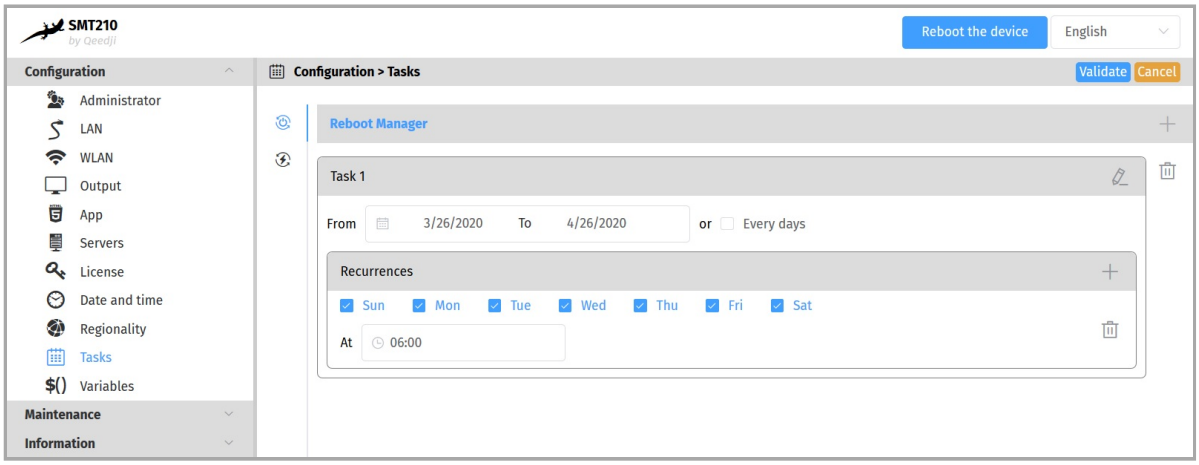
3.1.10 Configuration > Tasks

From the `Configuration` pane, select the **Tasks** menu to:

- program a device reboot task,
- program an energy management task for the appliance to reduce its energy consumption.

Device restart tasks

To create a restart task, click on the button and then the `+` button.



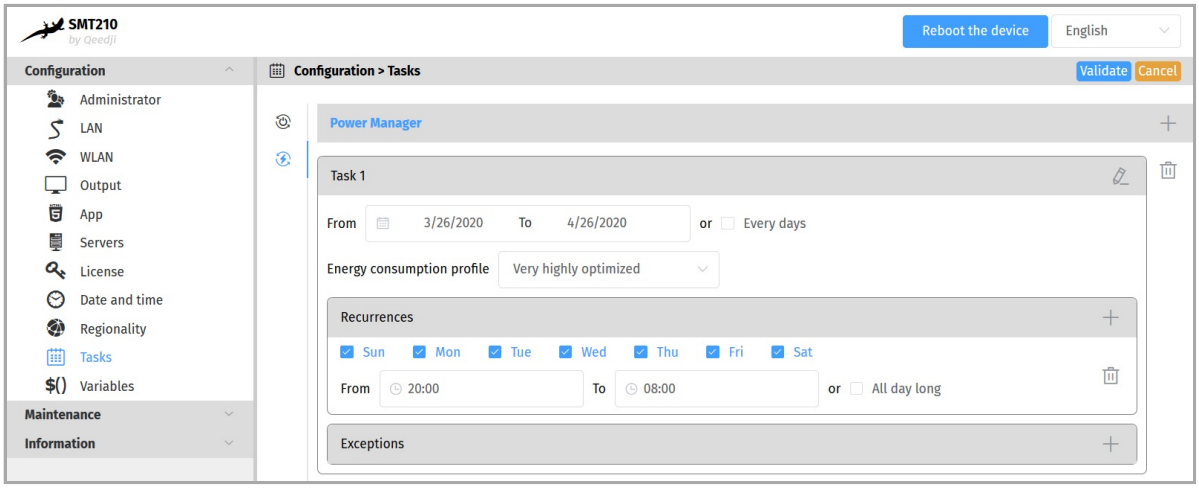
It is therefore possible to program in time several reboot occurrences whose parameters are stored in an ICAL format in the user preference `innes.reboot-manager.calendar`.

