Qeedji

User manual

TAB10s

9.10.10 003C

Legal notice

TAB10s 9.10.10 (003C_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 TAB10s device. It explains also how to install a third party APK and make a AQS operating system upgrade.

Content of the package

Items	Description	Quantity
Device	TAB10s device with `AQS` embedded	1
Screen protection film	Stuck on the screen	1
Mounting bracket	Bracket for wall mounting	1
Drilling pattern leaflet	Drilling pattern	1
Screws	M2 x 35 mm (1,37 ") slotted countersunk screw (DIN 963) - a2 stainless steel	2
Adhesive tape	3M double sided tape 4905, material: VHB W x H x D: 65 mm (2.56 ") x 19 mm (0.75 ") x 0.5 mm (0.02 ")	2
Pads	3M single sided tape, material: silicone ∅: 8 mm (0,314 "), D: 1 mm (0,039 ")	4

Recommendations and warnings

This device is designed to be used indoor and can work 24/7.

The device is delivered without a power supply unit. Depending on your needs, `Qeedji` is making recommendation for suitable power supply references in the chapter § Power supply.

> ⚠ Before supply the TAB10s device with the USB connector of your computer, check with your computer's manufacturer that the USB connectors is suitable to deliver a sufficient power.
>
> ⚠ In case you had to remove the micro SD card, ensure first that the TAB10s device is powered off before removing or inserting the micro SD card. In case of bad handling, the micro SD card replacement would not be covered by the warranty.

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.

> ☛ *In this documentation, the unit of measurement for dimensions is done in millimeters followed by its equivalent value in inches.*

1.2 Labelling

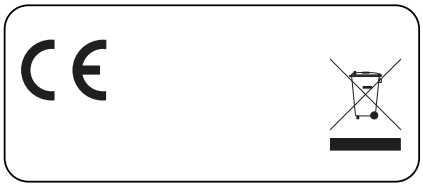
Product label

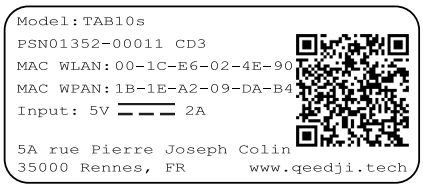
These are the labels stuck on the case. They are showing information embedded also in the QR code:

- the device model,
- the product serial number (PSN),
- the MAC addresses.

They are showing also:

- the power supply characteristics,
- the manufacturer Website,
- the conformity logo.





> ☛ *FCC certification in pending.*

> ☛ *The QR code on the product label is corresponding to the product identification URL, for example:* `i.qeedji.tech?model=TAB10e&sn=01352-00011&mac.wlan1=00-1C-E6-02-4E-90&mac.wpan1=1B-1E-A2-09-DA-B4`.

Packingbox label

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

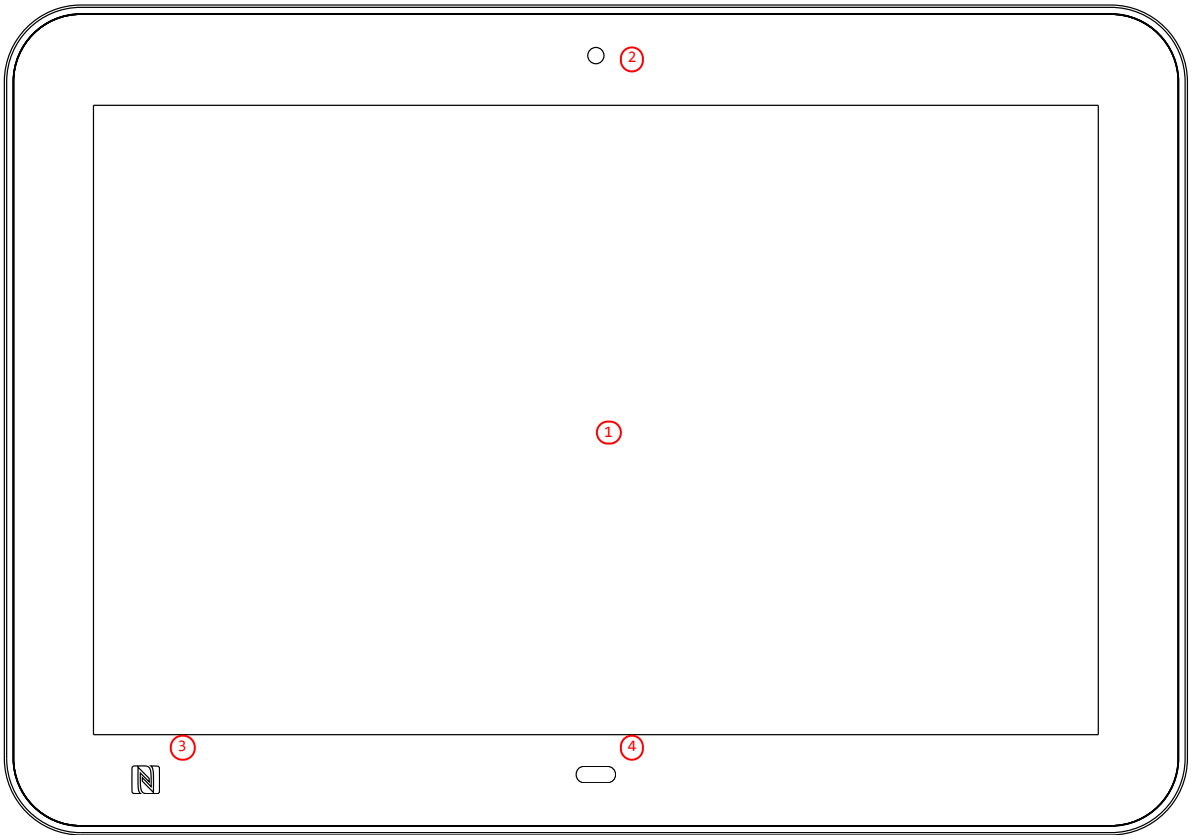
- the device model,
- the QR code embedding the product serial number (PSN),
- the manufacturer Website.

> ☛ *The QR code on the packingbox label is corresponding to the product PSN, for example:* `PSN01352-00011 CD3`.

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

1.3 Product faces

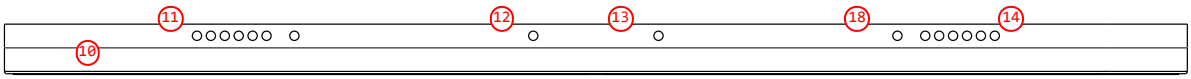
Device's front face



- (1) Touch screen,
- (2) Camera,
- (3) Built-in NFC/RFID sensor,
- (4) [1].

[1] *In the default factory preferences, the distance threshold for the proximity sensor is 1.5 meter. For further information contact support@qeedji.tech.*

Device's up face

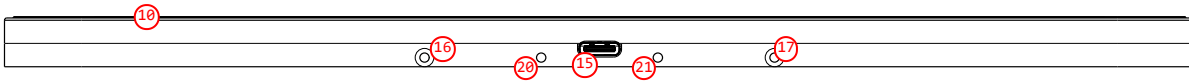


- (10) Surround light,
- (11) Mono speaker,
- (12) System button[2],
- (13) Built-in microphone n°1,
- (18) Built-in microphone n°2,
- (14) Heat pipe.

[2] The system button is hidden inside the hole.

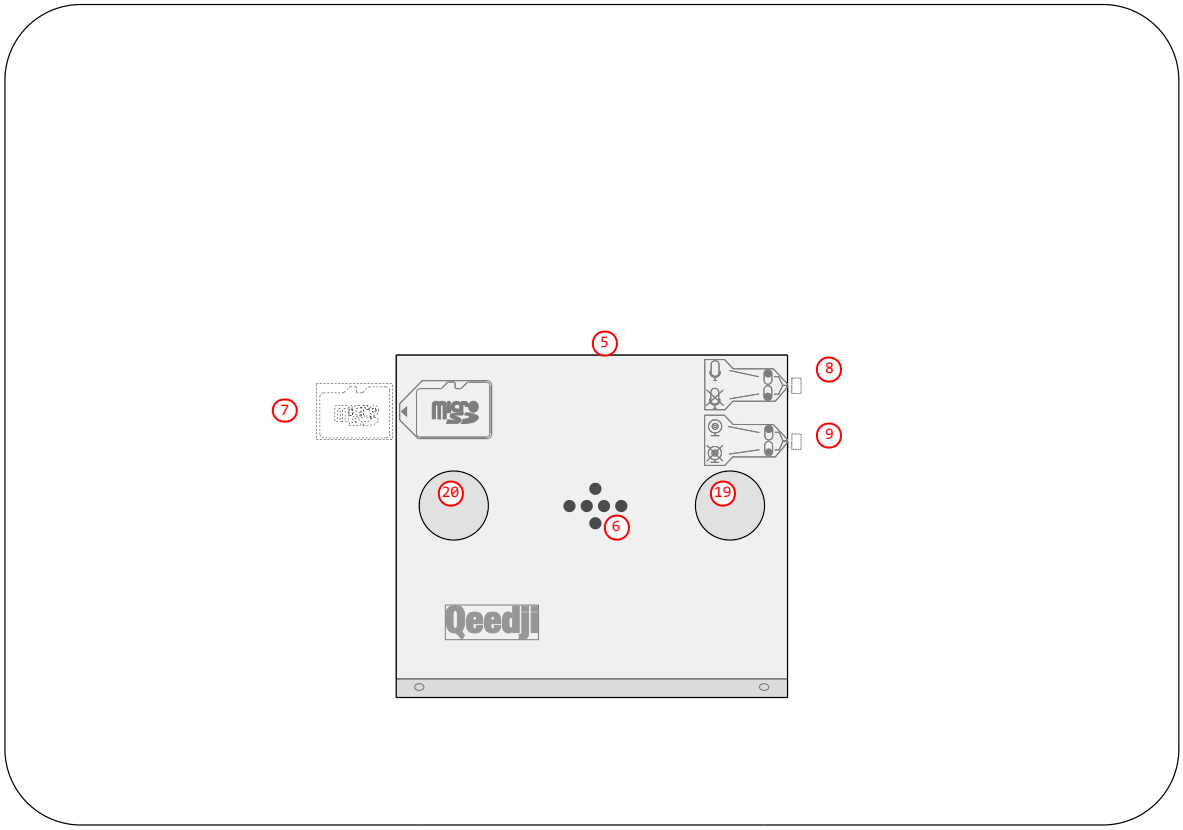
> ⚠ Do not cover the top of the heat pipe which is designed to evacuate naturally the heat of the device when it is running.

Device's bottom face



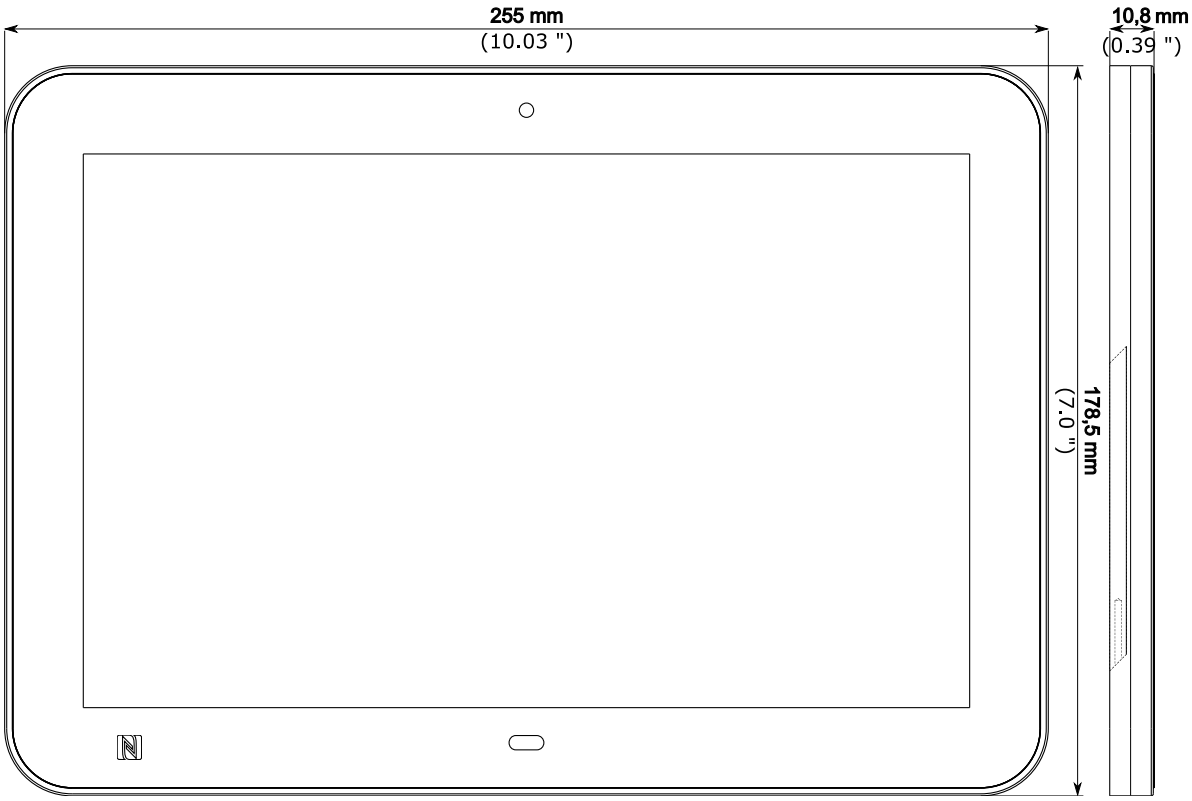
- (10) Surround light,
- (15) USB-C connector,
- (16) Mounting bracket orifice/screw n°1,
- (17) Mounting bracket orifice/screw n°2,
- (20) USB-C locking orifice n°1,
- (21) USB-C locking orifice n°2.

Device's rear face



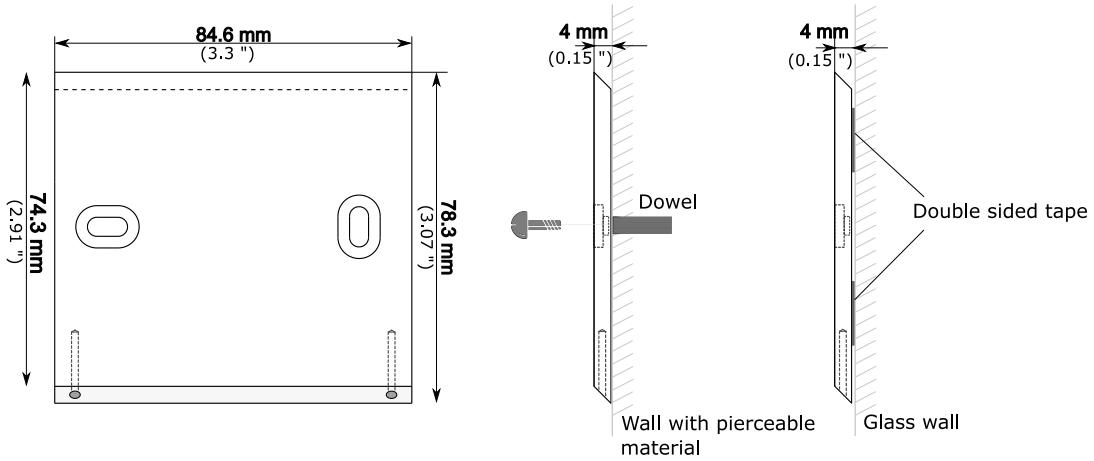
- (5) Bevelled profile to welcome the mounting bracket,
- (6) POGO type connector,
- (7) Micro SD card connector with its micro SD card,
- (8) Microphone DIP switch,
- (9) Camera DIP switch,
- (19) (20) Holes to host screws heads to fix the mounting bracket.

1.3.1 Device dimensions



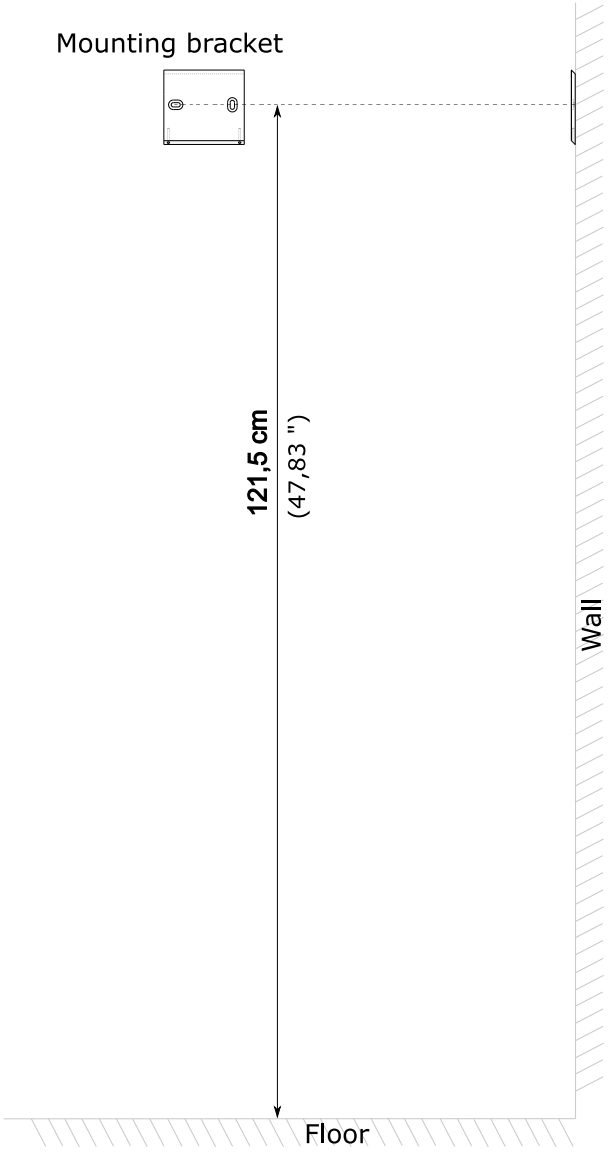
1.3.2 Device fixture

The TAB10s device can be hung on the wall using a mounting bracket (supporting or not the POGO type interface).



⚠ To know the device fixture height, refer to the legislation in force in your country, related to the accessibility to disabled persons of establishments open to the public during their construction and of facilities open to the public during their development.

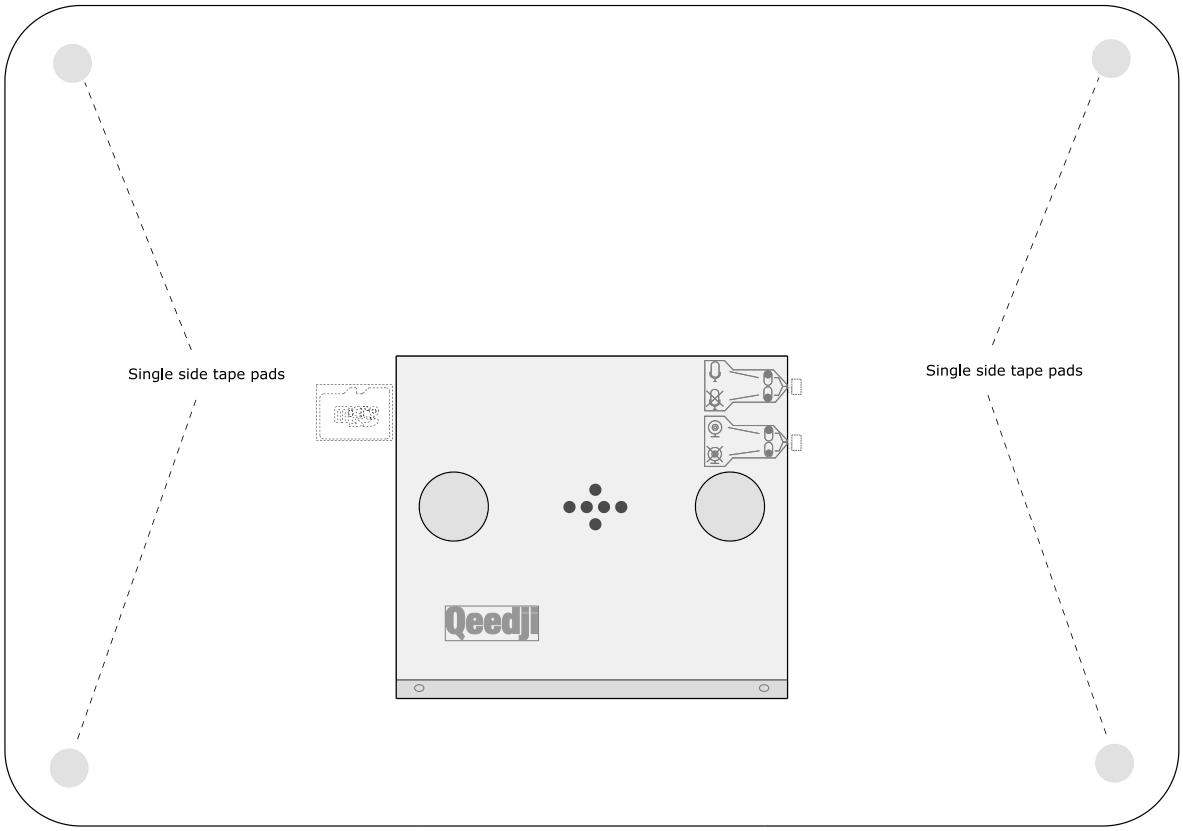
☛ *The legislation in force in France, for example implies to install the top of the display at 130 cm (51,181 ") maximum far from the floor. For the TAB10s device, add 2.4 cm (or 0,787 ") to this height to determine the maximum height of the top edge of the TAB10s device. For example, for the France country, the top edge of the device should be (130 + 2.4) = 132.4 cm (52,125 ") far from the floor. So, to find the center of the hole of the mounting bracket should be at 130 cm (51,18 ") - 8,5 cm (3.35 ") = 121,5 cm (47,83 ").*

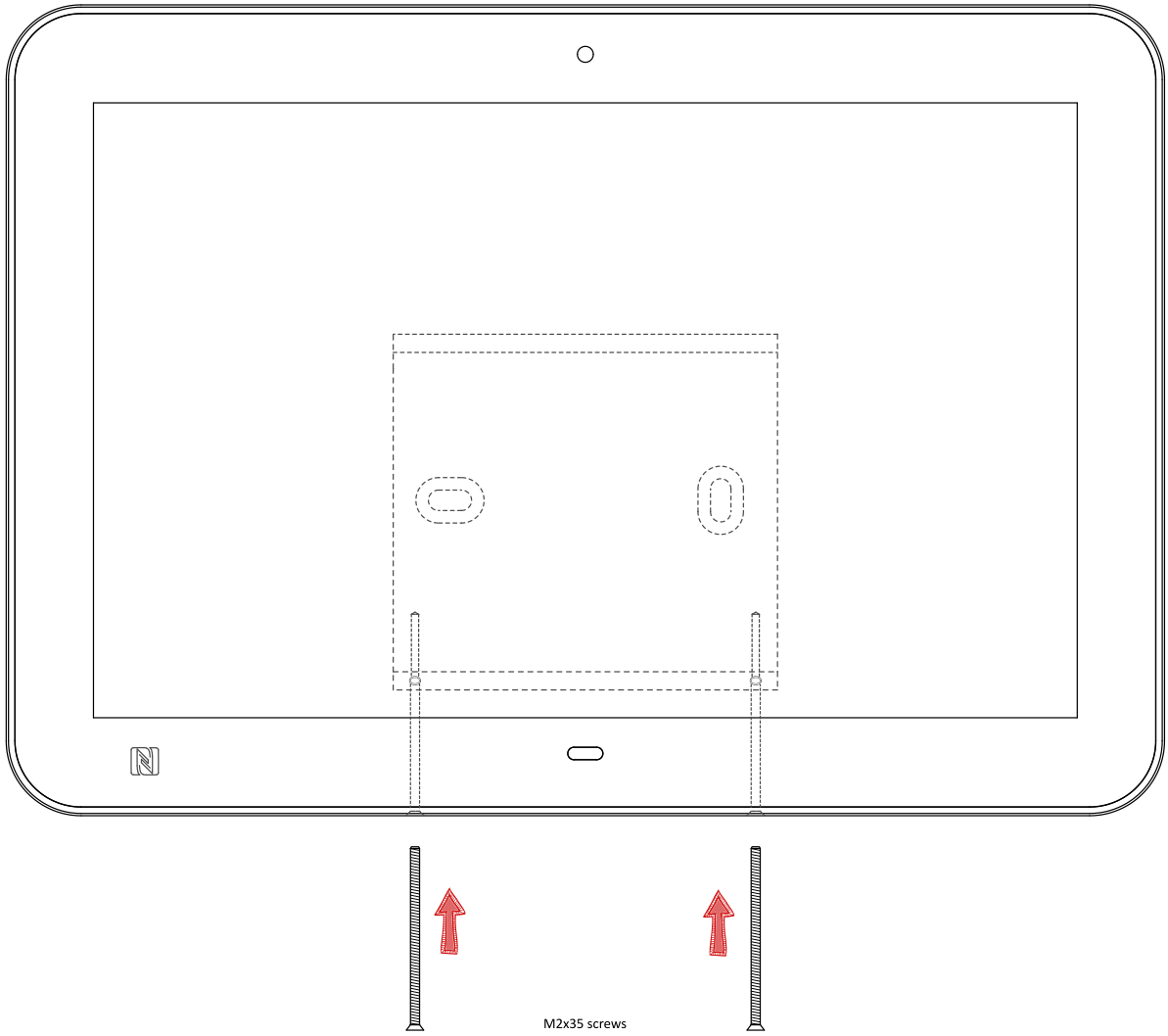


⚠ The TAB10s device is designed to be installed in landscape mode only.

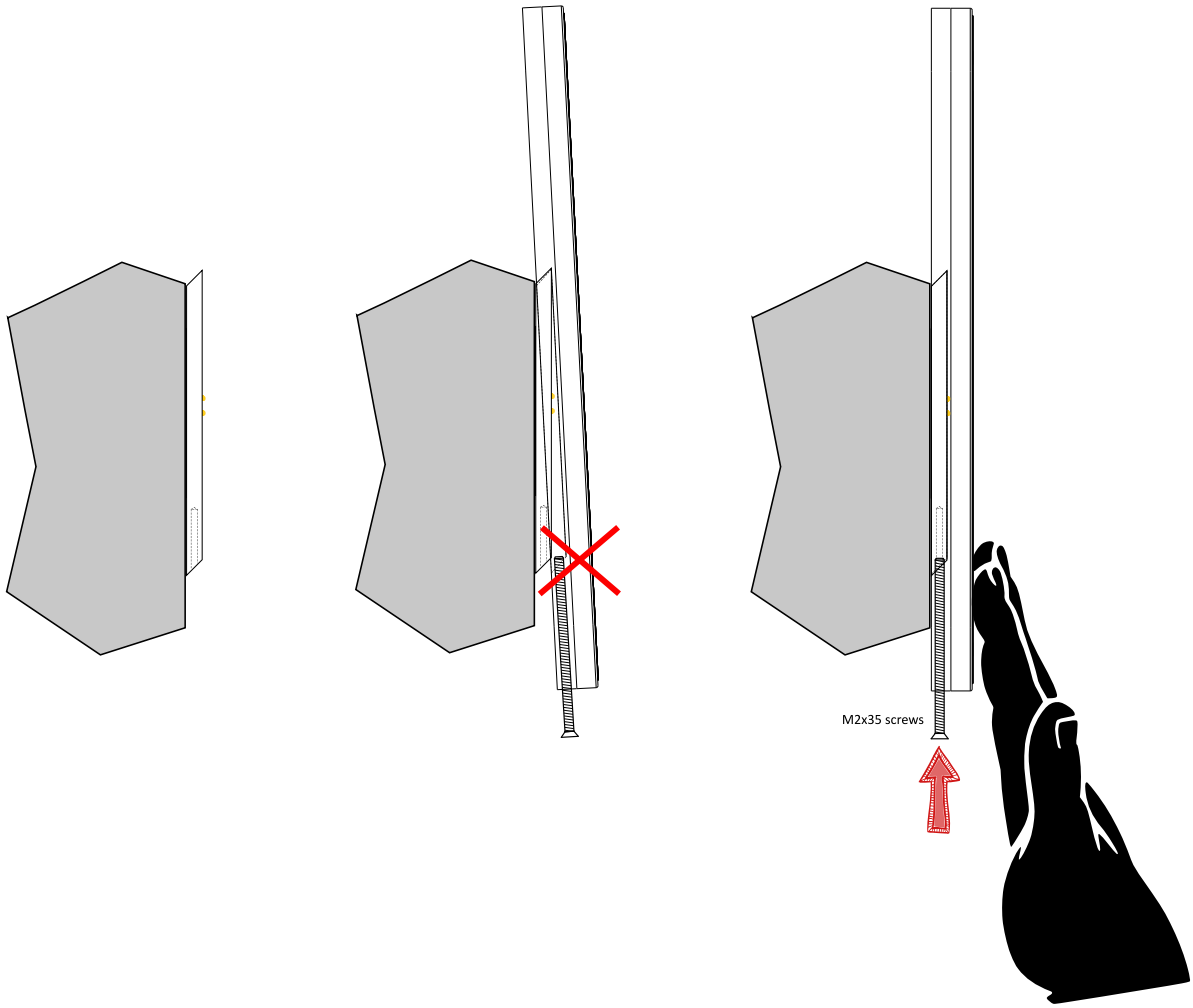
Before installing the TAB10s device:

- check that the position of the microphone DIP switch and the camera DIP switch is matching the customer needs,
- stick, like explained below, the 4 single side tape pads at the back of the TAB10s device, respectively at the 4 corners.




M2x35 screws

> ⚠ When installed on the `NAPOE109kt` or `NAPOE109ft` products having a mounting bracket with a `POGO` connector, before mounting the screws to lock the device, check that the TAB10s device is installed on the `NAPOE109kt` or `NAPOE109ft` products stricly on the vertical position else some unexpected power supply issue could be faced.



To check that the tablet is properly supplied, ensure that the tablet is displaying the `AQS` desktop content, or any App on the screen.

Swipe from the extreme top of the screen to the bottom of the screen to check the pictogram inside the notification banner.

`WLAN_1` **network connectivity**	**Information**
	When this WIFI pictogram is displayed and filled with the number of bars corresponding to the WIFI reception level, the `WLAN_1` connection is up.
	If the WIFI pictogram is displayed but stays empty, the `WLAN_1` connection is down.

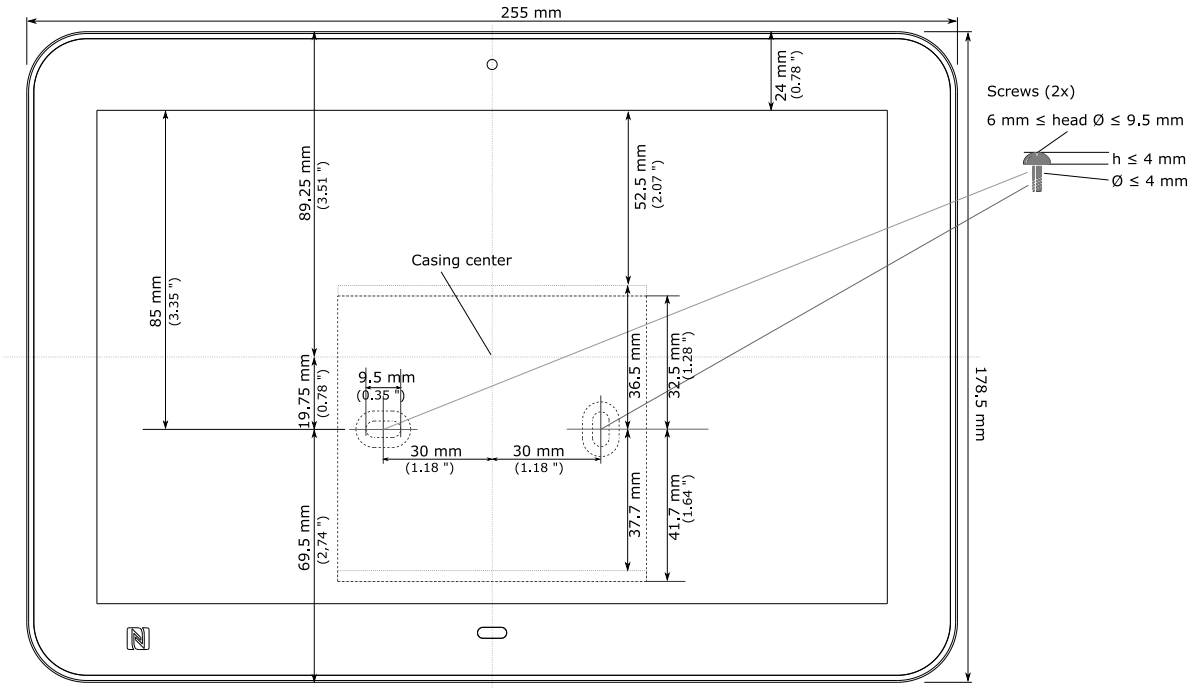
`LAN_1` **network connectivity**	**Information**
	When this LAN pictogram is displayed, the `LAN_1` connection is up. When this LAN pictogram is not displayed, the `LAN_1` connection is down.

Only one of the interface can be up at a time.

When the TAB10s device is properly installed with `AQS` running with a consistent network pictogram, you can remove the protective film from the screen.

1.3.3 Drilling pattern

In case you want to hang the TAB10s device on the wall, you can do it using the provided mounting bracket.
Follow the drilling pattern to install it.

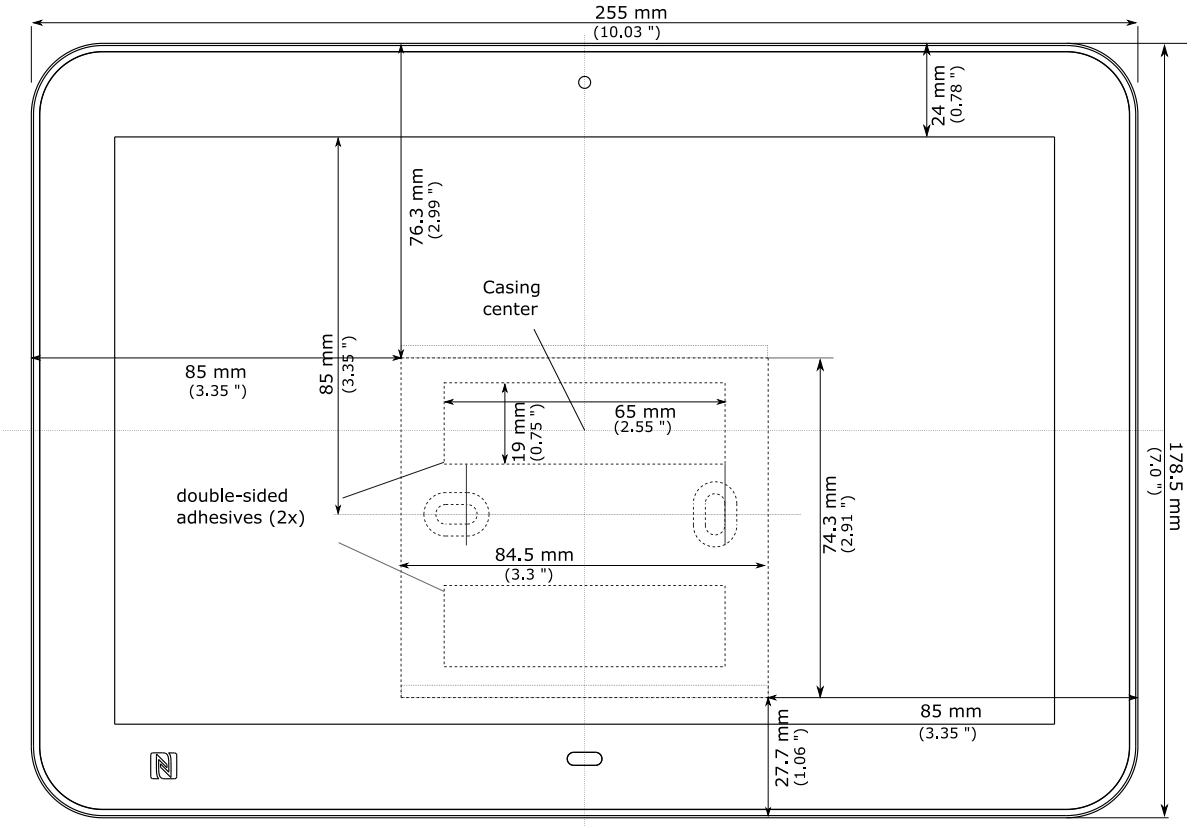


This mounting bracket can be fixed using screws (recommended for walls with pierceable material).

