

Qeedji

User manual

TAB10b

9.11.10 001A



Legal notice

TAB10b 9.11.10 (001A_en)

© 2024 Qeedji

Rights and Responsibilities

All rights reserved. No part of this manual may be reproduced in any form or by any means whatsoever, or by any means whatsoever without the written permission of the publisher. The products and services mentioned herein may be trademarks and/or service marks of the publisher, or trademarks of their respective owners. The publisher and the author do not claim any rights to these Marks.

Although every precaution has been taken in the preparation of this document, the publisher and the author assume no liability for errors or omissions, or for damages resulting from the use of the information contained in this document or the use of programs and source code that can go with it. Under no circumstances can the publisher and the author be held responsible for any loss of profits or any other commercial prejudice caused or alleged to have been caused directly or indirectly by this document.

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

| | |
|--|-------|
| Introduction | 1.1 |
| Labelling | 1.2 |
| Product faces | 1.3 |
| Device dimensions | 1.3.1 |
| Device fixture | 1.3.2 |
| Drilling pattern | 1.3.3 |
| Power supply | 1.4 |
| Device start-up steps | 1.5 |
| Surround light behaviour at power-up | 1.6 |
| Connectors pin-out | 1.7 |
| Procedure to access to the back connectors | 1.8 |
| Test card | 1.9 |

Part II : System configuration

| | |
|--|-------|
| Introduction | 2.1 |
| AQS operating system upgrade with a fqs firmware | 2.1.1 |
| APK deployment | 2.1.2 |
| Device configuration by script | 2.1.3 |
| Hardware reset | 2.1.4 |
| Factory recovery | 2.2 |

Part III : Applicative console Web user interface

| | |
|--|-----|
| Applicative console web user interface | 3.1 |
|--|-----|

Part IV : Administration console Web user interface

| | |
|---|--------|
| Device configuration console web user interface | 4.1 |
| Configuration > Administrator | 4.1.1 |
| Configuration > LAN_1 | 4.1.2 |
| Configuration > WLAN_1 | 4.1.3 |
| Configuration > Output | 4.1.4 |
| Configuration > Apps | 4.1.5 |
| Configuration > Servers | 4.1.6 |
| Configuration > Certificates | 4.1.7 |
| Configuration > Date and time | 4.1.8 |
| Configuration > Regionality | 4.1.9 |
| Configuration > Tasks | 4.1.10 |
| Configuration > Variables | 4.1.11 |
| Maintenance > Test card | 4.1.12 |
| Maintenance > Files | 4.1.13 |
| Maintenance > Firmware | 4.1.14 |
| Maintenance > Preferences | 4.1.15 |
| Information > Device | 4.1.16 |
| Information > USB adapters | 4.1.17 |
| Information > Network | 4.1.18 |
| Information > Screens | 4.1.19 |

Part V : Built-in Apps

| | |
|---|-----|
| Media Folder Injector | 5.1 |
| Power BI Online Viewer | 5.2 |
| URL Launcher | 5.3 |
| Qeedji PowerPoint Publisher for Media Players | 5.4 |

Part VI : Technical information

| | |
|--------------------------|-----|
| Technical specifications | 6.1 |
| Built-in RFID reader | 6.2 |
| Antenna return loss | 6.3 |
| Conformities | 6.4 |

Part VII : Contacts

Contacts

7.1

Part VIII : Appendix

| | |
|--|------|
| Appendix: Qeedji PowerPoint Publisher for Media Players | 8.1 |
| Appendix: Qualified third party references | 8.2 |
| Appendix: ISO image burning with BalenaEtcher | 8.3 |
| Appendix: TFTP and DHCP server configuration | 8.4 |
| Appendix: Timezone | 8.5 |
| Appendix: Device network disk mounting in MS-Windows explorer | 8.6 |
| Appendix: USB mass storage | 8.7 |
| Appendix: File transfer from a computer | 8.8 |
| Appendix: Factory reset | 8.9 |
| Appendix: Remove an App with Android Settings App | 8.10 |
| Appendix: 802.1X security configuration with Android Settings App | 8.11 |
| Appendix: Certificates installation with Android Settings App | 8.12 |
| Appendix: Power manager and Screen Saver modes | 8.13 |
| Appendix: Identifier and password self-filling and self-confirmation in a web page form | 8.14 |
| Appendix: URI for Media Folder Injector | 8.15 |
| Appendix: Microsoft Azure AD portal for Microsoft Power BI application | 8.16 |
| Appendix: Azure AD Application Powershell module for Power BI Online Viewer application | 8.17 |
| Appendix: Power BI Online Viewer with Microsoft OAuth application mode: additional permissions | 8.18 |
| Appendix: Test your report with the Power BI Playground platform | 8.19 |
| Appendix: Power BI Online Viewer known limitations | 8.20 |
| Appendix: Devices configuration using Powershell | 8.21 |

Part I

Description and installation

1.1 Introduction

This manual explains how to install and configure your TAB10b 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 | TAB10b device | 1 |
| Micro SD card | Installed in the TAB10b device, embedding AQS | 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 Ø: 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, Qeedjia is making recommendation for suitable power supply references in the chapter § [Power supply](#).

 Before supply the TAB10b 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 TAB10b 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

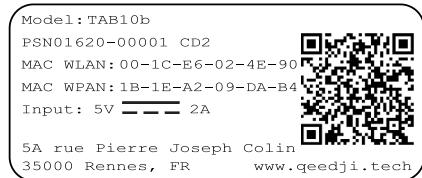
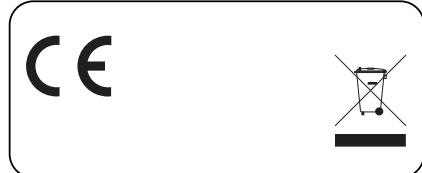
Product label

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.

☞ This is an example of registration QR code URL:

i.qeedji.tech?model=TAB10b&sn=01620-00001&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:
`PSN01620-00011 CD3`.

☞ The serial number of the device may be requested in case of technical support.

1.3 Product faces

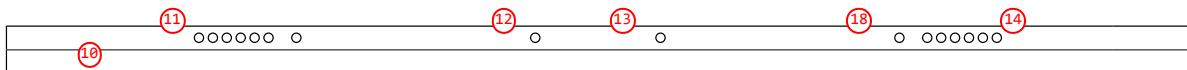
Device's front face



- ① Touch screen,
- ② Built-in NFC/RFID sensor.

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

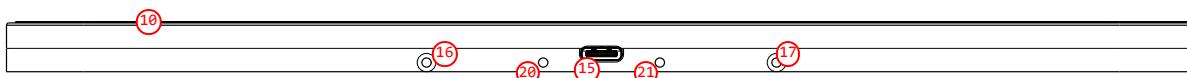


- ⑩ Surround light,
- ⑪ Mono speaker,
- ⑫ System button²,
- ⑬ Built-in microphone #1,
- ⑯ Built-in microphone #2,
- ⑭ Heat pipe.

² The system button is hidden inside the hole.

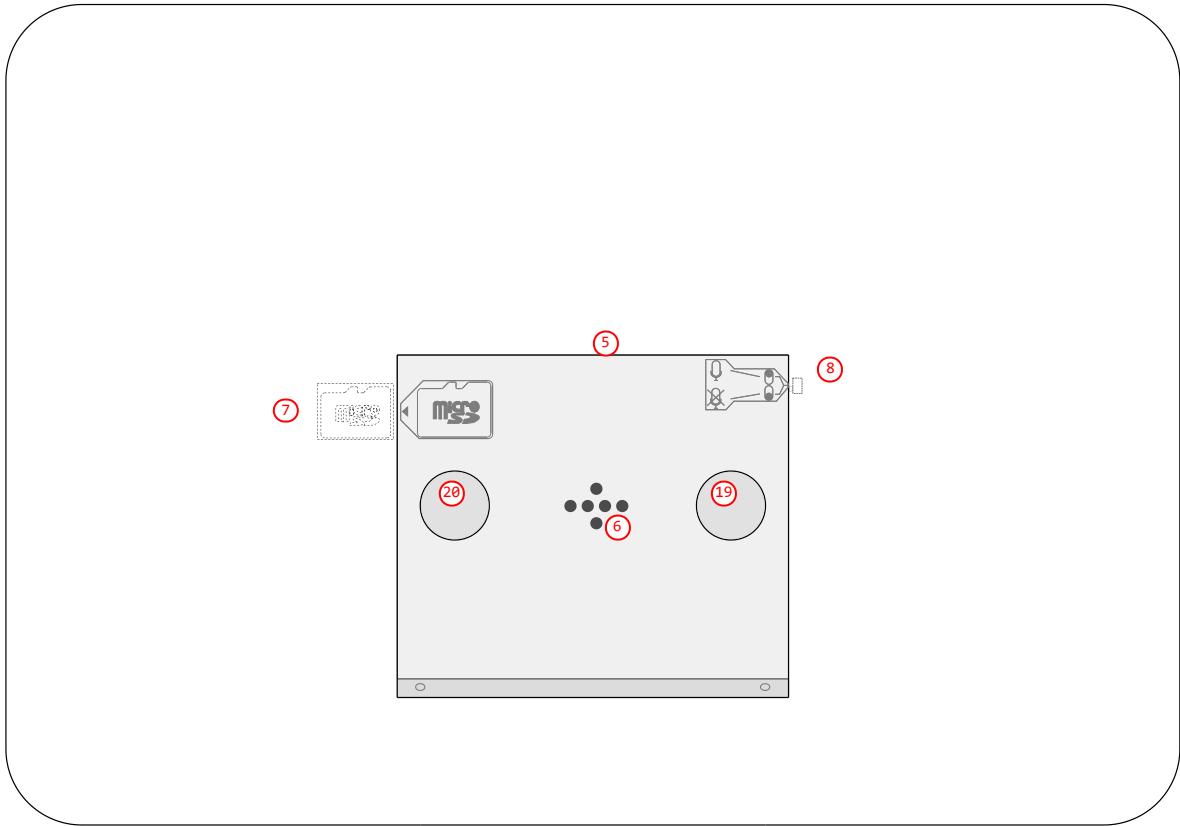
 Do not cover the top of the heat pipe which is designed to evacuate naturally the heat of the device when it is running.

Device's bottom face



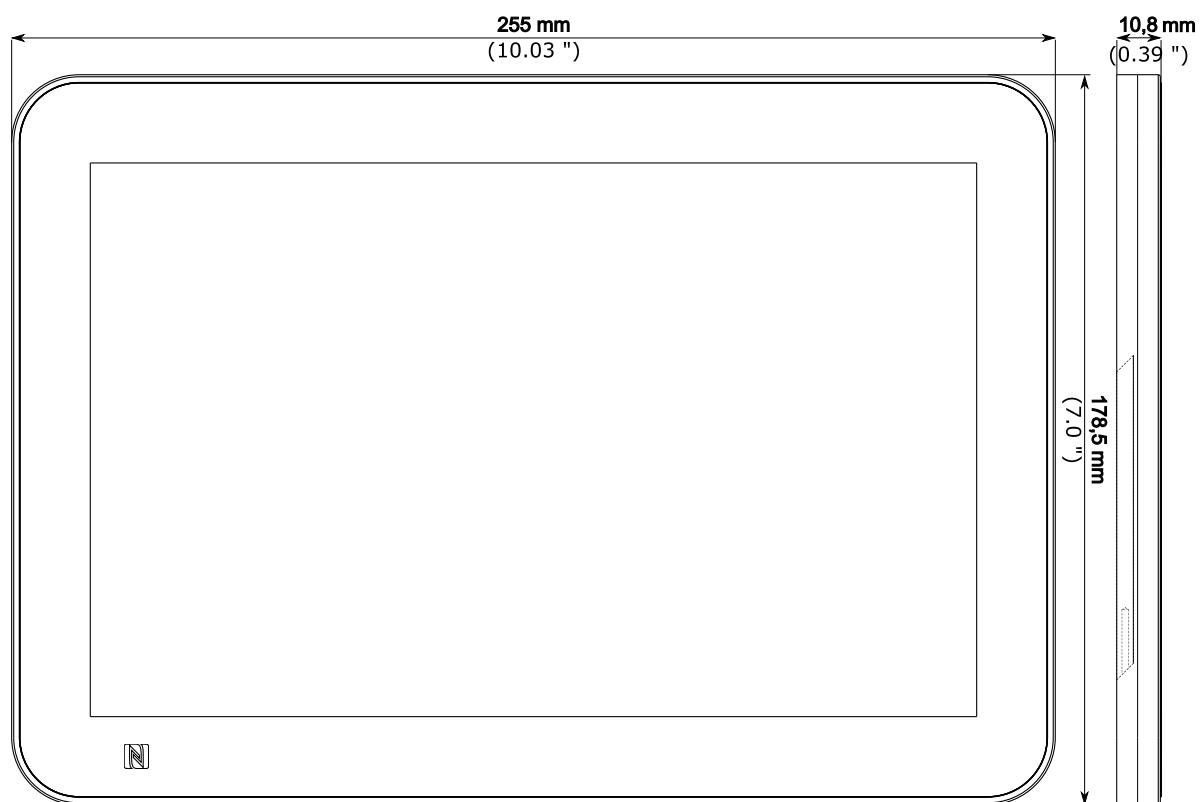
- ⑩ Surround light,
- ⑯ USB-C connector,
- ⑯ Mounting bracket orifice/screw #1,
- ⑰ Mounting bracket orifice/screw #2,
- ㉑ USB-C locking orifice #1,
- ㉒ USB-C locking orifice #2.