Example of value (ICAL format):

```
BEGIN:VCALENDAR
VERSION:1.0
BEGIN:VEVENT
SUMMARY: Reboot Task 1
DTSTART:20200407T091800
DTEND:20200407T091805
RRULE:FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR,SA,SU;UNTIL=20200507T235959
END:VENT
END:VCALENDAR
```

Device power manager tasks

To create a device power manager task, click on the button and then the `+` button.



The possible values programmable in time are

- *Very highly optimized*,
- *Highly optimized*,
- *Optimized means*,
- *Nominal mode*.

It is possible to create several energy manager tasks in the same day. These settings for scheduled power level, start time, end time, occurrence, and exception are stored in ICAL format in the user preference `innes.power-manager.calendar`.

Example value (ICAL format):

```
BEGIN:VCALENDAR
VERSION:1.0
BEGIN:VEVENT
SUMMARY:Standby Task 1
X-POWER-MANAGER-LEVEL:MIN
DTSTART:20190805T090000
DTEND:20190805T120000
RRULE:FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR,SA,SU;UNTIL=20200416T0000
END:VENT
END:VCALENDAR
```

> ☛ *The Power Manager task scheduled at the device Web user interface has no effect when another sleep task is scheduled within the App.*

In this version, here is the state of the device when the power manager is in the *Very highly optimized* state:

Function	**Associated User Preferences**
Sound: inactivated	`innes.power-manager.level.min.<>.mute` = true
Screen: off	`innes.power-manager.level.min.<>.power-mode` = 0
Volume: 0%	`innes.power-manager.level.min.<>.volume` = 0
Opacity: 100%	`innes.power-manager.level.min.<>.opacity` = 100
Brightness: 0%	`innes.power-manager.level.min.<>.brightness` = 0
Backlight: 0%	`innes.power-manager.level.min.<>.backlight` = 0

In this version, here is the state of the device when the power manager is in the *Highly optimized* state:

Function	**Associated User Preferences**
Sound: activated	`innes.power-manager.level.low.<>.mute` = false
Screen: on	`innes.power-manager.level.low.<>.power-mode` = 1
Volume: 10%	`innes.power-manager.level.low.<>.volume` = 10
Opacity: 80%	`innes.power-manager.level.low.<>.opacity` = 80
Brightness: 10%	`innes.power-manager.level.low.<>.brightness` = 10
Backlight: 10%	`innes.power-manager.level.low.<>.backlight` = 10

In this version, here is the state of the device when the power manager is in the *Medium Optimized* state:

Function	**Associated User Preferences**
Sound: activated	`innes.power-manager.level.high.<>.mute` = false
Screen: on	`innes.power-manager.level.high.<>.power-mode` = 1
Volume: 80%	`innes.power-manager.level.high.<>.volume` = 80
Opacity: 20%	`innes.power-manager.level.high.<>.opacity` = 20
Brightness: 80%	`innes.power-manager.level.high.<>.brightness` = 80
Backlight: 80%	`innes.power-manager.level.high.<>.backlight` = 80

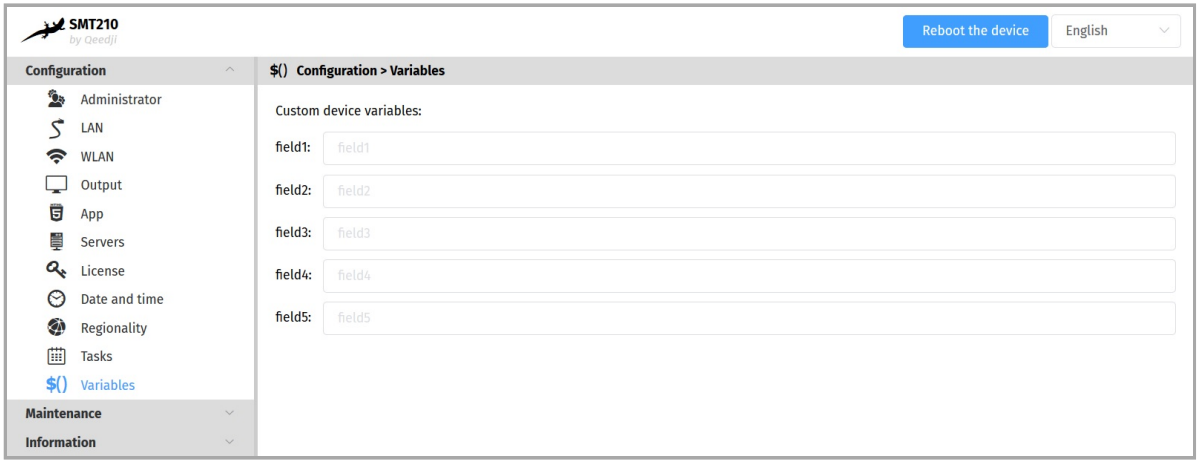
In this version, here is the status of the device when the power manager is in the *Nominal mode* state, meaning the default mode when no other power manager tasks are running.