> ☛ *The screws and dowels required to fix the mounting bracket on the wall are not provided with the product. They can depend on the wall material.*

Adhesive pattern

If it is not possible to fix the device with screws, for example when needing to be fixed on a glass wall, you can use the provided adhesive tapes.



> ⚠ Clean carefully the surface before sticking the adhesive tapes.
>
> ⚠ Press firmly the mounting bracket against the glass wall before hanging and locking the TAB10s device on it.

1.4 Power supply

This device is intended to work with an external power supply, not provided by default. The two ways to supply the device are:

- either through the USB-C connector,
- or through the POGO type connector.

Power supply references

Depending on your needs, you can order among several power supply unit references recommended by Qeedji.

Commercial reference	Model	Information
`EXC.NAPOE109KT` [1]	`NAPOE109kt`	The POGO connector supports `power delivery` and Ethernet network connectivity
`EXC.NAPOE109KU` [2]	`NAPOE109ku`	The USB-C connector supports `power delivery` and Ethernet network connectivity
`EXC.NAPOE109FT` [3]	`NAPOE109ft`	The POGO connector supports `power delivery` and Ethernet network connectivity

> ☛ *For supply need only, you can purchase a single 110 V~/230 V~ to USB-C 5 V / 3 A wall plug.*
>
> ☛ *The device can be power supplied by USB-C or POGO type connector. Once supplied by one side, the device won't never change its power supply origin, even if the second side becomes available afterwards. The choice of power supply origin is renegociated each time the device is rebooting; if the USB-C and POGO type connectors are both power supplied, the device will select POGO type connector origin each time the device is rebooting.*

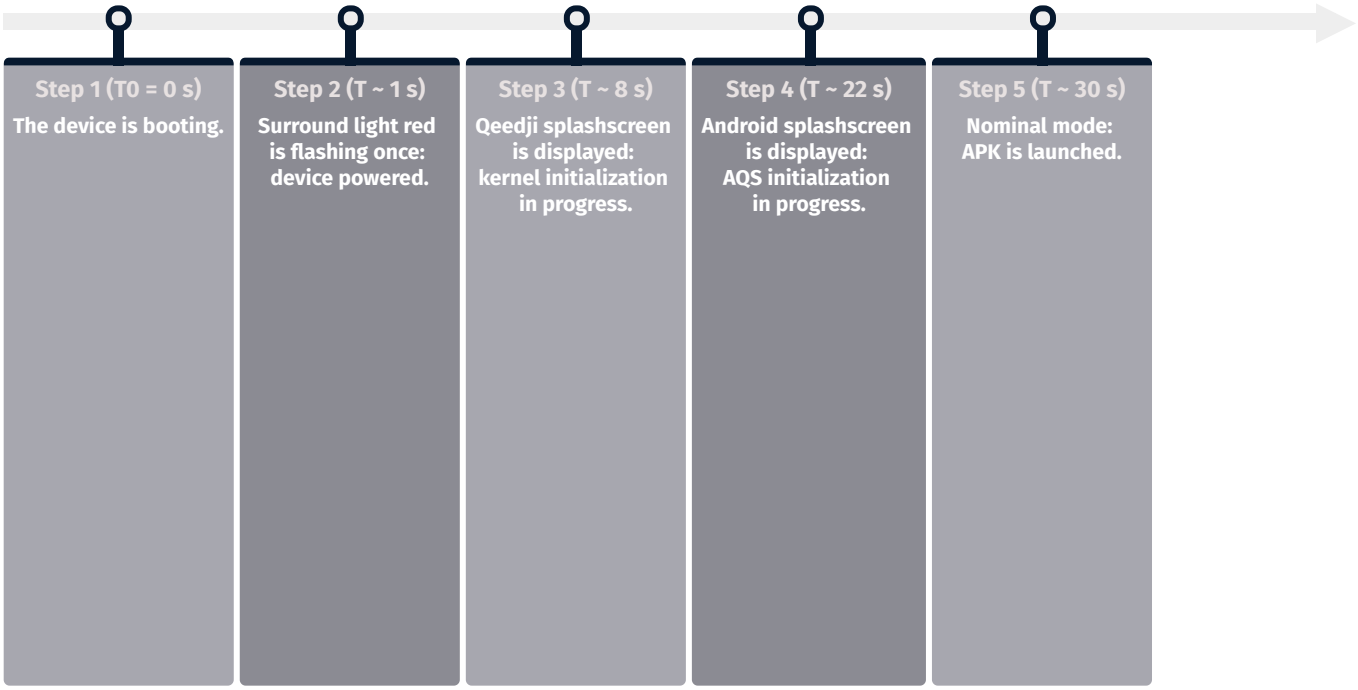
[1] For further information, refer to the NAPOE109kt user manual.

[2] For further information, refer to the NAPOE109ku user manual.

[3] For further information, refer to the NAPOE109ft user manual.

For further information before ordering, contact sales@qeedji.tech.

1.5 Device start-up steps



1.6 Surround light behaviour at power-up

State	Information
Sequence of **1** short green flash of 300 ms, periodic in alternance with 4 seconds Off.	Error: the used power supply has not enough power to launch the software[1].
Sequence of **2** consecutive short green flashes of 300 ms, periodic in alternance with 4 seconds Off.	Error: the micro SD card is not present, or has been removed[2]. Don't forget to power off your device before installing back your micro SD card.
Sequence of **3** consecutive short green flashes of 300 ms, periodic in alternance with 4 seconds Off.	Error: the micro SD card is unusable or the boot software is missing. If the problem persists, contact support@qeedji.tech.
Sequence of **4** consecutive short green flashes of 300 ms, periodic in alternance with 4 seconds Off.	Error: an internal issue has been detected during power sequencing. If the problem persists, contact support@qeedji.tech.
Sequence of **5** consecutive short green flashes of 300 ms, periodic in alternance with 4 seconds Off.	Error: the micro SD card or the AQS is corrupted and cannot be launched. Follow the factory recovery process to restore your micro SD card. If the problem persists, contact support@qeedji.tech.

[1] Try with another suitable power supply unit. If the problem persists despite of an appropriate power-supply unit, contact support@qeedji.tech.

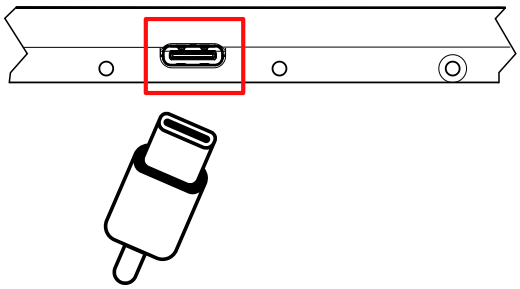
[2] Remove the mounting bracket from the device, or remove the device from the mounting bracket, and check that your micro SD card is properly inserted in the device.

1.7 Connectors pin-out

> ☛ *The access to some connectors or DIP switches may require to remove the mounting bracket or remove the TAB10s device from the wall. Refer to the chater § Procedure to access to the back connectors.*

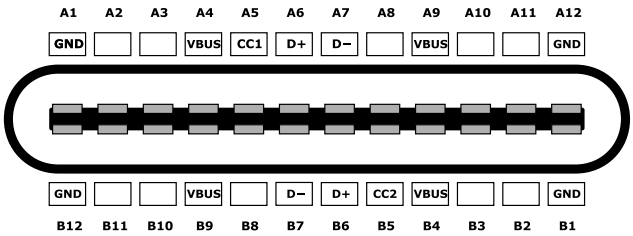
USB-C connector

The device can be supplied by the USB-C connector located at the bottom face of the product.



Information type	Value
Type	USB type-C
Data	USB 2.0
Power	USB PD[1] (Power delivery)

This is the USB-C pin-out for the TAB10s:

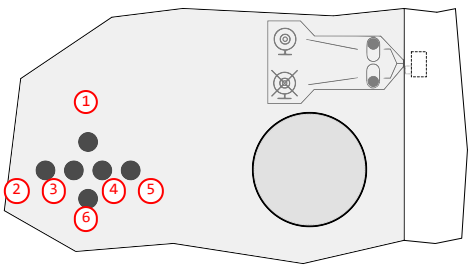


> ☛ *The USB-C connector is supporting Ethernet over USB.*

[1] *The TAB10s device is an USB sink device by default, in order to be supplied by an external power source device. It implements data-role swap, in order to be able to become the data host, and hence, to support ethernet-to-usb external bridges while being supplied by this bridge. When operating in sink mode, you must take care when selecting your power supply source and usb cable, select a power source able to drive 5 V - 3 A, and choose high quality cables, especially when you have a long distance between source and the TAB10s device.* `Qeedji` *advises to use* `EXC.NAPOE109KU` *accessory, as it is fully qualified with the TAB10s device. The TAB10s device can be an USB source device only when supplied by the POGO type connector. So it can support an external USB dongle for example. In this case, you have to take care to not sink too much current through USB-C connector.*

POGO type connector

The device can be supplied by the POGO type connector located at the back of the product.



- (1) VCC,
- (2) GND,
- (3) USB+,
- (4) USB-,
- (5) GND,
- (6) VCC.

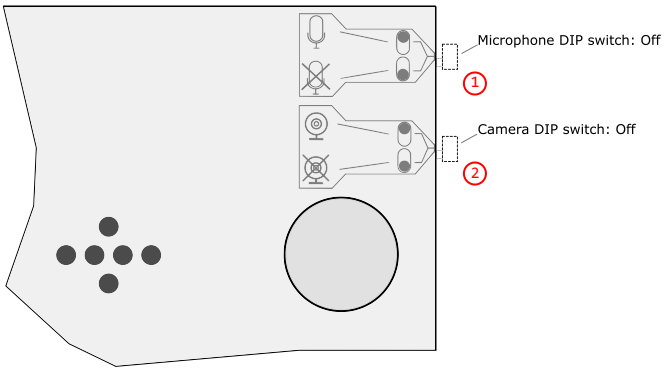
> ☛ *The POGO type connector allows to supply the device and offers an USB 2.0 host interface, for Ethernet over USB for example.*

Dipswitches for microphone and camera

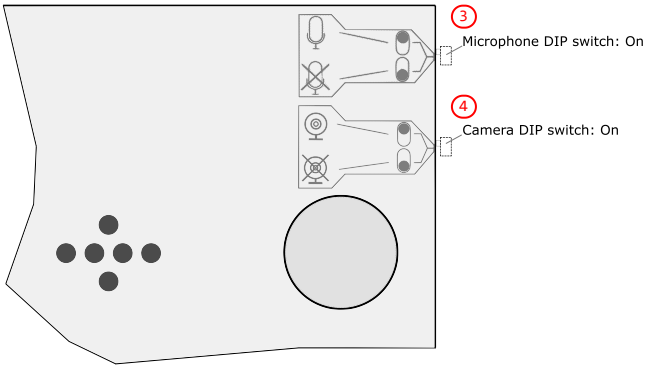
For confidentiality purpose, the TAB10s device has two switches at the back of the product allowing to activate or inactivate respectively the microphone and the camera peripherals.

When the DIP switch is facing the crossed microphone, the microphone peripheral is inactivated.
When the DIP switch is facing the crossed camera, the camera peripheral is inactivated.

Example of configuration when the microphone (1) and the camera (2) peripherals are inactivated:



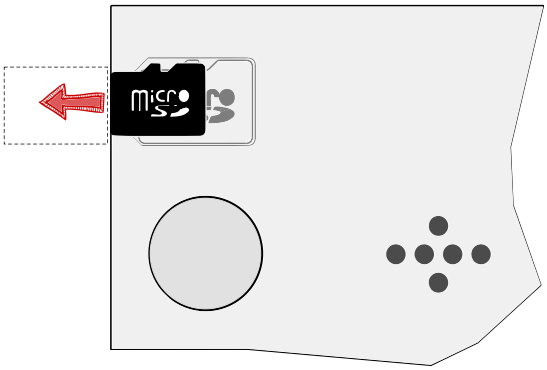
Example of configuration when the microphone (3) and the camera (4) peripherals are activated:



Micro-SD card

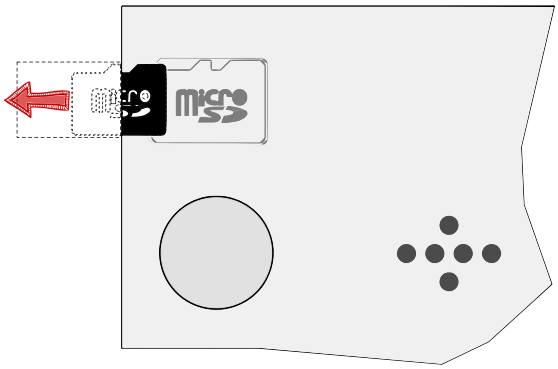
The micro SD card connector is located on the rear face of the TAB10s. A `micro SD` serigraphy is showing the connector location.

Step 1: Place the micro SD card in the right sense close to the connector entry.

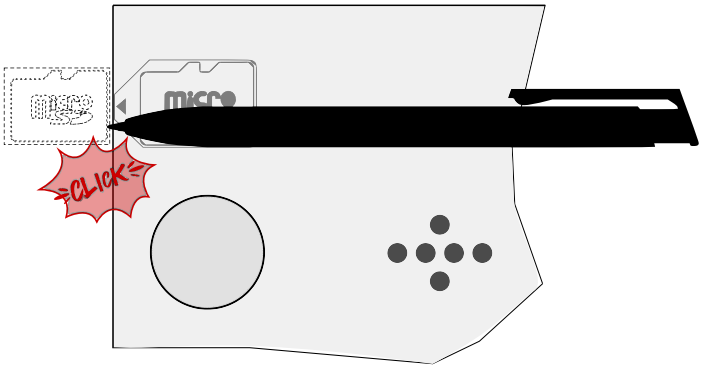


> ☛ *It may be required to lift the micro SD card so that it can enter into the connector. Press a little on it to tilt it.*

Step 2: Glide the micro SD card in the right sense with the hand towards the micro SD card connector until you feel the spring.



Step 3: When the spring of the SD card connector is responding properly, helped with a pen, push the micro SD card towards the connector until hearing a clic.



The 16 GB micro SD card, containing the `AQS` for TAB10s device, is provided by default and is already installed in the product.
The micro SD card is partitioned to be compliant with `AOSP` . This is the micro SD card partition mapping:

Number	Name	Size	File system	Function
1	dtbo_a	4 MB		dtbo.img (device tree)
2	dtbo_b	4 MB		dtbo.img (device tree)
3	boot_a	48 MB		boot.img
4	boot_b	48 MB		boot.img
5	system a	2,5 GB	Ext4	Android system files under /system
6	system b	2,5 GB	Ext4	Android system files under /system
7	misc	4 MB		recovery store bootloader message, reserve
8	metadata	2 MB		system slide show
9	persist data	1 MB		option to operate lock\unlock
10	vendor_a	256 MB	Ext4	vendor.img
11	vendor_b	256 MB	Ext4	vendor.img
12	fbmisc	1 MB		state of lock\unlock
13	vbmeta_a	1 MB		verify boot's metadata
14	vbmeta_b	1 MB		verify boot's metadata
15	userdata	8,4 GB	Ext4	application data storage for system application, and for internal media partition, in /mnt/sdcard/ dir.

If you have to remove the micro SD card,

- power off the device,
- use a little pen and press on the micro SD card. The spring will eject automatically the card.

If you have to insert again the micro SD card,

- power off the device,
- use a little pen and press on the micro SD card until hearing a clic,
- power on back the device.

> ⚠ The warranty does not cover the micro SD card RMA in case it is burnt by a wrong respect of this procedure.

1.8 Procedure to access to the back connectors

Do follow this procedure to get access to:

- the camera hardware DIP switch,
- the microphone hardware DIP switch,
- the micro SD card connector,
- the POGO type connector.

Procedure when the device is supplied by the USB-C connector:

- unplug the USB-C cable from the device,
- untighten the two screws at the bottom of the product,
- remove the mounting bracket from the device.

Procedure when the device is hung on the wall with a mounting bracket:

- untighten the two screws at the bottom of the product,
- remove the device from the wall.

The connectors are now visible at the back of the product.

Part II

System configuration

2.1 Introduction

To support the APK deployment, the AQS operating system version upgrade and the TAB10s device configuration update, the TAB10s device embeds the `Qeedji System` service which is launched automatically as soon as the AQS is running. It supports:

- APK installation thanks to a `.apk` file:
  - uploaded with the device configuration Web user interface,
  - hosted on one USB storage device,
  - pushed on the `.apps` WebDAV directory with a WebDAV client,
- device configuration thanks to a Javascript configuration script:
  - uploaded with the device configuration Web user interface,
  - hosted on one USB storage device,
  - pushed on the `.configuration` WebDAV directory with a WebDAV client,
  - hosted on a TFTP server + DHCP server (code 66),
- `AQS` operating system upgrade thanks to a `.fqs` firmware:
  - uploaded with the device configuration Web user interface,
  - hosted on one USB storage device,
  - pushed on the `.software` WebDAV directory with a WebDAV client.

2.1.1 AQS operating system upgrade with a fqs firmware

The TAB10s device embeds an `AQS` operating system (V9.10.10 or above). It can be upgraded by some maintenance `.fqs` firmware having some evolutive or corrective changes.

To update your TAB10s device with a new `AQS` operating system version, download the `aosp-tab10-setup-9.YY.ZZ.fqs` firmware from the Qeedji Website.

> ☛ *Both `AQS` operating system upgrade or downgrade are supported.*
>
> ☛ *After an `AQS` operating system upgrade, the TAB10s device configuration, the user data partition and the user APK are kept.*

The `AQS` operating system version upgrade can be done by:

- uploading the `.fqs` firmware with the device configuration Web user interface. For further information, refer to the chapter § AQS operating system upgrade with the device configuration Web user interface,
- putting the `.fqs` firmware on an USB storage device then by inserting it in the TAB10s USB-C connector, or through the third party equipment connected to the USB-C connector. For further information, refer to the chapter § AQS operating system upgrade by USB,
- putting the `.fqs` firmware on the `.software/` directory of the WebDAV server. That requires to use credentials values of any connection profiles except `Application user`. For further information, refer to the chapter § AQS operating system upgrade by WebDAV.

AQS operating system upgrade with the device configuration Web user interface

It is possible to upgrade the `AQS` operating system version of the TAB10s device by connecting to the device configuration Web user interface with a Web browser and upload a `.fqs` firmware.

For further information, refer to the chapter § Maintenance > Firmware.

For further information about the connection to the device configuration Web user interface, refer to the chapter § Applicative user interface.

AQS operating system upgrade by USB

Prerequisite:

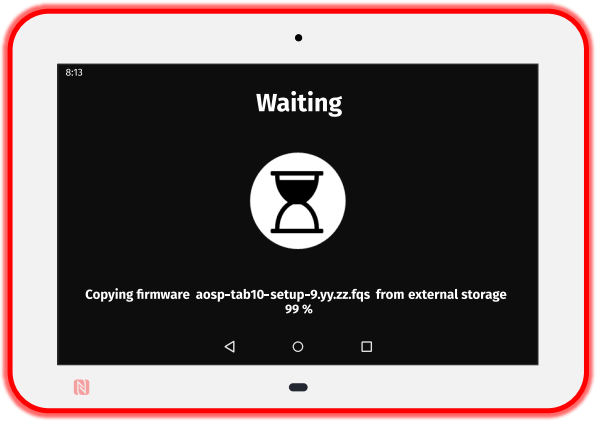
- the TAB10s device needs to have a suitable power supply equipment allowing to support `AQS` operating system upgrade by the USB-C connector.

Copy the `aosp-tab10-setup-9.YY.ZZ.fqs` archive at the root directory of an USB storage device and insert it on the USB-C connector of the TAB10s device (or on the third party equipment connected to the USB-C connector).

> ☛ *In case several supported files type are present like `.fqs`, `.apk` and `.js`, only the `AQS` operating system will be done.*
>
> ⚠ If the USB storage device contains several supported `.fqs` firmware files, the `AQS` operating system upgrade can not be done and no message appears.

Plug the USB storage device. This message should be displayed.

> ☛ *The copy duration is depending on the `.fqs` firmware size. It is roughly 1 min.*

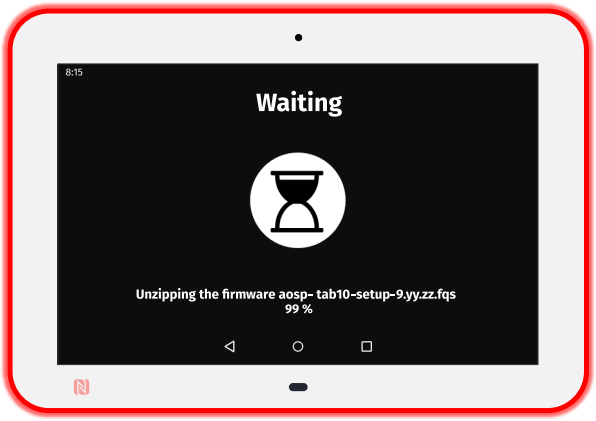


This message is then displayed until the USB storage device is unplugged.

Unplug the USB storage device.

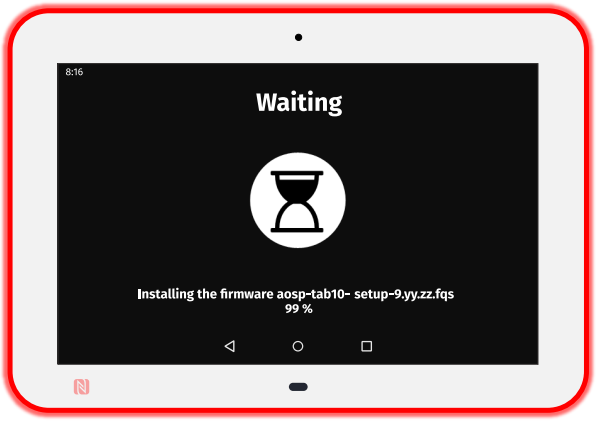
> ☛ *Once the USB storage is unplugged, the `AQS` operating system upgrade duration is depending on the `.fqs` firmware content. It can be for example: 8 minutes and 30 seconds.*

This message is displayed showing that the `.fqs` firmware is being unzipped.

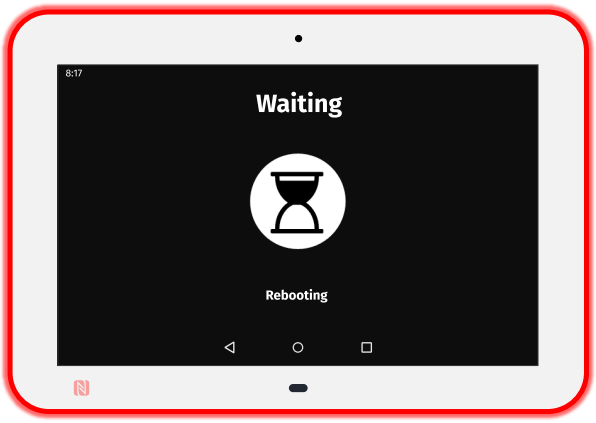


This message is then displayed showing that the `.fqs` firmware is being installed.

> ☛ *The installation duration is depending on the `.fqs` firmware version.*



After the `.fqs` firmware installation, the device is rebooting automatically once. This message is displayed while the device has not yet restarted.



AQS operating system upgrade by WebDAV

Prerequisite:

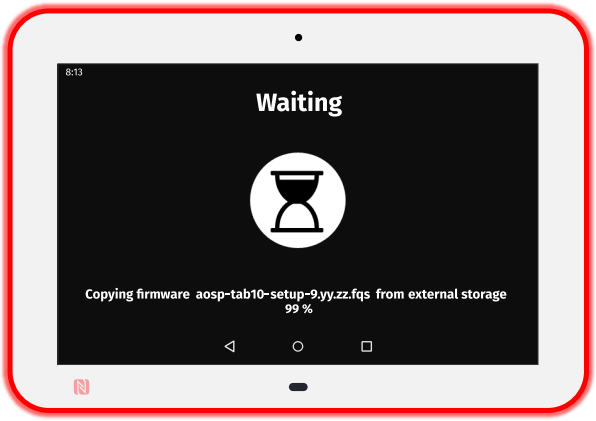
- a WebDAV client (*CarotDAV* or *BitKinex* for example) is installed on your computer or
- the TAB10s device is mounted as a disk on the MS-Windows explorer. For further information, refer to the chapter § device network disk mounting in MS-Windows explorer.

> ☛ *The credentials values of any connection profile except `Application user` is required to write on the `.software` WebDAV directory.*
>
> ☛ *The port value put at factory to access to the WebDAV directory is `80`. The port value can be modified by using a configuration script. For further information, refer to the chapter § Device configuration by script.*
>
> ☛ `https://` *scheme to access to the TAB10s is not yet supported.*

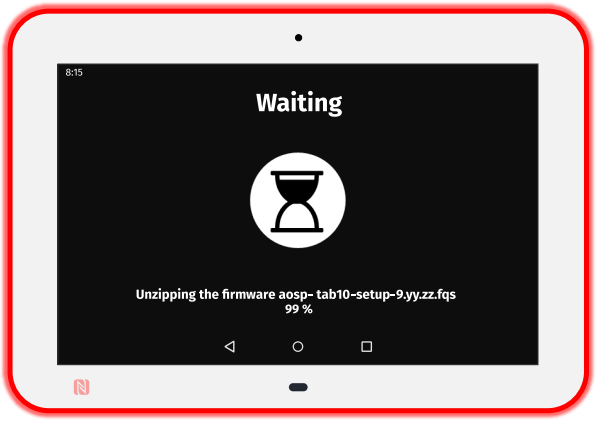
Copy the `aosp-tab10-setup-9.YY.ZZ.fqs` archive in the `.software/` directory located at the root of the TAB10s WebDAV server.

This message should be displayed.

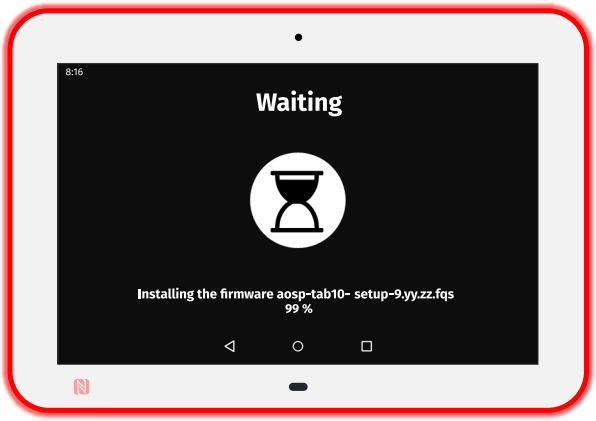
> ☛ *The copy duration is depending on the `.fqs` firmware size.*



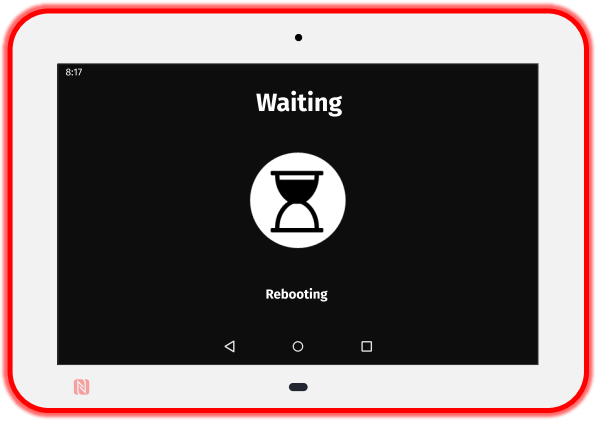
This message is displayed showing that the firmware is being unzipped.



This message is then displayed showing that the firmware is being installed. The installation duration is depending on the `AQS` version.



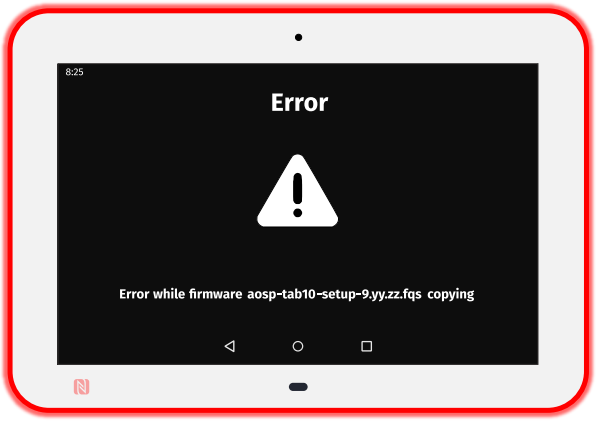
After the `AQS` version installation, the device is rebooting automatically once. This message is displayed while the device has not yet restarted.



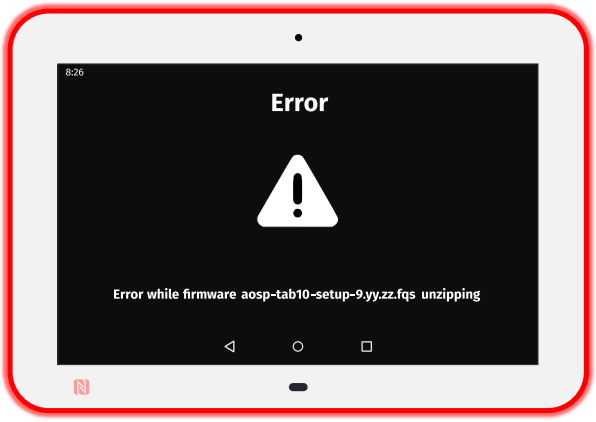
> ☛ *Once the `AQS` operating system is installed, the `.fqs` firmware is removed from the device.*

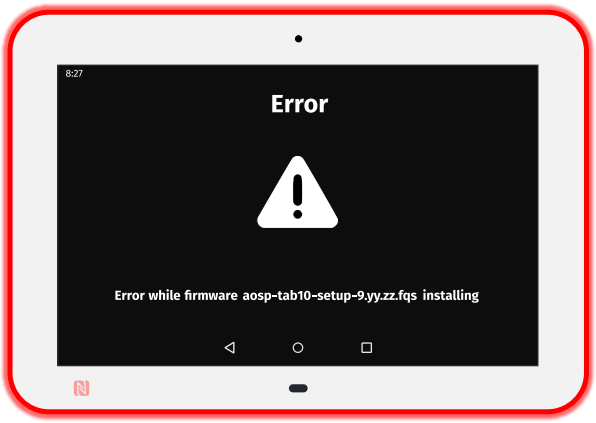
Error messages when following the previous procedures

This message is displayed for ten seconds when an error occured while copying the `.fqs` firmware. The USB storage device is not properly supported. Restart again the operation with another USB storage device. If the problem persists, you can contact support@qeedji.tech



One of these messages could occur when the `.fqs` firmware is corrupted or when the USB storage device has been removed when the copy was still in progress. If required, download again the `.fqs` firmware from the Qeedji Website and try again. If the problem persists, contact support@qeedji.tech.





2.1.2 APK deployment

Prerequisite:

- the APK has to be an Android application with the `.apk` file extension,
- the APK has to be fully compatible with `AQS` 9 and suitable for TAB10s (peripherals, ...),
- the APK, requiring `system user` execution rights, should be either signed with a Java keystore, or set as `system App` by a configuration script.

For further information, refer to the TAB10s developer manual.

Some APK examples can be donwloaded from the Qeedji Website. For further information, contact sales@qeedji.tech.

Third party APK

The TAB10s device is intended to work with one or several custom Android APKs. The third party APK are not provided.

The TAB10s device is embedding `AQS` 9 based on the AOSP SDK 28.

To develop your third party APK, `Qeedji` provides a TAB10s developer manual which is giving links to github to start to work on `AQS` 9 for TAB10s device (APK examples) and explains also the procedure to sign an APK, or to set App as system App, the APK requiring `system user` execution rights.

> ☛ *To develop your third party APK, `Android` software development skills and `Android Studio` skills are required.*

The APK installation is done by:

- uploading an `.apk` file with the device configuration Web user interface. For further information, refer to the chapter § APK installation with the device configuration Web user interface,
- putting an `.apk` file on an USB storage device then by inserting it in the TAB10s USB-C connector, or through the third party equipment connected to the USB-C connector. For further information, refer to the chapter § APK version upgrade by USB.
- putting an `.apk` file on the `.apps/` directory of the WebDAV server. For further information, refer to the chapter § APK installation by WebDAV.

> ☛ *The APK installation by USB is allowed by default in the `AQS` 9. This feature can be inactivated by using the `disableExternalStorageCopyApk();` function in the configuration script. For further information, refer to the chapter § Device configuration by script.*

APK installation with the device configuration Web user interface

It is possible to install `APK` on the TAB10s device by connecting to the device configuration Web user interface with a Web browser and upload a `.apk` file in the `.apps` WebDAV directory.

For further information, refer to the chapter § Maintenance > Files.

For further information about the connection to the device configuration Web user interface, refer to the chapter § Applicative user interface.

APK installation by USB

> ☛ *The necessary rights for each APK are temporarily granted during the APK installation.*

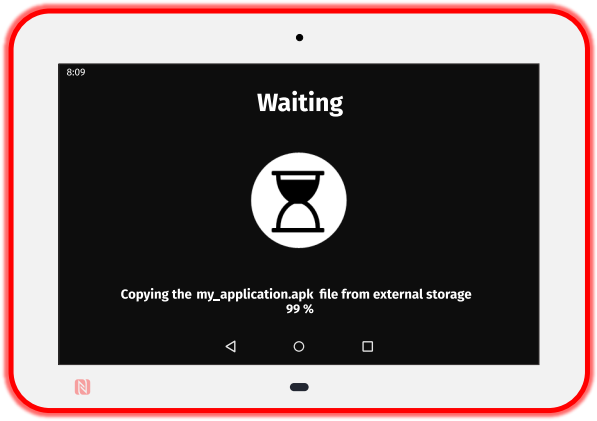
Prerequisite:

- the TAB10s device needs to have a suitable power supply equipment allowing to support APK installation by the USB-C connector.