Device's rear face



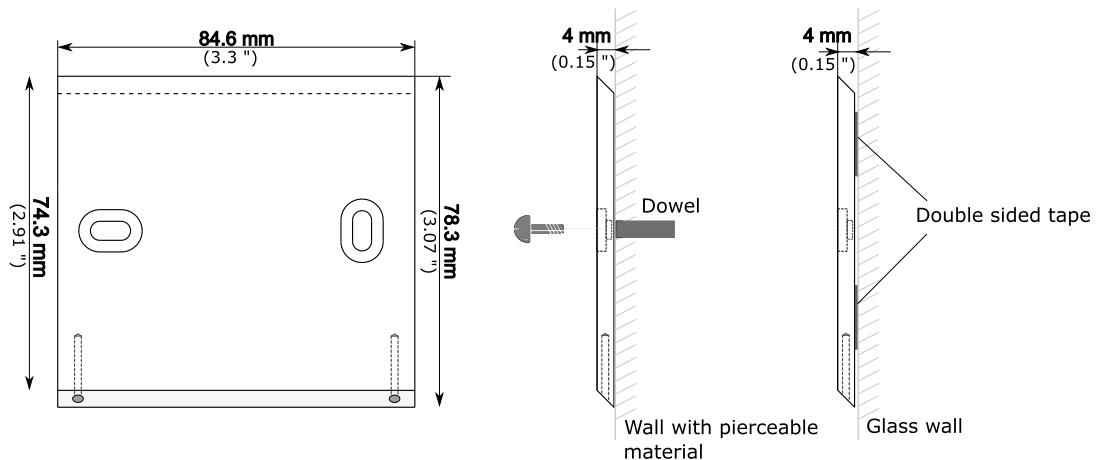
- (5) Bevelled profile to welcome the mounting bracket,
- (6) POGO type connector,
- (7) Micro SD card connector with its micro SD card,
- (8) Microphone DIP switch,
- (19)(20) Holes to host screws heads to fix the mounting bracket.

1.3.1 Device dimensions



1.3.2 Device fixture

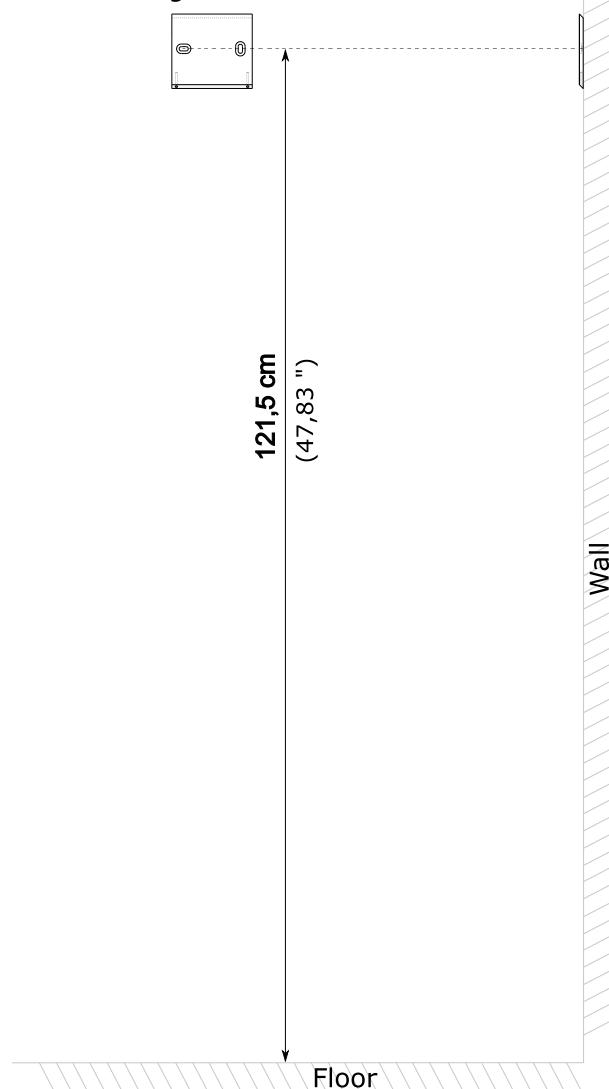
The TAB10b device can be hung on the wall using a mounting bracket (supporting or not the POGO type interface).



⚠ 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 (51,18") maximum far from the floor. For the TAB10b device, add 2.4 cm (or 0,787") to this height to determine the maximum height of the top edge of the TAB10b 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").

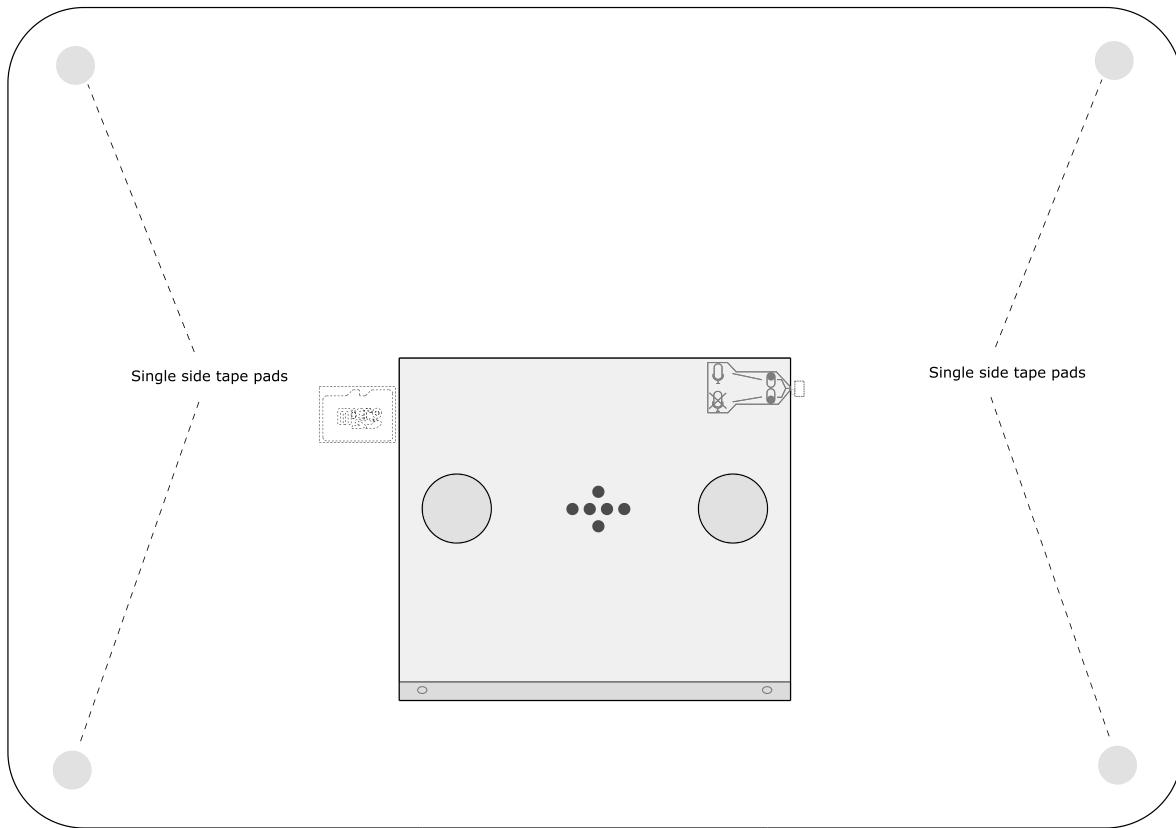
Mounting bracket

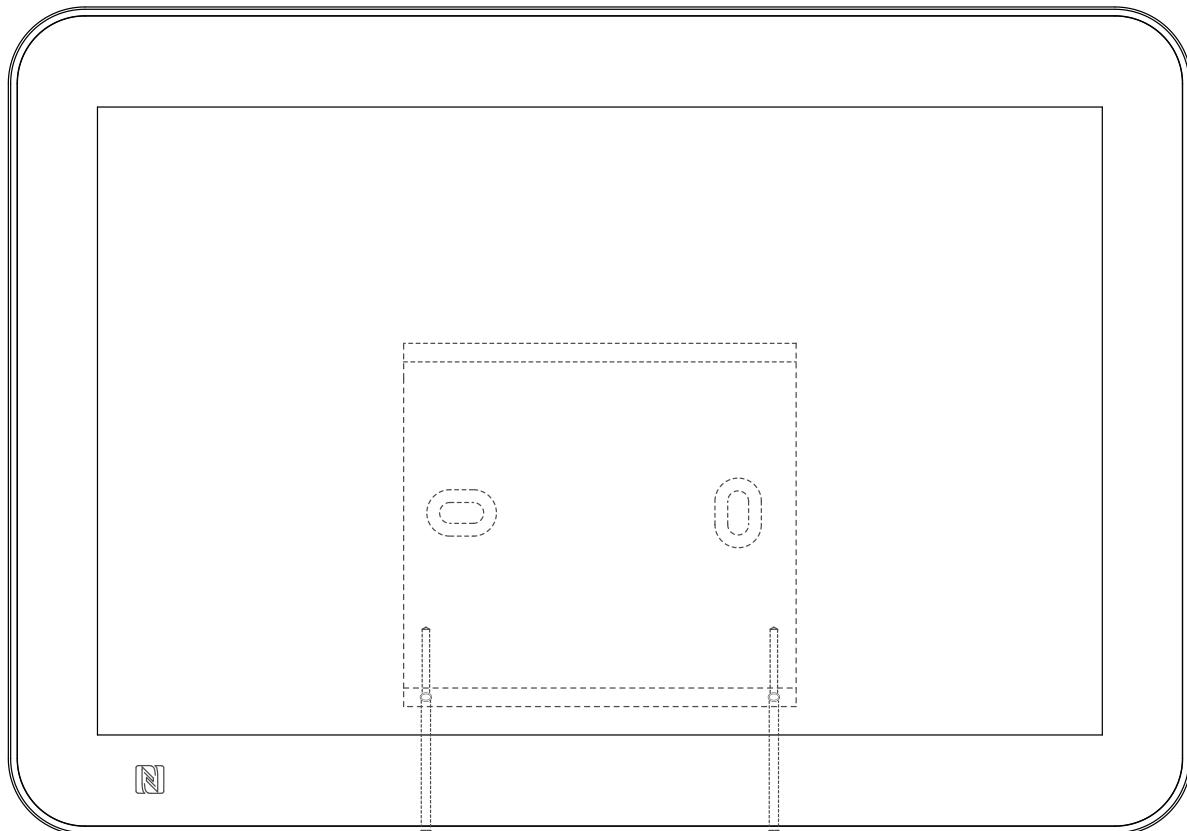


⚠ The TAB10b device is designed to be installed in landscape mode only.

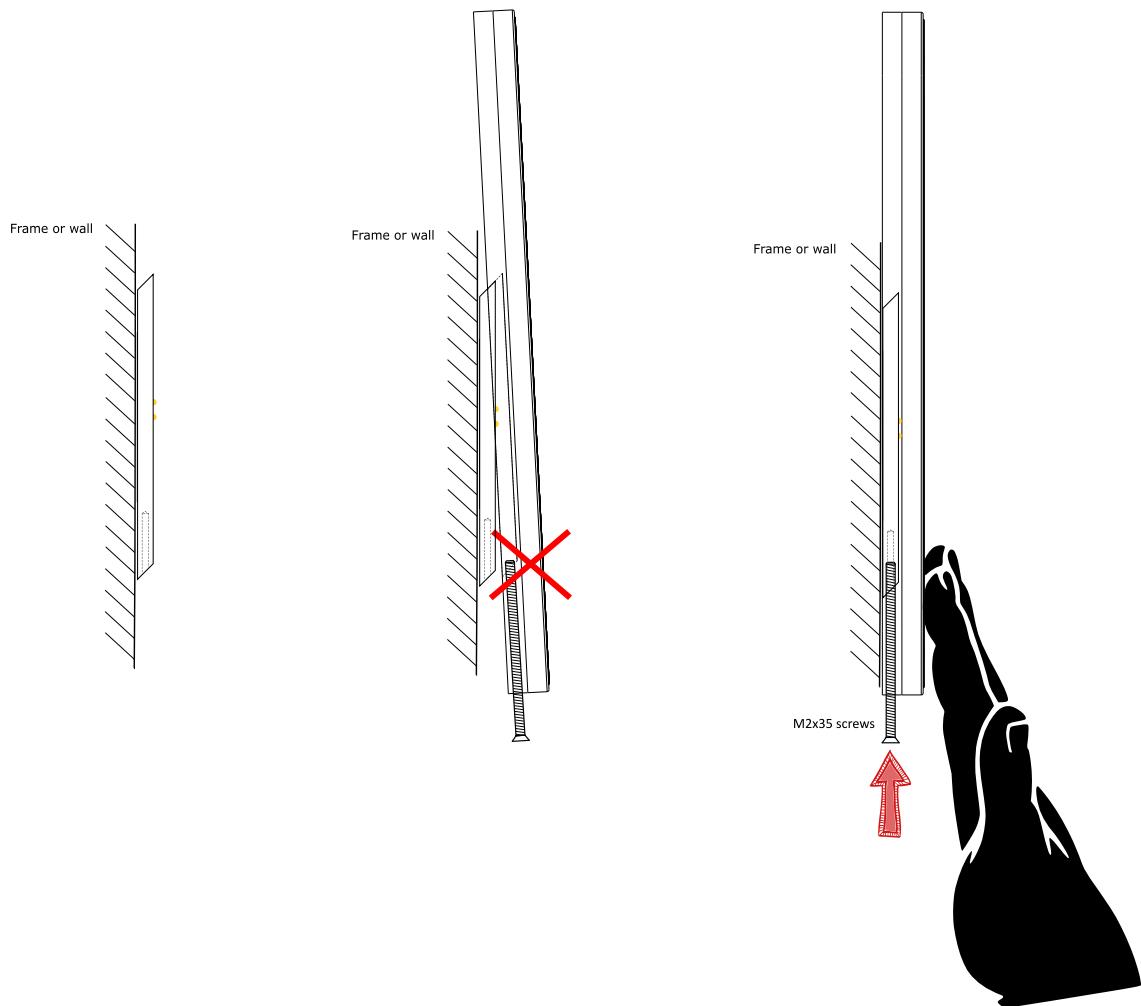
Before installing the TAB10b device:

- check that the position of the microphone DIP switch is matching the customer needs,
- stick, like explained below, the four single side tape pads at the back of the TAB10b device, respectively at the four corners.