Function	**Related User Preferences**
Sound: activated	`innes.power-manager.level.max.<>.mute` = false
Screen: on	`innes.power-manager.level.max.<>.power-mode` = 1
Volume: 100%	`innes.power-manager.level.max.<>.volume` = 100
Opacity: 0%	`innes.power-manager.level.max.<>.opacity` = 0
Brightness: 100%	`innes.power-manager.level.max.<>.brightness` = 100
Backlight: 100%	`innes.power-manager.level.max.<>.backlight` = 100

☛ *The values of these user preferences are all modifiable.*

3.1.11 Configuration > Variables

From the `Configuration` pane, select the **Variables** menu to set variable (or TAG) values for this device.



The variable names are:

- `field1`,
- `field2`,
- `field3`,
- `field4`,
- `field5`.

These variable values can then be used in Apps to perform specific processing for certain devices only.

> ☛ *Variable values can only contain characters from the ASCII-7bits table.*

3.1.12 Maintenance > Test card

From the `Maintenance` pane, select the **Test card** menu to enable or disable the test pattern. The test pattern is often enabled during:

- installing devices on the network,
- the development of the output resolution and overscan.

> ☛ *When the test card is activated, the content of the App is not played.*

3.1.13 Maintenance > Middleware

From the `Maintenance` pane, select the **Middleware** menu to view the version of the middleware installed on your device.

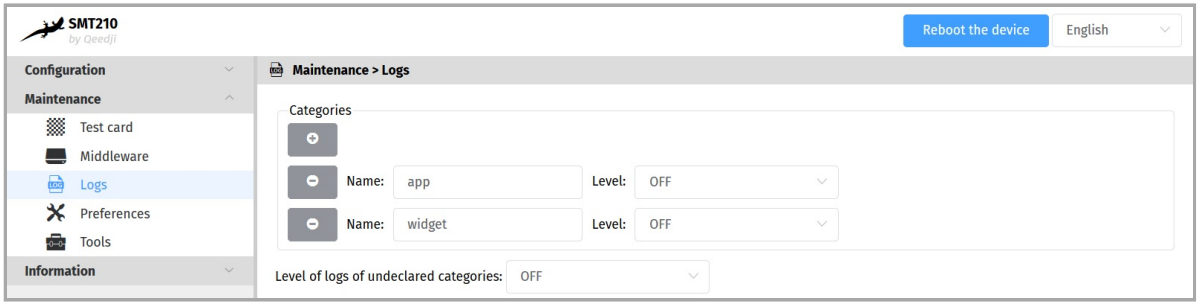
> ☛ *Corrective and evolutive maintenance software versions are regularly made available on the Qeedji Web site. It is therefore advised to regularly update the device firmware. From this website, download the latest version available for your device model. Unzip the `.zip` archive and get the `.frm` file.*

Drop your `.frm` file in the `Drop file here` location or click on it to add one, then click on the `Send` button to update the `Gekkota OS` version of your device. Wait a few minutes, the time to load and install the new middleware version. Go back to the `Administration console` user interface and check the new Gekkota OS version number of the device.

> ⚠ Do not electrically disconnect the device during the firmware upgrade. For further information, refer to the chapter § LED behaviour.

3.1.14 Maintenance > Logs

From the `Maintenance` pane, select the **Logs** menu to activate logs.



The log levels are:

- `DEBUG` : activation of level logs: ERROR + WARN + DEBUG,
- `WARN` : activation of level logs: ERROR + WARN,
- `ERROR` : activation of level logs: ERROR,
- `OFF` : disabling logs.