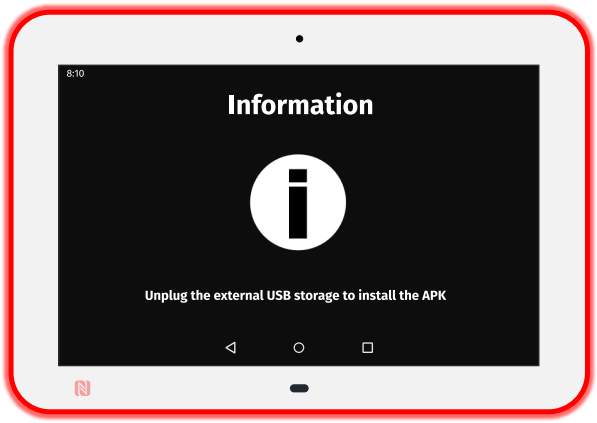
Copy the `.apk` file at the root directory of an USB storage device and insert it on the USB-C connector of the TAB10s device (or on the third party equipment connected to the USB-C connector).

> ☛ *If the USB storage device contains several APK at the root, each APK is installed in the alphabetical order.*
>
> ☛ *To reinstall a same version of an APK, you have to remove it before.*
>
> ☛ *To upgrade an APK with a different signature, you have to remove it before.*

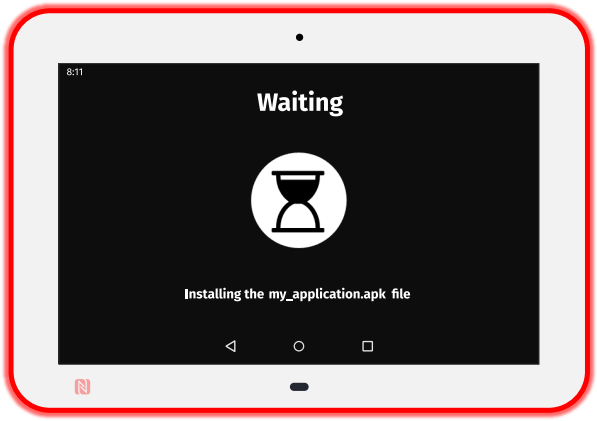
Plug the USB storage device. This message should be displayed while the APK copy has not been completed.



This message is displayed until the USB storage device is unplugged.

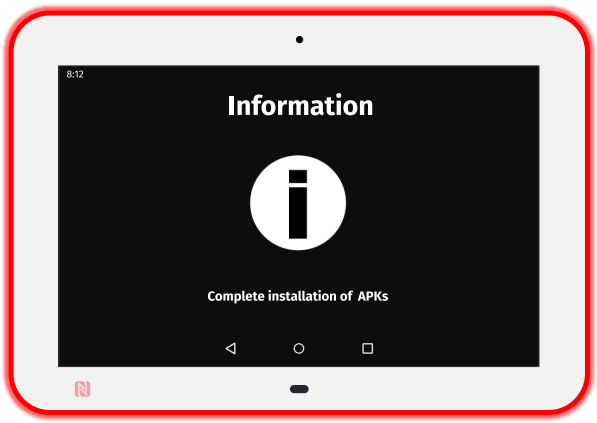


Unplug the USB storage device. This message should be displayed for few seconds, the time for the `AQS` to install the APK.

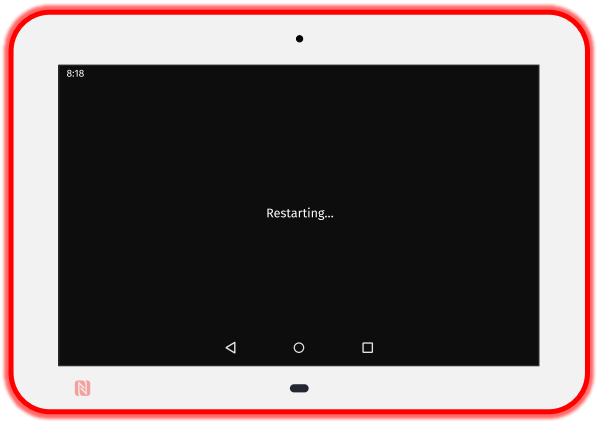


> ☛ *In case several APK are available on the USB storage device, the installing message appears for each new APK to install.*

When the APK installation is completed, this message should be displayed for 10 seconds.



This message is then displayed until the device is rebooting automatically once.



APK installation by WebDAV

Prerequisite:

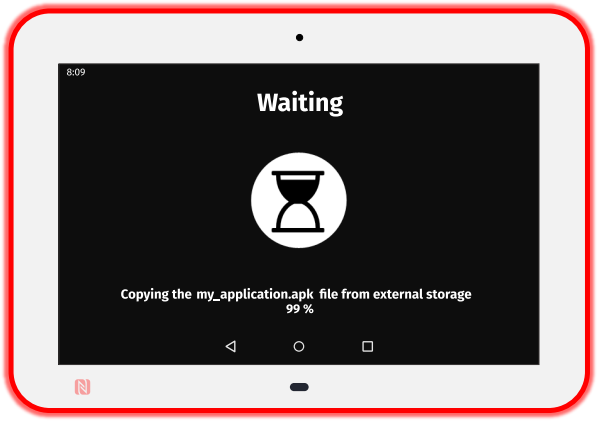
- a WebDAV client (*CarotDAV* or *BitKinex* for example) is installed on your computer or
- the TAB10s is mounted as a disk on the MS-Windows explorer. For further information, refer to the chapter § Device network disk mounting in MS-Windows explorer.

> ☛ *The default credentials values for all the connection profiles having access rights to push on the Web directories are:* `admin` / `admin` .
>
> ☛ *The port value put at factory to access to the WebDAV directory is:* `80` . *The port value can be modified by using a configuration script. For further information, refer to the chapter § Device configuration by script.*
>
> ☛ *The same version of this APK can not be reinstalled twice withour being removed before.*
>
> ☛ `https://` *scheme to access to the TAB10s is not supported.*

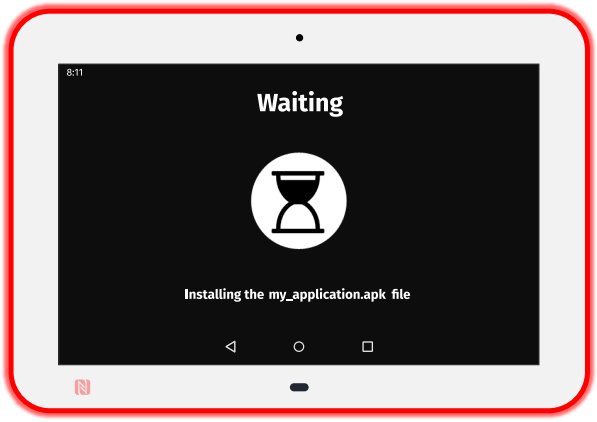
Copy the `<your_apk>.apk` file in the `.apps/` directory located at the root of the TAB10s WebDAV server.

This message should be displayed while the APK copy has not been completed.

> ☛ *The* `.apk` *file is installed only when the APK version is different from the one already installed. Once installed, the APK file is removed.*
>
> ☛ *One or more APK can be installed (or upgraded) all at once.*



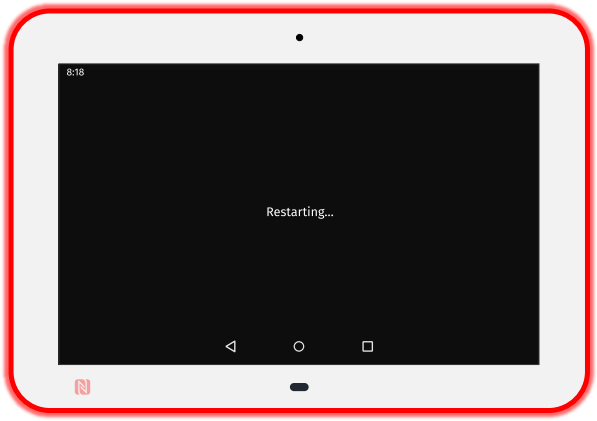
Unplug the USB storage device. This message should be displayed for few seconds, the time for the `AQS` to install the APK.



> ☛ *In case several APK are available on the USB storage device, the installing message appears for each new APK to install.*

When the APK installation is completed, this message should be displayed for 10 seconds.

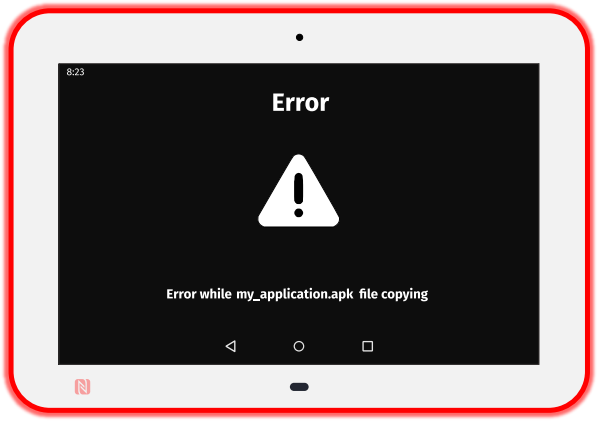
This message is then displayed until the device is rebooting automatically once.



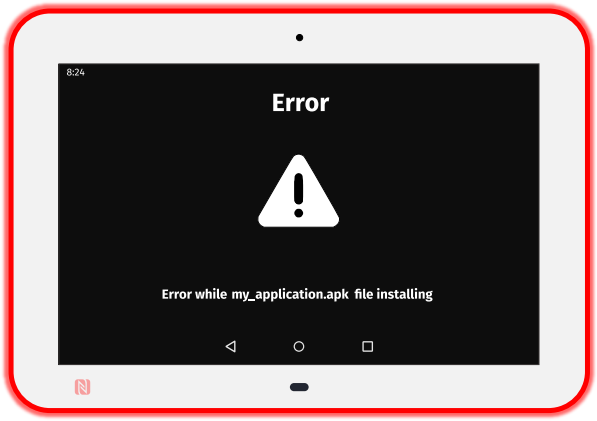
Each APK installed should be then visible on the `AQS` desktop.

Error messages when following the previous procedures

This message is displayed for ten seconds when an error occured while copying the APK. The USB storage device is not properly supported. Restart again the operation with another USB storage device. If the problem persists, you can contact support@qeedji.tech.



This error message is displayed for ten seconds when the APK is corrupted or when the USB storage device has been removed when the copy was still in progress. Try again. If the problem persists, you can contact support@qeedji.tech.



2.1.3 Device configuration by script

> ☛ *The device can be configured with a configuration script. When it is properly customized and loaded in the device, this configuration script is allowing to set some preferences values allowing to configure the device.*

The device configuration by script can be done by different ways:

- Device configuration by USB,
- Device configuration by WebDAV,
- Device configuration by server TFTP and server DHCP with code 66.

Configuration script

The list of the functions supported in the script are shown in the release note Configuration script release note.

The configuration script can be also downloaded at this location.

Rename the configuration script according to the supported filename pattern:

- common for multiple TAB10s devices:
- `configuration.js`,
- `000000000000.js`,
- when using an USB-C to USB-A hub device having also an Ethernet to USB bridge:
- `<device_ETH0_MAC_address>.js` with the format `ABCDEFABCDEF.js`,
- for a specific TAB10s device:
- `<device_WLAN0_MAC_address>` with the format `ABCDEFABCDEF.js`.

Edit the configuration script. To customize it according to your needs, uncomment one of the available functions in the `BEGIN of the user configuration` section by removing the `//` comment symbol.

For example:

```
/** ---------------------------------------
* ---- BEGIN of the user configuration
* ---------------------------------------*/
enableExternalStorageCopyApk(); /* default mode */
//disableExternalStorageCopyApk();
/** ---------------------------------------
* ---- END of the user configuration
* ---------------------------------------*/
```

> ☛ *The number of supported functions can depend on the configuration script version.*

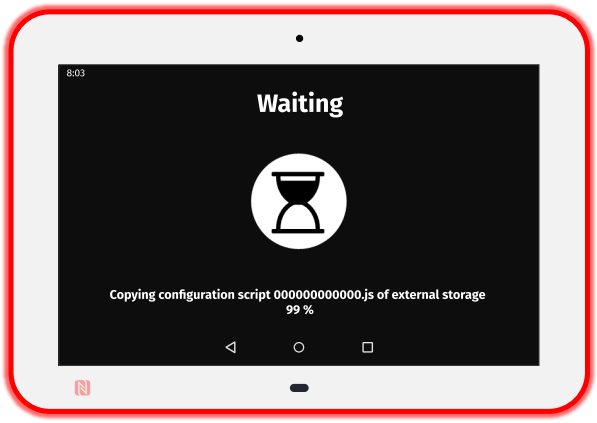
Device configuration by USB

Prerequisite:

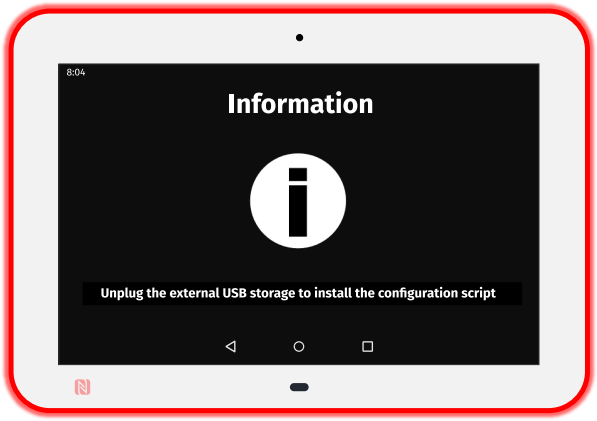
- the TAB10s device needs to have a suitable power supply equipment allowing to support TAB10s device configuration by the USB-C connector.

Copy the configuration script at the root directory of an USB storage device and insert it on the USB-C connector of the TAB10s device (or on the third party equipment connected to the USB-C connector).

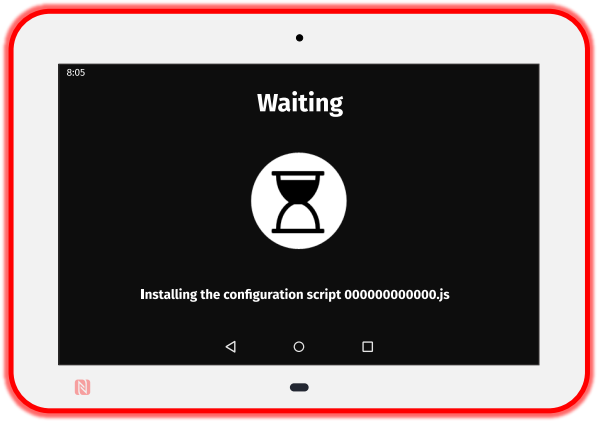
This message is displayed for only few seconds.



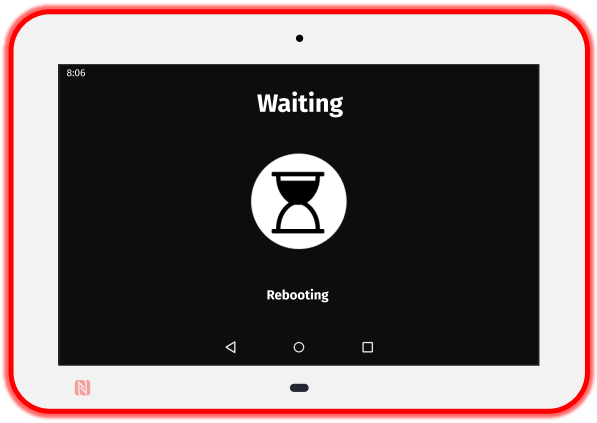
This message is displayed until the USB storage device is unplugged.



When the USB storage device is unplugged this message is displayed for less than 5 seconds.



This message is then displayed until the device is rebooting automatically once.



Device configuration by WebDAV

Prerequisite:

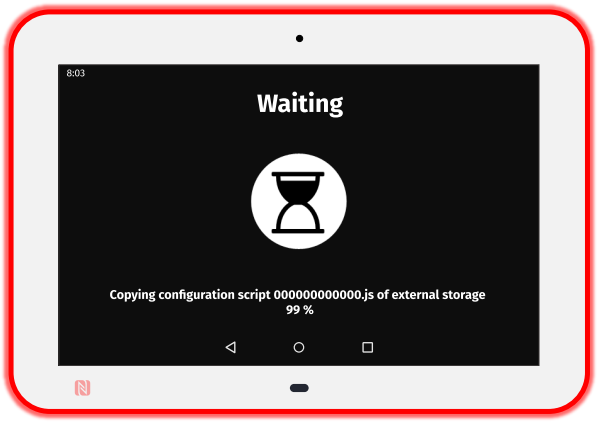
- a WebDAV client (*CarotDAV* or *BitKinex* for example) is installed on your computer or
- the TAB10s is mounted as a disk on the MS-Windows explorer. For further information, refer to the chapter § Device network disk mounting in MS-Windows explorer.

> ☛ *The default credentials values, put at factory, for all the connection profiles are:* `admin` / `admin` .
>
> ☛ *The port value put at factory to access to WebDAV directory is:* `80` *. The port value can be modified by using a configuration script.*

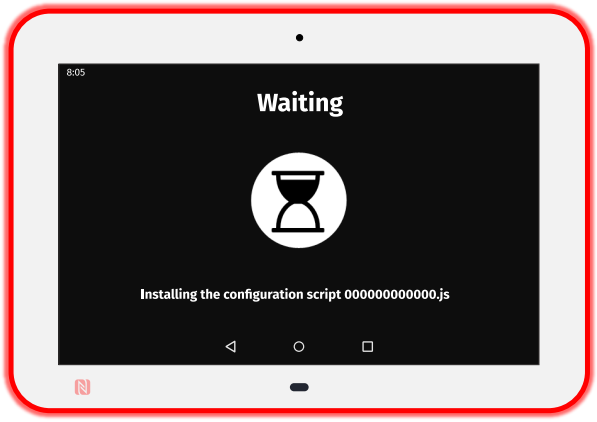
☛ `https://` *scheme to access to the TAB10s is not yet supported.*

Copy the configuration script in the `.configuration/` directory located at the root of the TAB10s WebDAV server.

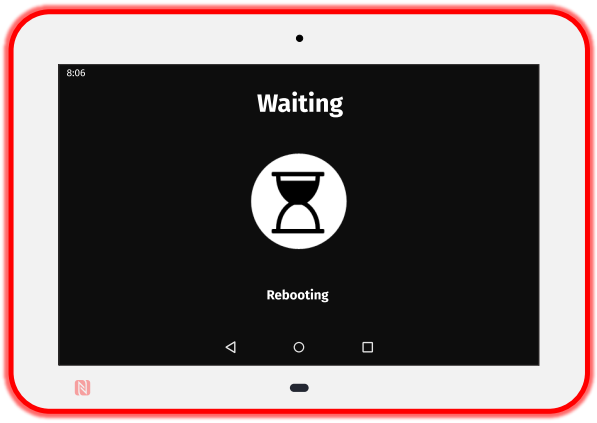
This message is displayed for only few seconds.



Then this message is displayed for less than 5 seconds.



This message is then displayed until the device is rebooting automatically once.



> ☛ *Once the configuration script is installed, the* `.js` *file is removed.*

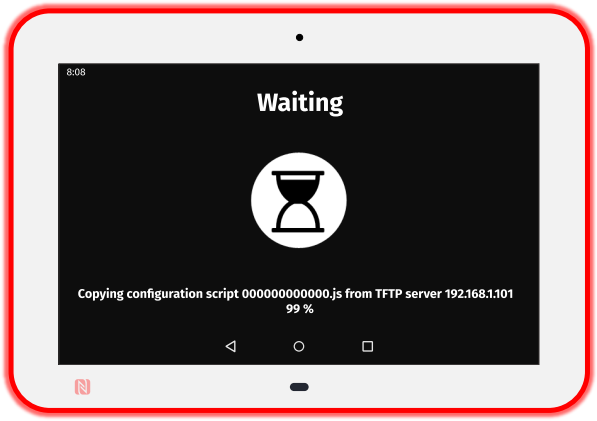
Device configuration by server TFTP and server DHCP with code 66

The TAB10s device can be configured thanks to a configuration script hosted on a TFTP server + DHCP server (code 66).

Prerequisites:

- the LAN or the WLAN interface is configured in DHCP mode,
- a TFTP server and a DHCP server are properly configured, are working properly and are available on the network. For further information, refer to the chapter § TFTP and DHCP server configuration,
- the Javascript configuration script is available in the exported directory of the `TFTP server`,
- a new configuration script is taken into account by the device only when a modification has been done and only after a device restart.

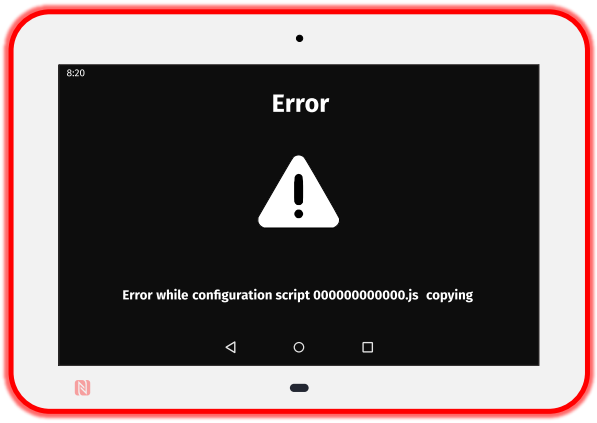
At each device boot-up, the JavaScript configuration script is downloaded from the TFTP server. The script is then executed once only if it has never been downloaded before or if the configuration script has been modified since the last reboot. The message should be displayed showing the IP address of your TFTP server.



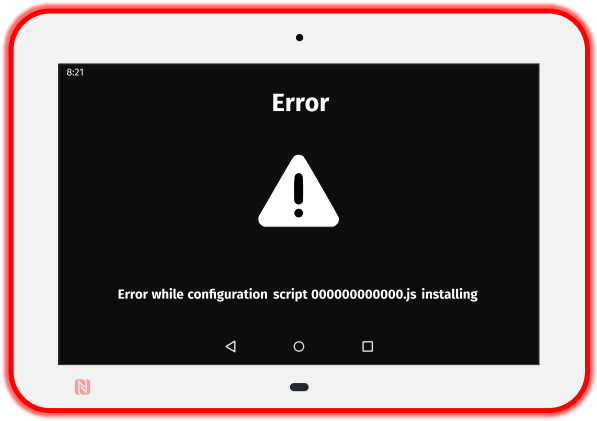
Then you should see the same messages as the chapter § Device configuration by USB (after the USB storage device is unplugged).

Error messages when following the previous procedures

This error message is displayed for ten seconds when the copy of the script from the USB storage device has failed. If the proble persists, try again with another USB storage device.



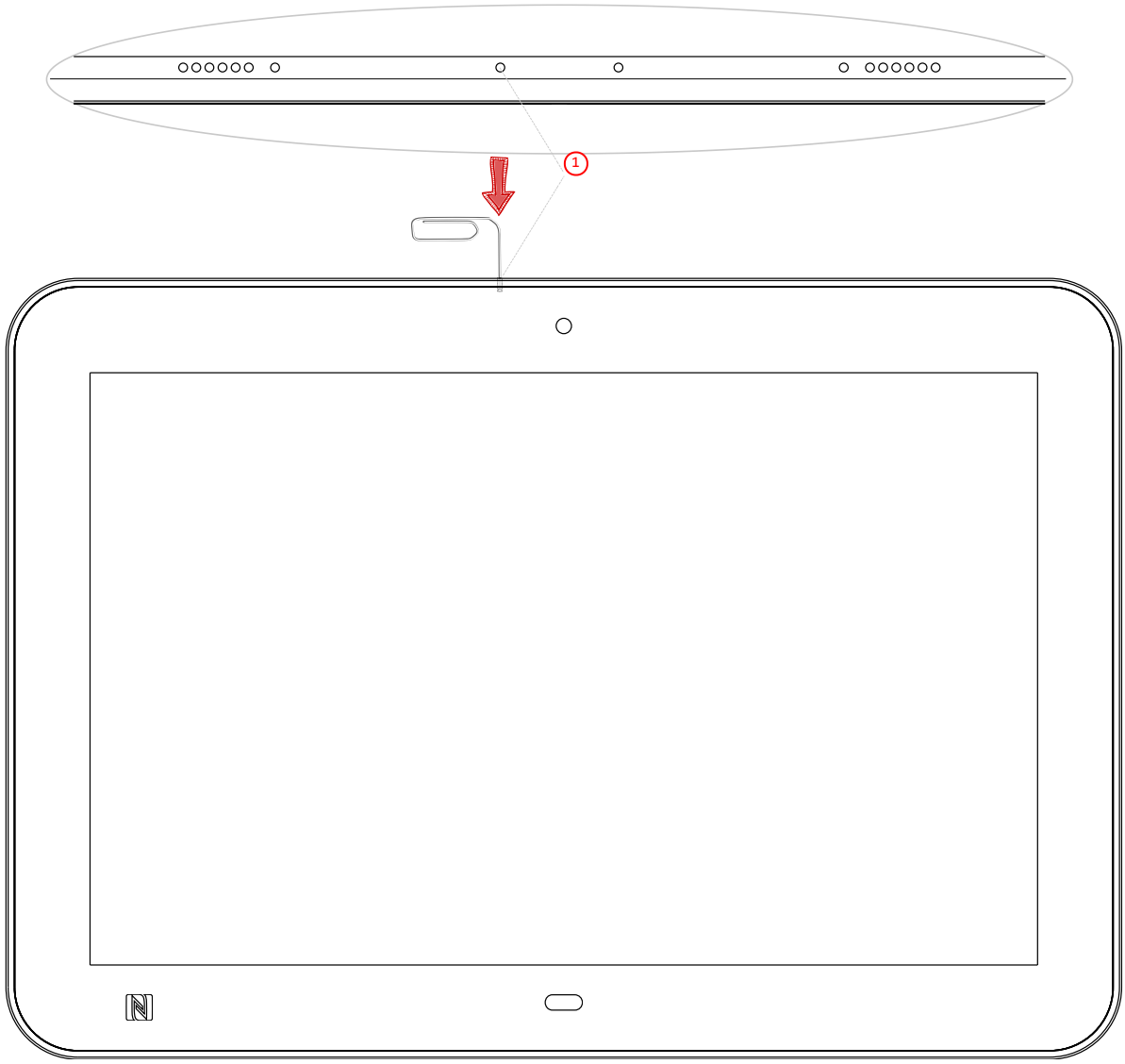
This error message is displayed for ten seconds when the configuration script contains a Javascript syntax error. Double check that the configuration script content is consistent for the TAB10s device.



2.1.4 Hardware reset

In case your APK or the `AQS` would not respond anymore, you can proceed to a TAB10s hardware reset:

- insert for example a paper clip inside the `System button` hole until feeling the button,
- hold the `System button` pressed for more than 5 seconds,
- release the `System button` by removing the paper clip.



- (1) System button.

2.2 Factory recovery

The factory recovery consists in recovering the OS and data like it was at the factory. Consequently, the different APK installed by the user and the TAB10s device configuration data will be lost. So, it is highly recommended to save all the required settings to be able to reconfigure your TAB10s device afterwards.

Before proceeding to the recovery, if it is still possible, save the safe partition: user data and APK.

Micro SD card removal

Procedure:

In case the device is hung on the wall on a mounting bracket:

- with a screw driver, untighten the two screws at the bottom of the TAB10s,
- remove the device from the mounting bracket.
  In case the device is powered by the USB-C connector:
- unplug the USB-C power supply,
- with a screw driver, untighten the two screws at the bottom of the TAB10s,
- remove the mounting bracket from the product.

With a little pen, push on the micro SD card and let the spring eject it from the `micro SD` connector.

> ☛ *The micro SD has to eject itself totally from its connector as soon as your pen is removed. If not, start again by pushing again the micro SD card with you pen, and when the spring is responding sufficiently, remove you pen rapidly.*

Micro SD card burning

Download the `aosp-tab10-setup-xx.yy.zz.iso` file for the factory recovery from the Qeedji Website (~ 16 GB).

> ☛ *The download time will depending on the network connection quality.*

Insert the `micro SD card` in a plastic SD card adapter (31 x 24 x 2.1 mm) and insert it in the approriate SD card slot, supported by any recent computer.

> ☛ *In case Windows is showing a message inviting to format the SD card, choose `No` .*

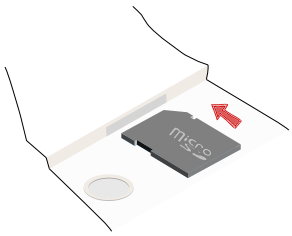
The ISO version suitable for your device, for example `aosp-tab10-setup-xx.yy.zz.iso`, can be burnt on your `micro SD card` by any ISO image burning software.

> ☛ *However `Qeedji` recommends to use the `BalenaEtcher` software (version V1.5.102, for example). For further information about the procedure with `BalenaEtcher` software, refer to the chapter § ISO image burning with BalenaEtcher.*

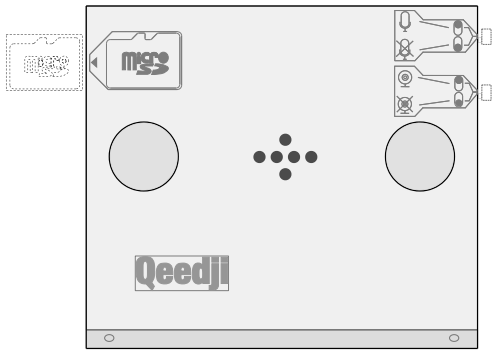
Micro SD card installation

Once the micro SD card content has been updated:

- remove the SD card adapter from your computer,
- remove the `micro SD card` from the SD card adapter,
- insert back the `micro SD card` inside the micro SD connector of the TAB10s device, in the right sense, and push it until hearing a clic. For further installation, refer to the chapter § Connectors pin-out.



When the micro SD card is installed properly, the SD card should be not visible.



In case the device has to be hung on the wall with a mounting bracket:

- hang again the product on the mounting bracket,
- with a screw driver, tighten the two screws at the bottom of the TAB10s device to lock the device on the wall.

In case the device is powered by the USB-C connector:

- install again the mounting bracket on the product,
- plug again the USB-C power supply.

Part III

Applicative user interface

3.1 Applicative user interface

The TAB10s device supports 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>/`.

The defaut credentials values put at factory for the `Administration user` connection profile are:

- identifier: `admin`,
- password: `admin`.

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

This is an example of content when the TAB10s device is supplied by a standard USB-C wall-plug and connected to a WIFI network.

This is an example of content when the TAB10s device is supplied by a `NAPOE109ku` Ethernet adapter which is connected to a `PoE` switch.

Part IV

Administration console user interface

4.1 device configuration Web user interface

The TAB10s device supports a Web user interface that can be accessed with a Web browser. The supported Web browsers are: `Google Chrome`, `Mozilla Firefox` and `MS-Edge (Chromium)`.

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

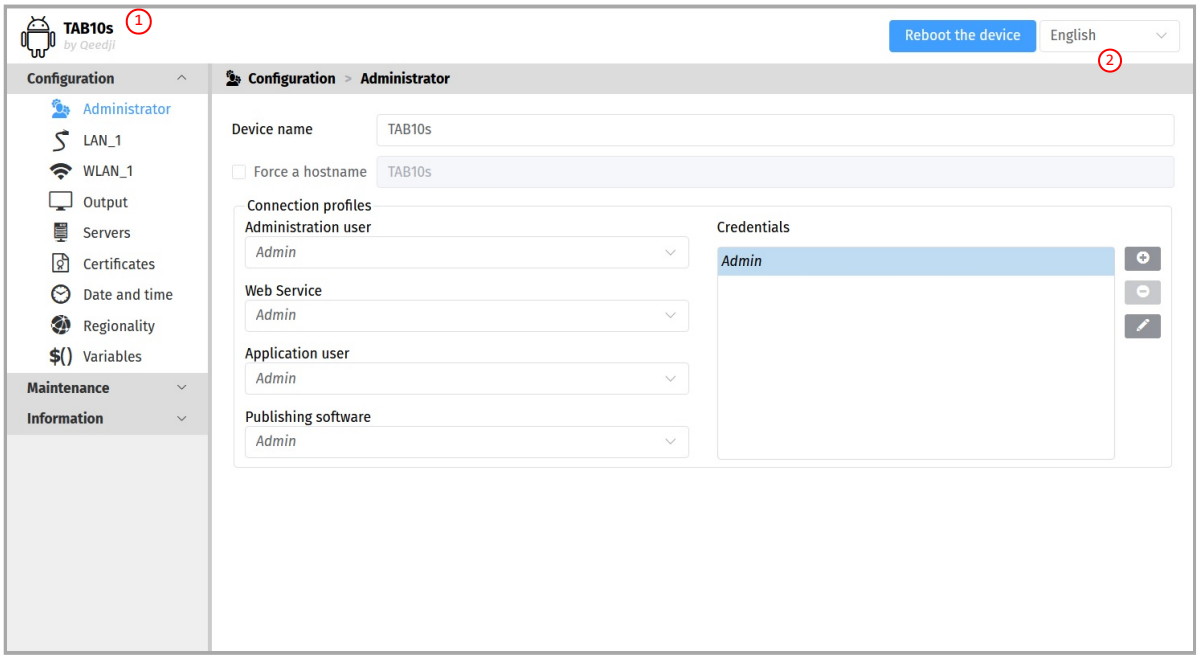
The default credentials values of the `Administration user` connection profile are:

- identifier: `admin`,
- password: `admin`.

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

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

This is the device configuration Web 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.

> ⚠ The Web user interface and the WebDAV server are not accessible in https.

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

4.1.1 Configuration > Administrator

In the `Configuration` tab, select the **Administrator** menu to:

- change the `Device name`,
- view the `Hostname` value which is automatically generated from the `device name` by limiting it to 15 characters max and keeping only its alpha numeric character, the dot (`.`) characters and the dash (`-`) characters. The *check box* before the `Force a hostname` label allows to force the device to have a `Hostname` value set by the user.