⚠ 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 TAB10b device is installed on the NAPOE109kt or NAPOE109ft products strictly 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. |

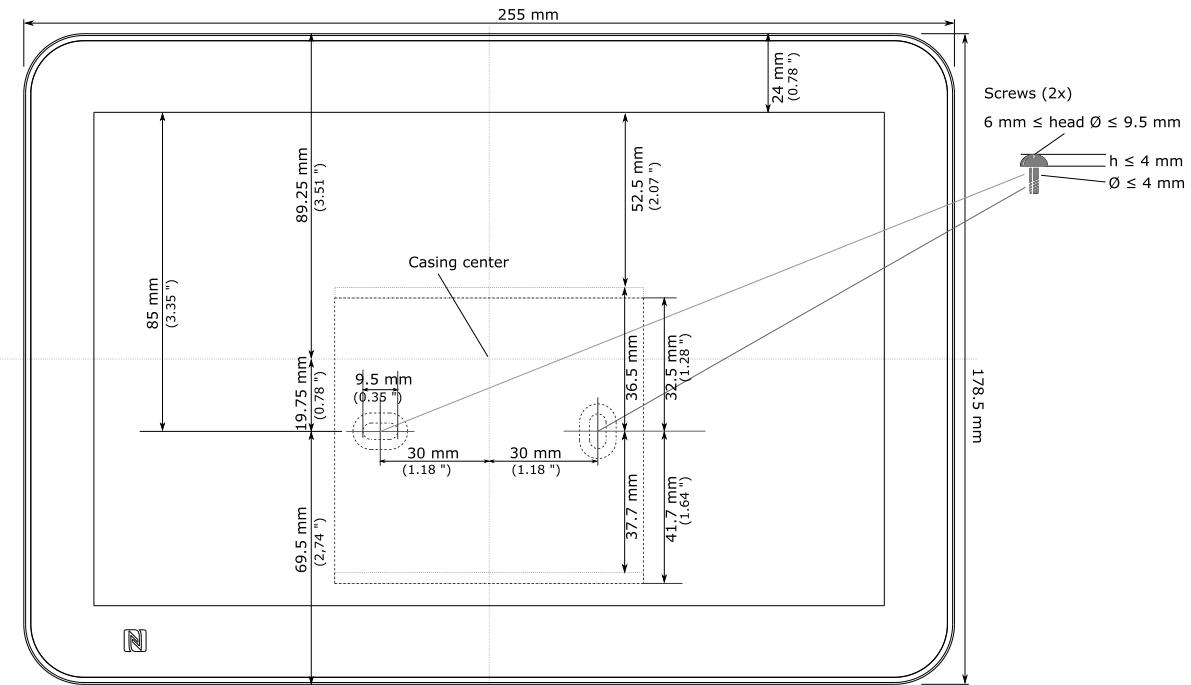
| LAN_1 network connectivity | Information |
|-----------------------------------|--|
| | When this LAN pictogram is displayed, the LAN_1 connection is up. When this LAN pictogram is not displayed, the LAN_1 connection is down. |

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

When the TAB10b 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 TAB10b device on the wall, you can do it using the provided mounting bracket. Follow the drilling pattern to install it.

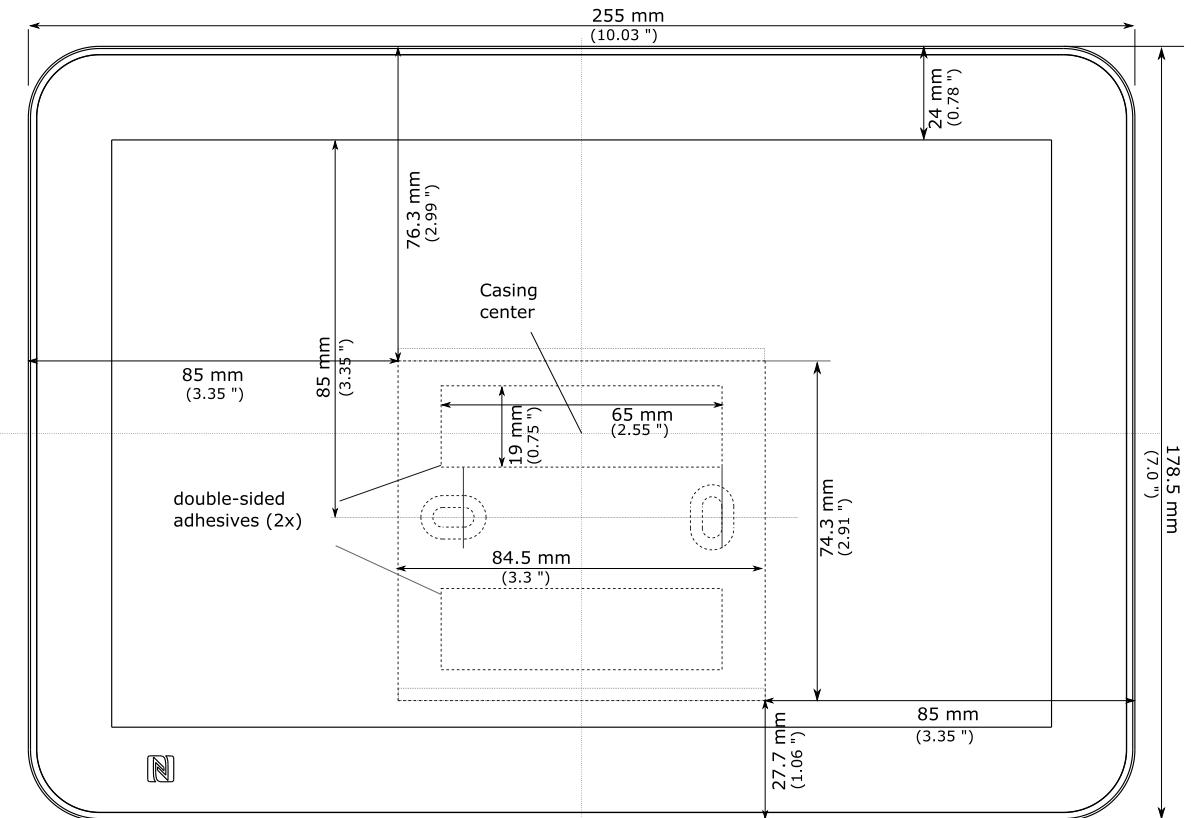


This mounting bracket can be fixed using screws (recommended for walls with pierceable material).

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 TAB10b 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 |

¹ For supply need only, you can purchase a single 110 V~/230 V~ to USB-C 5 V / 3 A wall plug.

² 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 though the second side becomes available afterwards. The choice of power supply origin is renegotiated 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.

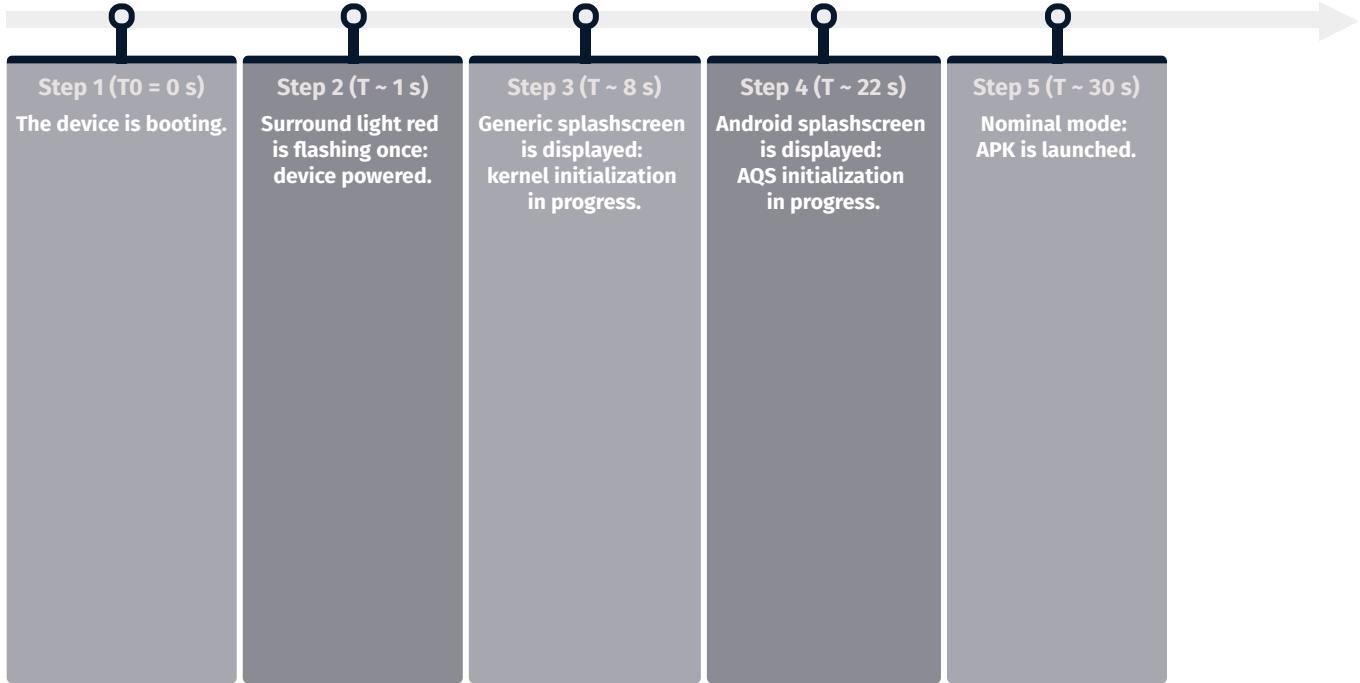
¹ For further information, refer to the [NAPOE109kt user manual](#).

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 . |
| Sequence of 6 consecutive short green flashes of 300 ms, periodic in alternance with 4 seconds Off. | Error : an internal issue has been detected during bootloader execution. Try to unplug and plug the power supply. 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.

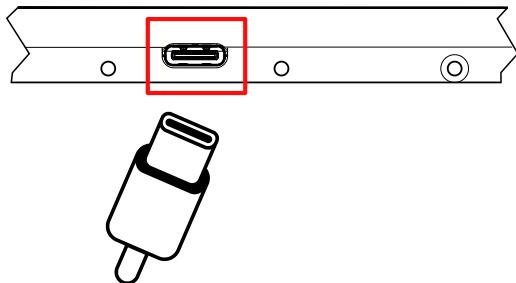
² Remove the mounting bracket from the device, or remove the device from the mounting bracket, and check that your micro SD card is properly inserted in the device.

1.7 Connectors pin-out

⚠ The access to some connectors or DIP switches may require to remove the mounting bracket or remove the TAB10b device from the wall. Refer to the chapter § [Procedure to access to the back connectors](#).

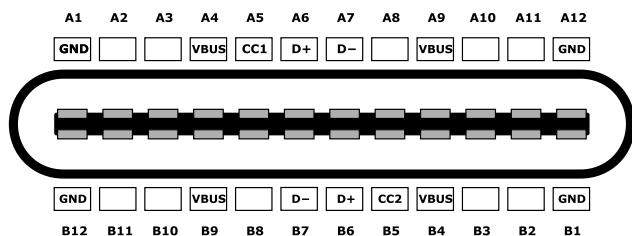
USB-C connector

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) |

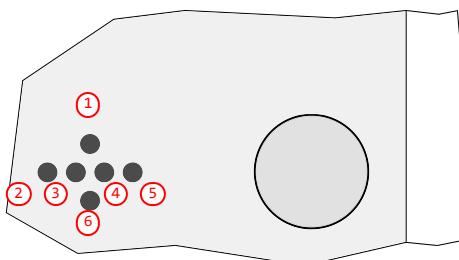
This is the USB-C pin-out for the TAB10b device:



⚠ The USB-C connector is supporting Ethernet over USB. ¹ The TAB10b 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 TAB10b device. Qeedji advises to use EXC.NAPOE109KU accessory, as it is fully qualified with the TAB10b device. The TAB10b 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.

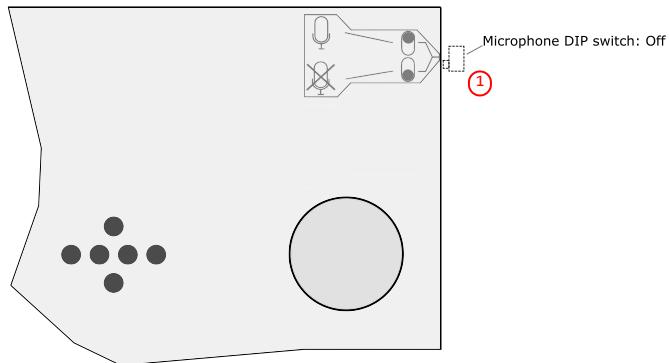
⚠ The POGO type connector allows to supply the device and offers an USB 2.0 host interface, for Ethernet over USB for example.