Logs are compartmentalized according to software functions such as:

- `app` : App debug,
- `widget` : HTML widget debugging,
- `network` : debug of the network related layer,

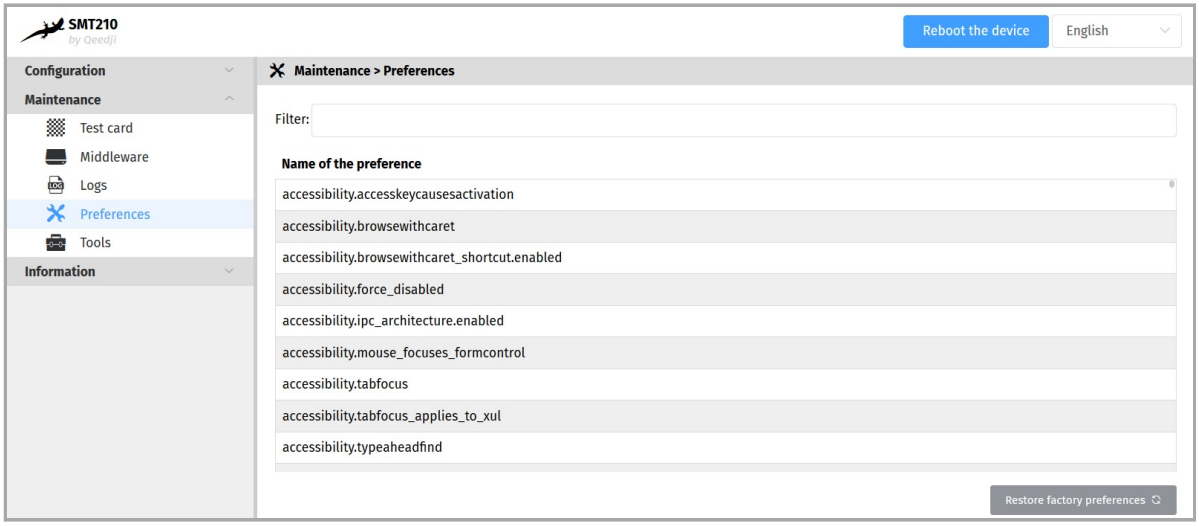
> ☛ *These logs may be activated on support request in exceptional debug cases.*
>
> ☛ *These logs can only be interpreted only by software developers who are familiar with the software bricks that have been developed.*

Activating the logs with a level other than `OFF` should only be done after a request from `Qeedji` support.

> ⚠ Enabling traces `All trace levels of undeclared categories` with a `DEBUG` or `WARN` level can significantly disrupt the operation of the device.
>
> ⚠ After a debug session with support, in nominal operation, all levels should be reset to `OFF` .

3.1.15 Maintenance > Preferences

In the `Maintenance` pane, select the **Preferences** menu to view all the preferences.



The filter allows to display only the preferences whose name contains the string entered in the filter. All the preferences have optimal default values.

Double click on a preference to change its value.

At the bottom right of the page, the `Restore factory preferences` button resets a subset of preferences allowing the device to reprogram its factory preferences.

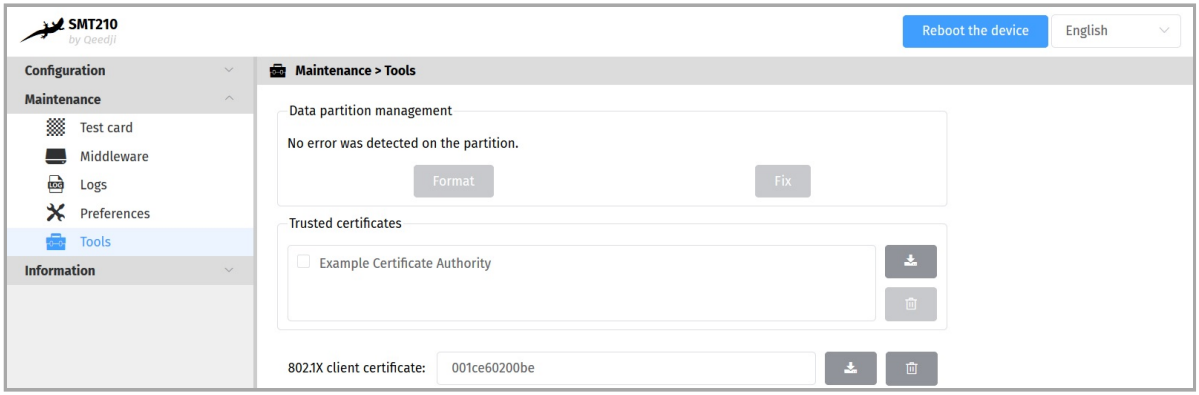
Here are some user preferences that may be useful.