> ☛ *The `Hostname` value is the device identification name communicated during a network UPnP discovery.*

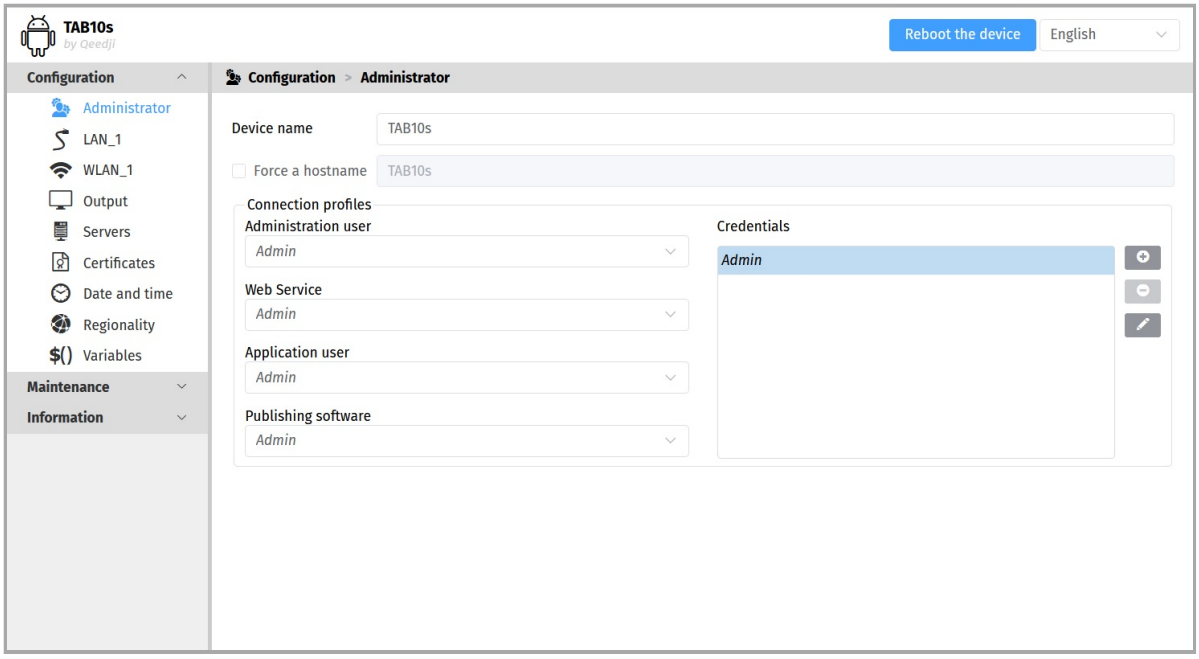
You can add also some private credentials values, with its *identifier/password* by using the ✚ button of the `Credentials`

Then associate your private credentials values to the different `connection profiles` :

- `Administration user` : the access rights of this connection profile allow to:
  - access to the device configuration Web user interface and make modifications,
  - use the Web Services supported by the device,
  - publish on the WebDAV server directories of the device (Apps, configuration scripts, firmwares and APKs),
- `Web Service` : the access rights of this connection profile allow to:
  - use the Web Services supported by the device,
  - publish on the WebDAV server directories of the device (Apps, configuration scripts, firmwares and APKs),
- `Publishing software` : the access rights of this connection profile give allow to:
  - publish on the WebDAV server directories of the device (Apps, configuration scripts, firmwares and APKs),
- `Application user` : the access rights of this connection profile allow to:
  - access to the device configuration Web user interface in *Read Only* [1] and to the applicative Web interface in *Read/Write*.

[1] *Out of the applicative Web page, when some modification attempts are done in one of the device configuration Web page, the user is disconnected from the device configuration Web user interface.*

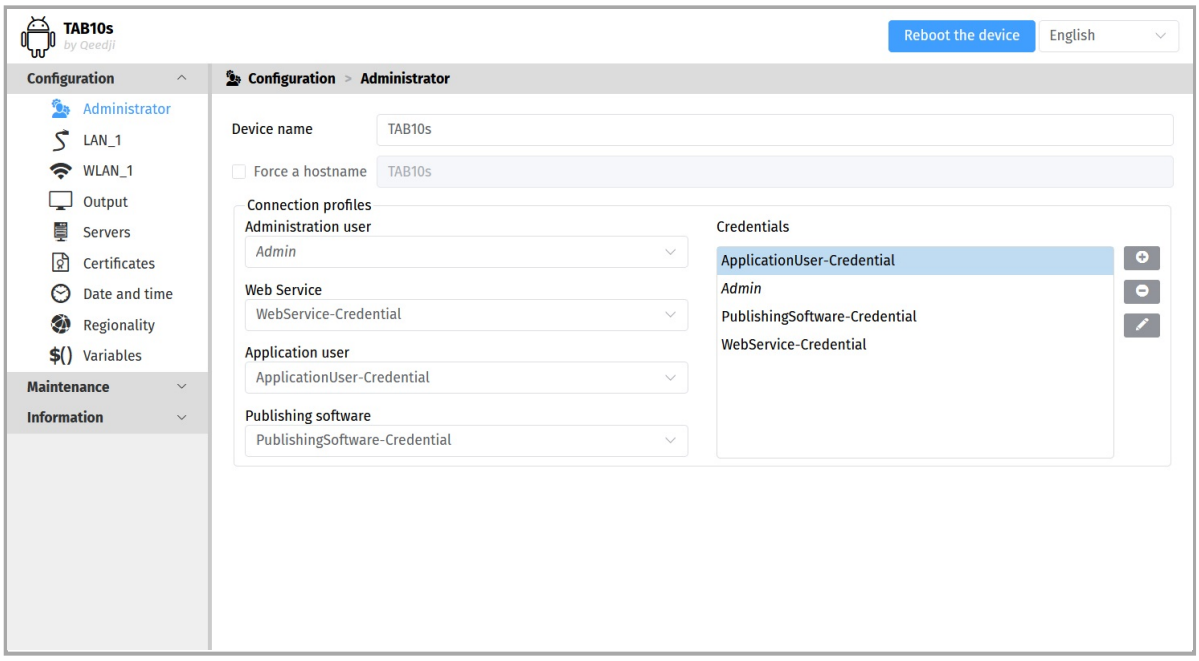
> ☛ *The default credential label for all connection profiles is `Admin`, corresponding to the default identifier/password `admin` / `admin`.*
>
> ⚠ In case you have lost the credentials values of all the `Administration user` connection profiles, the only way to restore some known credentials is to inject an USB-C mass storage having an appropriate configuration script through the USB-C connector (*USB 1* or *USB 2*) of the TAB10s device. For further information, refer to the chapter § Device configuration by script.



> ☛ *It is recommended that you enter one unique `Hostname` value for each device. In case several TAB10s 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`).*

For security reasons, it may be useful to change the credentials value for the `Administration user` profile. Please keep these login credentials in a safe place afterwards.

This is an example with different credentials for the four connection profiles.

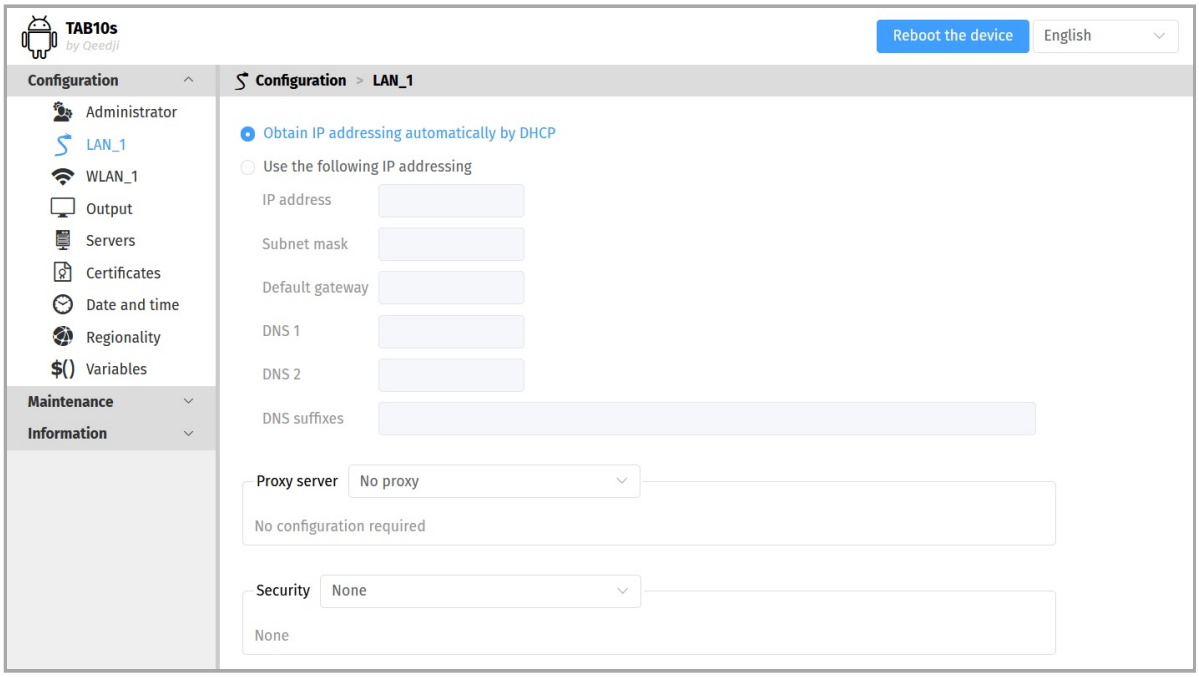


> ☛ *The association of the credentials to the connection profiles are taken into account only after a device reboot. In case the user takes more than 5 minutes to create the credentials, associate them to the profile and reboot, the user may have to reauthenticate (with the credentials not modified).*

4.1.2 Configuration > LAN_1

In the `Configuration` tab, select the **LAN_1** menu to set up the network configuration of the `LAN_1` interface of your device.

> ☛ *The `LAN_1` menu may not be available when the TAB10s device is connected to a WIFI network and supplied by a standard USB-C wall plug.*

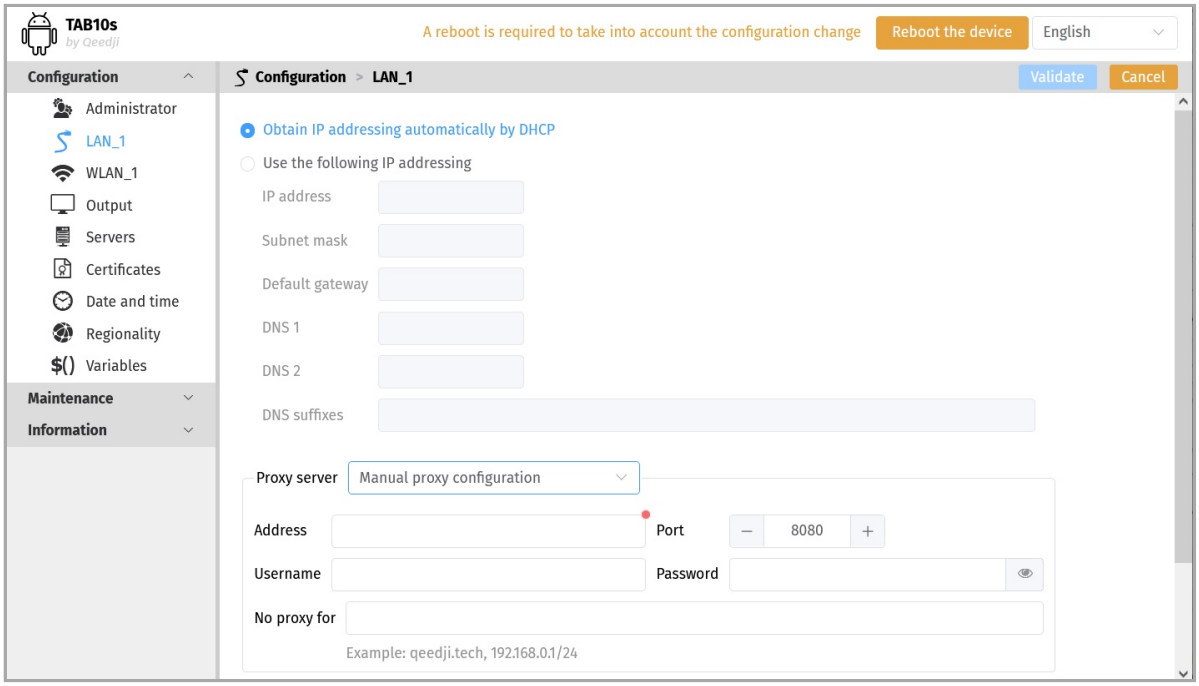


> ☛ *The device supports the UPnP and can be for example detected automatically in the local network environment of your computer.*
>
> ☛ *By default, the device is configured with DHCP activated.*

Choose whether the IP address is static or given by the `DHCP` server. If static, fill the suitable parameters like `subnet mask`, `gateway` and `DNS`.

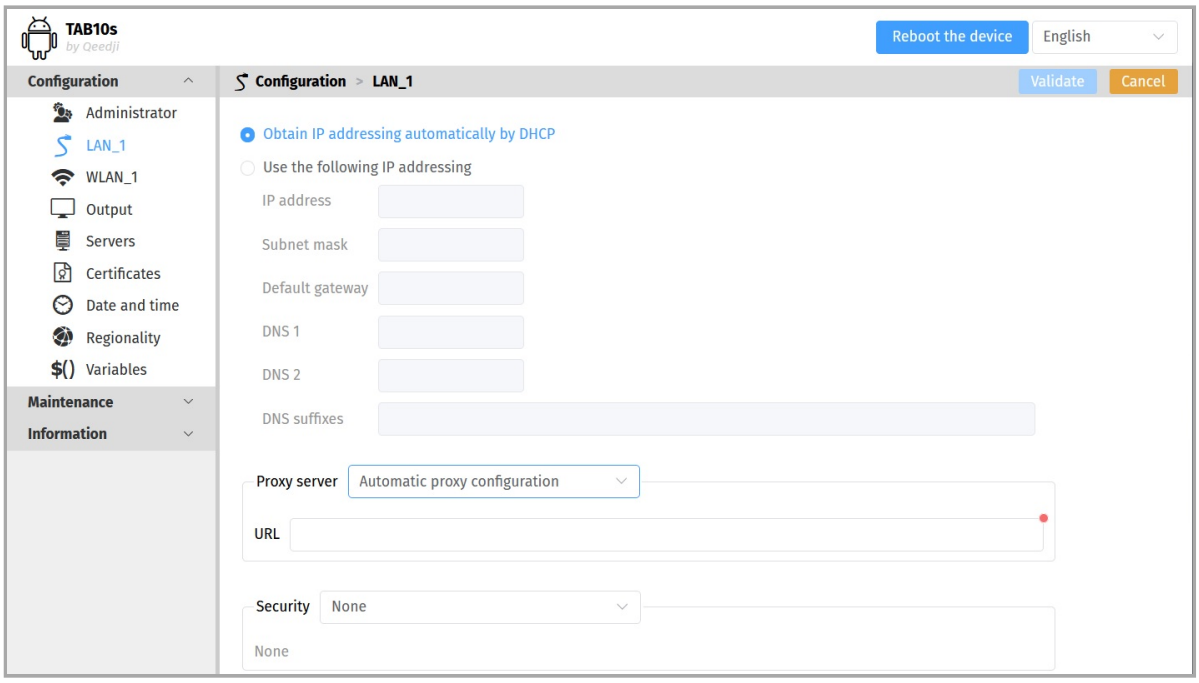
> ⚠ The `LAN_1` configuration is modified dynamically without rebooting after having pressed on the `Validate` button. If the IP address is changing after having pressed on the `Validate` button, you need to reconnect to the device configuration Web user interface with the new `LAN_1` device IPV4 address or with the `LAN_1` device IPV6 address.
>
> ☛ *The connection from a computer to the device configuration Web user interface with the device IPV6 address, computed from the device `LAN_1` MAC address value, is supported. To connect to the IPV6 address of the `LAN_1` interface, ensure that the `WLAN_1` connection is down. For example, if the `LAN_1` MAC address of the device is 00-1c-e6-02-27-bf, type the URL `http://[fe80::21c:e6ff:fe02:27bf]/` or type `http://[fc00::21c:e6ff:fe02:27bf]/` in a Web browser. The routable prefix (fc00, fe80, and so on...) are depending on your network configuration. Your computer must be configured properly to support the IPV6 protocol.*

To use a specific `proxy server`, select the `Manual proxy configuration` in the `Proxy servers` drop down list then enter your proxy configuration.



To use an automatic `proxy server` configuration, select the `Automatic proxy configuration` in the `Proxy server` drop down list then enter the PAC file URL allowing to get automaticall the proxy server configuration.

For example: `https://domain.contoso.en/dir/my-proxy-auto-conf.pac`



> ⚠ The `LAN_1` configuration is dynamically taking into account the new `LAN_1` parameter as soon as the user changes from IP address allocated by DHCP to static IP address or changes the static IP address value then click on the *Validate* button of the device configuration Web user interface.
>
> ⚠ The devices uses only one network interface at a time. The `WLAN_1` has priority over `LAN_1`.
>
> ⚠ In DHCP mode, if neither the `LAN_1` connectivity nor the `WLAN_1` connectivity is working or the `WLAN_1` interface is inactivated, the IP address value is *unavailable*. In some case, a valid IP address can be got back few dozens of seconds after the network connectivity is restored on `WLAN_1` interface or on `LAN_1` interface.

Procedure to configure the `LAN_1` interface with the configuration Web user interface when your network supports DHCP:

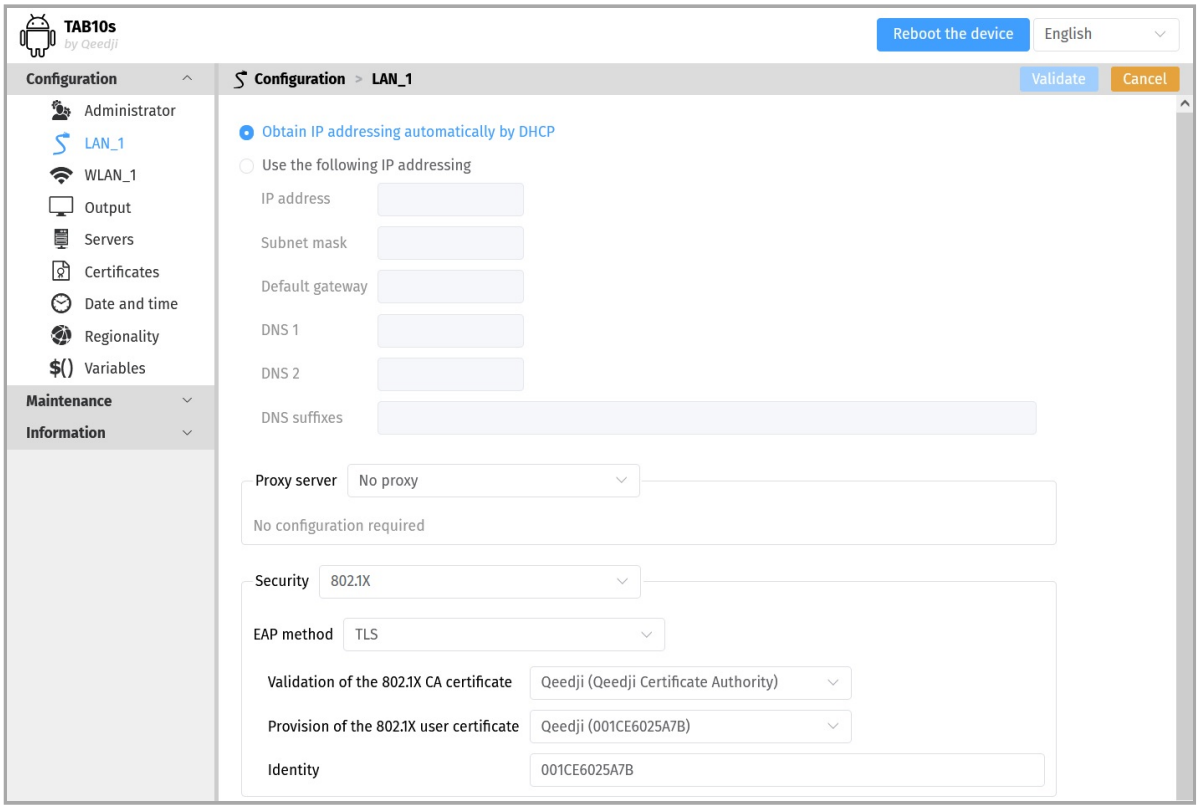
> 1. it is considered here that the network connectivity is OK over the `LAN_1` interface,
> 2. connect to the device configuration Web user interface with a Web browser with the DHCP IP address of the `LAN_1` interface. You can still connect to the device configuration Web user interface with its `LAN_1` IPV6 address (for example `http://[fe80::21c:e6ff:fe02:5694]` get from the `MAC` value written at the back of the NAPOE109XX device).

Procedure to configure the `LAN_1` interface with the configuration Web user interface when your network does not support DHCP:

> 1. it is considered here that the TAB10s device is connected to a *NAPOE109ku* device or to a *NAPOE109kt*, or to a *NAPOE109ft* device which is connected to a PoE switch,
> 2. disconnect the RJ45 cable (*cable1* for *network1*) from your computer,
> 3. connect a RJ45 cable (*cable2* for *network2*) between your computer and the PoE switch,
> 4. connect to the device configuration Web user interface with a Web browser with its `LAN_1` IPV6 address (for example `http://[fe80::21c:e6ff:fe02:5694]` get from the `MAC` value written at the back of the NAPOE109XX device),
> 5. inactivate `IP address get by DHCP` for `LAN_1` and enter a suitable static address configuration (IP address, subnet mask, gateway, DNS),
> 6. reboot the device with the device configuration Web user interface,
> 7. disconnect the RJ45 cable (*cable2* for *network2*) from your computer and reconnect the previous RJ45 cable (*cable1* for *network1*),
> 8. connect to the device configuration Web user interface with a Web browser with the valid `LAN_1` IP address of the device. You can still connect to the device configuration Web user interface with its `LAN_1` IPV6 address (for example `http://[fe80::21c:e6ff:fe02:5694]` get from the `MAC` value written at the back of the NAPOE109XX device).

To activate `802.1X` security on `LAN_1` interface, set the `Security` field to *802.1X* instead of *None*.

Choose one `EAP method` among *PWD*, *MD5*, *GTC*, *PEAP*, *TLS*, *TTLS*. The chosen `EAP method` must be supported by your RADIUS server.



> ☛ *In the context of a secure network, your device must be first declared in your dedicated RADIUS server with a `identity` / `password`. For further information, please contact your IT department.*

When required, fill the `Identity` / `password` declared for your device in your RADIUS server.

> ☛ *When displayed, the `Anonymous identity` field value is optional.*

Required only by the *PEAP* or *TTLS* `EAP methods`, choose then among the `Phase 2 authentication` mode supported by your RADIUS server: *NONE*, *PAP*, *MSCHAP*, *MSCHAPV2*, *CHAP*, *GTC*, *MD5*, *EAPMSCHAPV2*.

The *TLS* `EAP methods` and *TLS* `Phase 2 authentication` allows to provide a `802.1X user certificate` installed in your TAB10s device when required by your RADIUS server configuration.

The *TLS*, *TTLS*, and *PEAP* `EAP methods` allow to activate the `802.1X CA certificate` validation. The `802.1X CA certificate` must be installed first in your TAB10s device. For further information about certificates installation, refer to the chapter § Certificates.

> ☛ *The `802.1X CA certificate` is the certificate with the highest autority for your RADIUS server. For further information, please contact your IT department.*
>
> ☛ *In this `AQS` version, it is not possible to select the `Use system certificates` value for the `Validation of the 802.1X CA certificate` input for `LAN_1` interface.*
>
> ☛ *When using `802.1X` certificates, in case your device is not on time or when the `802.1X` certificates 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 suitable configuration script to install an appropriate certificate or to update the device date and time.*
>
> ☛ *A new negociation with the RADIUS server with the programmed `LAN_1` 802.1X security is required as soon as a down/up event is detected at the input of the port of the 802.1X router, meaning when a RJ45 cable is unplugged or when the device is restarting. If intermediate network devices are present between the device and the 802.1X router, the 802.1X router may not detect down/up event and may keep a previous negociation alive if one has been successful just before.*

4.1.3 Configuration > WLAN_1

In the `Configuration` tab, select the **WLAN_1** menu to set up the network configuration of the `WLAN_1` interface on your device.

⚠ As soon as the `WLAN_1` configuration is inactivated through the device configuration Web user interface, or if the `WLAN_1` interface is not properly configured, the network connection with the device is lost. The only way to connect to it again is to create again a `WLAN_1` connection again with Android settings or to inject, with an USB-A storage device and a USB-A to USB-C hub, a configuration script having a suitable `WLAN_1` configuration.

⚠ After having removed a registered `WLAN_1` network, the removal is effective as soon as the user clicks on the *Validate* button. If there is no other valid registered `WLAN_1` network, the only way to connect to the device again is to connect a RJ45 Ethernet cable or to inject, with an USB-C storage device, a configuration script having a suitable `WLAN_1` configuration.

⚠ The devices uses only one network interface at a time. The `WLAN_1` has priority over `LAN_1` .

⚠ In DHCP mode, if neither the `LAN_1` connectivity nor the `WLAN_1` connectivity is working or the `WLAN_1` interface is inactivated, the IP address value is *unavailable*. In some case, a valid IP address can be got back few dozens of seconds after the network connectivity is restored on `WLAN_1` interface or on `LAN_1` interface.

☛ *The connection from a computer to the device configuration Web user interface with the device IPV6 address, computed from the device `WLAN_1` MAC address value, is supported. To connect to the IPV6 address of the `WLAN_1` interface, the `LAN_1` connection must be down. For example, if the `WLAN_1` MAC address of the device is 00-1c-e6-02-27-bf, type the URL `http://[fe80::21c:e6ff:fe02:27bf]/` or `http://[fc00::21c:e6ff:fe02:27bf]/` in a Web browser. The routable prefix (fc00, fe80, and so on...) is depending on your IPV6 network configuration. Your computer must be configured properly to support the IPV6 protocol.*

Procedure to configure the `WLAN_1` interface with the configuration Web user interface when your network supports DHCP:

1. it is considered here that the network connectivity is OK over the `LAN_1` interface,
2. connect to the device configuration Web user interface with a Web browser:
3. add a valid `WLAN_1` configuration (SSID, authentication, crypto key),
4. reboot the device with the device configuration Web user interface.
5. connect to the device configuration Web user interface with a Web browser with the valid `WLAN_1` IP address of the device. If the WIFI connection is done, you can connect to the device configuration Web user interface also now with its `WLAN_1` IPV6 address (for example `http://[fe80::21c:e6ff:fe02:62e3]` get from the `MAC.WLAN1` value written at the back of the device).

Procedure to configure the `WLAN_1` interface with the configuration Web user interface when your network does not support DHCP:

1. it is considered here that the TAB10s device is connected to a *NAPOE109ku* device, a *NAPOE109kt*, or a *NAPOE109ft* device which is connected to a PoE switch,
2. disconnect the RJ45 cable (*cable1* for *network1*) from your computer,
3. connect a RJ45 cable (*cable2* for *network2*) between your computer and the PoE switch,
4. connect to the device configuration Web user interface with a Web browser with its `LAN_1` IPV6 address (for example `http://[fe80::21c:e6ff:fe02:5694]` get from the `MAC` value written at the back of the NAPOE109XX device),
5. inactivate `IP address get by DHCP` for `WLAN_1` and enter a valid static address configuration (IP address, subnet mask, gateway, DNS),
6. add a valid `WLAN_1` configuration (SSID, authentication, crypto key),
7. reboot the device with the device configuration Web user interface,
8. disconnect the RJ45 cable (*cable2* for *network2*) from your computer and reconnect the previous RJ45 cable (*cable1* for *network1*),
9. connect to the device configuration Web user interface with a Web browser with the valid `WLAN_1` IP address of the device. If the WIFI connection is done, you can connect to the device configuration Web user interface also now with its `WLAN_1` IPV6 address (for example `http://[fe80::21c:e6ff:fe02:62e3]` get from the `MAC.WLAN1` value written at the back of the device).

Procedure to configure the `WLAN_1` interface with a configuration script:

1. inject a USB storage device having a suitable configuration script on the USB hub connected to the USB-C connector of the TAB10s. And wait device reboot.
2. connect to the device configuration Web user interface with a Web browser with the valid `WLAN_1` IP address of the device. If the WIFI connection is done, you can connect to the device configuration Web user interface also now with its `WLAN_1` IPV6 address (for example `http://[fe80::21c:e6ff:fe02:62e3]` get from the `MAC.WLAN1` value written at the back of the device).

Procedure to configure the `WLAN_1` interface with a configuration script pushed by file transfer[1] with an USB cable between the computer and the TAB10s device (the device must be supplied properly by the computer, by the *NAPOE109kt* device or by the *NAPOE109ft* device):

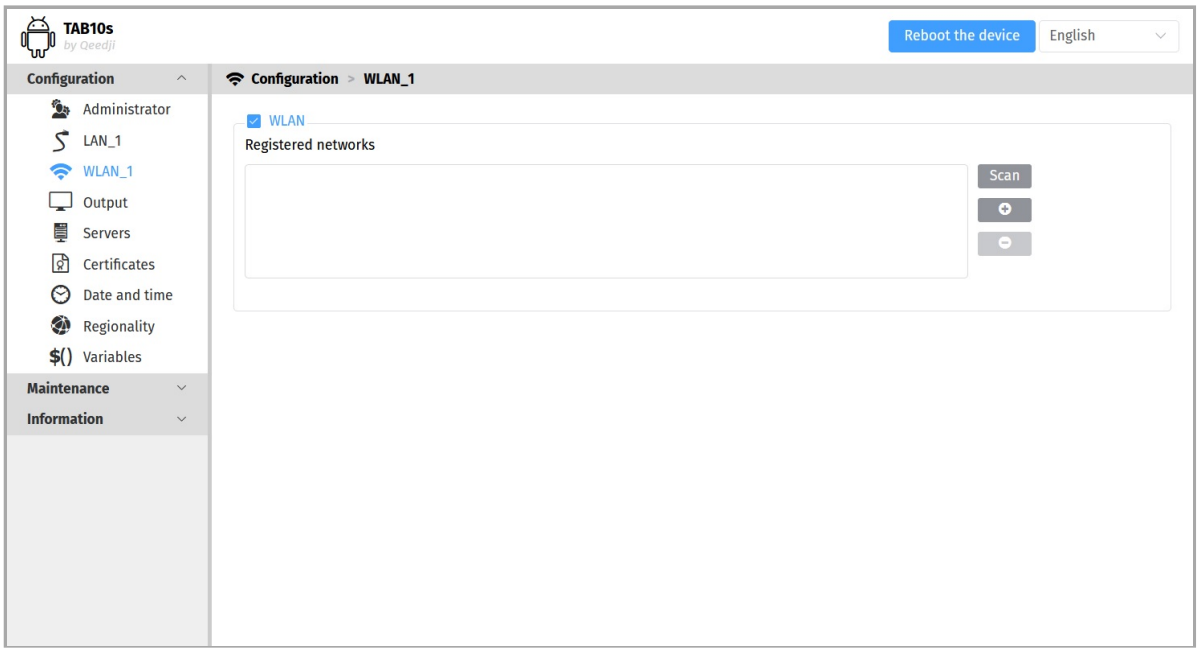
1. push a suitable configuration script on the `.configuration` directory of the device file system from a computer. And wait device reboot.
2. connect to the device configuration Web user interface with a Web browser with the valid `WLAN_1` IP address of the device. You can connect to the device configuration Web user interface also now with its `WLAN_1` IPV6 address (for example `http://[fe80::21c:e6ff:fe02:62e3]` get from the `MAC.WLAN1` value written at the back of the device).

[1] *For further information, refer to the chapter § Appendix: File transfer from a computer. appendix-file-transfer.md.*

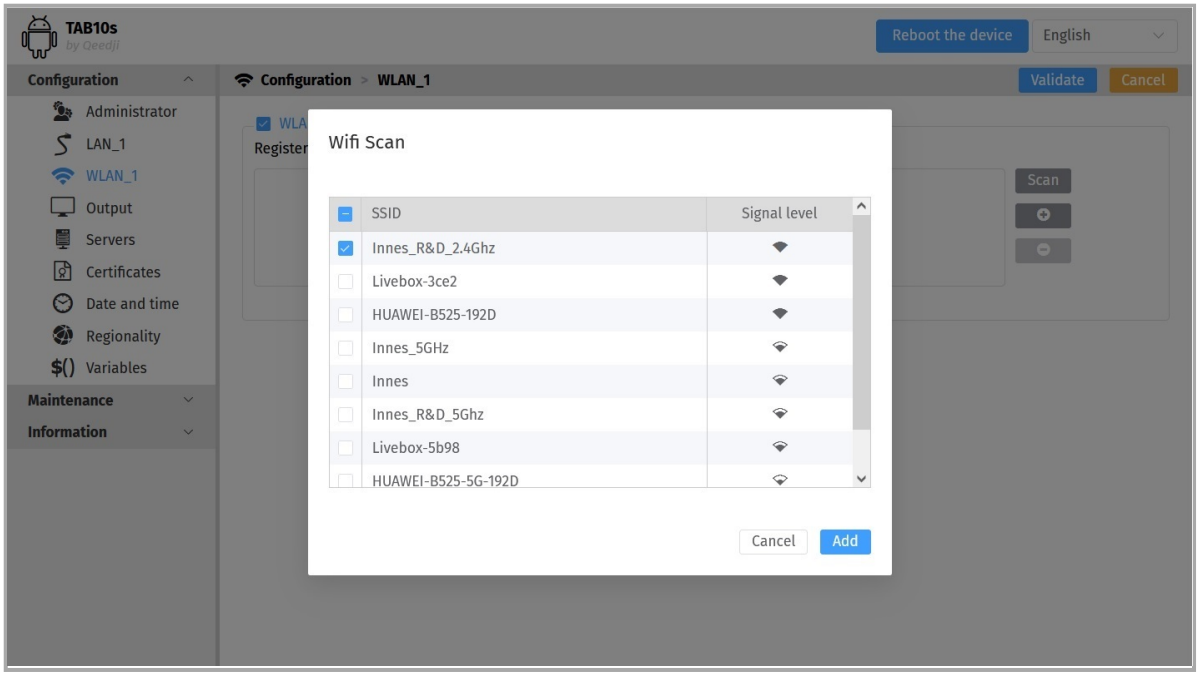
It is also possible to configure the `WLAN_1` interface directly with Android settings.

To detect the `WIFI spots SSID`, click on the `Scan` button.