Dipswitch for microphone

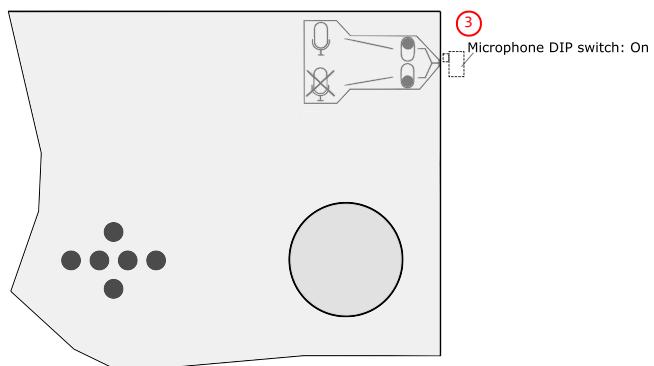
For confidentiality purpose, the TAB10b device has a switch at the back of the product allowing to activate or deactivate the microphone peripheral.

When the DIP switch is facing the crossed microphone, the microphone peripheral is deactivated.

Example of configuration when the microphone (1) peripheral are deactivated:

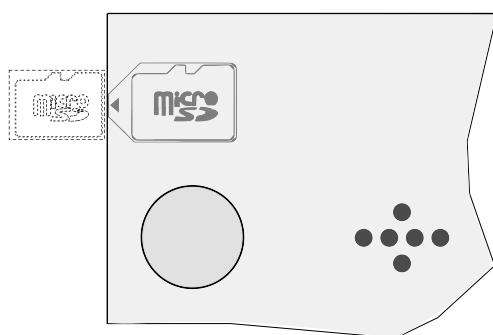


Example of configuration when the microphone (3) peripheral are activated:



Micro SD card

The micro SD card embedding AQS is already installed in the TAB10b device at factory. The micro SD card connector is located on the rear face of the TAB10b device. A micro SD serigraphy is showing the connector location.



The 16 GB micro SD card, containing the AQS for TAB10b 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 | vbmota_a | 1 MB | | verify boot's metadata |
| 14 | vbmota_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 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.

1.9 Test card

When the `Test card` App launching at device start-up is activated, the device displays alternatively one test pattern content per network interface supported by the device every ten seconds and this for one minute. The test pattern displays important information to assist in the device configuration.

▪ When the `Test card` App is executed at device start-up for one minute, the other App cannot be executed and the user cannot access to AQS desktop by pressing on the `system` button.

On a TAB10b device, the test pattern content is displayed thanks to a `Test Card` App that is launched at device start-up when the `Test card` is activated in the device configuration console web user interface.

⚠ When the `Test Card` App must be executed, no other App can be executed. To execute successfully another App, your must deactivated the `Test Card` App in the device configuration console web user interface.



If you are using a NAPOE109ku adapter, a NAPOE109kt adapter, a NAPOE109ft adapter or a PoE to USB-C adapter, the `Test card` displays in alternance:

- the test pattern content for the `LAN1` network interface for ten seconds,
- the test pattern content for the `WLAN1` network interface for ten seconds.

If not, the `Test card` displays only the test pattern content for the `WLAN1` network interface.

▪ When using a NAPOE109kt adapter, a NAPOE109ft adapter, a NAPOE109ft adapter or a PoE to USB-C adapter, the `up STATE` (2) on the `LAN1` network interface means that the adapter is able to provide the network connectivity. The `down STATE` means that the adapter is not able to provide the network connectivity due to either a wrong installation of the TAB10b device on the wall-mount or due to a wire crimping trouble on the krone connector.

▪ For TAB10b devices, the `MAC id` value is the MAC address value of the WLAN interface. It is identified in the test pattern content by the `MAC` key pictogram (1).

▪ The `up STATE` (2) on the `WLAN1` network interface means that the device is connected to a WIFI router. The `down STATE` means that the device is not connected to a WIFI router.

▪ Only one network interface can be activated at a time. The `I/F on` (3) status means that the current interface displayed is kept activated by the OS; the `I/F off` (3) status means that the current network interface (or I/F) displayed has been deactivated by the OS.

▪ The white circles (4) are filled with a white dot from the left to the right, each time a test pattern content for a new network interface is displayed. When there is one `LAN1` interface and one `WLAN1` interface supported by the device, two white circles are displayed: the left one for the `LAN1` interface, the right one for the `WLAN1` interface.

▪ In native mode, when navigating in the Android Settings App, if the `Test card` App was running, the `Test card` App is stopped. To relaunch it, you can either restart the device or launch the `Test card` App available in the Android Apps view.

▪ If you have a USB keyboard plug on a USB hub connected to the TAB10b device, you can activate/deactivate the Test Card with the key sequence

- [left, right, left, right] in less than ten seconds.

The test card can be displayed/undisplayed by applying the key sequence after having plugged an USB keyboard on the USB connector of the TAB10b device. In this case, only this user preference needs to be set to true:

- `persist.sys.testcard.key-event.all.authorized` .

☞ When a key sequence is done to stop the Test Card App, this one may take five seconds to disappear.

Part II

System configuration

2.1 Introduction

To support the APK deployment, the AQS operating system version upgrade and the TAB10b device configuration update, the TAB10b device embeds the AQS 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 console 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 console 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 console 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 TAB10b device embeds an AQS operating system (V9.10.19 or above). It can be upgraded by some maintenance .fqs firmware having some evolutive or corrective changes.

To update your TAB10b device with a new AQS operating system version, download the `aosp_qeedji-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 TAB10b 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 console web user interface. For further information, refer to the chapter § [AQS operating system upgrade with the device configuration console web user interface](#),
- putting the .fqs firmware on an USB storage device then by inserting it in the TAB10b 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 console web user interface

It is possible to upgrade the AQS operating system version of the TAB10b device by connecting to the device configuration console 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 console web user interface, refer to the chapter § [Applicative console web user interface](#).

AQS operating system upgrade by USB

Prerequisite:

- the TAB10b device needs to have a suitable power supply equipment allowing to support AQS operating system upgrade by the USB-C connector.

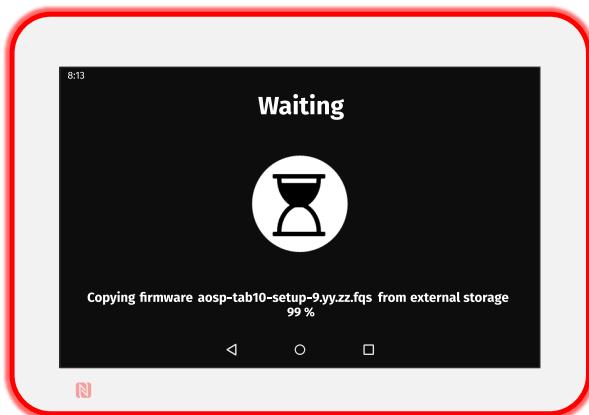
Copy the `aosp_qeedji-tab10-setup-9.YY.ZZ.fqs` archive at the root directory of an USB storage device and insert it on the USB-C connector of the TAB10b device (or on the third party equipment connected to the USB-C connector).

■ In case several supported files type are present like .fqs, .apk and .js, only the AQS operating system will be done.

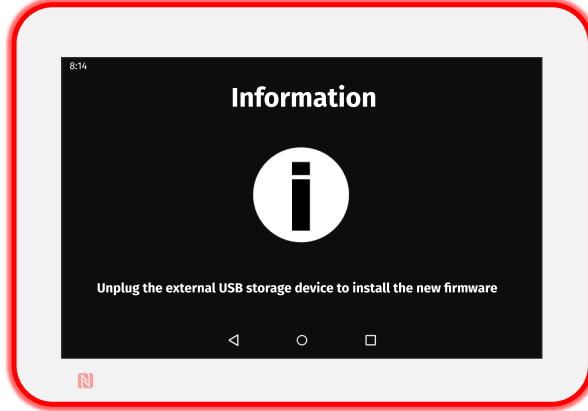
⚠ If the USB storage device contains several supported .fqs firmware files, the AQS operating system upgrade can not be done and no message appears.

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.



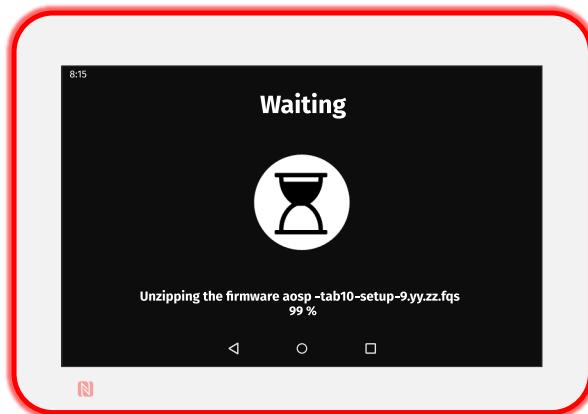
This message is then displayed until the USB storage device is unplugged.



Unplug the USB storage device.

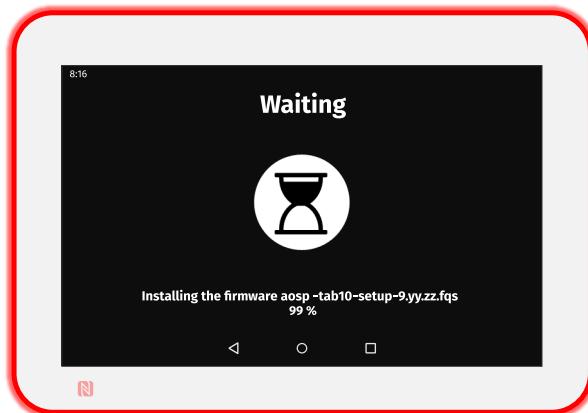
Once the USB storage is unplugged, the AQS operating system upgrade duration is depending on the .fqs firmware content. It can be for example: 8 minutes and 30 seconds.

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

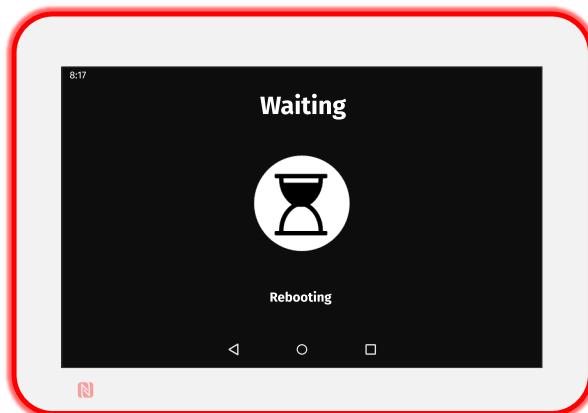


This message is then displayed showing that the `.fqs` firmware is being installed.

 *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

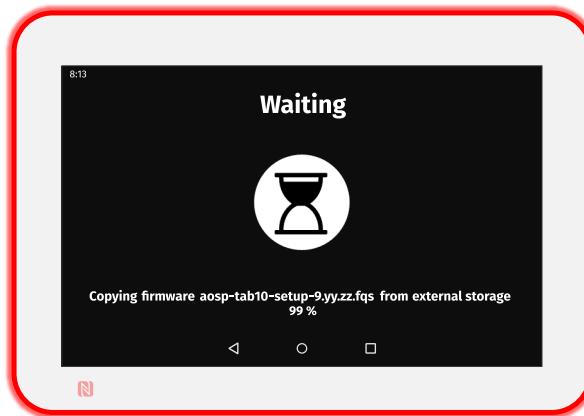
Prerequisite:

- a WebDAV client (*CarotDAV* or *BitKinex* for example) is installed on your computer or
- the TAB10b 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 TAB10b device is not supported.

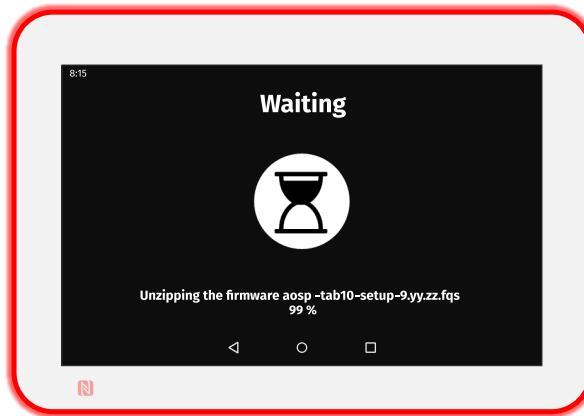
Copy the `aosp_qeedji-tab10-setup-9.yy.zz.fqs` archive in the `.software/` directory located at the root of the TAB10b WebDAV server.

This message should be displayed.

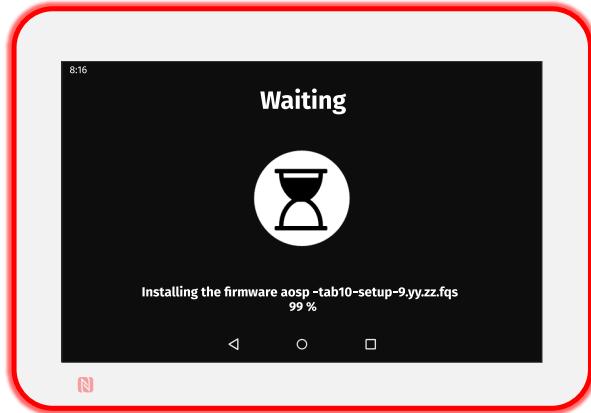
- The copy duration is depending on the `.fqs` firmware size.