user preference	value	description
`innes.video.decoding-group.enabled`	*false* (default)	If a second video is trying to start while a first one is already running, the first video is stopped and the second video starts. A temporarily unavailable message content is displayed for the last stopped video media.
`innes.video.decoding-group.enabled`	*true*	In case a second video media tries to start while a first one is already running, the second video does not start. Temporarily unavailable message content is displayed for the second video media.
`innes.webserver.providers.http.enabled`	*true*	Allows to support access to the device in http://.
`innes.webserver.providers.https.enabled`	*true*	Allows to support access to the device in https://.

3.1.16 Maintenance > Tools

In the `Maintenance` pane, select the **Tools** menu to:

- `Fix` errors detected on the SD card data partition,
- format the data partition of the SD card,
- add `Trusted certificates` ,
- add `802.1X client certificate` (*.p12*).



The encryption algorithms supported to decrypt the .p12 certificates are:

- *128 bits RC4 with SHA1*,
- *40 bits RC4 with SHA1*,
- *3 keys 3DES with SHA1 (168 bits)*,
- *2 keys 3DES with SHA1 (112 bits)*,
- *128 bits RC2-CBC with SHA1*,
- *40 bits RC2-CBC with SHA1*.

> ☛ *The `format` and `fix` buttons are only active if the Gekkota OS middleware has actually detected writing or reading errors on the partition.*

A message indicates on the screen that an error has occurred on the partition and that a device reboot is necessary.

If the `Fix` button is accessible, clicking on the `Fix` button will repair the content without purging the App. If the problem persists, and the `Format` button is available, clicking on the `Format` button will format the content. It is then necessary to publish again the App.

> ☛ *If the problem persists after formatting the SD card, contact your `Qeedji` support.*