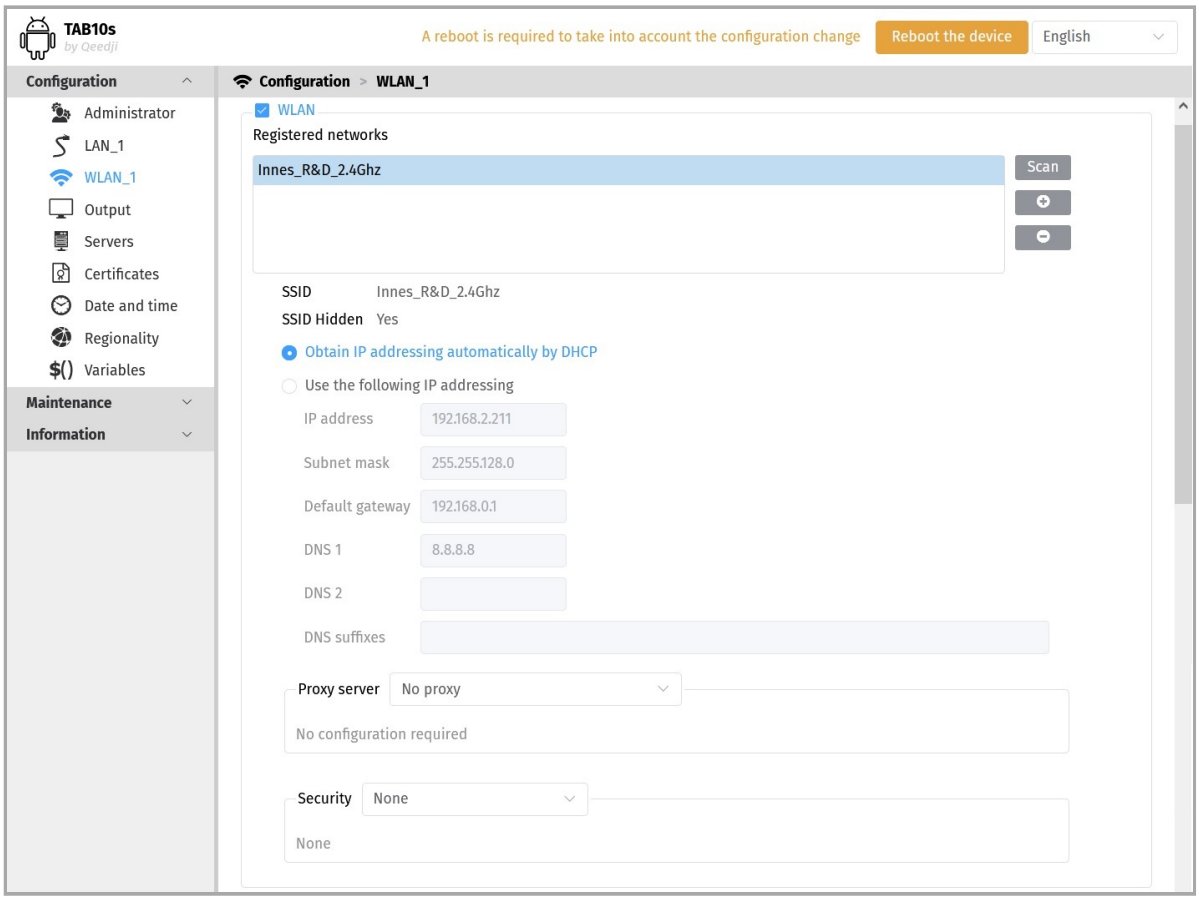
> ☛ *In case the `SSID` of your WIFI router is not broadcasted (or hidden), click on the `Add` button to add manually a `WLAN_1` interface. Enter the wished `SSID` value and check the option `The SSID is hidden`.*



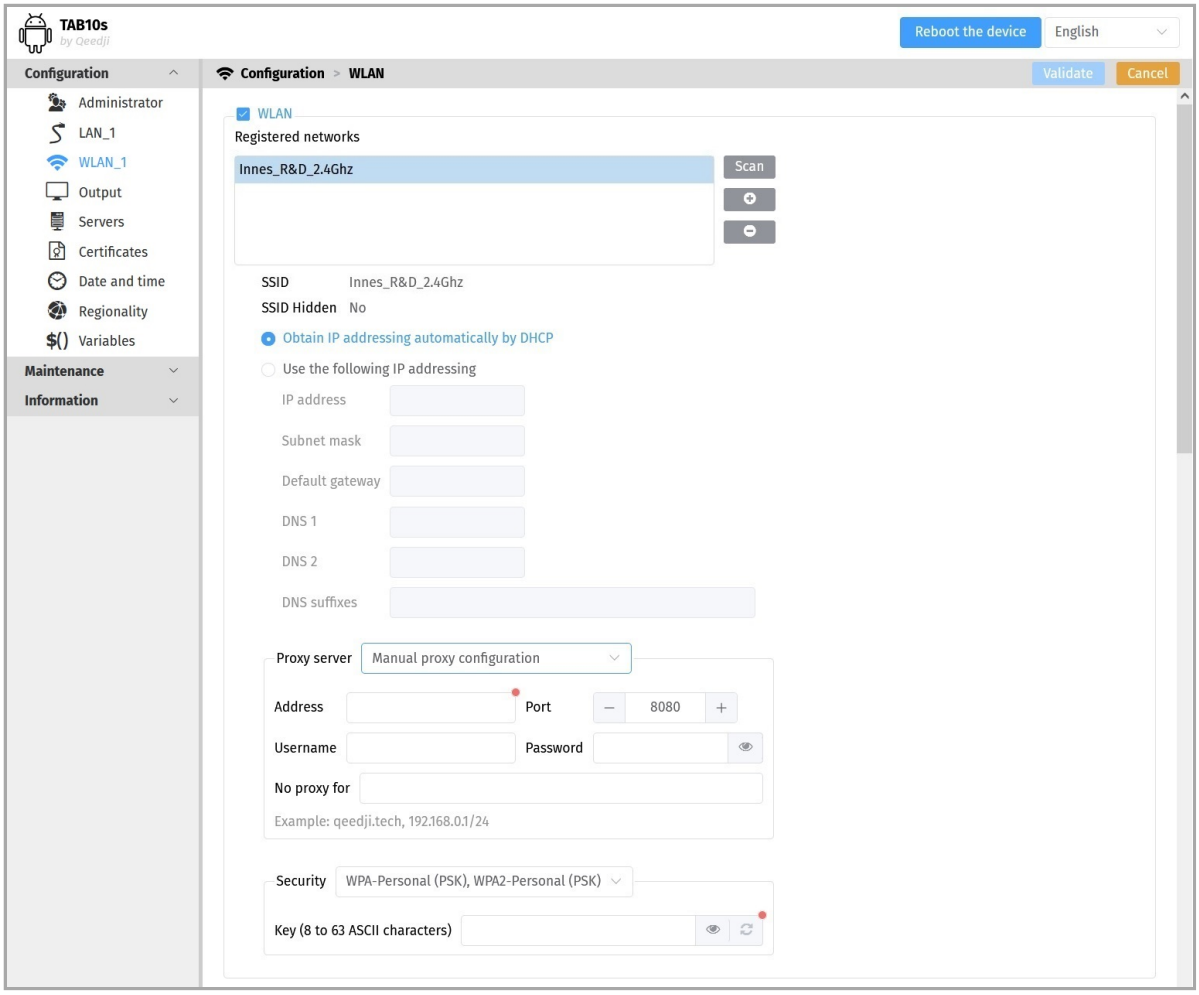
Select one of the detected `WIFI spots SSID` and press on the `Add` button.



Choose whether the IP address is static or given by the `DHCP` server. If static, fill the suitable parameters like `subnet mask`, `gateway` and `DNS`.

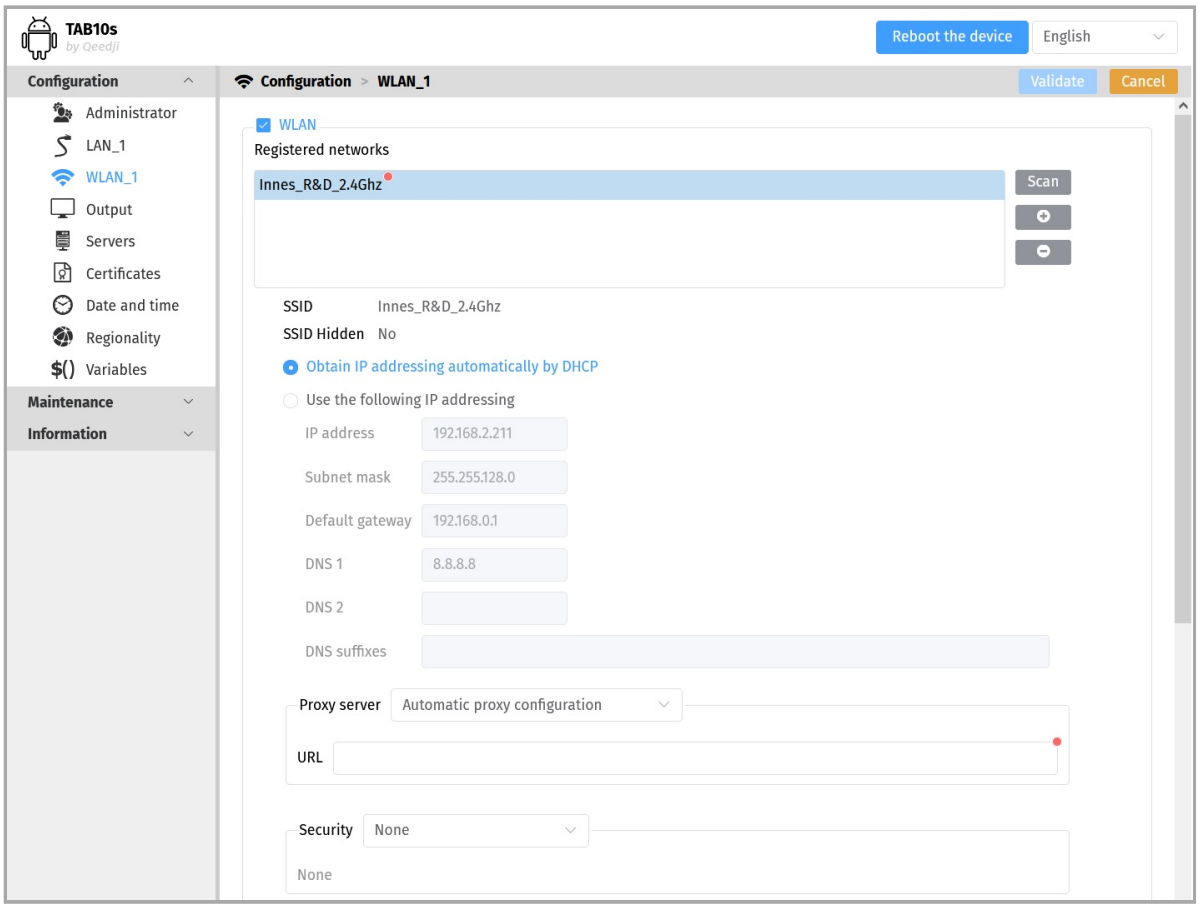


To use a specific `Proxy server` for `WLAN_1` interface, select the `Manual proxy configuration` in the `Proxy servers` drop down list then enter your proxy configuration.



To use an automatic `Proxy server` configuration for `WLAN_1` interface, select the `Automatic proxy configuration` in the `Proxy server` drop down list then enter the PAC file URL allowing to get automatically the proxy server configuration.

For example: `https://domain.contoso.en/dir/my-proxy-auto-conf.pac`



The supported securities[1] are:

- *None*,
- *WEP*,
- *WPA-Personal (PSK)*,
- *WPA2-Personal (PSK)*,
- *WPA-Enterprise (EAP)*[2],
- *WPA2-Enterprise (EAP)*[2].

[1] *Ad hoc Wi-Fi is not supported.*

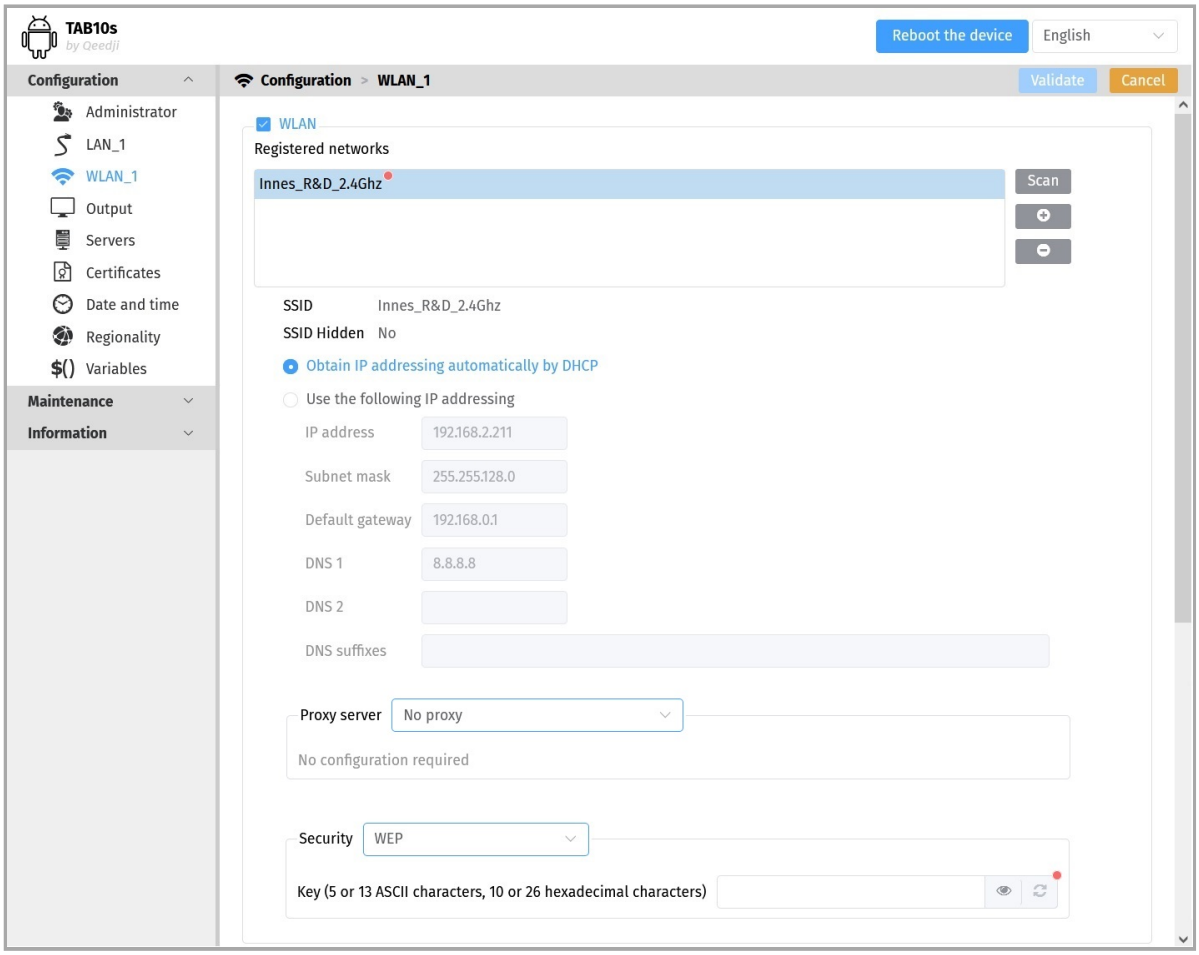
[2] *This securities requires to have a RADIUS server properly configured and to have specific WIFI router supporting* `WPA-Enterprise` *or* `WPA2-Enterprise` *.*

Fill the required crypto keys for these securities:

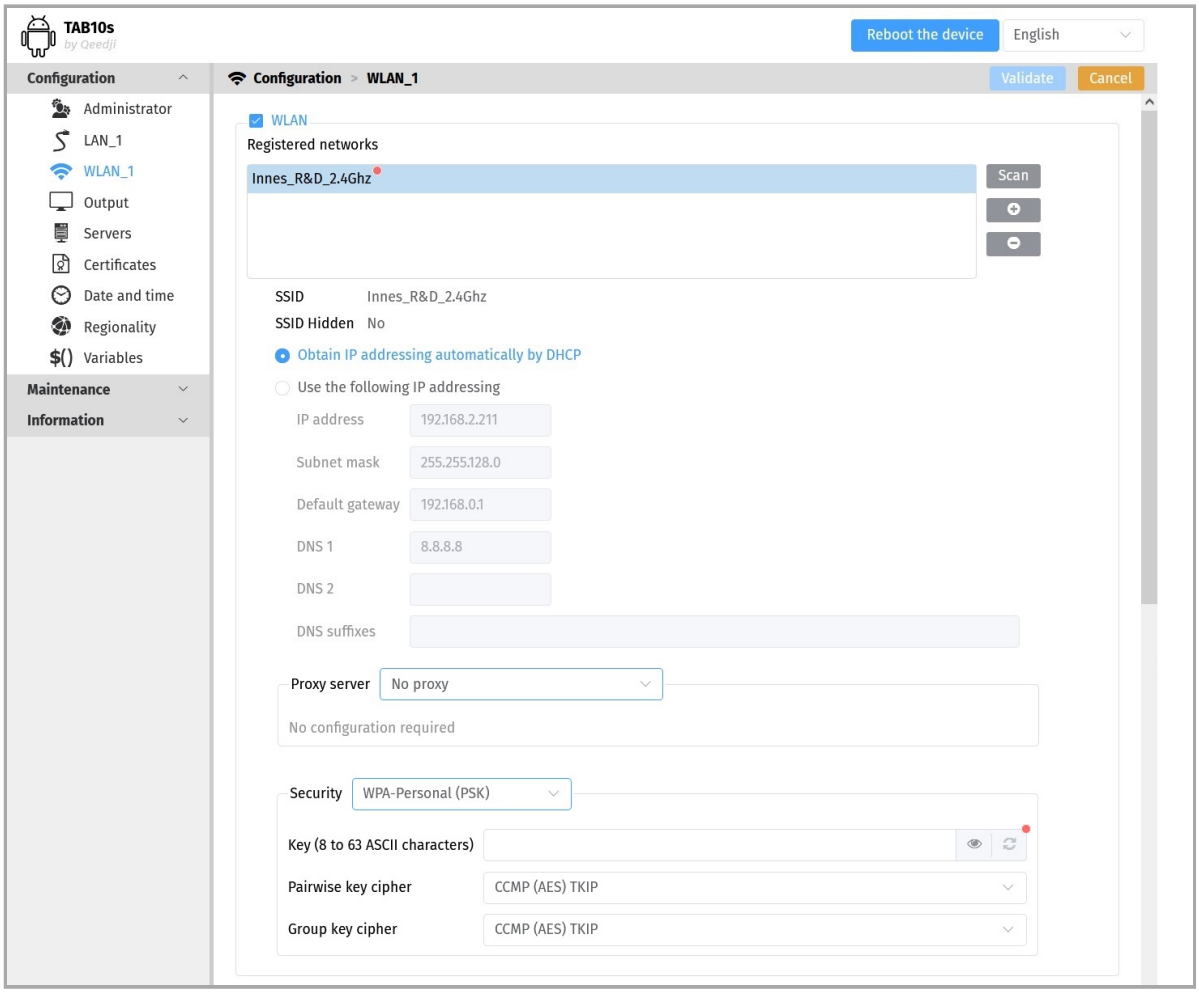
- `WEP`,
- `WPA-Personal (PSK)`,
- `WPA2-Personal (PSK)`.

The allowed length for `WEP` crypto key is:

- 5 or 13 digits when using ASCII-7bits characters,
- 10 or 16 digits when using hexadecimal characters.



The allowed length for `WPA-Personal (PSK)` and `WPA2-Personal (PSK)` crypto key is 8 to 63 digits. Only ASCII-7bits characters are allowed for the crypto key.



If the WPA encryption of your router is unknown or if the WPA encryption of your router is `Auto`, do rather use the default value corresponding to the automatic mode:

`Pairwise key cipher`	`Group key cipher`
CCMP (AES) TKIP	*CCMP (AES) TKIP*

If the WPA encryption of your router is `TKIP`, it is possible to use:

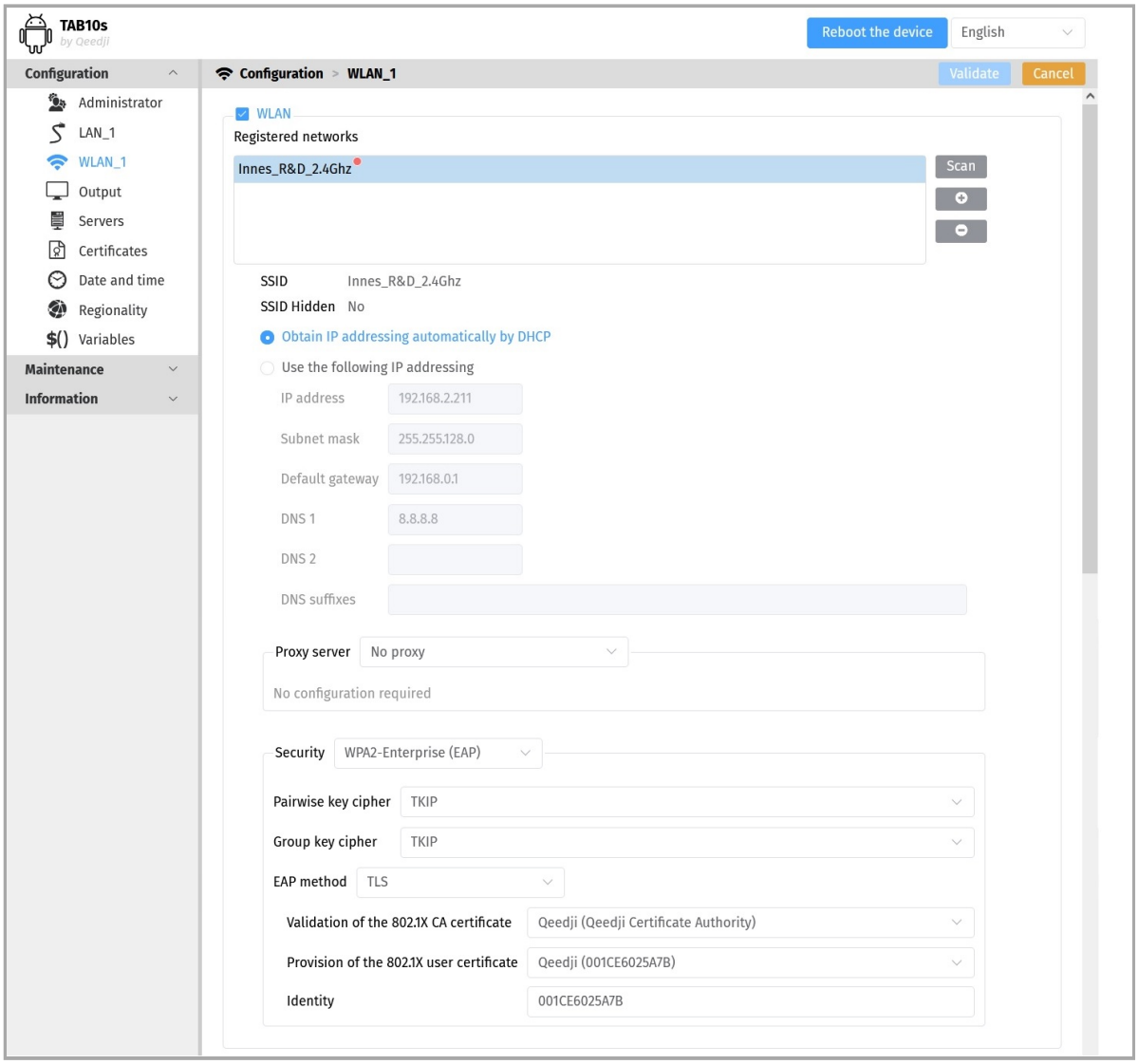
`Pairwise key cipher`	`Group key cipher`
TKIP	*TKIP*
CCMP (AES) TKIP	*CCMP (AES) TKIP*

If the WPA encryption of your router is `CCMP (AES)`, it is possible to use:

`Pairwise key cipher`	`Group key cipher`
CCMP (AES)	*CCMP (AES)*
CCMP (AES) TKIP	*CCMP (AES) TKIP*

In case *WPA-Enterprise (EAP)* and *WPA2-Enterprise (EAP)* security:

- choose one `EAP method` among *PWD*, *PEAP*, *TLS* and *TTLS*. The chosen `EAP method` must be supported by your RADIUS server,
- choose the `Phase 2 authentication` among: *NONE*, *PAP*, *MSCHAP*, *MSCHAPV2*, *GTC*. The chosen `Phase 2 authentication` must be supported by your RADIUS server and is required only for *PEAP* and *TTLS* `EAP methods`.



> ☛ *In the context of a secure network, your device must be first declared in your dedicated RADIUS server with a `identity` / `password`. For further information, please contact your IT department.*

When required, fill the `Identity` / `password` declared for your device in your RADIUS server.

> ☛ *When displayed, the `Anonymous identity` field value is optional.*

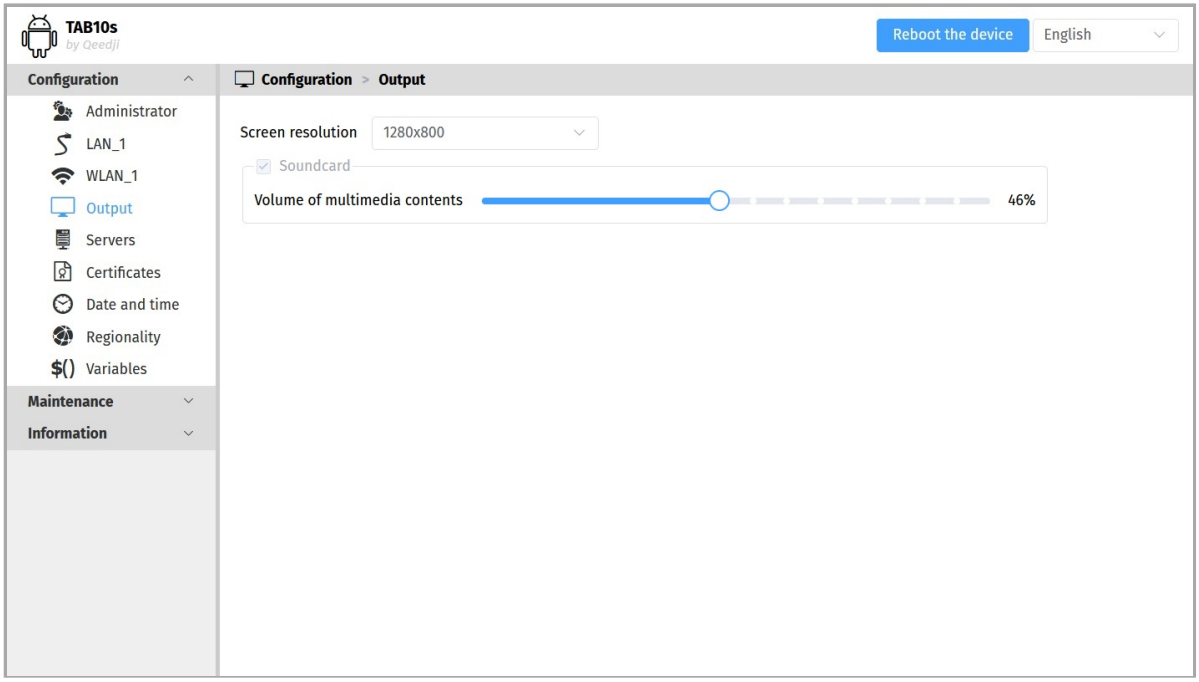
The *TLS* `EAP methods` and *TLS* `Phase 2 authentication` allow to provide a `802.1X user certificate` installed in your TAB10s device when required by your RADIUS server configuration.

The *TLS*, *TTLS*, and *PEAP* `EAP methods` allow to activate the `802.1X CA certificate` validation. The `802.1X CA certificate` must be installed first in your TAB10s device. For further information about certificates installation, refer to the chapter § Certificates.

> ☛ *The `802.1X CA certificate` is the certificate with the highest autority for your RADIUS server. For further information, please contact your IT department.*
>
> ☛ *The `Domain of the 802.1X CA certificate` input is diplayed only when using the `Use system certificates` value for the `Validation of the 802.1X CA certificate` input. The `Domain of the 802.1X CA certificate` input must not be kept `empty`. In case the certificate with highest authority for your RADIUS server is already embedded in the AOSP SYSTEM trusted credential, you can select the `Use system certificates` input value for the `Validation of the 802.1X CA certificate` input. In this case, during the communication with the RADIUS server, `AQS` checks whether the trusted certificate of the Radius is really trusted by a certificate with a higher authority embedded in the AOSP SYSTEM trusted credential basis, then checks its trustness chain. `AQS` checks then, in addition, that the `commonName` value of the Radius certificate is properly reported in the `Domain of the 802.1X CA certificate` input.*
>
> ☛ *When using `802.1X` certificates, in case your device is not on time or when the `802.1X` certificates 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 suitable configuration script to install an appropriate certificate or to update the device date and time.*

4.1.4 Configuration > Output

In the `Configuration` tab, select the **Output** menu to watch the video output configuration and set the audio output configuration.



- `Screen resolution` :
  - *1280x800.*

> ☛ *The rotation is not supported on the tablet.*

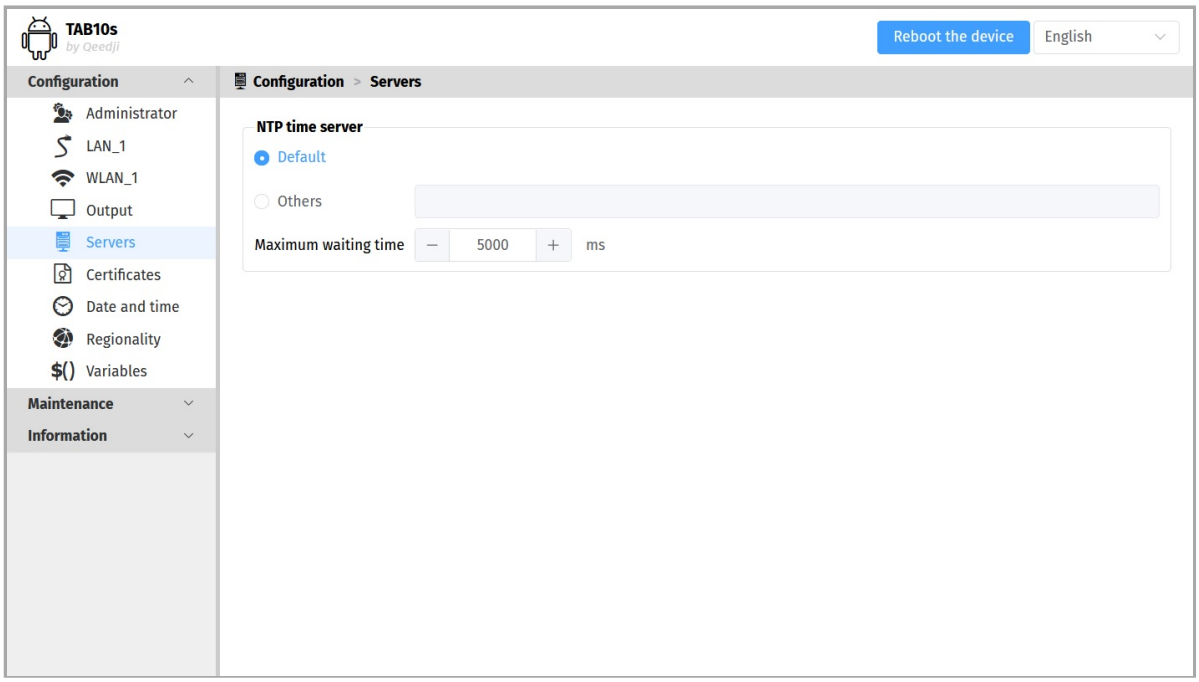
- `Sound card` :
  - `Volume of multimedia contents` bargraph: allows to tune the audio volume.

4.1.5 Configuration > Servers

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

The NTP server input allows to either choose the default `AQS` NTP server[1] or enter your favorite NTP server domain so that the device is always on time.

[1] *the `default` NTP server URL is `time.android.com`.*

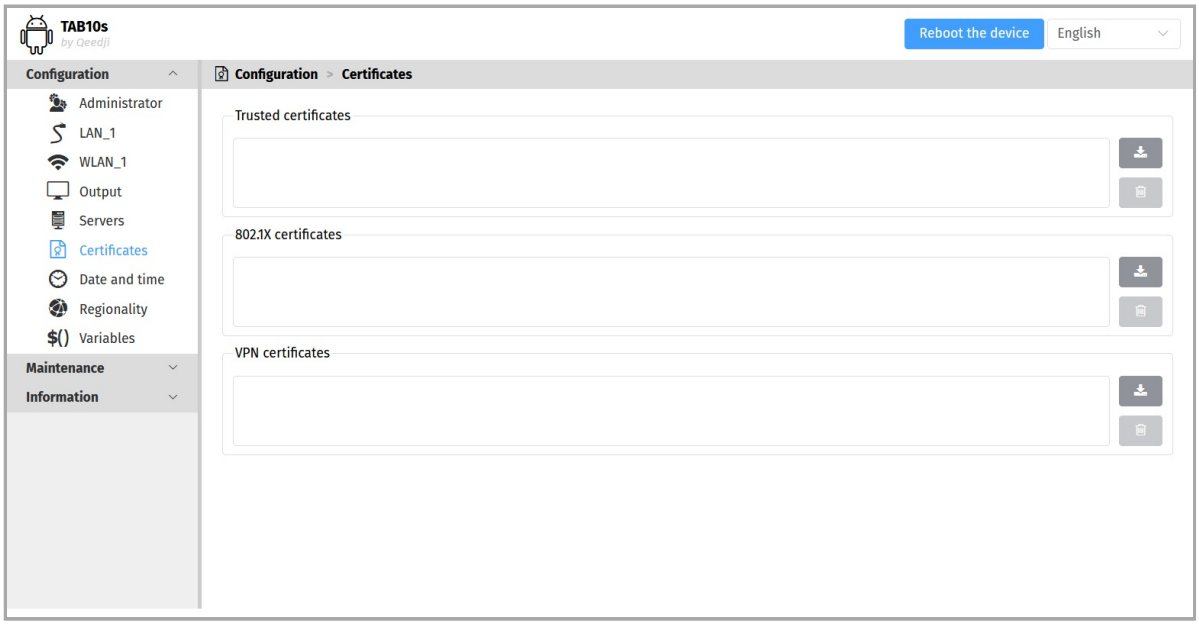


4.1.6 Configuration > Certificates

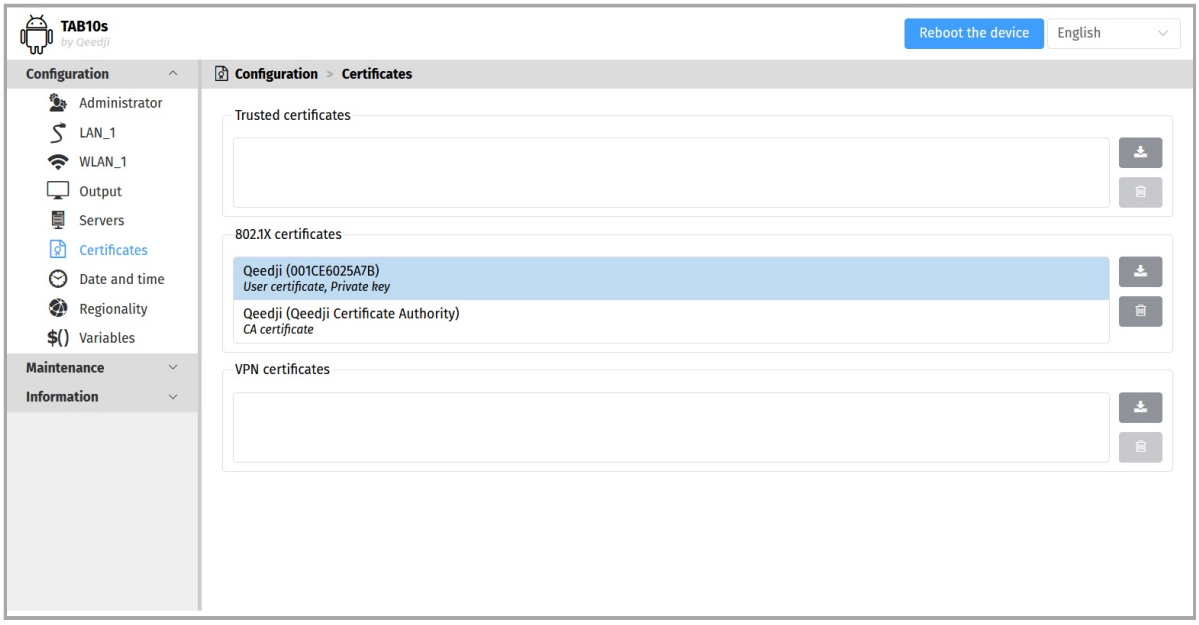
In the `Configuration` tab, select the **Certificates** menu to install:

- *Trusted* certificates,
- *802.1X* certificates (related to the RADIUS server),
- *VPN* certificates.