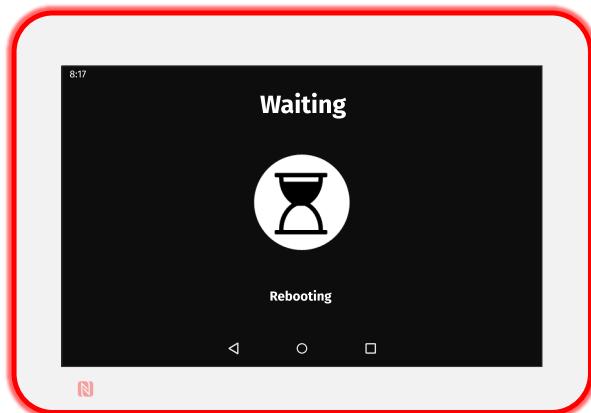
This message is displayed showing that the firmware is being unzipped.



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



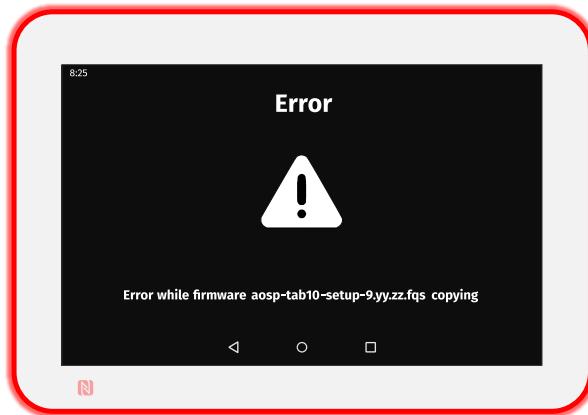
After the AQS version installation, the device is rebooting automatically once. This message is displayed while the device has not yet restarted.



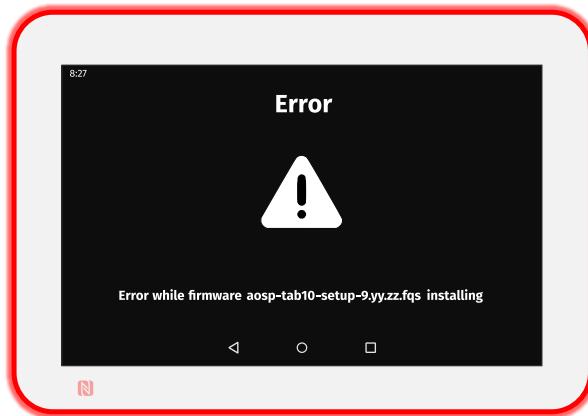
Once the AQS operating system is installed, the .fqs firmware is removed from the device.

Error messages when following the previous procedures

This message is displayed for ten seconds when an error occurred 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 `TAB10b` (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 [TAB10b developer manual](#).

Some APK examples can be downloaded from the [Qeedji Website](#). For further information, contact sales@qeedji.tech.

Third party APK

The `TAB10b` device is intended to work with one or several custom Android APKs. The third party APK are not provided.

The `TAB10b` device is embedding `AQS 9` based on the AOSP SDK 28. The `AQS 9.10.19` embeds `Chromium Web engine 83`.

To develop your third party APK, Qeedji provides a [TAB10b developer manual](#) which is giving links to github to start to work on `AQS 9` for `TAB10b` 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 console web user interface. For further information, refer to the chapter § [APK installation with the device configuration console web user interface](#),
- putting an `.apk` file on an USB storage device then by inserting it in the `TAB10b` 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 deactivated by using the `disableExternalStorageCopyApk();` function in the configuration script. For further information, refer to the chapter § [Device configuration by script](#).

☞ With the native `Chromium Web engine` of `AQS 9`, some custom App may face trouble to display properly the content of Website supporting the `X-Frame-Options` HTTP response header. To work around, the content provider may turn off `X-Frame-Options` HTTP response header.

APK installation with the device configuration console web user interface

It is possible to install APK on the TAB10b device by connecting to the device configuration console 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 console web user interface, refer to the chapter § [Applicative console web user interface](#).

APK installation by USB

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

Prerequisite:

- the TAB10b 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 TAB10b 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.*

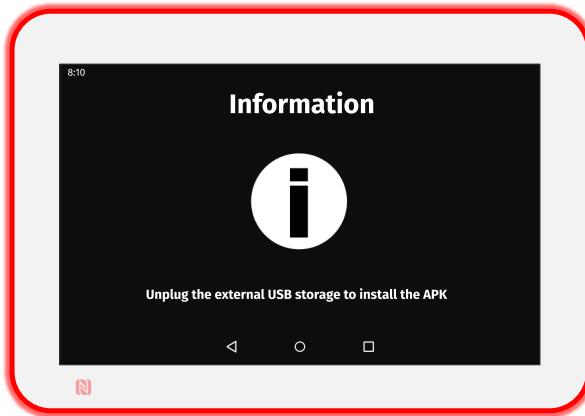
 *To reinstall a same version of an APK, you have to remove it before.*

 *To upgrade an APK with a different signature, you have to remove it before.*

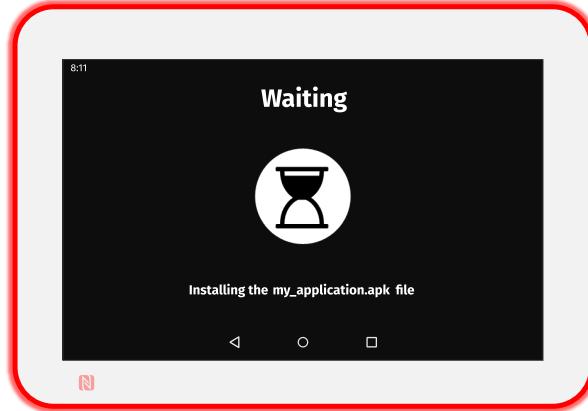
Plug the USB storage device. This message should be displayed while the APK copy has not been completed.



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

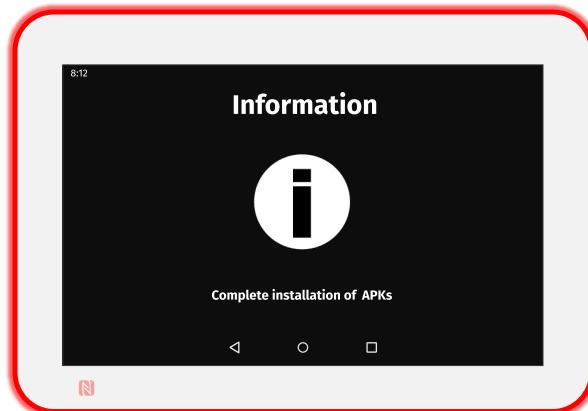


Unplug the USB storage device. This message should be displayed for few seconds, the time for the AQS to install the APK.

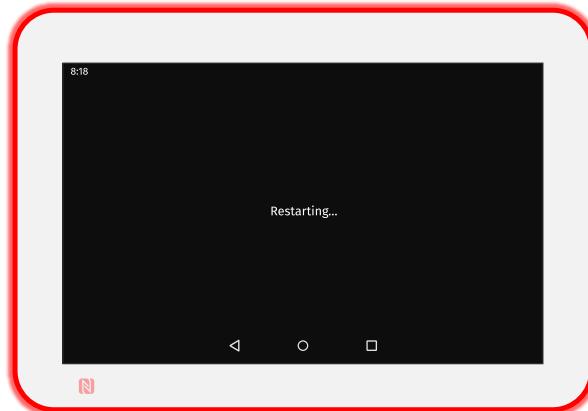


In case several APK are available on the USB storage device, the installing message appears for each new APK to install.

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:

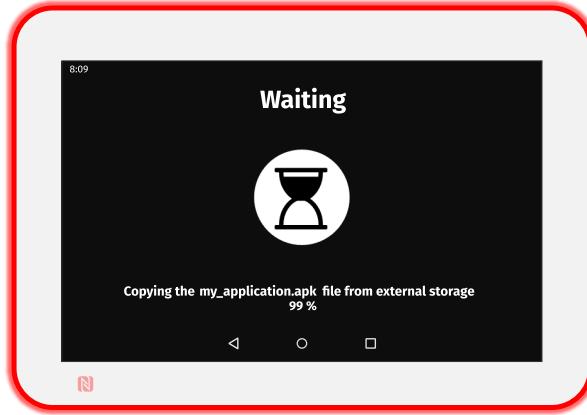
- a WebDAV client (*CarotDAV* or *BitKinex* for example) is installed on your computer or
- the TAB10b is mounted as a disk on the MS-Windows explorer. For further information, refer to the chapter § [Device network disk mounting in MS-Windows explorer](#).

- ☞ The default credentials values for all the connection profiles having access rights to push on the WebDAV 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 without being removed before.
- ☞ `https://` scheme to access to the TAB10b device is not supported.

Copy the `<your_apk>.apk` file in the `.apps/` directory located at the root of the TAB10b 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.

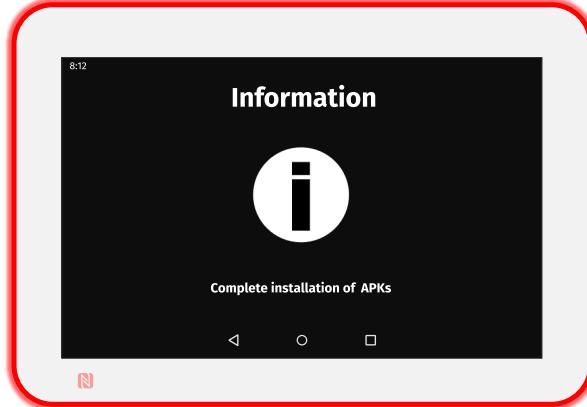


Unplug the USB storage device. This message should be displayed for few seconds, the time for the AQS to install the APK.

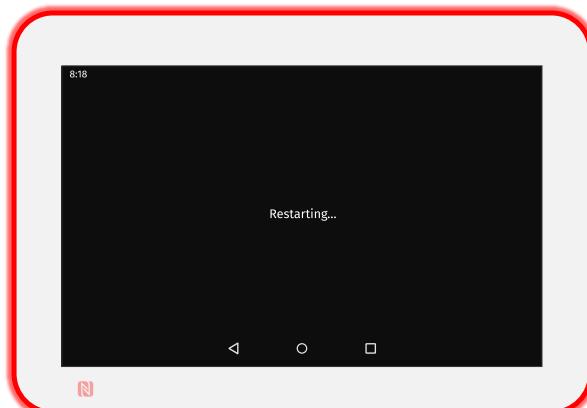


- ☞ In case several APK are available on the USB storage device, the installing message appears for each new APK to install.

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



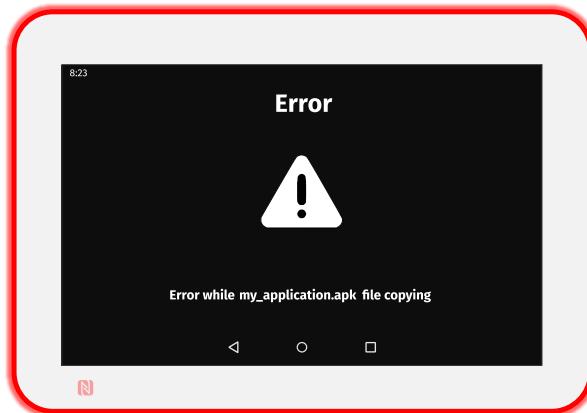
This message is then displayed until the device is rebooting automatically once.



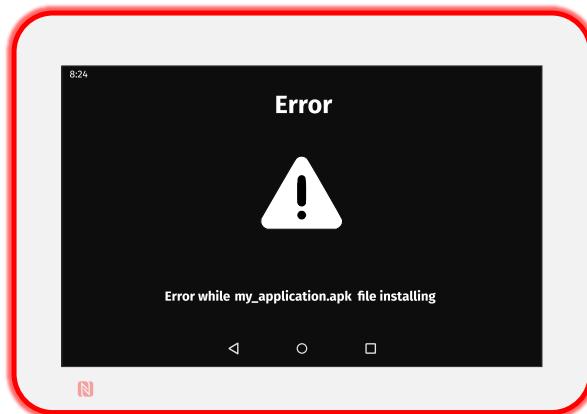
Each APK installed should be then visible on the AQS desktop.

Error messages when following the previous procedures

This message is displayed for ten seconds when an error occurred 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 TAB10b 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 TAB10b 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.

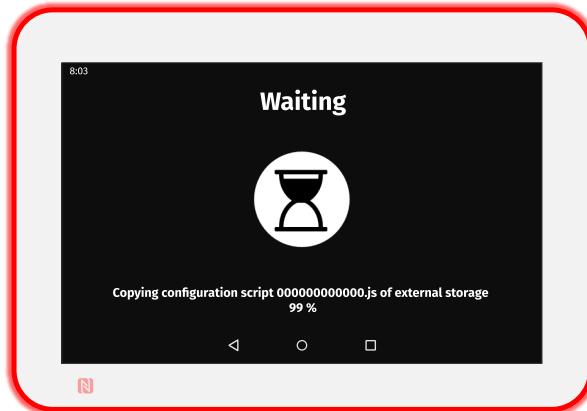
Device configuration by USB

Prerequisite:

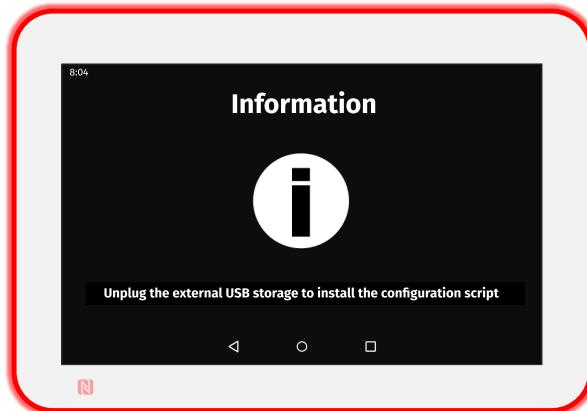
- the TAB10b device needs to have a suitable power supply equipment allowing to support TAB10b device configuration by the USB-C connector.