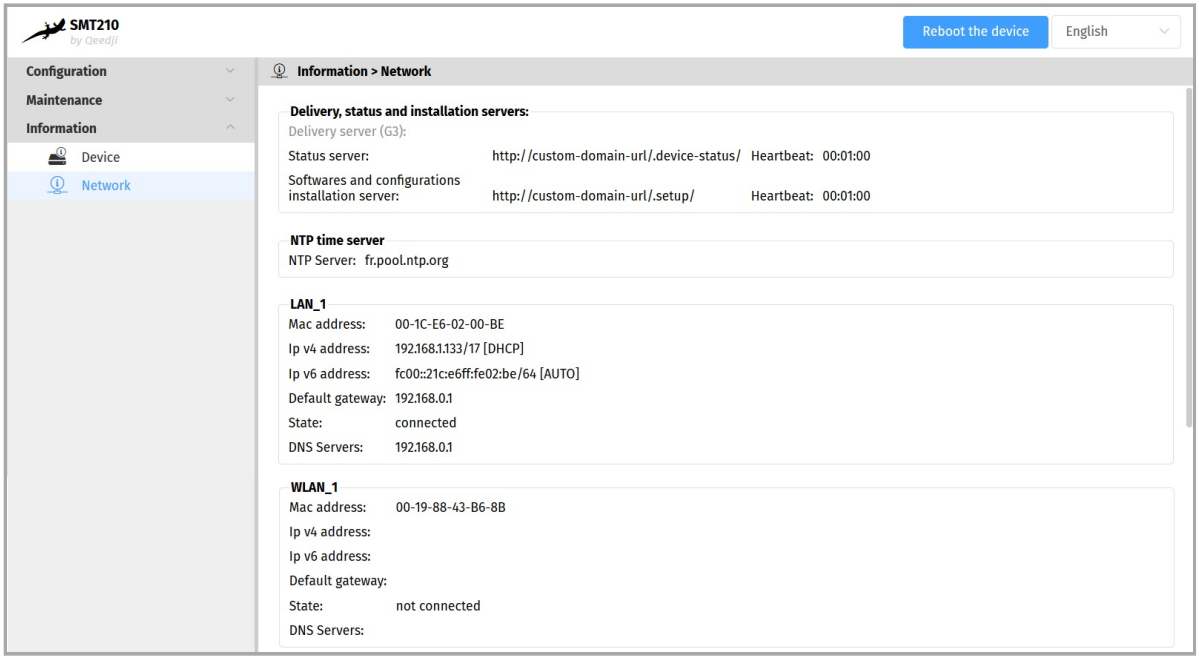
3.1.17 Information > Device

In the `Information` pane, select the **Device** menu to view system information about the device.

- `Middleware` : label and version of the embedded middleware,
- `Model` : model of the `Qeedji` device,
- `Hostname` : name of the device on the network,
- `MAC` : MAC address (value used in particular to generate the license key of the device),
- `UUID` : Universal Unique IDentifier,
- `PSN` : Product Serial Number.

3.1.18 Information > Network

In the `Information` pane, select the **Network** menu to view a summary of the device's network configuration.



Part IV

Configuration by script

4.1 Configuration by script

The SMT210 device can auto-configure with a configuration script. The configuration script can be either:

- hosted on a remote WebDAV server or
- broadcasted by your DHCP server (code 66) or
- injected through an USB storage device or
- dropped in the device `.extension` WebDAV directory with a WebDAV client.

For further information, refer to the configuration-by-script application note.

In case the script is containing an error, the syntax error is reported in the `http://<device-ip-addr>/.status/status.xml` file.

Part V

Technical information

5.1 Built-in RFID reader

The device SMT210 has a RFID tag reader allowing to recognize the badges supporting the NFC technology.

Type	Modulation frequency	Brand (Manufacturer)	Applicable standard	Data rate (kbps)	Supported	Tested configuration
NFC type A	13.56 MHz	Mifare Classic 1K/4K EV1 & mini [1] (NXP)	ISO 14443 typeA	106	Yes	1K, 106 kbps
NFC type A	13.56 MHz	Mifare Plus 2K/4K S/X [1] (NXP)	ISO 14443 typeA	106	Yes	
NFC type A	13.56 MHz	Mifare UltraLight / UltraLight C (NXP)	ISO 14443 typeA	106	Yes	106 kbps
NFC type A	13.56 MHz	Mifare DESFire D40, EV1 2K/4K/8K (NXP)	ISO 14443 typeA	106	Yes	4K, 106 kbps
NFC type A	13.56 MHz	Mifare NTAG203	ISO 14443 typeA	106	Yes	NTAG203, 106 kbps
NFC type A	13.56 MHz	Jewel (Innovision)	ISO 14443 typeA	106	Yes	106 kbps
NFC type A	13.56 MHz	Topaz 512 (BCM512)	ISO 14443 typeA	106	Yes	BCM 512, 106 kbps
NFC type A	13.56 MHz	Kovio (Kovio)	ISO 14443 typeA	106	NC	
NFC type A	13.56 MHz	SLE66 (Infineon), SmartMx (NXP)	ISO 14443 typeA	106	NC	
NFC type B	13.56 MHz	Cartes de transport (Innovatron), Calypso	ISO 14443 typeB	106	Yes	
NFC type B	13.56 MHz	Micropass, Vault (Inside), 16RF (ST), SLE66 (Infineon)	ISO 14443 typeB	106	NC	
NFC type F	13.56 MHz	Felica (Sony) JIS 6319,	ISO 18092	212, 424	Yes	
NFC type V	13.56 MHz	Icode (NXP), iclass (Hid), Tag-it (TI), LR (ST)	ISO 15693		No	
RFID LF	125 KHz	Hitag (NXP), 125KHz Prox (HID)	ISO 18000-2, ISO11784/11785/14223		No	

[1] not fully compliant with the ISO14443A relevant standard

5.2 Technical specifications

Model	Manufacturer
SMT210	Qeedji

Processor	
CPU	DM3730 1 GHz

Peripherals
2x USB 2.0 Host (Low/Full/High Speed)
1x USB client
1x GPIO for the internal relay driving
3x GPIO bidirectional
2x side LEDs

Storage
Internal flash memory: 2 GB
SD card: 2 GB

Middleware
Gekkota OS 4

Audio output
Build-in mono speaker

Screen	Resolution
Touch screen 10.1"	1024x600
Brightness	250 cd/m2 typ.