Click on the ✚ button of the appropriate sections to add a certificate.



This is an example with some `802.1X` certificates loaded in the TAB10s device.

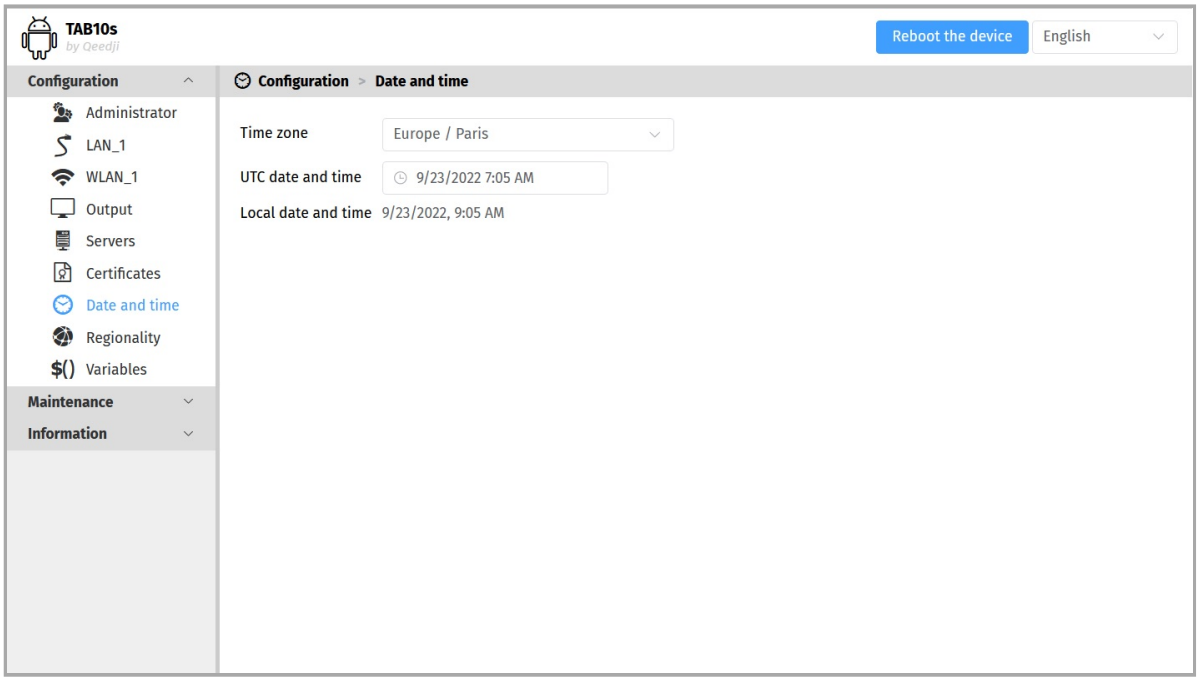


> ☛ *In case the remote content (for example an .ics) must be read on a server available in https, but the server's certificate is not signed, it may be required to install the server certificate both in the `Trusted` certificates section and in the `VPN` certificates sections to make the certificate trusty.*
>
> ☛ *When both the `802.1X CA certificate` and the `802.1X user certificate` are installed by a configuration script, they are regrouped under only one certificate in this pane. This certificate available in this pane can be used as well in the `Validation of the 802.1X CA certificate` input as in the `Provision of the 802.1X user certificate` input of the `LAN_1` or the `WLAN_1` interface.*
>
> ☛ *When configuring `EAP method` with a configuration script, some of the `802.1X certificates` (`CA` or/and `user`) not required anymore by the chosen `EAP method` will be deleted by the operating system from this pane. Consequently, when `802.1X CA certificates` and/or `802.1X user certificates` are required again with the chosen `EAP method`, it is advised to reinstall them with the configuration script as well.*

4.1.7 Configuration > Date and time

In the `Configuration` tab, select the **Date and Time** menu to check the time configuration:

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

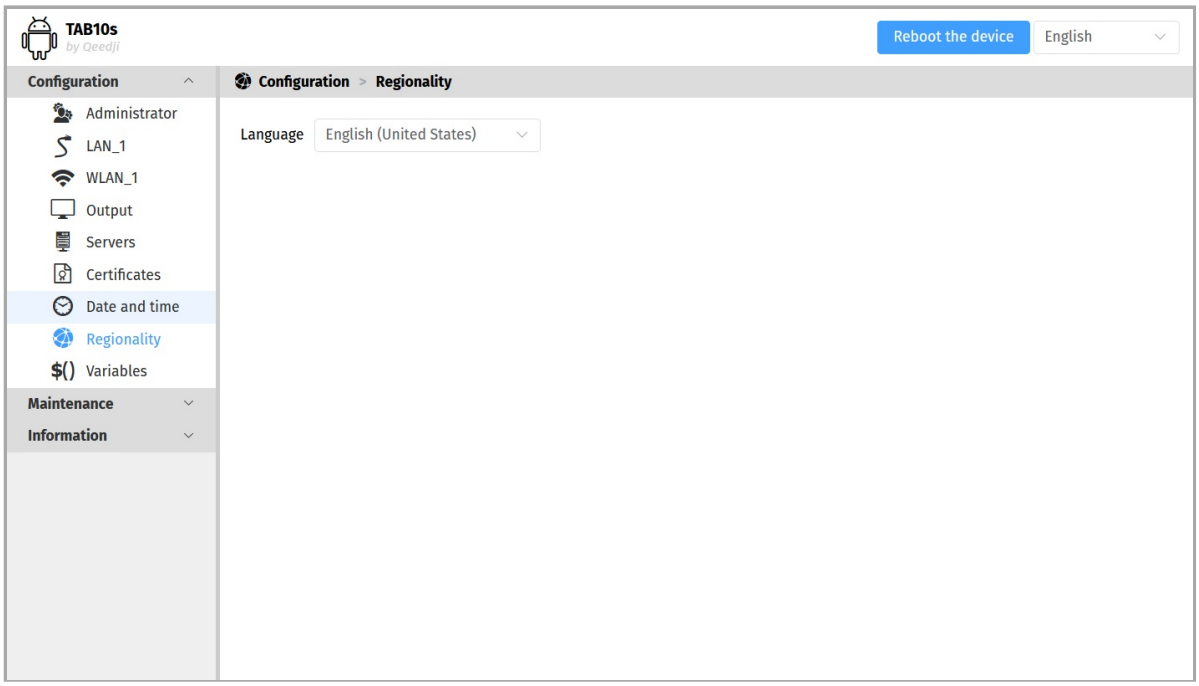


To update the date and time of your device, click on the `UTC Date and Time` value and then click on the `Now` button.

> ☛ *The `Date an time` set by the user can be taken into account only if the NTP server is not activated, or if the NTP server is not accessible.*
>
> ☛ *Setting a new date and time involves to restart 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.*

4.1.8 Configuration > Regionality

In the `Configuration` tab, select the **Regionality** menu to choose the language in which information messages or error messages related to the device need be displayed on the screen.

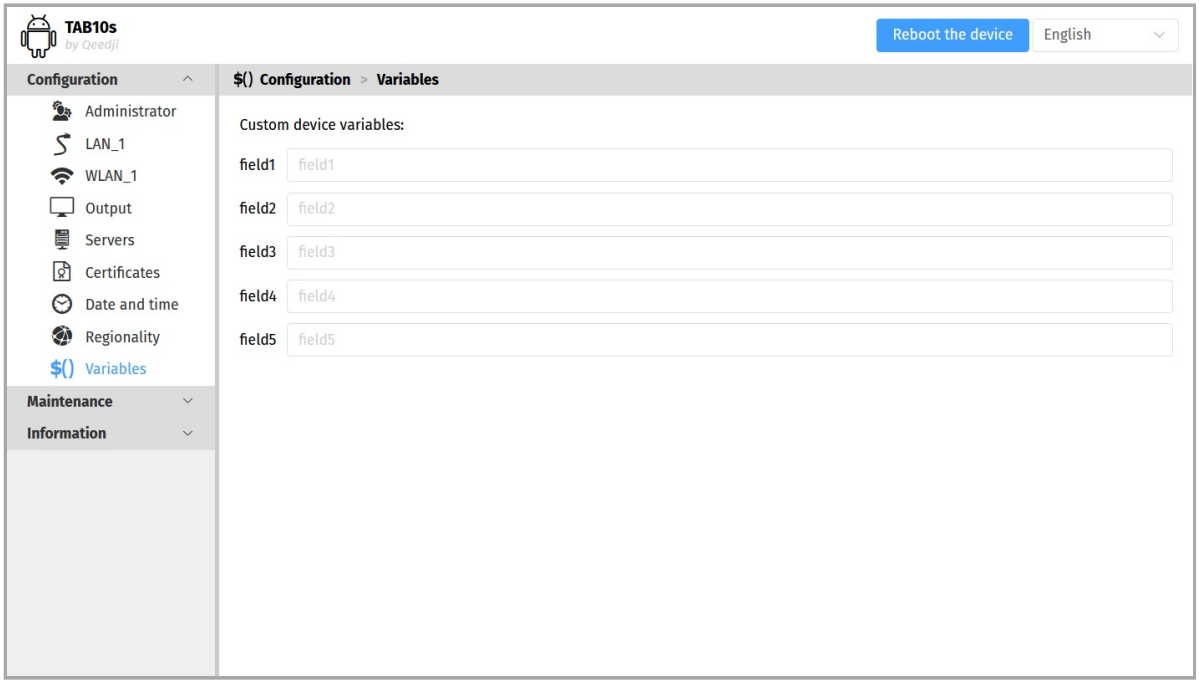


The supported languages are:

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

4.1.9 Configuration > Variables

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



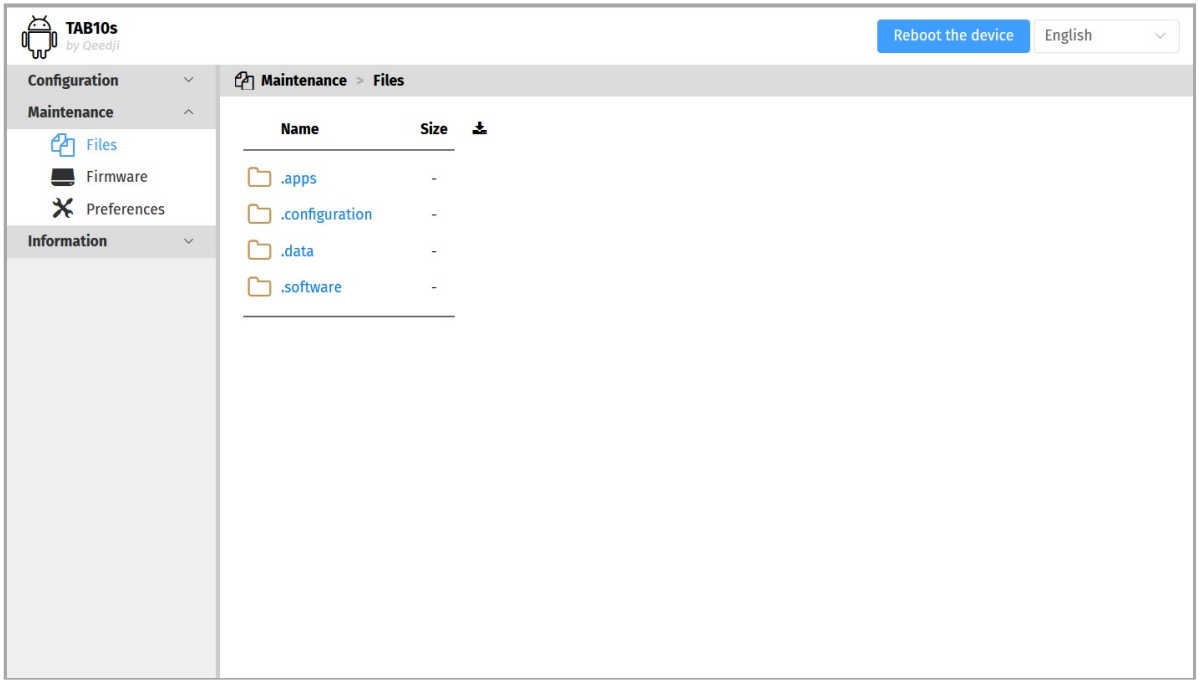
The variable names are:

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

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

4.1.10 Maintenance > Files

In the `Maintenance` tab, select the **Files** menu to see the directories and files hosted at the root directory of the WebDAV server.



These are the available WebDAV directories:

- `.apps` : directory allowing to upload APK and install it on the TAB10s device,
- `.configuration` : directory allowing to upload a configuration script to auto-configure the device,
- `.data` : directory hosting the App content,
- `.software` : directory allowing to upload a `.fqs` firmware and upgrade the `AQS` operating system version of the TAB10s device.

Firmware upgrade

The AQS firmware can be upgraded by pushing a new firmware file `aosp-tab10-setup-9.YY.ZZ.fqs` in the `.software` directory of the device WebDAV directory (`http://<device-ip-addr>/.software`).

> ☛ *The credentials values to access to the `.software` directory must be those of any connection profile except `Application user` one.*

Configuration update

The configuration of the device can be updated also by pushing an suitable `.js` configuration script in the `.configuration` WebDAV directory (`http://<device-ip-addr>/.conf`) with the Web user interface. In this case, the file pattern must be either:

- `000000000000.js` ,
- `configuration.js` or,
- `<device_LAN1_MAC_address>.js` (with ab-cd-ef-ab-cd-ef, the MAC address of the device).

> ☛ *The credentials values to access to the `.configuration` directory must be those of any connection profile except `Application user` one.*

Download the configuration script example from the Qeedji Website it then:

- edit the 000000000000.js configuration script and uncomment/modify the appropriate lines according to your needs,
- rename the configuration script if required,
- once saved, drop it in the WebDAV directory like explained above,
- when suitable for your device, save it preciously for future use.

After a `.js` configuration script loading, the device is rebooting automatically once to take the new configuration into account.

4.1.11 Maintenance > Firmware

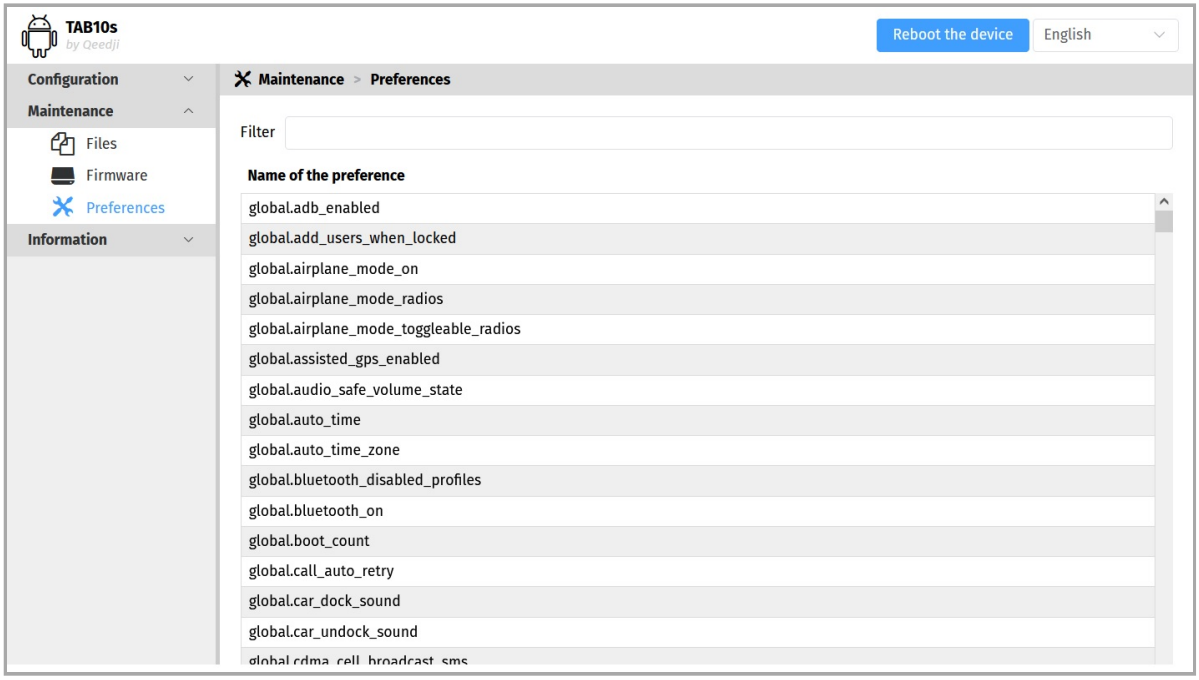
In the `Maintenance` tab, select the **Firmware** menu to view the version of the `AQS` operating system installed on your device.

Drop your `.fqs` firmware in the `Drop file here or click to add one` location or click on the button `Drop file here or click to add one` to pick up the appropriate firmware, then click on the `Send` button to update the `AQS` (for `AOSP Qeedji System`) version of your device. Wait a few minutes, the time to install the new `AQS` operating system version. Go back to the device configuration Web user interface and check that the `AQS` operating system version of the device has changed.

> ☛ *Corrective and evolutive maintenance software versions are regularly made available on the http://www.qeedji.tech/en/support/index.php?TAB10s/AQS_firmware_and_documentations. It is therefore advised to regularly update the `AQS` operating system of your device. From this website, download the latest version available for your device model.*
>
> ⚠ Do not electrically disconnect the device during the firmware upgrade. For further information, refer to the chapter § Surround light behaviour at power-up.

4.1.12 Maintenance > Preferences

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

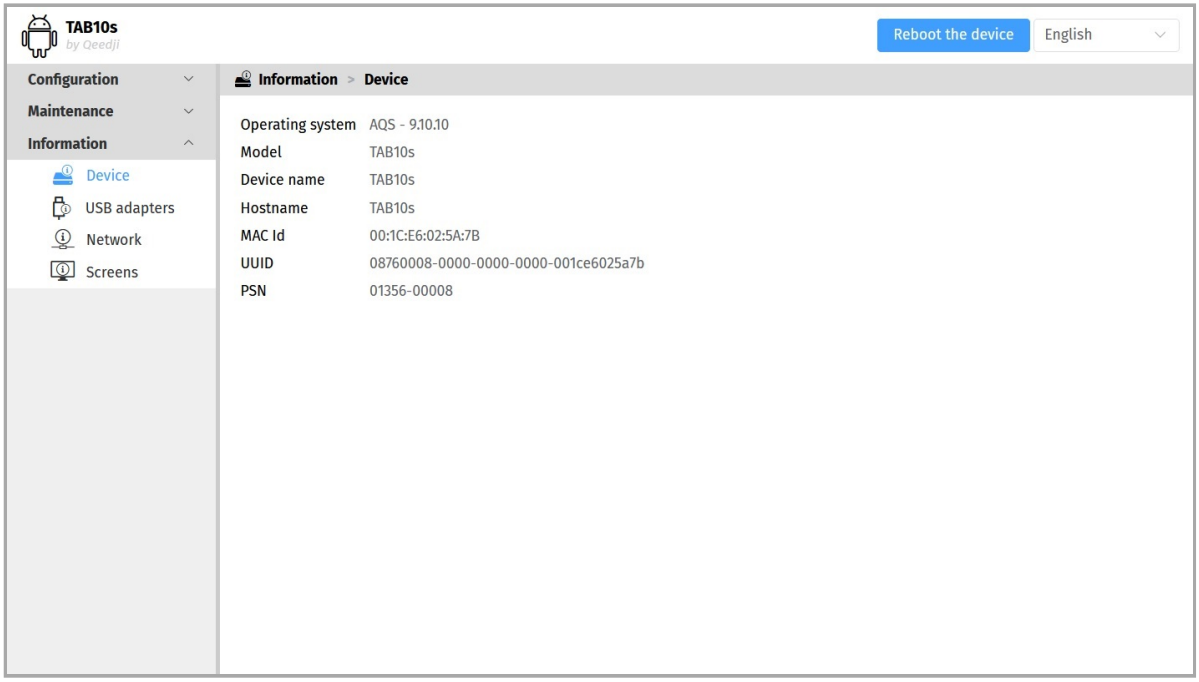


The filter allows to display only the preferences whose name contains the string entered in the filter. All the preferences have optimal default values.

Double click on a preference to change its value.

4.1.13 Information > Device

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

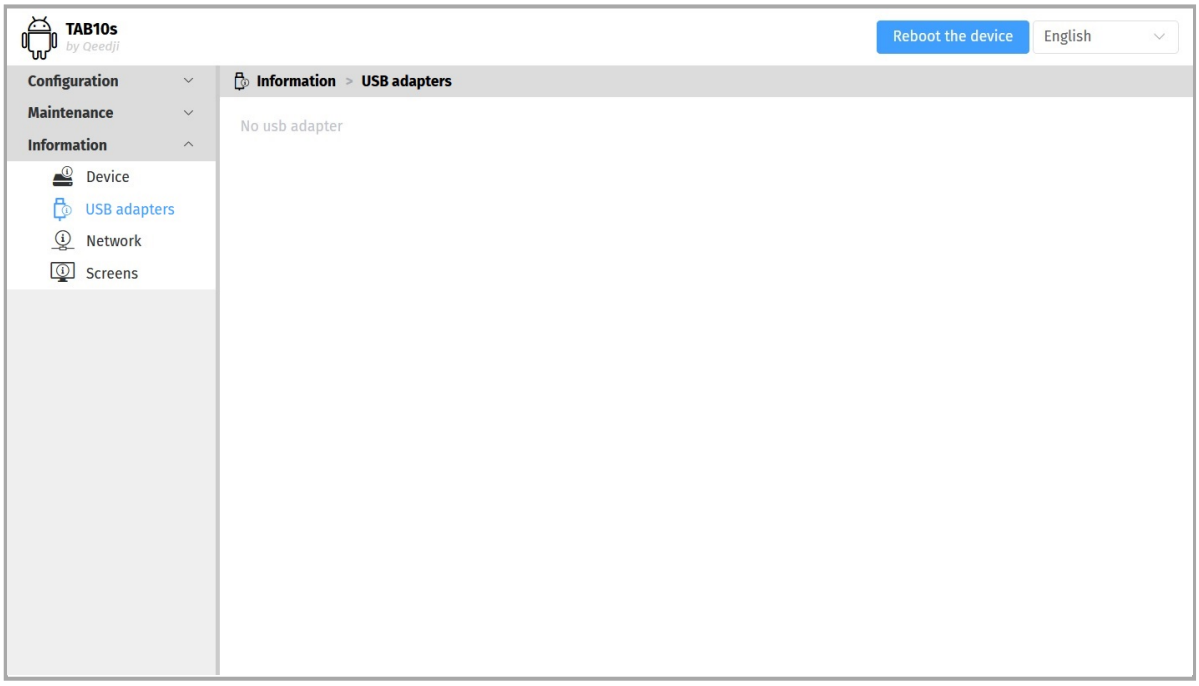


- `Operating system` : label and version of the embedded `AQS` operating system,
- `Model` : model of the `Qeedji` device,
- `Device name` : name of the device,
- `Hostname` : name of the device on the network,
- `MAC Id` : MAC address of the WLAN interface,
- `UUID` : Universal Unique IDentifier,
- `PSN` : Product Serial Number.

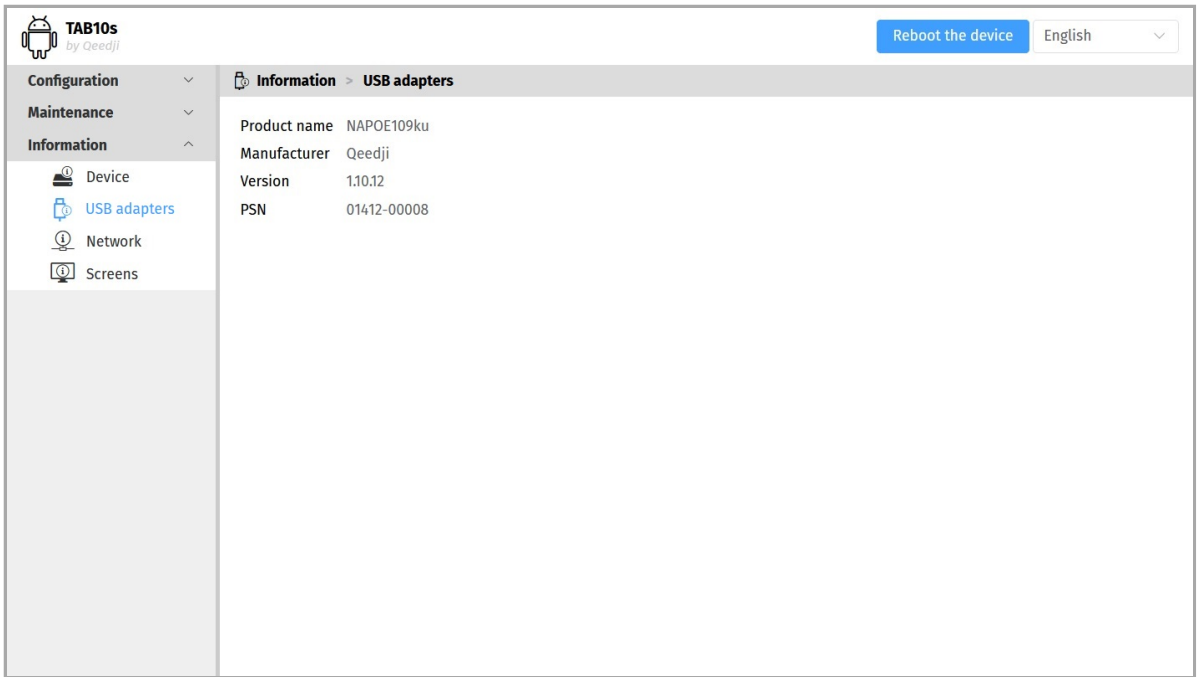
4.1.14 Information > USB adapters

In the `Information` tab, select the **USB adapters** menu to see the product name and manufacturer name of the USB adapter devices connected to the TAB10s device.

This is an example of content when the TAB10s device is supplied by a standard USB-C wall-plug and connected to a WIFI network.



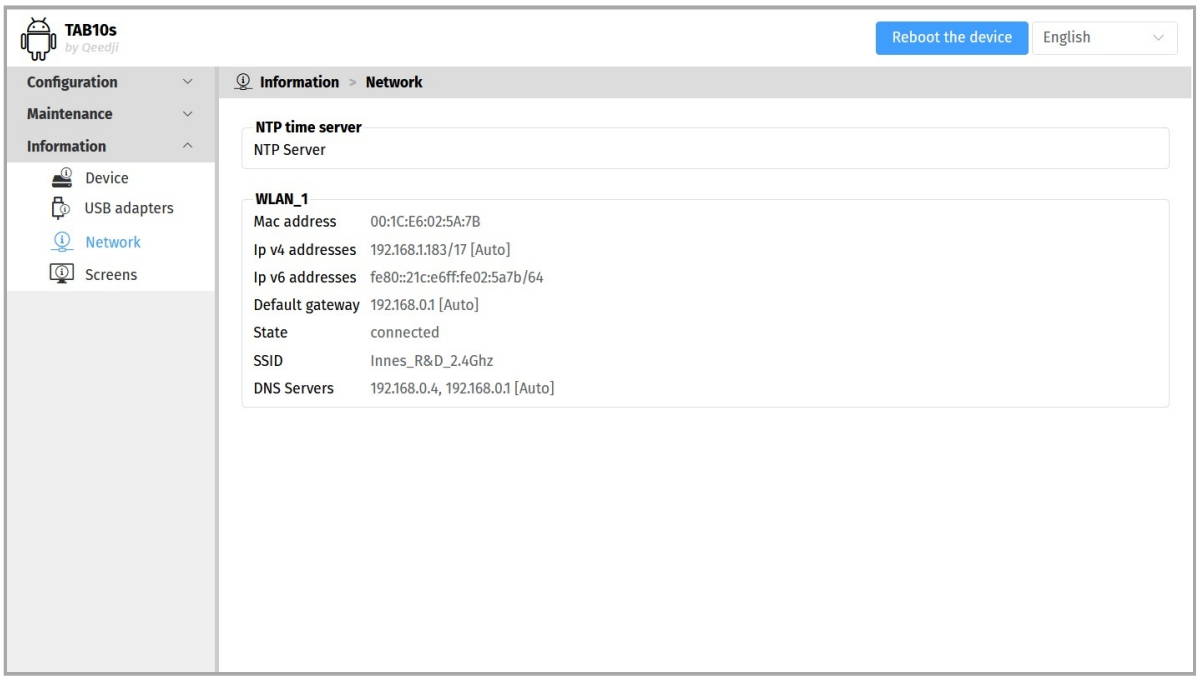
This is an example of content when the TAB10s device is supplied by a `NAPOE109ku` Ethernet adapter which is connected to a `PoE` switch.



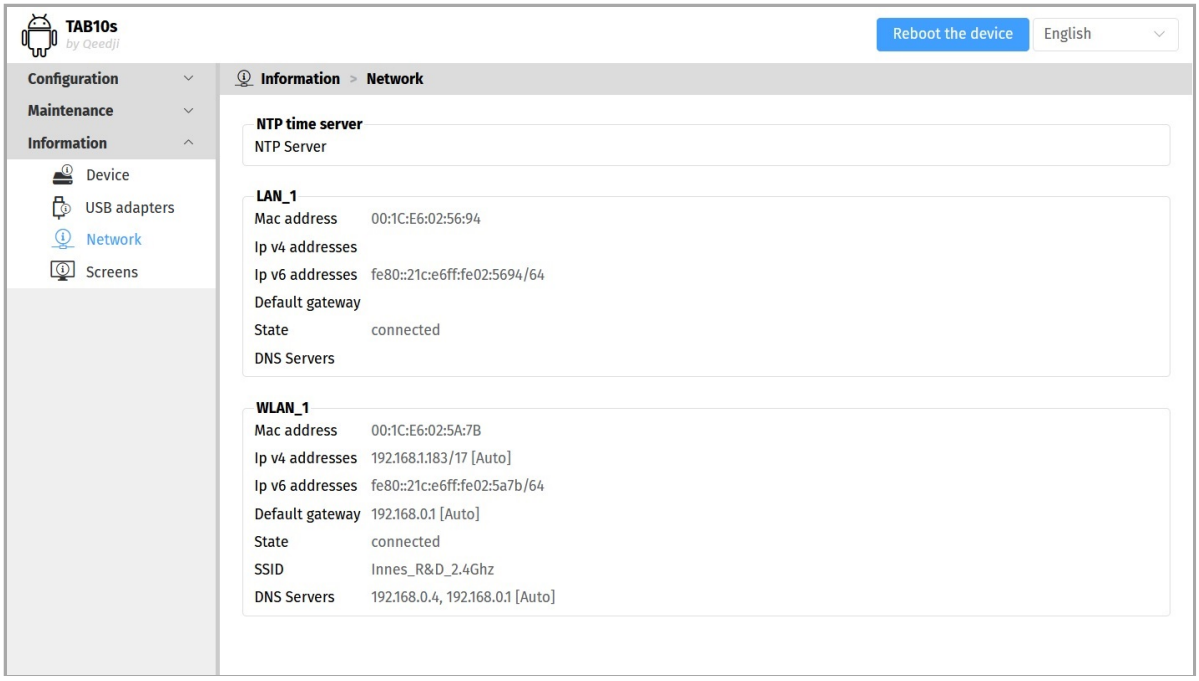
4.1.15 Information > Network

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

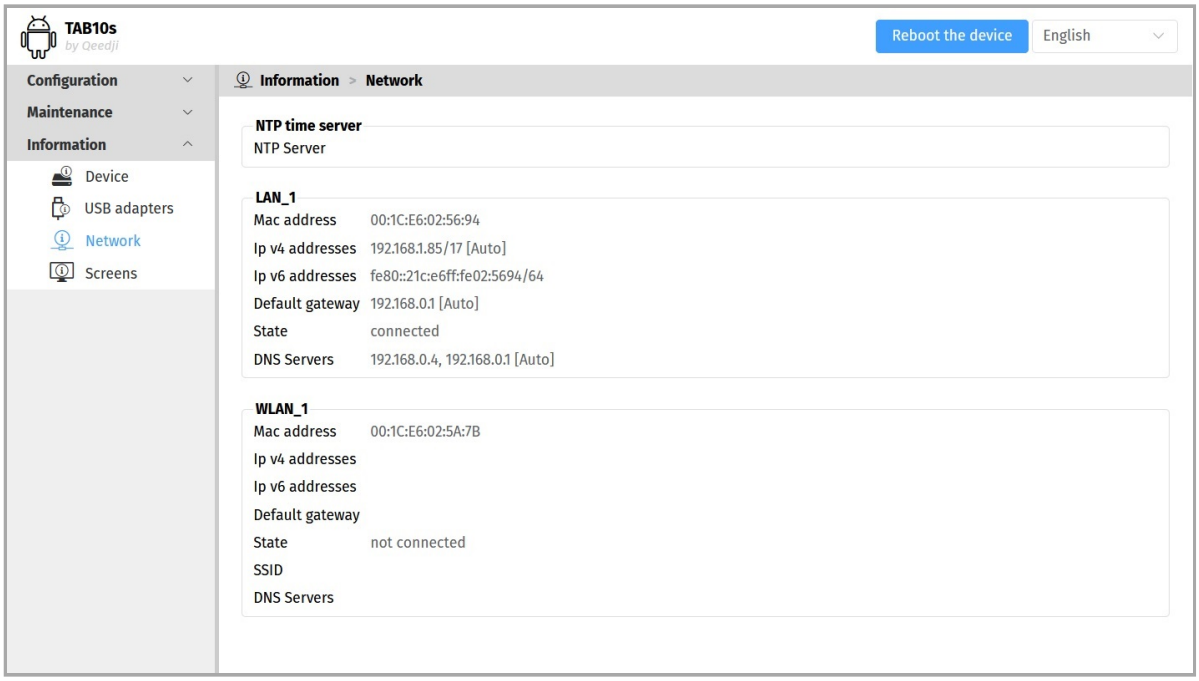
This is an example of pane content when the TAB10s device is supplied by a standard USB-C wall-plug and connected to the WIFI network.



This is an example of pane content when the TAB10s device is supplied by a `NAPOE109ku` Ethernet adapter which is connected to a `PoE` switch, which is not connected to the network. The TAB10s device is connected to the WIFI network.