Copy the configuration script at the root directory of an USB storage device and insert it on the USB-C connector of the TAB10b device (or on the third party equipment connected to the USB-C connector).

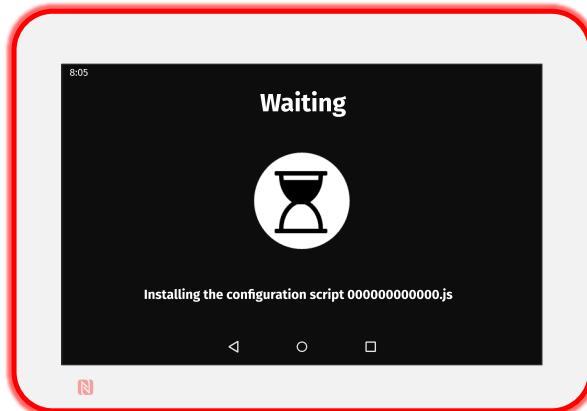
This message is displayed for only few seconds.



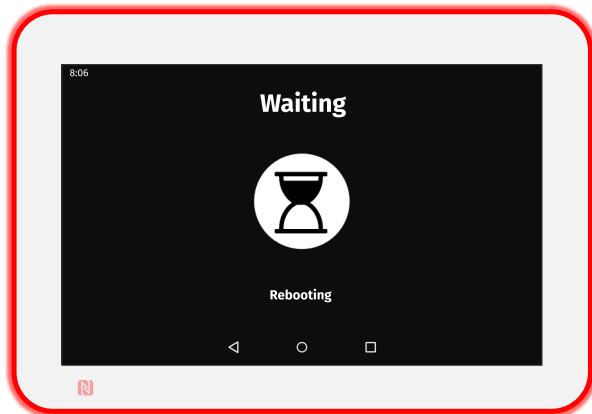
This message is displayed until the USB storage device is unplugged.



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 TAB10b 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](#).

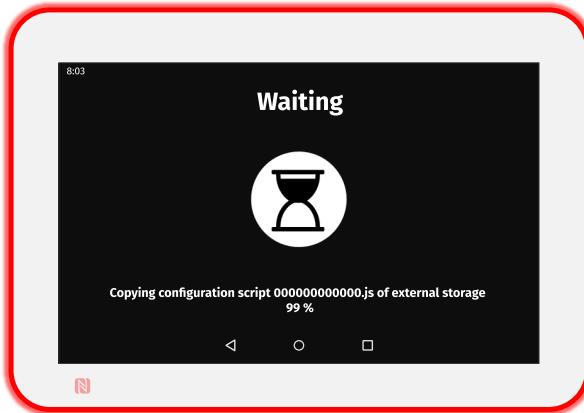
■ The default credentials values, put at factory, for all the connection profiles are: *admin / admin*.

■ The port value put at factory to access to WebDAV directory is: *80*. The port value can be modified by using a [configuration script](#).

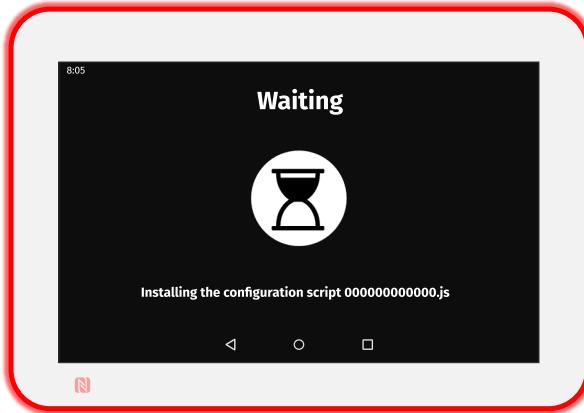
■ *https://* scheme to access to the TAB10b device is not yet supported.

Copy the configuration script in the `.configuration/` directory located at the root of the TAB10b WebDAV server.

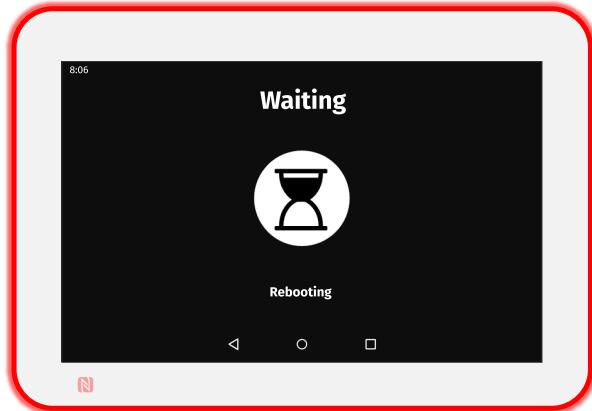
This message is displayed for only few seconds.



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.

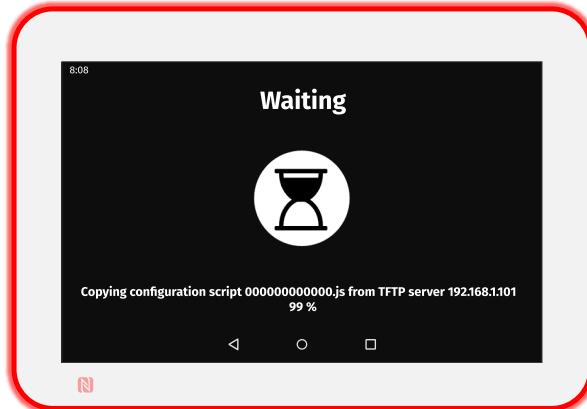
Device configuration by server TFTP and server DHCP with code 66

The TAB10b 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.

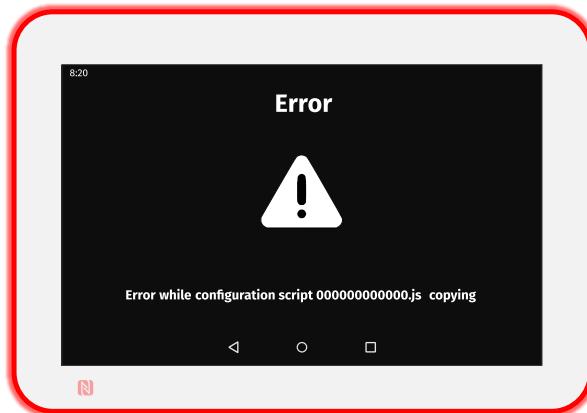
At each device boot-up, the JavaScript configuration script is downloaded from the TFTP server. The script is then executed once only if it has never been downloaded before or if the configuration script has been modified since the last reboot. The message should be displayed showing the IP address of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



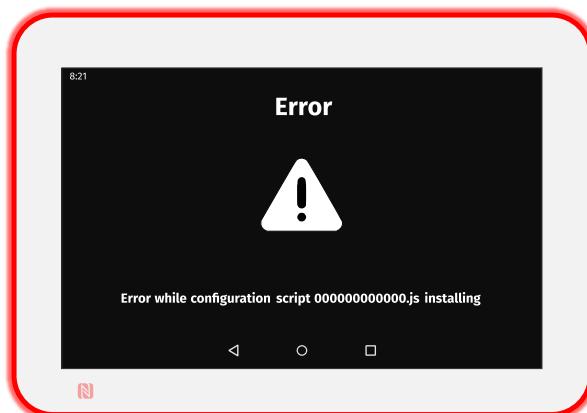
Then you should see the same messages as the chapter § [Device configuration by USB](#) (after the USB storage device is unplugged).

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 problem persists, try again with another USB storage device.



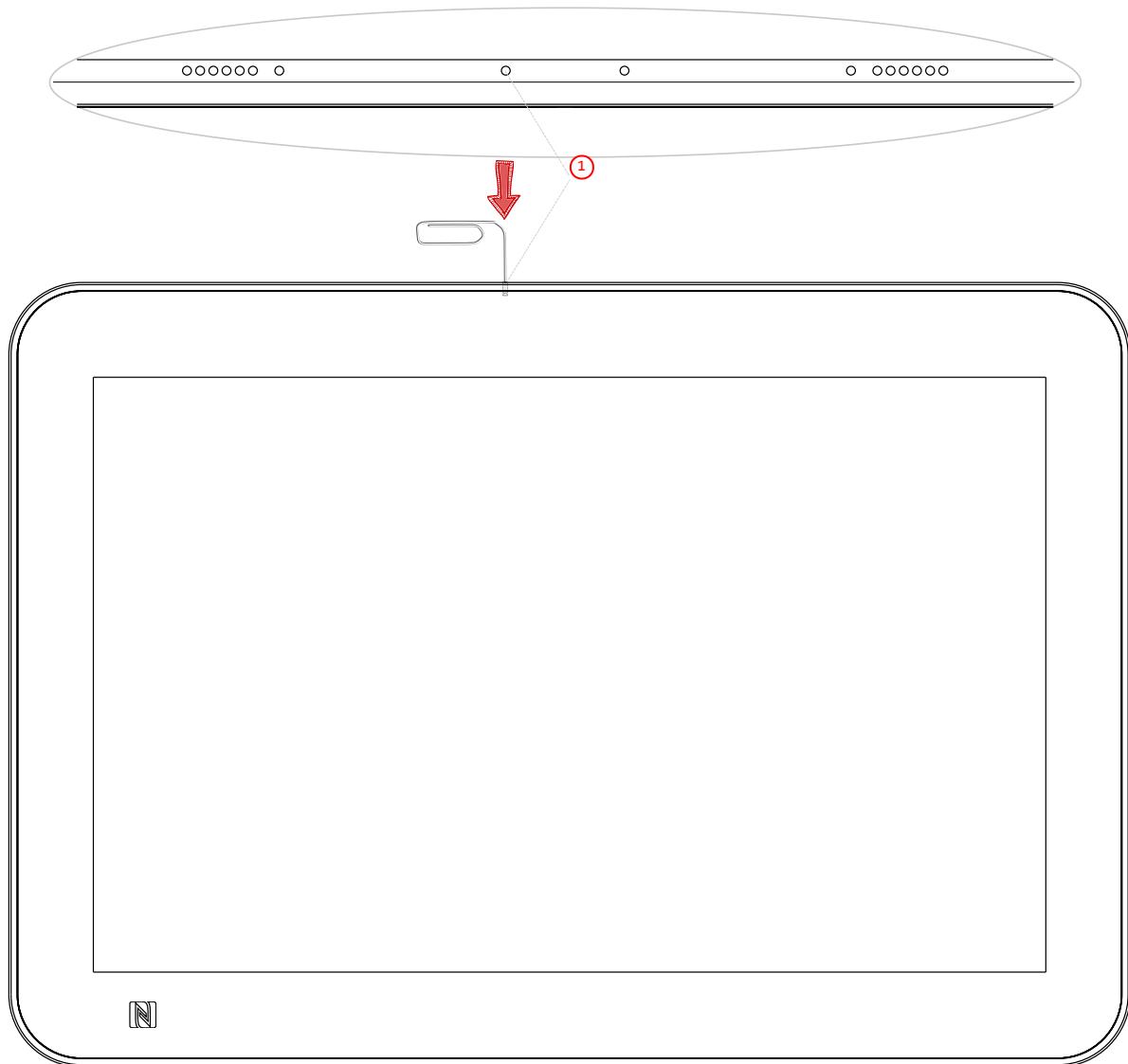
This error message is displayed for ten seconds when the configuration script contains a Javascript syntax error. Double check that the configuration script content is consistent for the TAB10b device.



2.1.4 Hardware reset

In case your APK or the AQS would not respond anymore, you can proceed to a TAB10b 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 TAB10b device configuration data will be lost. So, it is highly recommended to save all the required settings to be able to reconfigure your TAB10b 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:

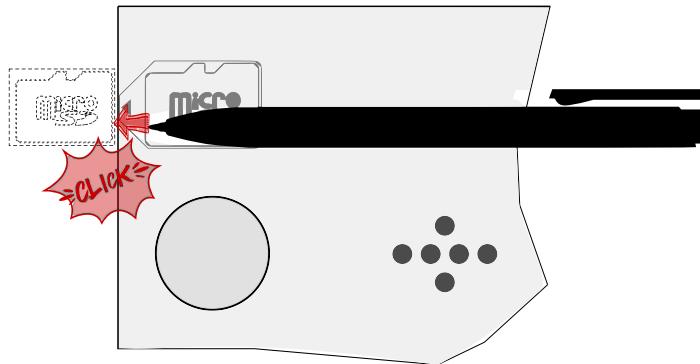
In case the device is hung on the wall on a mounting bracket:

- with a screw driver, untighten the two screws at the bottom of the TAB10b,
- remove the device from the mounting bracket.

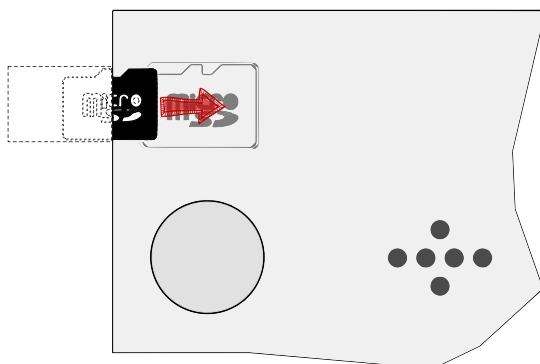
In case the device is powered by the USB-C connector:

- unplug the USB-C power supply,
- with a screw driver, untighten the two screws at the bottom of the TAB10b,
- remove the mounting bracket from the product.