Network
1x Ethernet 10/100 BaseT

RFID reader	Information
Type NFC	A, B, F
Modulation frequency	13.56 MHz

Options
HSDPA 3G+ modem
WIFI 802.11 b/g (WIFI 3)

Power supply	Information
12 V DC (830 mA)	
PoE	`IEEE802.3af` (Class 0, Alternative A and B compatible)

Operating temperature	Storage temperature
+0 °C to +45 °C	-20 °C to +60 °C

Operating humidity	Storage humidity
< 80 %	< 85 %

Display duration per per day for the touch screen
On: 16 hours (max.)
Standby: 8 hours

Weight	Dimensions (W x H x D)
With WIFI: 0,897 Kg (1,97 lb) Without WIFI: 0,876 Kg (1,93 lb)	258 x 176 x 35 (10,15" x 6,93" x 1,37")

Warranty
1 year

5.3 Conformities

In conformity with the following European directives:

- `LVD 2014/35/EU`,
- `EMC 2014/30/EU`.

Part VI

Contacts

6.1 Contacts

For further information, please contact us:

- **Technical support**: support@qeedji.tech,
- **Sales department**: sales@qeedji.tech.

Refer to the `Qeedji` Web site for FAQ, application notes, and software downloads: https://www.qeedji.tech/

```
Qeedji FRANCE
INNES SA
5A rue Pierre Joseph Colin
35700 RENNES

Tel: +33 (0)2 23 20 01 62
Fax: +33 (0)2 23 20 22 59
```

```
Qeedji GERMANY
INNES SA
Verbindungsbüro Deutschland
Lebacher Str. 4
66113 Saarbrücken

Tel: +49 (0)9386-979 39-14
Fax: +49 (0)9386-979 39-15
Mob: +49 (0)175 853 67 81
```

Part VII

Appendix

7.1 Appendix: Device status (status.xml)

The SMT210 device is updating regularly its device status stored in its `/.status` WebDAV directory:

```
http://<device-ip-addr>/.status/
```

This file can be periodically sent to a remote WebDAV server for monitoring purpose.

Status.xml example:

```
<device-status xmlns="ns.innes.device-status">
<device>
<id-type>MAC</id-type>
<mac>00-1c-e6-02-20-e2</mac>
<hostname>smt210</hostname>
<uuid>05c00002-0000-0000-0000-001ce60220e2</uuid>
<modelName><gekkota_os-model></modelName>
<modelNumber>4.13.13</modelNumber>
<serialNumber>00920-00002</serialNumber>
<middleware>gekkota-4</middleware>
<field1/>
<field2/>
<field3/>
<field4/>
<field5/>
<ip-addresses>
<ip-address>
<if-type>LAN</if-type>
<origin>dhcp</origin>
<value>192.168.1.119/17</value>
</ip-address>
<ip-address>
<if-type>LAN</if-type>
<origin>auto</origin>
<value>fc00::21c:e6ff:fe02:20e2/64</value>
</ip-address>
</ip-addresses>
<addons/>
</device>
<status>
<date>2020-03-31T17:40:16.055055+02:00</date>
<launcher>
<power-manager level="MAX"/>
<manifest-metadata xmlns:pzpm="ns.innes.gekkota.manifest">
<pzpm:publish-size>0</pzpm:publish-size>
<pzpm:publish-generator>gekkota_ui</pzpm:publish-generator>
<pzpm:publish-date>2020-03-30T06:45:26.759Z</pzpm:publish-date>
</manifest-metadata>
<state>NO_CONTENT</state>
</launcher>
<storage>
<total unit="byte">1912532992</total>
<used unit="byte">22161408</used>
</storage>
<display-outputs/>
<setup>
<configuration>
<metadatas/>
<version>2019-06-21T13:25:25Z</version>
</configuration>
</setup>
</status>
</device-status>
```