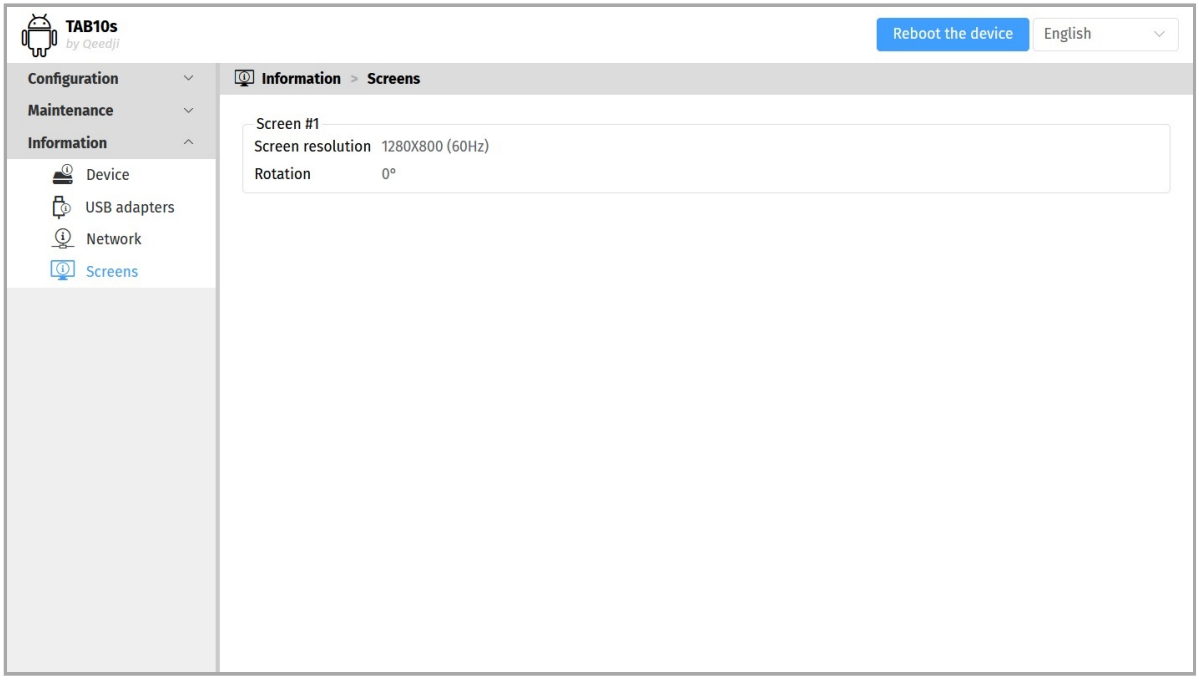


This is an example of content when the TAB10s device is supplied by a `NAPOE109ku` Ethernet adapter which is connected to a `PoE` switch, which is connected to the network.


TAB10s
by Qeedji
Reboot the device
English
Configuration
Maintenance
Information
Device
USB adapters
Network
Screens
Information > Network
NTP time server
NTP Server
LAN_1
Mac address 00:1C:E6:02:56:94
Ip v4 addresses 192.168.1.85/17 [Auto]
Ip v6 addresses fe80::21c:e6ff:fe02:5694/64
Default gateway 192.168.0.1 [Auto]
State connected
DNS Servers 192.168.0.4, 192.168.0.1 [Auto]
WLAN_1
Mac address 00:1C:E6:02:5A:7B
Ip v4 addresses
Ip v6 addresses
Default gateway
State not connected
SSID
DNS Servers

4.1.16 Information > Screens

In the `Information` tab, select the **Screens** menu to view information about the screen.



Part V

Technical information

5.1 Technical specifications

Model	Manufacturer
TAB10s	Qeedji

Processors	Model	Information
CPU	SoC NXP i.MX8	4 ARM Core Cortex A53, up to 1.8GHz per core Integrated 2D/3D GPU 1080p60 VP9 Profile 0, 2 (10-bit) decoder, HEVC/H.265 decoder, AVC/H.264 Baseline, Main, High decoder VP8 decoder 1080p60 AVC/H.264 encoder, VP8 encoder

Screen	Information
Panel type	LCD TFT, capacitive
Screen size	10.1"
Resolution	16:10, 1280 x 800 px
Back light	LED
Touch screen	Multitouch 10 points max
Contrast ratio	800 (typ.)
Viewing angle	170° in all direction
Brightness	Brightness: 500 nit (typ.)
Display mode	Transmissive, normally black

Power supply	Information
Through POGO type connector	4.75 V to 5.45 V (recommended values) 4.70 V and 5.50 V as absolute minimum and maximum values
Through USB-C connector	4.75 V to 5.45 V[1] (recommended values) 4.70 V to 5.50 V[1] as minimum and maximum values
Power consumption	6/8 W[2] (typical value) 10 W [3] (maximum value) [2] depends on the APK running and the used peripheral. [3] the maximum current is 2.1 A, so you should select an external power supply accordingly. `Qeedji` recommends the `NAPOE109fu` model accessory, as it is fully qualified with TAB10s. For standard USB power supply adaptor, select a 5 V / 3 A capable device.

[1] *For TAB10s devices whose the PSN is 01352-xxxxx, the power supply specification through USB-C connector is 4.75 V to 5.35 V as recommended values, 4.70 V and 5.40 V as absolute minimum and maximum values.*

USB Data	Information
Through USB-C connector	USB 2.0
Through POGO type connector	USB 2.0

Network	Information
802.11 a/b/g/n/ac (WIFI 5)	LBEH5HY1MW-230, MURATA chip 2,4 GHz and 5 GHz, built-in antenna

Storage	Size	Form factor
Micro SD Card	16 GB	microSD 15 x 11 x 1 mm (0.59 x 0.43 x 0.04")

Volatile memory	Size
DDR4	2 GB (~1 GB for AQS, ~1 GB for user data and APK)

Sensor	Information
NFC/MIFARE	13,56 MHz
RFID	125 KHz

Surround light	Information
	3 colors: green, orange, red

Camera	Information
Sensor	5 Mpx
Inhibition	by DIP switch
Output format	RAW RGB, RGB565/555/444, CCIR656, YUV422/420, YCbCr422
Transfert rate	QSXGA (2592 x 1944 px) @ 15 fps 1080p @ 30 fps 1280x960 @ 45 fps 720p @ 60 fps VGA 640x480 @ 90 fps QVGA (320x240) @ 120 fps

Microphones	Information
Number	2
Inhibition	by DIP switch

Bluetooth	Information
Bluetooth 5.0	2,4 GHz, built-in antenna

Audio output	Information
Mono speaker	0.7W

FAN
Fanless

Operating system	Information
`AQS` for TAB10s	`AQS` = `AOSP` (Android Open Source Project) `Qeedji System`

Operating temperature	Storage temperature
0 °C to +40 °C (32 °F to 104 °F)	-20 °C to +60 °C (-4 °F to 140 °F)

Operating humidity	Storage humidity
< 80 %	< 85 %

Weight	Dimensions (W x H x D)
0,719 Kg (1,58 lb)	255 mm x 178,5 mm x 10,8 mm (10,0" x 7,0" x 0,42")

Plastic enclosure flame rating
White material: PVC UL 94 V-0, diffusing material: PC b-S1,d0

Warranty
1 year

5.2 Built-in RFID reader

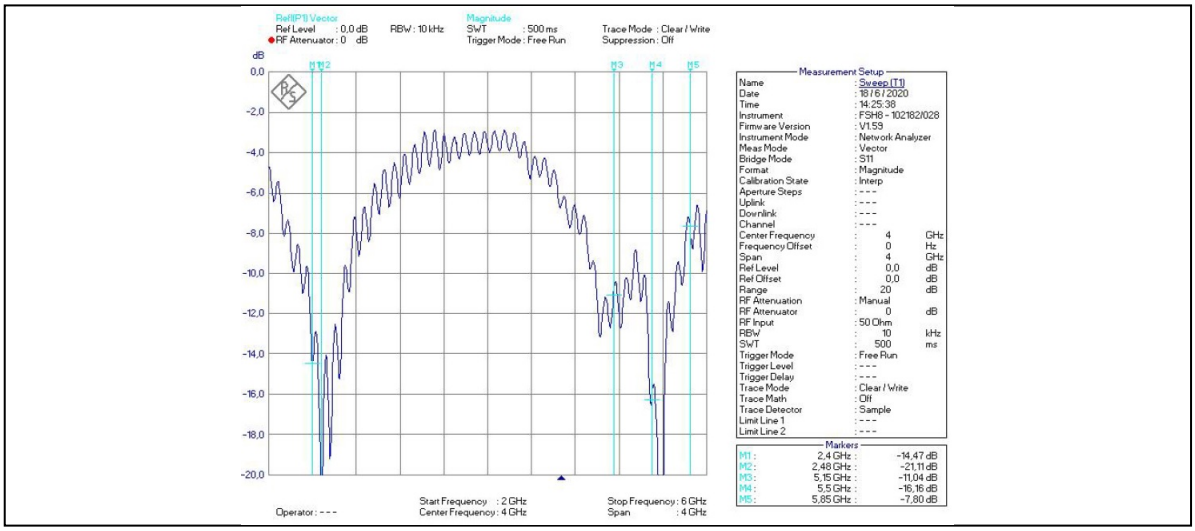
The device TAB10s has a badge reader allowing to recognize the badges supporting the RFID/NFC technology.

Type	Modulation frequency	Brand (Manufacturer)	Applicable standard	Data rate (kbps)	Supported	Tested configuration
NFC type A	13.56 MHz	Mifare Classic 1K/4K (NXP)	ISO 14443 typeA	106	Yes	
NFC type A	13.56 MHz	Mifare Plus EV1/EV2 2K/4K (NXP)	ISO 14443 typeA	106	Yes	
NFC type A	13.56 MHz	Mifare UltraLight EV1/C (NXP)	ISO 14443 typeA	106	Yes	
NFC type A	13.56 MHz	Mifare DESFire D40/EV1/EV2 2K/4K/8K (NXP)	ISO 14443 typeA	106	Yes	
NFC type A	13.56 MHz	Mifare NTAG203	ISO 14443 typeA	106	Yes	
NFC type A	13.56 MHz	Jewel (Innovision)	ISO 14443 typeA	106	Yes	
NFC type A	13.56 MHz	Topaz 512 (BCM512)	ISO 14443 typeA	106	Yes	
NFC type A	13.56 MHz	Kovio (Kovio)	ISO 14443 typeA	106	Yes	
NFC type A	13.56 MHz	SLE66 (Infineon), SmartMx (NXP)	ISO 14443 typeA	106	Yes	
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	Yes	
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		Yes	
RFID LF[1]	125 KHz	Hitag (NXP), 125KHz Prox (HID)	ISO 18000-2, ISO11784/11785/14223		Yes	

[1] only UID of RFID is supported.

5.3 Antenna return loss

This is the return loss diagram for the WIFI/Bluetooth antenna:



5.4 Conformities

EUROPE

In conformity with the following European directives:

- `LVD 2014/35/EU`,
- `EMC 2014/30/EU`,
- `RED 2014/53/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` Website 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
```

Part VII

Appendix

7.1 Appendix: Qeedji PowerPoint publisher for Media Players

This appendix explains how to publish `.pptx` MS-Powerpoint presentation on TAB10s devices using your MS-Office PowerPoint, on which the `Qeedji PowerPoint Publisher For Media Players` PowerPoint Add In is installed.

> ☛ *The `Qeedji PowerPoint Publisher For Media Players` PowerPoint Add In can deal with several TAB10s devices with the same MS-PowerPoint presentation.*
>
> ☛ *In this version, only the TAB10s devices, whose WebDAV servers are available with the `http://` scheme (default value), are supported.*

> ☛ *The TAB10s device needs to be purged from any other existing APK.*

Qeedji PowerPoint Publisher For Media Players: installation

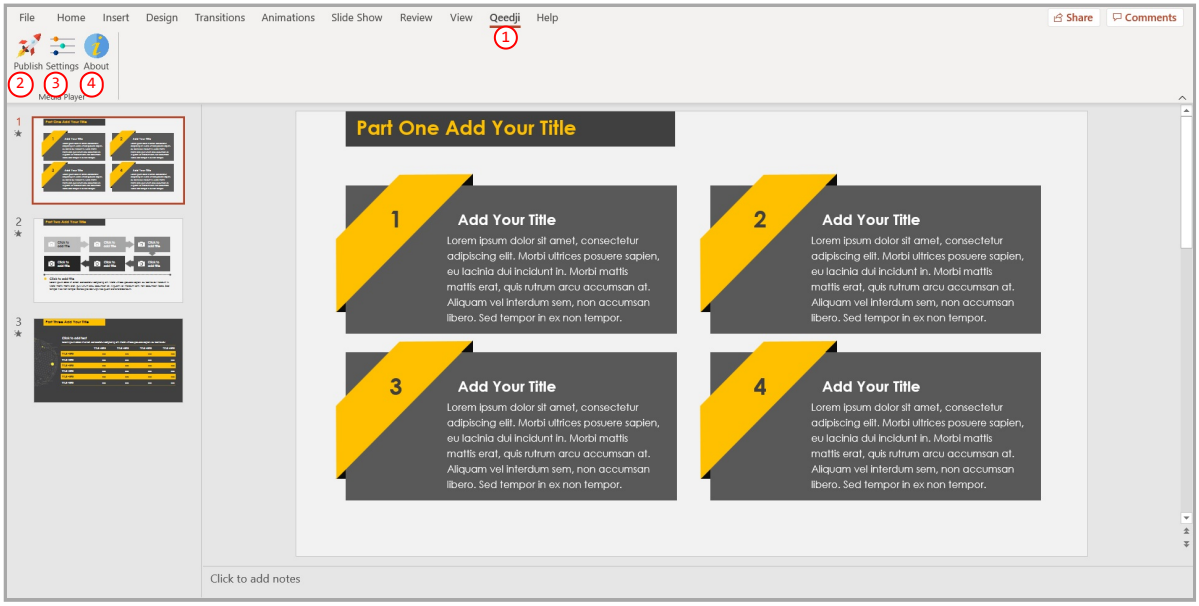
The `Qeedji PowerPoint Publisher For Media Players` PowerPoint Add In needs to be installed once:

- download the appropriate installer (.msi file):
  - Qeedji PowerPoint Publisher For Media Players (nt_ia64) for your *MS-Office* (nt_ia64),
  - Qeedji PowerPoint Publisher For Media Players (nt_ia32) for your *MS-Office* (nt_ia32).
- execute the installer and choose the `Everyone` or `Just for me` installation according to your needs. For example, choose `Just me`,
- click on *Next* button at each step by checking the default installation settings.

> ☛ *Choosing `Everyone` may require to run the PowerPoint with the Administrator rights to be able to inactivate the `Qeedji PowerPoint Publisher For Media Players` PowerPoint Add In afterwards.*
>
> ☛ *Warning: one of the installation steps is quite long and can take several minutes (for example, 2 minutes) and may depend on the computer.*

Open MS-Office PowerPoint and check that a `Qeedji` (1) menu has appeared. Clicking on it makes appear a `Qeedji` ribbon which has 3 items:

- `Publish` (2),
- `Settings` (3),
- `About` (4).

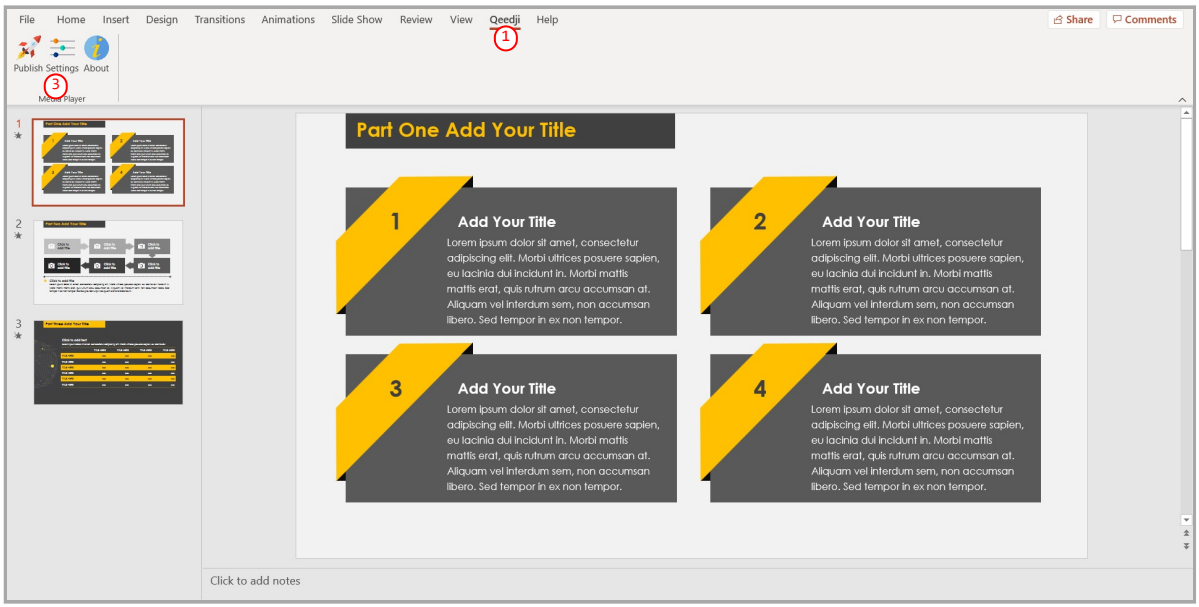


> ☛ *If the `Qeedji` menu (1) does not appear after a successful installation, contact support@qeedji.tech.*
>
> ☛ *In the `Qeedji` ribbon, click on the `About` (4) item to see the version of the `Qeedji PowerPoint Publisher For Media Players` PowerPoint Add In.*
>
> ☛ *For older computer, it could be requested to install first `.NET framework version 4.X.Y` before installing the `Qeedji PowerPoint Publisher For Media Players` PowerPoint Add In.*
>
> ☛ *The same language is used for `Qeedji PowerPoint Publisher For Media Players` PowerPoint Add In interface and MS-Windows.*
>
> ☛ *In case you need to upgrade `Qeedji PowerPoint Publisher For Media Players` PowerPoint Add In, it is required to close MS-Office PowerPoint and open it again to use the new version.*
>
> ☛ *In some rare cases, the warning message `PowerPoint has problems with the Qeedji complement. If the problem persists, disable this add-on and check for updates. Do you want to disable it now? (yes/no)` could be prompted when opening a MS-Office PowerPoint. In this case, do ignore the message by clicking `No`. It should not prevent the `Qeedji PowerPoint Publisher For Media Players` to work properly.*

Qeedji PowerPoint Publisher For Media Players: Uninstallation

In case you need to uninstall `Qeedji PowerPoint Publisher For Media Players` PowerPoint Add In, use the `Add or remove programs` Windows menu, then remove the `Qeedji PowerPoint Publisher For Media Players` program.

Qeedji PowerPoint Publisher For Media Players: register one or several devices

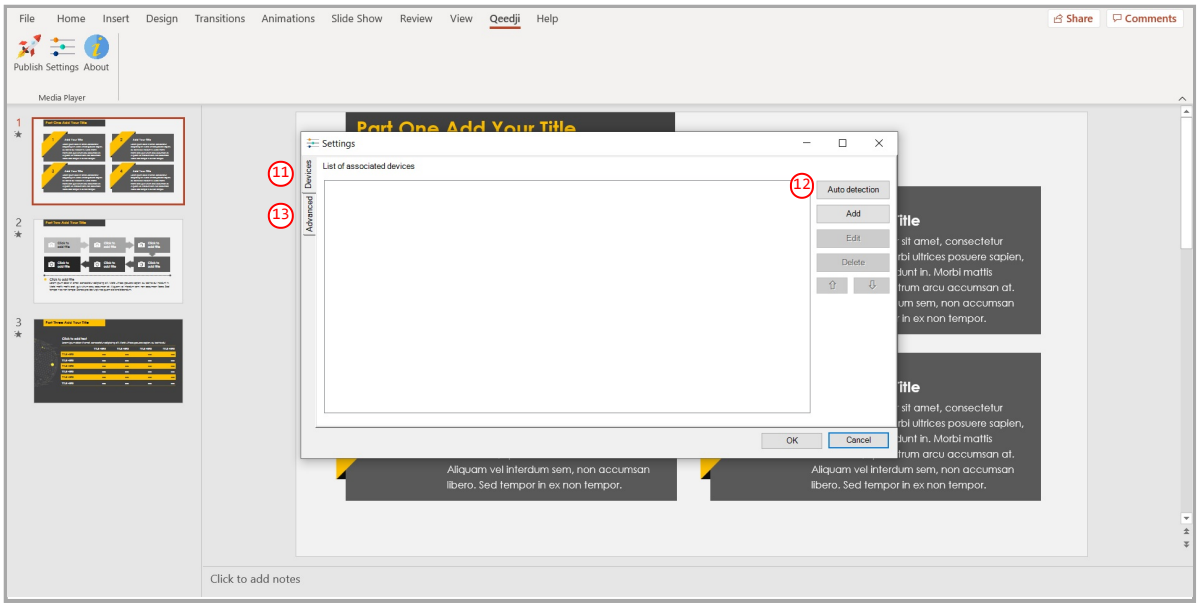


To register one or several TAB10s devices, open you MS-Office Powerpoint presentation then:

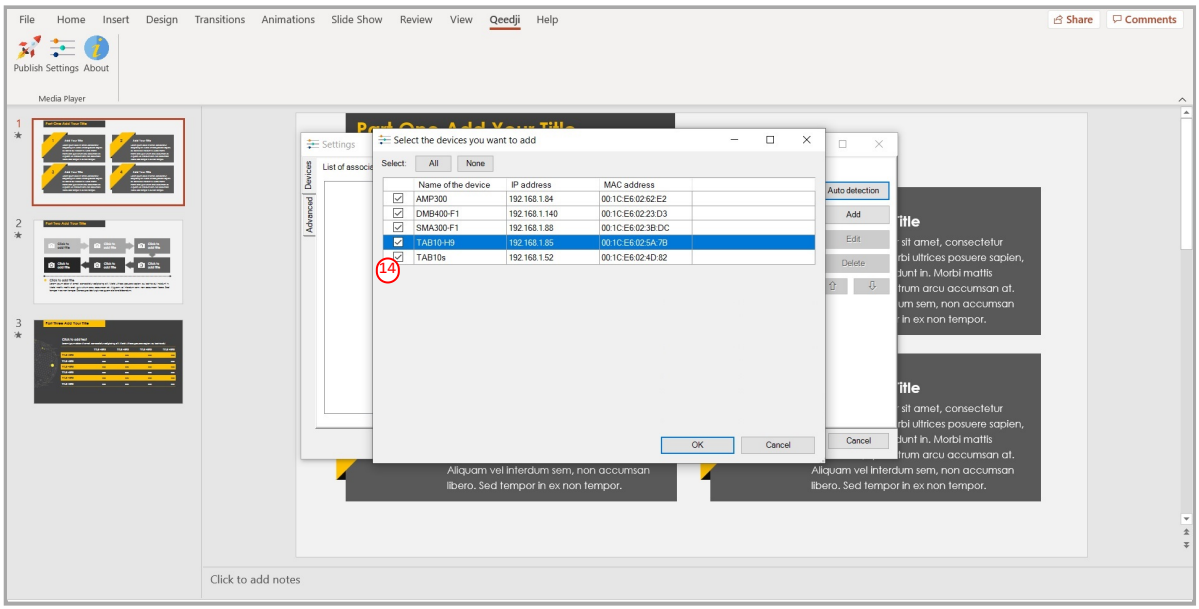
- click on the `Qeedji` (1) menu,
- on the `Qeedji` ribbon, click on the `Settings` (3) item then select the `Devices` tab.

> ⚠ Some of the MS-PowerPoint transition effects may be not yet supported. For further information, refer to the media player release note.

On the `Devices` (11) tab, click on the `Auto detection` (12) button to detect the TAB10s devices available on your local network.



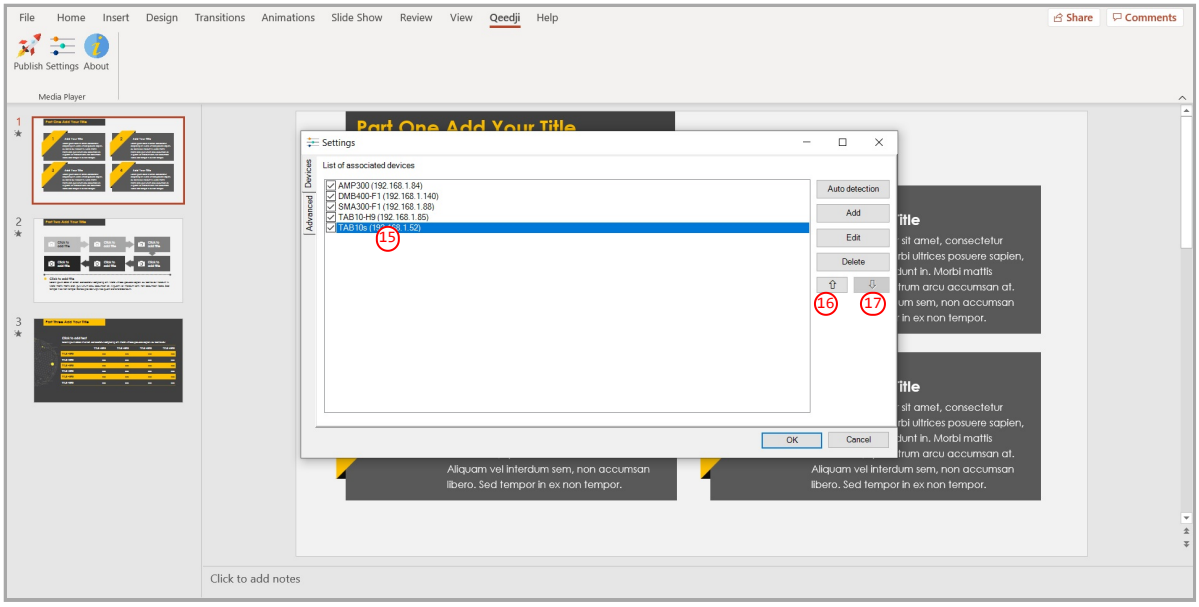
Select (14) the appropriate TAB10s devices to create a list of appropriate TAB10s devices as possible applicant for the MS-Powerpoint presentation.



Select then the only TAB10s devices on which you want to publish, by double clicking on them.

> ☛ *The TAB10s devices sorting order in the list is decisive because it is taken into account during the publication. The slides of the first section, or the first ten slides, are always affected to the TAB10s device located at the top of the list. Then the publication is continuing with the next TAB10s device located immediately below, and so on.*

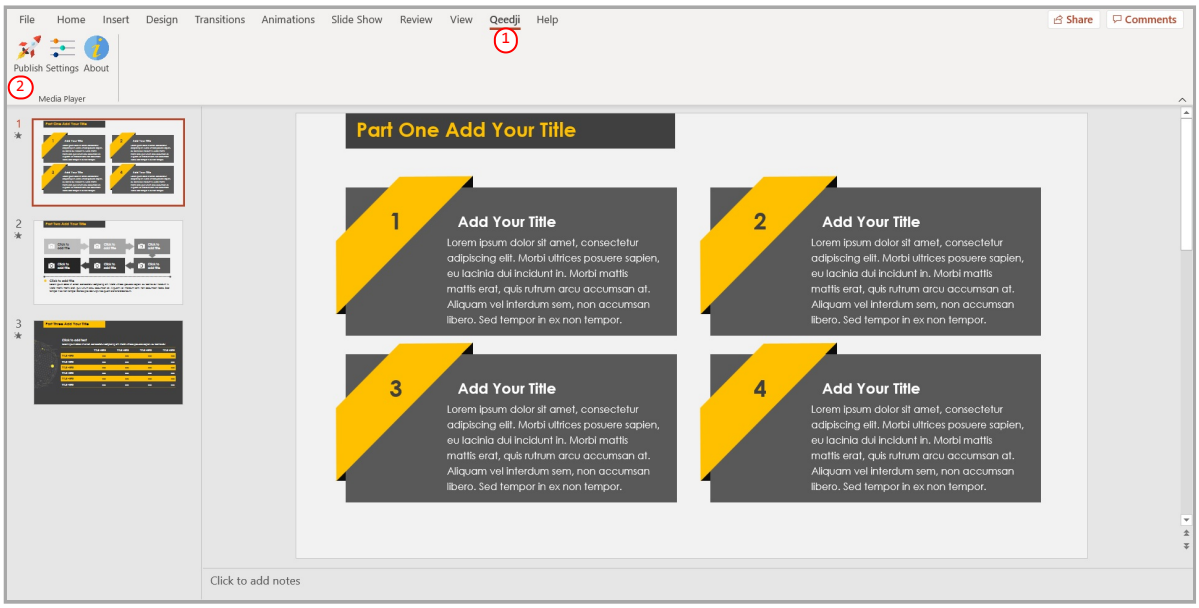
Select a TAB10s device and use the *up* (16) arrow or the *down* (17) arrow to sort them in the right order to match the MS-PowerPoint sections.



Qeedji PowerPoint Publisher For Media Players: publish

To publish a MS-Powerpoint content on your tablet, open your MS-Powerpoint presentation in MS-PowerPoint software. Then:

- click on the `Qeedji` (1) menu,
- on the `Qeedji` ribbon, click on the `Publish` (2) item.



> ☛ *Before publishing with the `Publish` item, it is advised to check in the `Settings` item, that the registered TAB10s devices are consistent and sorted in the right order.*

The *Publishing status report* is showing whether the publishing on each TAB10s devices has succeeded or not:

- `Publishing succeeded` : the publication has succeeded
- `Publishing failure (Error: 503)` : the publishing has failed. In this case, check the network connection between your computer and the TAB10s.

Publishing status report example:

```
1/5 - Publishing on device: AMP300 (192.168.1.84)
    Publishing succeeded

2/5 - Publishing on device: DMB400-F1 (192.168.1.140)
    Publishing succeeded

3/5 - Publishing on device: SMA300-F1 (192.168.1.88)
    Publishing succeeded

4/5 - Publishing on device: TAB10-H9 (192.168.1.85)
    Publishing succeeded

5/5 - Publishing on device: TAB10s (192.168.1.52)
    Publishing succeeded

Publishing completed
    Warning - Unable to find the following fonts:
    Arvo, Montserrat Black
```

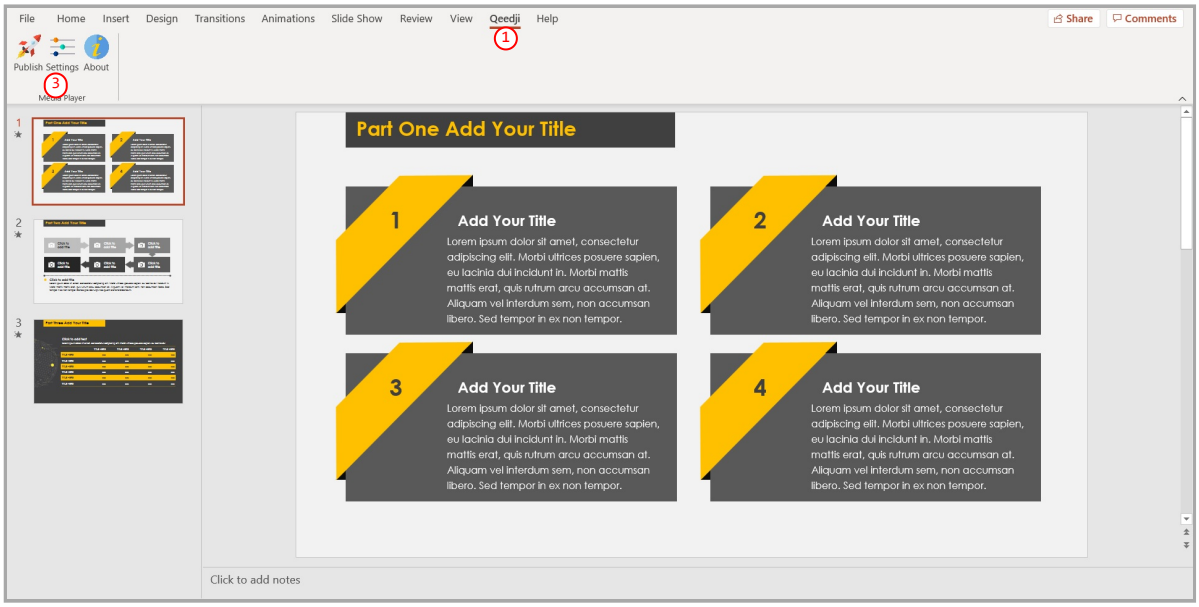
The *Publishing status report* is showing also whether the MS-PowerPoint medias can be rendered with the right fonts. In case some fonts can not be found on the Windows OS, a message `Warning - Unable to find the following fonts` is displayed followed by the missing fonts names. To solve the rendering issue, install the missing fonts on your Windows OS and publish again.

The PowerPoint presentation slideshow is now displayed on your tablet.

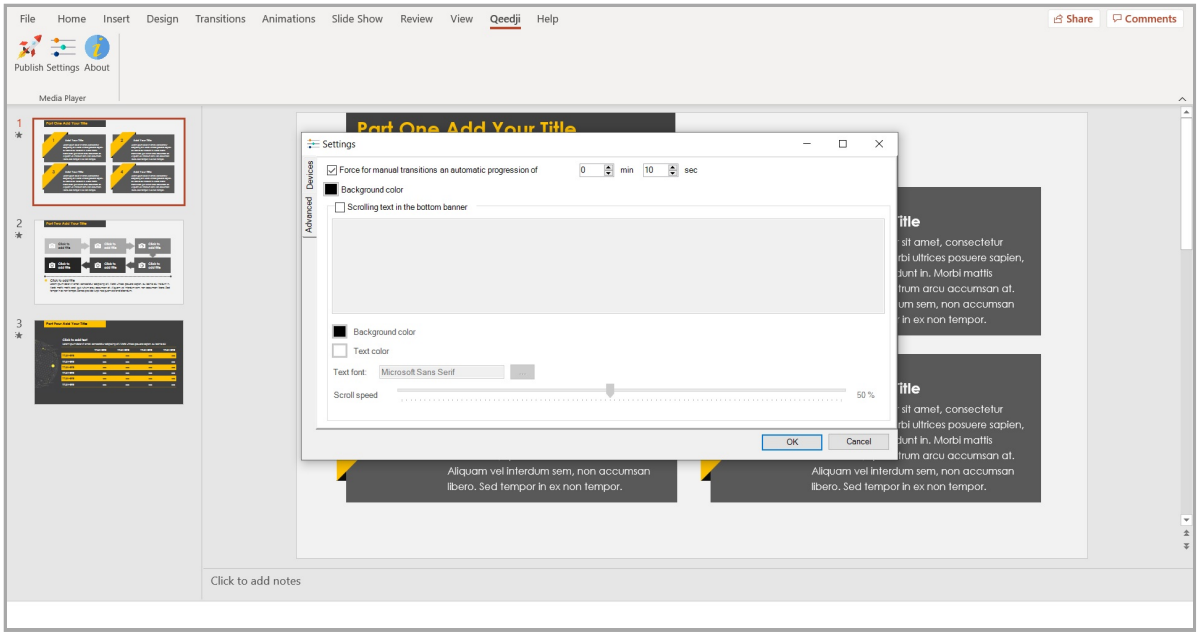
Qeedji PowerPoint Publisher For Media Players: define a default duration per page

To define a default duration per page to your MS-PowerPoint presentation, open you MS-Office Powerpoint presentation then:

- click on the `Qeedji` (1) menu,
- on the `Qeedji` ribbon, click on the `Settings` (3) item then select the `Advanced` tab.



It is possible then to `force for manual transitions a automatic progression of <m> min <n> sec` for slides having no duration per slide defined.

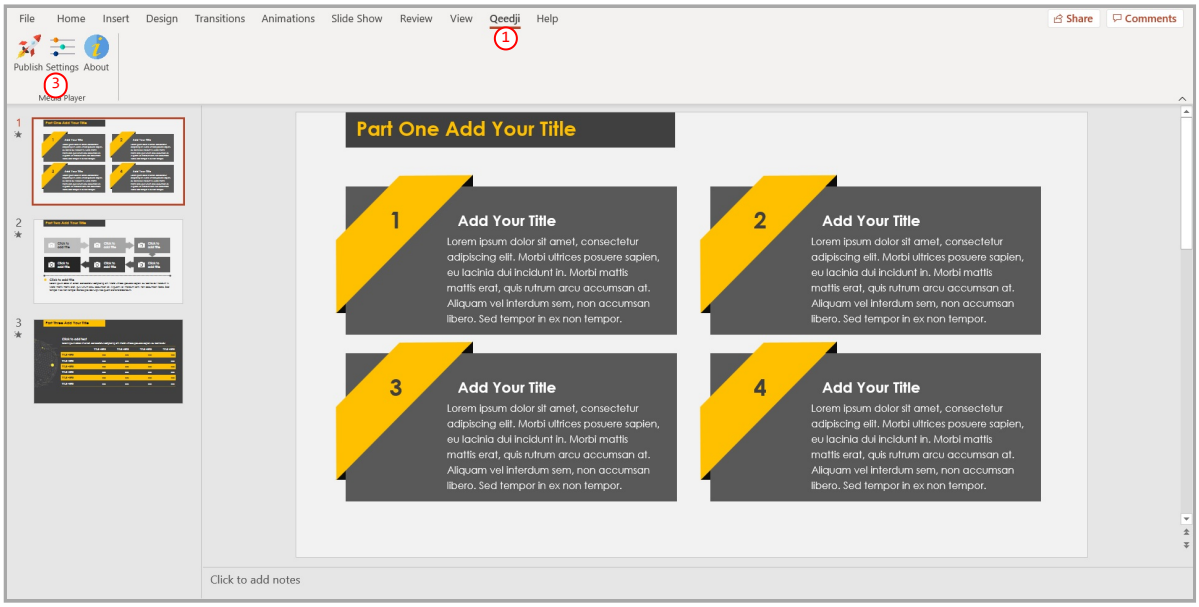


> ☛ *The `Background color` is used here only when the slide aspect ratio (`Slide Size` in MS-PowerPoint) is not 16:9.*

Qeedji PowerPoint Publisher For Media Players: add a scrolling text in a bottom banner

To activate a scrolling text in a bottom banner to your MS-PowerPoint presentation, open you MS-Office Powerpoint presentation then:

- click on the `Qeedji` (1) menu,
- on the `Qeedji` ribbon, click on the `Settings` (3) item.



Then select the `Advanced` (5) tab.

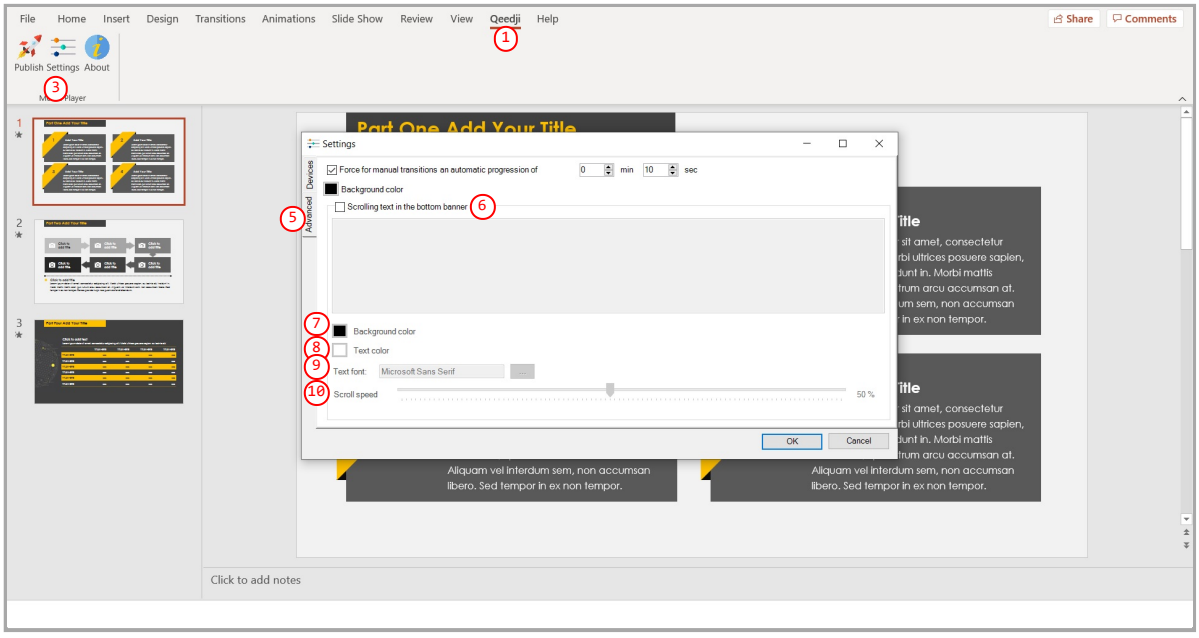
Select the `Scrolling text in the bottom banner` (6) option to activate the scrolling of a text at the bottom of the presentation.

These scrolling text properties can be modified:

- `Background color` (7),
- `Text color` (8),
- `Text font` (9),
- `Scroll speed` (10).

☛ *The banner height is 9.26% of the PowerPoint slide height.*

☛ *When the scrolling text overlay is supported by the TAB10s device, the max. number of character per line is depending on the display resolution of the TAB10s device and the chosen font. Outside this limit, the scrolling text cannot be displayed.*



Information on fonts

- The default Windows font are installed here: `C:\Windows\Fonts`
- The custom fonts installed by the user are installed here: `C:\Users\<username>\AppData\Local\Microsoft\Windows\Fonts`

To add a font to your Windows, retrieve the appropriate custom font (.ttf most of time) where you can, double click on it to install it on your Windows OS. Publish the PowerPoint again.

If you don't manage to retrieve a custom font, you can decide to replace the missing custom font by another one, existing this time, in the whole PowerPoint document. In this case, use the `Home > Replace > Replace Fonts` PowerPoint menu.

Addin uninstallation

To remove the `Qeedji PowerPoint Publisher for Media Player` addin from your Windows OS, use the `Add or remove programs` Windows menu, then remove the program `Qeedji PowerPoint Publisher for Media player`.

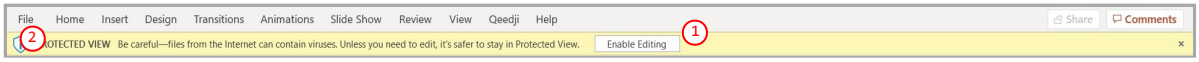
Miscellaneous

The scheme `https://` is not supported in this version.

When the App `Qeedji PowerPoint Publisher for Media Player` is not supported by a device (older OS, Smart monitor), the message below is displayed

```
Information
The App "Qeedji Powerpoint Publisher for Media player" is not supported on this device
```

> ☛ *The `protected view` may prevent to publish properly by returning this error: `Publishing failure (Error: Unable to save a copy of the current document)` (1). To work around, click on the `Enable editing` (2) button before publishing.*



Aspect ratio

For devices, the recommended aspect ratio for MS-PowerPoint slides is 16/10.

7.2 Appendix: Qualified third party references

Commercial reference	Type	Nb of USB-A connectors	Nb of USB-C (PD[1] input) connectors	Nb of USB-C (PD[1] output DRD[2]) connectors	Nb of other USB-C (DRD[2] only) connectors	Nb of RJ45 connectors (`Ethernet to USB` bridge)
QACQOC H01C-Gray	Hub USB	3	1	1	0	0
TRIPP-LITE U460-T04-2A2C-1	Hub USB	2	1	1	1	0
TRIPP-LITE U460-003-3AG-C	Hub USB + RJ45	3	1	1	0	1
Mevo Ethernet Power Adapter MV3-04A-BL[3]	PoE to USB-C adapter	0	1	1	0	1

[1] PD for `Power Delivery`.

[2] DRD for `Dual-Role-Data`.

[3] Not compatible with TAB10s devices whose the PSN is 01352-xxxxx .

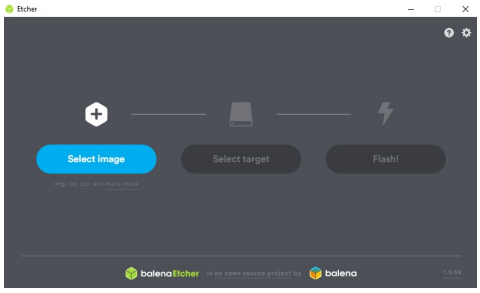
In case you wish to buy other references by your own, they need to be `Power delivery` compliant, 5 V / 3 A.

7.3 Appendix: ISO image burning with BalenaEtcher

BalenaEtcher filename	Version	OS Windows	Size	Download link
balenaEtcher-Portable-1.5.102.exe	1.5.102	x86, x64	115 MB	BalenaEtcher Website

After having installed `BalenaEtcher` software, execute it with `administrator` rights:

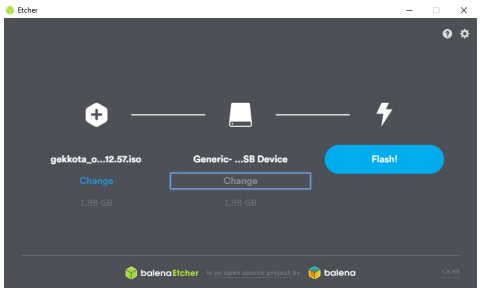
Click on the `Select image` button and select the file `aosp-tab10-setup-xx.yy.zz.iso`.



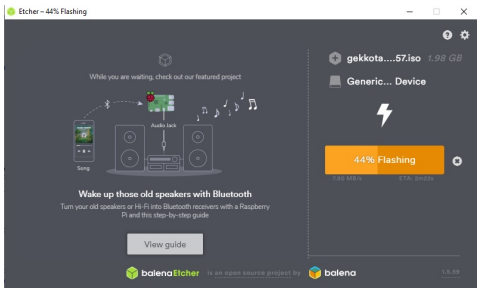
Insert the device micro SD card in the SD card slot of your computer.

> ☛ *If required, use a SD card adapter.*
>
> ☛ *After inserting the SD card in the computer, if MS-Windows 10 is displaying 14 times a format popup inviting to format the 14 partitions of the TAB10s SD card, click on the `Cancel` button of the format popups.*

Press on the `Select target` button and select carefully the storage media letter corresponding to your SD card.



Press on the `Flash!` button and wait that the micro SD card burning has completed.



7.4 Appendix: TFTP and DHCP server configuration

To use `TFTP configuration by script`, you need a `TFTP` [1] server with a `DHCP` server associated to it (code `66` option).

[1] Trivial File Transfer Protocol

The network interfaces of the TAB10s devices must be configured to obtain their IP address with the `DHCP` server.

The `TFTP configuration by script` downloading operation (specific or general) is done with the DHCP server (during the device booting). The Qeedji device configures first its network parameters obtained by `DHCP` server, and then launches `TFTP` download.

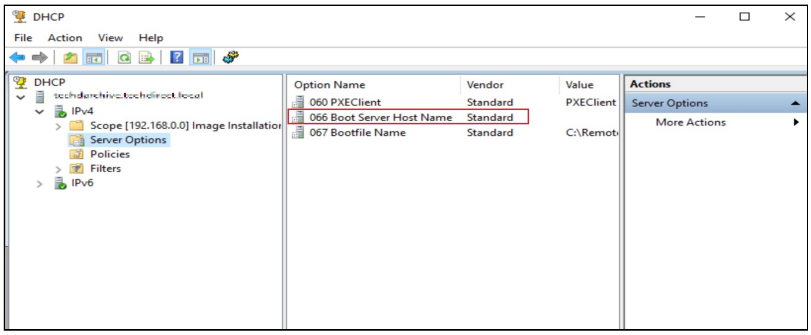
> ⚠ the installation phase is launched only when the script has never been downloaded before or if its content has been modified since the last download (md5 check).

DHCP server configuration

The `DHCP` must be configured to be associated to `TFTP` server. For that, you need to use code 66 option (`TFTP` Server), using the IPv4 address value of the `TFTP` server.

For example, for a `Microsoft DHCP server`, you need to define the option *Boot Server Host Name* and give the IPv4 address of the `TFTP server`. It can be in *Extended option* and/or *Server Options*.

> ☛ *The service must be restarted before the new parameters are fuly reflected.*

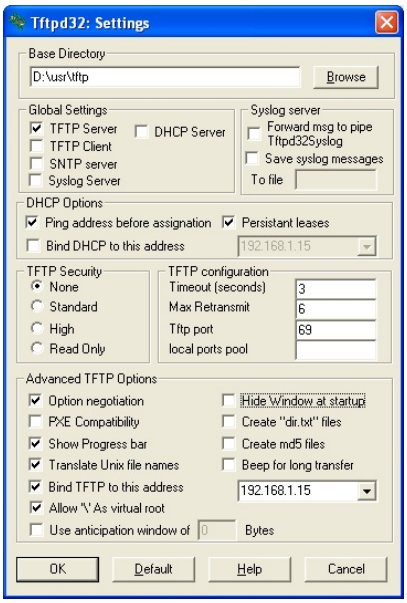


TFTP server configuration

The configuration is depending on the software client used. In all cases, you need to:

- get the directory URL that can be seen by `TFTP` clients ,
- choose the `TFTP` security *None*,
- keep the default port (*69*).

Here is an example of the `tftpd32` software with MS-Windows.



In this example, the server address is `192.168.1.15` and the exported directory is `D:/usr/tftp`.

Copy the Javascript configuration script in the exported directory of the `TFTP server`.

> ☛ *It is recommended to have one `.js` configuration script per device by following the pattern `<MAC>.js` (e.g. 00021Cfe1215.js).*

7.5 Appendix: Timezone

Area	*Country/Town* pair values supported for the `setTimezone` function of the configuration script (1 of 2)
Pacific	Pacific/Wallis, Pacific/Wake, Pacific/Tongatapu, Pacific/Tarawa, Pacific/Tahiti, Pacific/Saipan, Pacific/Rarotonga, Pacific/Port_Moresby, Pacific/Pohnpei, Pacific/Pitcairn, Pacific/Palau, Pacific/Pago_Pago, Pacific/Noumea, Pacific/Norfolk, Pacific/Niue, Pacific/Nauru, Pacific/Midway, Pacific/Marquesas, Pacific/Majuro, Pacific/Kwajalein, Pacific/Kosrae, Pacific/Kiritimati, Pacific/Honolulu, Pacific/Guam, Pacific/Guadalcanal, Pacific/Gambier, Pacific/Galapagos, Pacific/Funafuti, Pacific/Fiji, Pacific/Fakaofo, Pacific/Enderbury, Pacific/Efate, Pacific/Easter, Pacific/Chuuk, Pacific/Chatham, Pacific/Bougainville, Pacific/Auckland, Pacific/Apia,
Indian	Indian/Reunion, Indian/Mayotte, Indian/Mauritius, Indian/Maldives, Indian/Mahe, Indian/Kerguelen, Indian/Comoro, Indian/Cocos, Indian/Christmas, Indian/Chagos, Indian/Antananarivo,
Europe	Europe/Zurich, Europe/Zaporozhye, Europe/Zagreb, Europe/Warsaw, Europe/Volgograd, Europe/Vilnius, Europe/Vienna, Europe/Vatican, Europe/Vaduz, Europe/Uzhgorod, Europe/Ulyanovsk, Europe/Tirane, Europe/Tallinn, Europe/Stockholm, Europe/Sofia, Europe/Skopje, Europe/Simferopol, Europe/Saratov, Europe/Sarajevo, Europe/San_Marino, Europe/Samara, Europe/Rome, Europe/Riga, Europe/Prague, Europe/Podgorica, Europe/Paris, Europe/Oslo, Europe/Moscow, Europe/Monaco, Europe/Minsk, Europe/Mariehamn, Europe/Malta, Europe/Madrid, Europe/Luxembourg, Europe/London, Europe/Ljubljana, Europe/Lisbon, Europe/Kirov, Europe/Kiev, Europe/Kaliningrad, Europe/Jersey, Europe/Istanbul, Europe/Isle_of_Man, Europe/Helsinki, Europe/Guernsey, Europe/Gibraltar, Europe/Dublin, Europe/Copenhagen, Europe/Chisinau, Europe/Busingen, Europe/Budapest, Europe/Bucharest, Europe/Brussels, Europe/Bratislava, Europe/Berlin, Europe/Belgrade, Europe/Athens, Europe/Astrakhan, Europe/Andorra, Europe/Amsterdam,
Australia	Australia/Sydney, Australia/Perth, Australia/Melbourne, Australia/Lord_Howe, Australia/Lindeman, Australia/Hobart, Australia/Eucla, Australia/Darwin, Australia/Currie, Australia/Broken_Hill, Australia/Brisbane, Australia/Adelaide,
Atlantic	Atlantic/Stanley, Atlantic/St_Helena, Atlantic/South_Georgia, Atlantic/Reykjavik, Atlantic/Madeira, Atlantic/Faroe, Atlantic/Cape_Verde, Atlantic/Canary, Atlantic/Bermuda, Atlantic/Azores,
Asia	Asia/Yerevan, Asia/Yekaterinburg, Asia/Yangon, Asia/Yakutsk, Asia/Vladivostok, Asia/Vientiane, Asia/Ust-Nera, Asia/Urumqi, Asia/Ulaanbaatar, Asia/Tomsk, Asia/Tokyo, Asia/Thimphu, Asia/Tehran, Asia/Tbilisi, Asia/Tashkent, Asia/Taipei, Asia/Srednekolymsk, Asia/Singapore, Asia/Shanghai, Asia/Seoul, Asia/Samarkand, Asia/Sakhalin, Asia/Riyadh, Asia/Qyzylorda, Asia/Qostanay, Asia/Qatar, Asia/Pyongyang, Asia/Pontianak, Asia/Phnom_Penh, Asia/Oral, Asia/Omsk, Asia/Novosibirsk, Asia/Novokuznetsk, Asia/Nicosia, Asia/Muscat, Asia/Manila, Asia/Makassar, Asia/Magadan, Asia/Macau, Asia/Kuwait, Asia/Kuching, Asia/Kuala_Lumpur, Asia/Krasnoyarsk, Asia/Kolkata, Asia/Khandyga, Asia/Kathmandu, Asia/Karachi, Asia/Kamchatka, Asia/Kabul, Asia/Jerusalem, Asia/Jayapura, Asia/Jakarta, Asia/Irkutsk, Asia/Hovd, Asia/Hong_Kong, Asia/Ho_Chi_Minh, Asia/Hebron, Asia/Gaza, Asia/Famagusta, Asia/Dushanbe, Asia/Dubai, Asia/Dili, Asia/Dhaka, Asia/Damascus, Asia/Colombo, Asia/Choibalsan, Asia/Chita, Asia/Brunei, Asia/Bishkek, Asia/Beirut, Asia/Barnaul, Asia/Bangkok, Asia/Baku, Asia/Bahrain, Asia/Baghdad, Asia/Atyrau, Asia/Ashgabat, Asia/Aqtobe, Asia/Aqtau, Asia/Anadyr, Asia/Amman, Asia/Almaty, Asia/Aden,
Arctic	Arctic/Longyearbyen,
Antarctica	Antarctica/Vostok, Antarctica/Troll, Antarctica/Syowa, Antarctica/Rothera, Antarctica/Palmer, Antarctica/McMurdo, Antarctica/Mawson, Antarctica/Macquarie, Antarctica/DumontDUrville, Antarctica/Davis, Antarctica/Casey,
America	America/Yellowknife, America/Yakutat, America/Winnipeg, America/Whitehorse, America/Vancouver, America/Tortola, America/Toronto, America/Tijuana, America/Thunder_Bay, America/Thule, America/Tegucigalpa, America/Swift_Current, America/St_Vincent, America/St_Thomas, America/St_Lucia, America/St_Kitts, America/St_Johns, America/St_Barthelemy, America/Sitka, America/Scoresbysund, America/Sao_Paulo, America/Santo_Domingo, America/Santiago, America/Santarem, America/Rio_Branco, America/Resolute, America/Regina, America/Recife, America/Rankin_Inlet, America/Rainy_River, America/Punta_Arenas, America/Puerto_Rico, America/Porto_Velho, America/Port-au-Prince, America/Port_of_Spain, America/Phoenix, America/Paramaribo, America/Pangnirtung, America/Panama, America/Ojinaga, America/Nuuk, America/North_Dakota/New_Salem, America/North_Dakota/Center, America/North_Dakota/Beulah, America/Noronha, America/Nome, America/Nipigon, America/New_York, America/Nassau, America/Montserrat, America/Montevideo, America/Monterrey, America/Moncton, America/Miquelon, America/Mexico_City, America/Metlakatla, America/Merida, America/Menominee, America/Mazatlan, America/Matamoros, America/Martinique, America/Marigot, America/Manaus, America/Managua, America/Maceio, America/Lower_Princes, America/Los_Angeles, America/Lima, America/La_Paz, America/Kralendijk, America/Kentucky/Monticello, America/Kentucky/Louisville, America/Juneau, America/Jamaica, America/Iqaluit, America/Inuvik, America/Indiana/Winamac, America/Indiana/Vincennes, America/Indiana/Vevay, America/Indiana/Tell_City, America/Indiana/Petersburg, America/Indiana/Marengo, America/Indiana/Knox, America/Indiana/Indianapolis, America/Hermosillo, America/Havana, America/Halifax, America/Guyana, America/Guayaquil, America/Guatemala, America/Guadeloupe, America/Grenada, America/Grand_Turk, America/Goose_Bay, America/Glace_Bay, America/Fortaleza, America/Fort_Nelson, America/El_Salvador, America/Eirunepe, America/Edmonton, America/Dominica, America/Detroit, America/Denver, America/Dawson_Creek, America/Dawson, America/Danmarkshavn, America/Curacao, America/Cuiaba, America/Creston, America/Costa_Rica, America/Chihuahua, America/Chicago, America/Cayman, America/Cayenne, America/Caracas, America/Cancun, America/Campo_Grande, America/Cambridge_Bay, America/Boise, America/Bogota, America/Boa_Vista, America/Blanc-Sablon, America/Belize, America/Belem, America/Barbados, America/Bahia_Banderas, America/Bahia, America/Atikokan, America/Asuncion, America/Aruba, America/Argentina/Ushuaia, America/Argentina/Tucuman, America/Argentina/San_Luis, America/Argentina/San_Juan, America/Argentina/Salta, America/Argentina/Rio_Gallegos, America/Argentina/Mendoza, America/Argentina/La_Rioja, America/Argentina/Jujuy, America/Argentina/Cordoba, America/Argentina/Catamarca, America/Argentina/Buenos_Aires, America/Araguaina, America/Antigua, America/Anguilla, America/Anchorage,

Area	*Country/Town* pair values supported for the `setTimezone` function of the configuration script (2 of 2)
Africa	Africa/Windhoek, Africa/Tunis, Africa/Tripoli, Africa/Sao_Tome, Africa/Porto-Novo, Africa/Ouagadougou, Africa/Nouakchott, Africa/Niamey, Africa/Ndjamena, Africa/Nairobi, Africa/Monrovia, Africa/Mogadishu, Africa/Mbabane, Africa/Maseru, Africa/Maputo, Africa/Malabo, Africa/Lusaka, Africa/Lubumbashi, Africa/Luanda, Africa/Lome, Africa/Libreville, Africa/Lagos, Africa/Kinshasa, Africa/Kigali, Africa/Khartoum, Africa/Kampala, Africa/Juba, Africa/Johannesburg, Africa/Harare, Africa/Gaborone, Africa/Freetown, Africa/El_Aaiun, Africa/Douala, Africa/Djibouti, Africa/Dar_es_Salaam, Africa/Dakar, Africa/Conakry, Africa/Ceuta, Africa/Casablanca, Africa/Cairo, Africa/Bujumbura, Africa/Brazzaville, Africa/Blantyre, Africa/Bissau, Africa/Banjul, Africa/Bangui, Africa/Bamako, Africa/Asmara, Africa/Algiers, Africa/Addis_Ababa, Africa/Accra, Africa/Abidjan,

7.6 Appendix: Device network disk mounting in MS-Windows explorer

> ⚠ Do follow carefully the procedure below to mount properly the TAB10s device as network disk in MS-Windows explorer. Indeed, after a first mounting failure with wrong login credentials, it could be difficult to mount the device afterwards because MS-Windows keeps the wrong login credentials in cache memory for few tenths of minutes preventing to mount the device for a while.

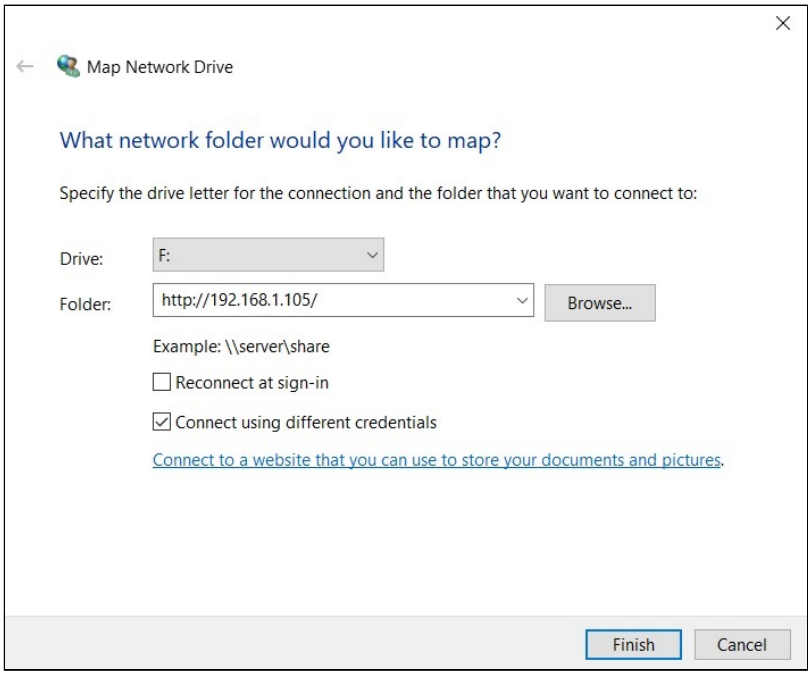
Prerequisite:

- the TAB10s is properly connected to your network with a correct network configuration (`WLAN` or `LAN` interface).

Open the MS-Windows explorer, right click on the `This computer` directory then select `Map network drive...`.
In the dialog:

- choose an available drive letter,
- enter the URL `http://<device-IP-addr>/`,
- unselect the option `Reconnect at sign in`,
- select the option `Connect using different credentials`,
- press on the `Finish` button

For example, if the IP address of the TAB10s device is *192.168.1.105*:

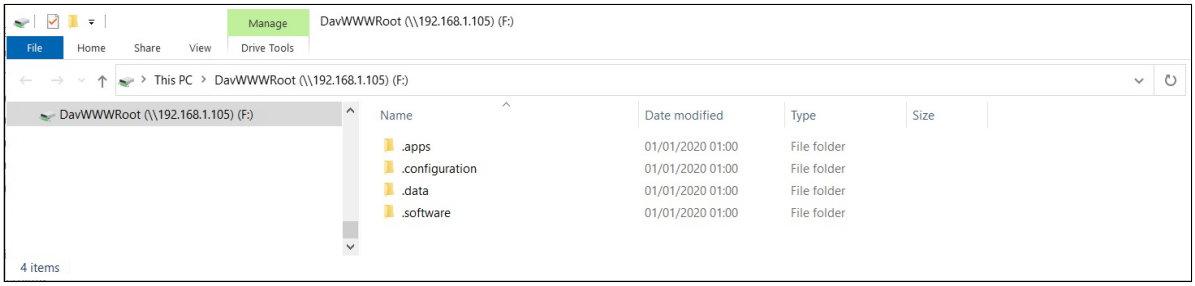


Enter the login credentials to connect to the TAB10s WebDAV server.

> ⚠ It is advised to double check the login credentials.

In case disk mapping success, the network drive should be mounted automatically on `\\<device-IP-addr>\DavWWWRoot`.

For example:



7.7 Appendix: USB mass storage

Some rare USB sticks could be not detected by the device because the USB partitionning is not supported by `AQS`. In this case, a *Unsupported General USB drive* notification is raised.

> ☛ *The notifications can be watched in `native` mode, but not in `kiosk` mode.*

7.8 Appendix: File transfer from a computer

Like any Android device, it is possible to access to the file system of the TAB10s device from a computer. That procedure can be used for example to push a configuration script or a firmware from a computer when no network is available on the TAB10s device.

The directories corresponding to the WebDAV directories are:

- /.configuration
- /.apps
- /.data
- /.software

Ensure that you computer is able to supply sufficient power through the USB-C connector to start the TAB10s device. Else use a `NAPOE109kt` or `NAPOE109ft` device to start the TAB10s device.

1. connect an USB-C cable between your computer and the TAB10s device,
2. if required, quit the Kiosk mode by pressing on the system button to access to the Android settings,
3. in the upper notification banner, press in the white area on the `Android system, charging the device via USB` button,
4. a `Tape for more options` button appears. Click on it to open an `USB preferences` pane,
5. in the `use USB for` section, select the `File transfer` radio button instead of the `No data transfer` radio button.

Check that the TAB10s device file system is mounted properly. This directories should be available:

- `<This PC>\TAB10\Internal shared storage\Android\data\tech.qeedji.system\files\.configuration`,
- `<This PC>\TAB10\Internal shared storage\Android\data\tech.qeedji.system\files\.apps`,
- `<This PC>\TAB10\Internal shared storage\Android\data\tech.qeedji.system\files\.data`,
- `<This PC>\TAB10\Internal shared storage\Android\data\tech.qeedji.system\files\.software`.

To update the network configuration of your TAB10s device, push a suitable configuration script in this directory:

- `<This PC>\TAB10\Internal shared storage\Android\data\tech.qeedji.system\files\.configuration`.

To upgrade the `AQS` Operating system, push a suitable firmware in this directory:

- `<This PC>\TAB10\Internal shared storage\Android\data\tech.qeedji.system\files\.software`.

7.9 Appendix: Factory reset

The factory reset consists in recovering the data like it was at the factory.

From the `AQS` desktop[1],

- swipe your finger to make appear the `AQS Desktop` ,
- click on the `Settings` application,
- scroll and click on the `System (Languages, time, backup)` menu,
- on the `Advanced` drop down list, select the `Reset options` menu,
- click on the `Erase all data (factory reset)` button,
- click on the `RESET TABLET` button.

[1] *The access to the `AQS` desktop requires that the TAB10s device is in `native` mode which needs to be activated thanks to a configuration script having the `setDeviceModeNative()` function uncommented. For further information, refer to the chapter § Device configuration by script.*

7.10 Appendix: Remove an App with Android settings

In case you have published on the `AQS` device, several Apps programmed in autostart mode, they are all starting after the device boot-up has ended.

To remove one of the Apps (from example, the `<APKname1>` App),

- if required, exit from the `Kiosk` mode by making a short press on the `system` button of the device,
- in the Android `settings` pane, press on the `Apps and notifications` menu,
- click on the button `See all <n> apps` ,
- among the Apps installed, remove the App by making a long press on it then press on the `UNINSTALL` button.

> ☛ *For each Apps, you may have to do twice this action, once for the `<APKname1>` APK, another one for the `<APKname1 UI>` APK.*

Exit the Android `settings` to return to use your App.

> ☛ *In case you have deleted all your Apps, push again the App on your device.*

7.11 Appendix: 802.1X security configuration with Android settings

Using 802.1X security requires to have:

- specific LAN switch or WiFi modem supporting `802.1X` security,
- a RADIUS server properly configured.

Several 802.1X modes are supported. Depending on the chosen `802.1X` security mode, you may have to install on the tablet:

- the CA certificate of your RADIUS server,
- one trusted client certificate per TAB10s device generated with the CA certificate of your RADIUS server.

> ⚠ When using a RADIUS certificate, it is recommended that the system date of the TAB10s device is properly set, else you may not be able to access to the secured network.

802.1X security on WLAN interface

Activate the WiFi connection (not activated by default) and connect to the WLAN access point supporting `802.1X security`.

When filling settings for WiFi connection, fill the `802.1X security` as well:

- `EAP method`,
  - *PEAP*,
  - *TLS*,
  - *TTLS*,
  - *PWD*.
- `Phase 2 authentication`
  - *PAP*[1],
  - *MSCHAP*[1],
  - *MSCHAPV2*[1],
  - *GTC*[1],
  - *None*[1]: the `AOSP` uses automatical the right Phase 2 authentication value given by the RADIUS server
- `CA certificate`: select the RADIUS CA certificate
- `Identity`: client identity registered in the RADIUS server for this TAB10s device for the WLAN interface
- `Anonymous identity`: identity used for the first identification phase. If the `Anonymous Identity` value is let empty, the `Anonymous Identity` value worths the `Identity` value set above.
- `Password`: client password registered in the RADIUS server for this TAB10s device for the WLAN interface
- `Advanced options`:
  - `Metered`,
  - `Proxy`,
  - `IP settings`:
    - *DHCP*,
    - *Static*:
      - `IP address`
      - `Gateway`
      - `Network prefix`
      - `DNS 1`
      - `DNS 2`

> ☛ *The virtual keyboard appears each time entering in the WiFi configuration window. To hide the virtual keyboard, press on the back menu of `AOSP`.*

[1] *The values available here are depending on the chosen EAP method.*

> ⚠ The 802.1X security configuration has to be done either entirely by the `AOSP Settings` application, or entirely by a configuration script. For further information, refer to configuration script template V1.10.16 (or above).

802.1X security on LAN interface

The `LAN` configuration can only be done with a configuration script. For further information, refer to configuration script template V1.10.16 (or above).

7.12 Appendix: Certificates installation with Android settings

The `AOSP` `Settings` App allows to view the certificates. Go in the `Security & location` menu, then scroll to `Encryption and Credentials` item and click on it. Several items are displayed:

- *Trusted credentials*,
- *User credentials*,
- *Install from SD card*.

> ⚠ An unsigned certificate, appearing only in the `User credentials` screen, cannot be used by APK to access to some files hosted on some Web server URL, available only with the HTTPS scheme and requiring certificates.
>
> ☛ *When installed with the `AOSP` `settings` App, the unsigned certificates cannot appear in the `Trusted certificate` screen. When they are installed with the configuration script 1.10.15 (or above), the unsigned certificates are made trusted by `AQS` (9.10.10 beta9 or above). Then they appear automatically in the `Trusted certificate` screen.*

Trusted credentials

After having been installed by the user, the CA certificates are viewable both:

- in the `User credentials` screen, with a private certificate *label* entered by the user,
- in the `USER` tab of the `Trusted certificate` screen.

> ☛ *The `SYSTEM` tab of the `Trusted certificate` screen is listing the trusted certificates already installed on the tablet when coming straight from factory.*

User credentials

The unsigned certificates installed by the user are only viewable in the `User credentials` screen.

Install from SD card

To install a certificate from your USB mass storage:

- copy the certificate file on your USB mass storage,
- insert the USB mass storage in the USB hub connected to the TAB10s device,
- select the `Install from SD card` item,
- press on the *bars* ☰ button at the top left of the screen and select the mounted USB disk:
  - enter a label *name* for the certificate,
  - select a credential and select a group value among the choices below:
    - *VPN and apps*: group usually hosting user CA certificate to access for example to some file hosted on remote server available in https,
    - *Wi-Fi*: group usually hosting user CA certificate for 802.1X for LAN and WLAN interface.

> ☛ *It is recommended to install the unsigned certificates with the configuration script.*