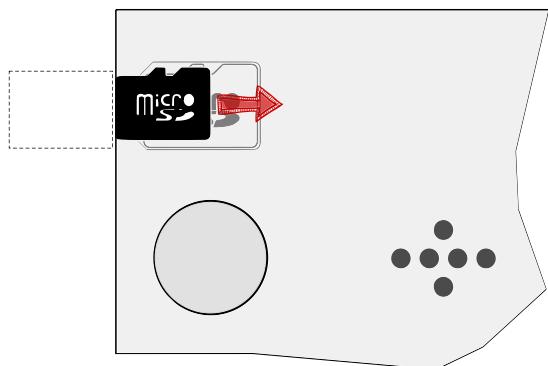
Step 1: Helped with a pen, push a little the micro SD card towards the connector until hearing a clic to unlock the micro SD card.



Step 2: Then put the pen down to let the micro SD card come a little out of its connector thanks to the built-in spring.



Step 3: Glide the micro SD card entirely out of its connector.



☞ It may be required to lift the micro SD card so that it can exit from the 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_qeedji-tab10-setup-xx.yy.zz.iso` file for the factory recovery from the [Qeedji Website](#) (~ 16 GB).

☞ The download time will depend 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 appropriate 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_qeedji-tab10-setup-xx.yy.zz.iso`, can be burnt on your `micro SD card` by any ISO image burning software.

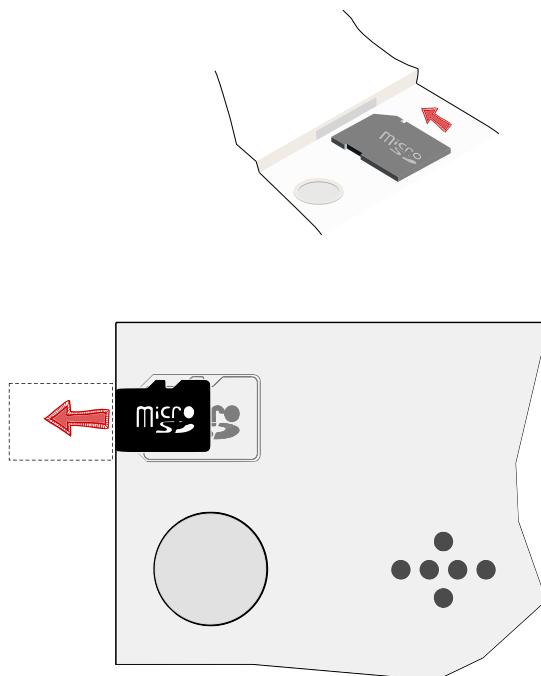
☞ However Qeedji recommends to use the `BalenaEtcher` software (version V1.14.3, for example). For further information about the procedure with `BalenaEtcher` software, refer to the chapter § [ISO image burning with BalenaEtcher](#).

Micro SD card installation

Once the micro SD card content has been updated:

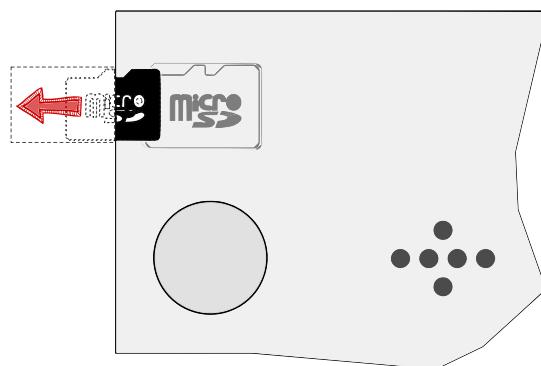
- remove the SD card adapter from your computer,
- remove the `micro SD card` from the SD card adapter,
- insert back the `micro SD card` inside the micro SD connector of the TAB10b device, in the right sense, and push it until hearing a click.

Step 1: Stand the micro SD card in the right sense in front of the connector entry.

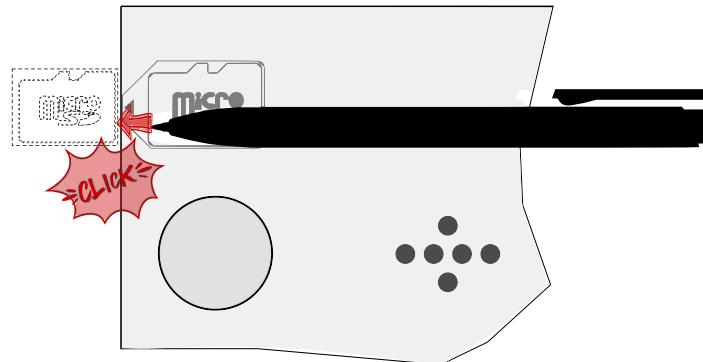


☞ It may be required to lift the micro SD card so that it can enter into the connector. Press a little on it to tilt it.

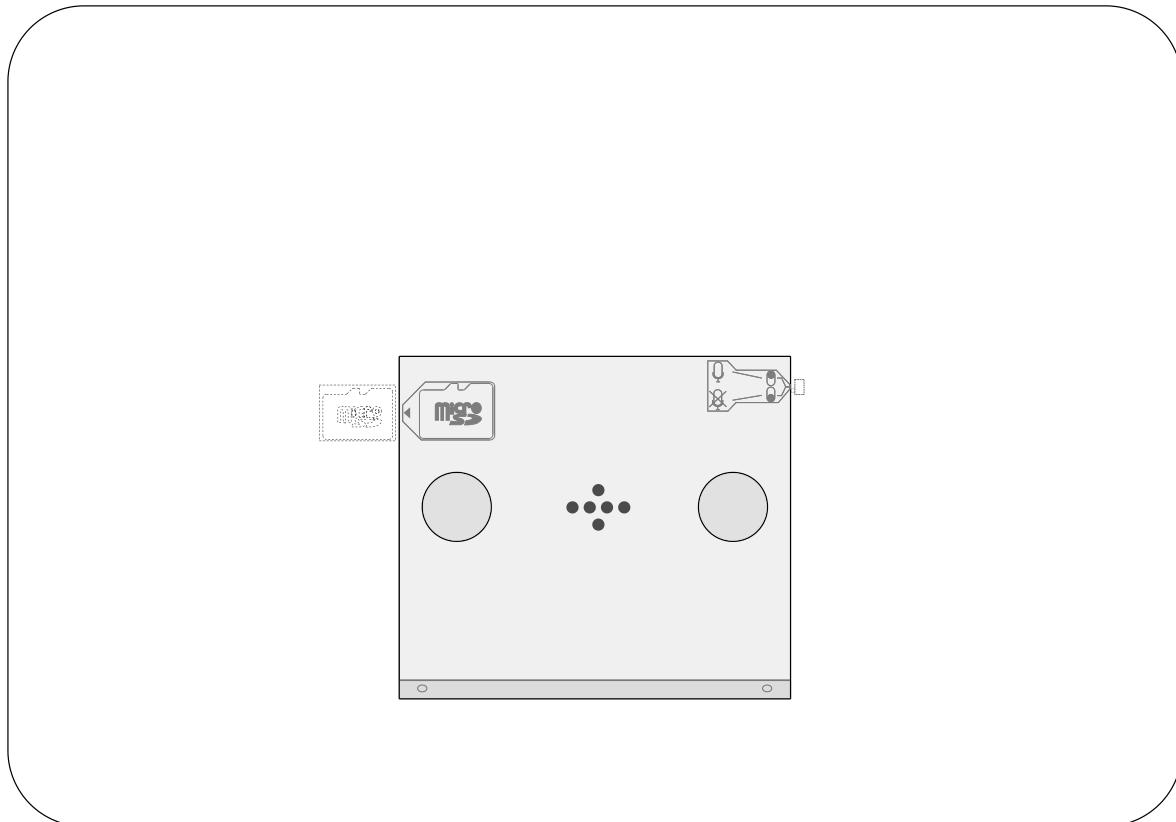
Step 2: Glide the micro SD card with your hand towards the micro SD card connector until you feel the spring of the connector responding.



Step 3: Helped with a pen, push the micro SD card towards the connector until hearing a clic to lock the SD card in its connector.



When the micro SD card is installed properly, the SD card is entirely hidden in the connector.



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 TAB10b 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 console Web user interface

3.1 Applicative console web user interface

The TAB10b device supports a console 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 default credentials values put at factory for the Administration user connection profile are:

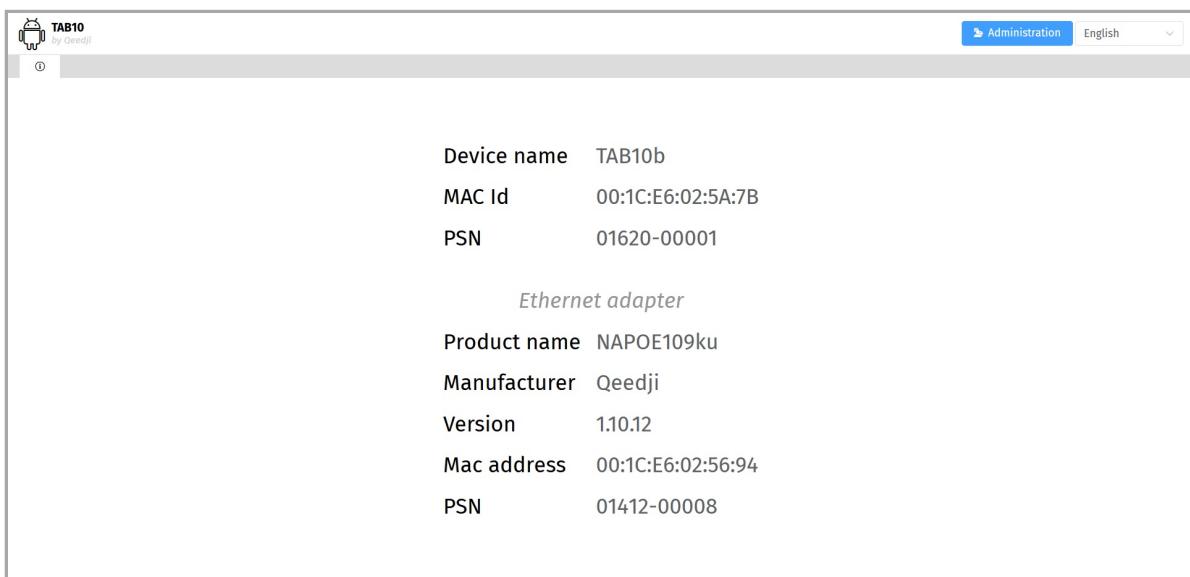
- identifier: admin ,
- password: admin .

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 TAB10b device is supplied by a standard USB-C wall-plug and connected to a WIFI network.



This is an example of content when the TAB10b device is supplied by a NAPOE109ku Ethernet adapter which is connected to a PoE switch.



Part IV

**Administration console Web user
interface**

4.1 Device configuration console web user interface

The TAB10b device supports a device configuration console 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 interface¹. At the top right corner, click on the `Administration` button.



¹ For further information, refer to the chapter § [Applicative console web user interface](#).

This is the device configuration console web user interface.

A screenshot of the device configuration console web user interface. The left sidebar shows navigation categories like Configuration, Maintenance, and Information. The main pane displays the "Configuration > Administrator" section. It includes fields for "Device name" (TAB10s), "Connection profiles" (Administration user, Admin selected), and a "Credentials" panel where "Admin" is listed. Top right buttons include "Reboot the device" and "English". A red circle labeled "1" is over the device logo in the top-left, and another red circle labeled "2" is over the "Administration" button in the top-right.

⚠ 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 console 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**

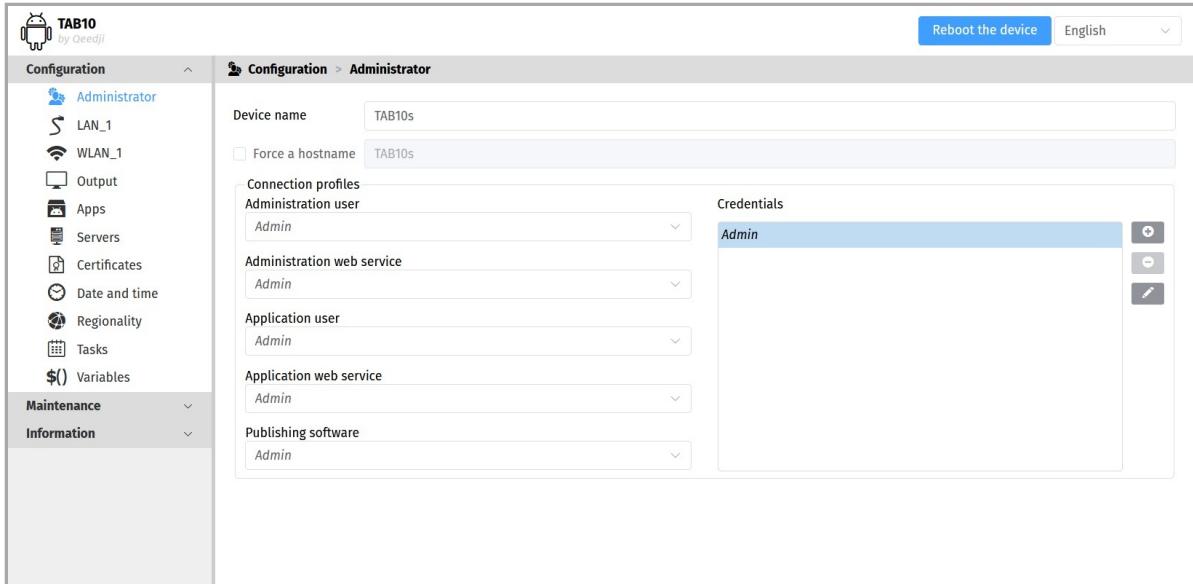
Then associate your private credentials values to the different **connection profiles**:

- **Administration user** : the access rights of this connection profile allow to:
 - access to the device configuration console 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),
- **Application web service** : the access rights of this connection profile allow to use only the additional web services supported by the App (ex: **odata demo APK**),
- **Administration web service** : the access rights of this connection profile allow to 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 console web user interface in **Read Only**¹ and to the applicative console web user 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 console web user interface.

☞ The default credential label for all connection profiles is **Admin, corresponding to the default identifier/password **admin / admin**.**

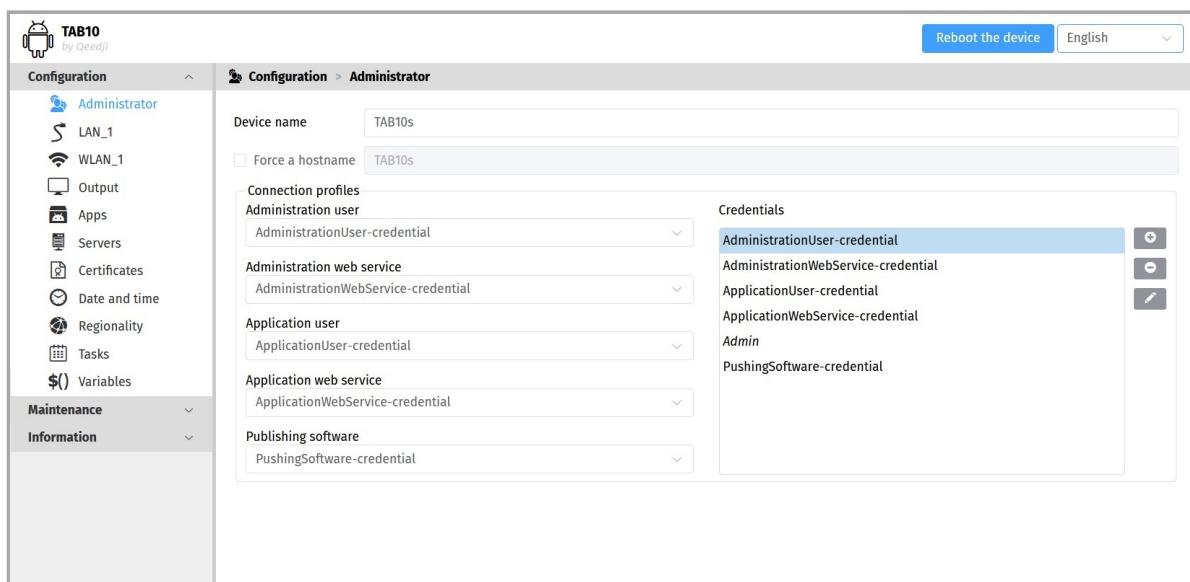
⚠ In case you have lost the credentials values of all the **Administration user connection profiles, the only way to restore some known credentials is to inject an USB-C mass storage having an appropriate configuration script through the USB-C connector (USB 1 or USB 2) of the TAB10b device. For further 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 TAB10b 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.

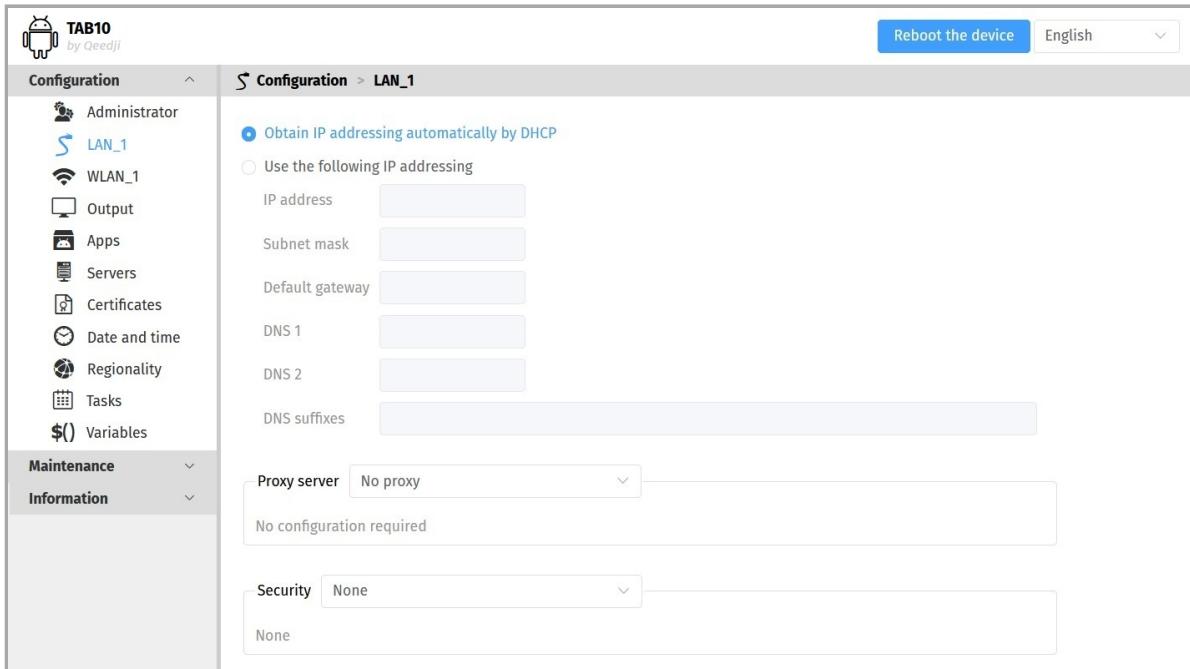


☞ The association of the credentials to the connection profiles are taken into account only after a device reboot. In case the user takes more than 5 minutes to create the credentials, associate them to the profile and reboot, the user may have to reauthenticate (with the credentials not modified).

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 TAB10b 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.

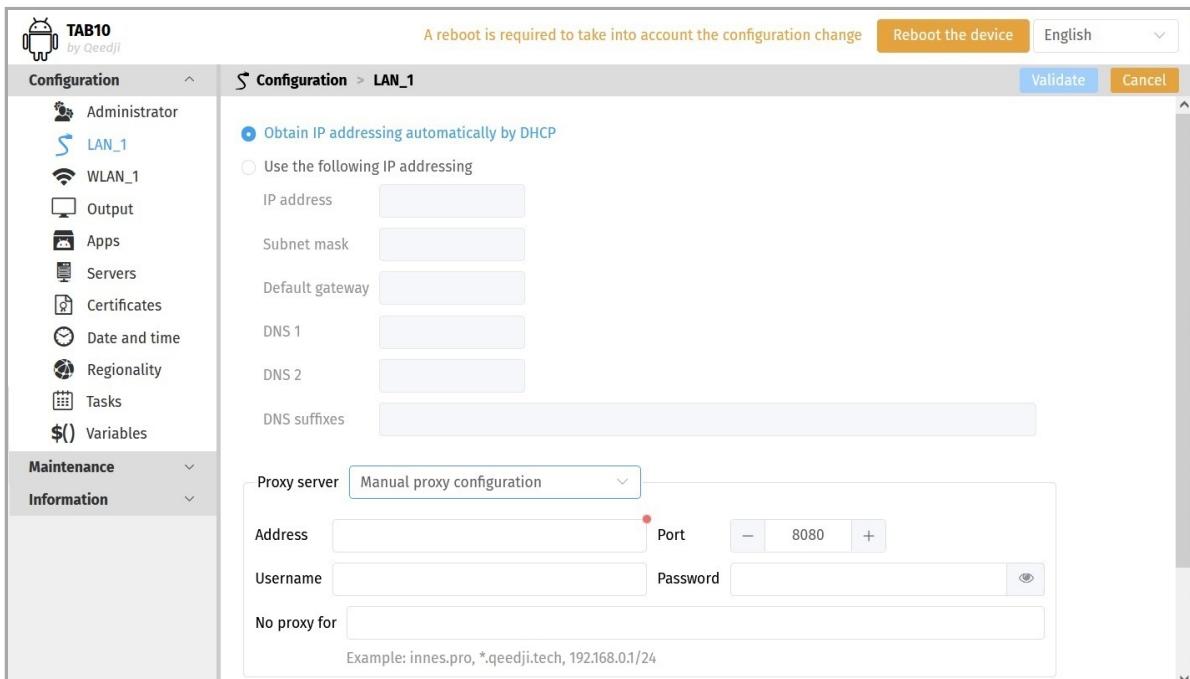
⚠ By default, the device is configured with DHCP activated.

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 console 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 console 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://\[fe80::21c:e6ff:fe02:27bf\]/](http://[fe80::21c:e6ff:fe02:27bf]/) or type [http://\[fc00::21c:e6ff:fe02:27bf\]/](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.

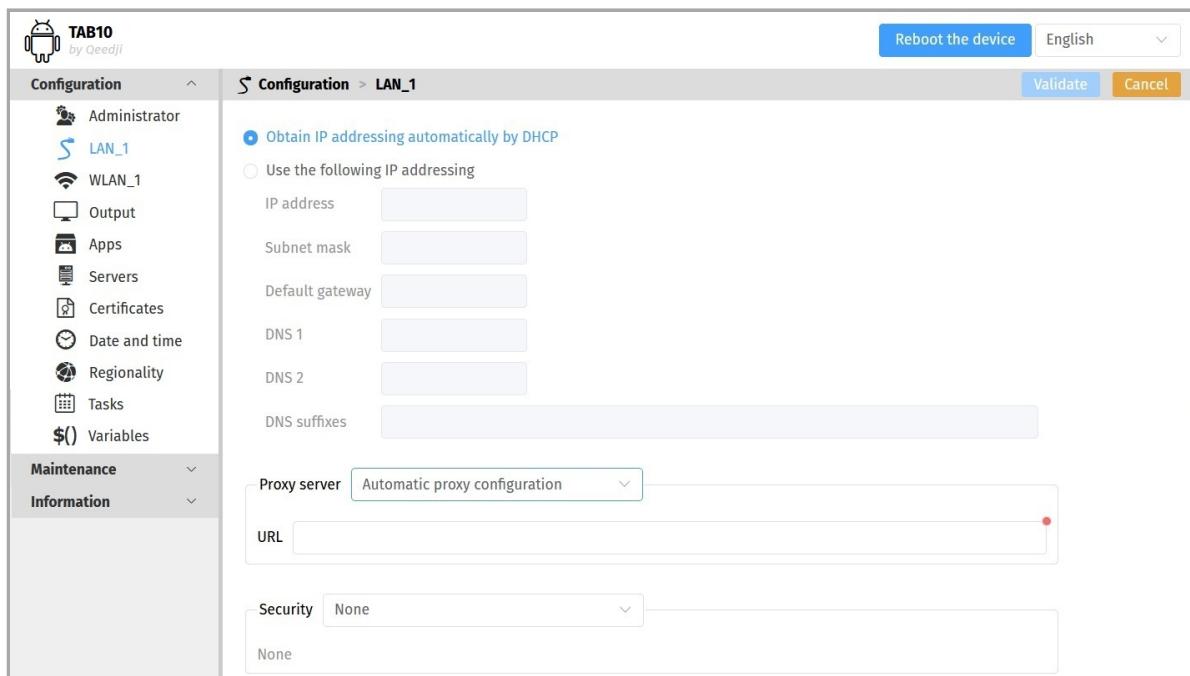


The `No proxy` for input support these format values:

- website URL (e.g. `innes.pro`),
- subset of subdomains by using the `*` wildcard (e.g.: `.qeedji.tech`),
- range of IP addresses by using a mask matching the syntax `network_ip_addr/xx` (e.g. `192.168.0.100/24`), XX going from 1 to 32.

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 automatically 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 console 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 deactivated, 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 console 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 console 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 console web user interface with its `LAN_1` IPV6 address (for example [http://\[fe80::21c:e6ff:fe02:5694\]](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 console web user interface when your network does not support DHCP:

1. it is considered here that the TAB10b 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 console web user interface with a web browser with its `LAN_1` IPV6 address (for example [http://\[fe80::21c:e6ff:fe02:5694\]](http://[fe80::21c:e6ff:fe02:5694]) get from the `MAC` value written at the back of the NAPOE109XX device),
5. deactivate `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 console 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 console 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 console web user interface with its `LAN_1` IPV6 address (for example [http://\[fe80::21c:e6ff:fe02:5694\]](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.

The screenshot shows the configuration interface for a TAB10 device. The left sidebar has sections for Configuration (Administrator, LAN_1, WLAN_1, Output, Apps, Servers, Certificates, Date and time, Regionality, Tasks, Variables), Maintenance, and Information. The main panel is titled 'Configuration > LAN_1'. It shows the following settings:

- IP Addressing:
 - Obtain IP addressing automatically by DHCP (selected)
 - Use the following IP addressing
- Networking:
 - IP address: [empty]
 - Subnet mask: [empty]
 - Default gateway: [empty]
 - DNS 1: [empty]
 - DNS 2: [empty]
 - DNS suffixes: [empty]
- Proxy server: No proxy
- No configuration required
- Security: 802.1X
- EAP method: TLS
- Validation of the 802.1X CA certificate: Qeedji (Qeedji Certificate Authority)
- Provision of the 802.1X user certificate: Qeedji (001CE6025A7B)
- Identity: 001CE6025A7B

At the top right are buttons for Reboot the device, English (language selection), Validate, and Cancel.

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 TAB10b 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 TAB10b device. For further information about certificates installation, refer to the chapter § [Certificates](#).

■ The `802.1X CA certificate` is the certificate with the highest authority for your RADIUS server. For further information, please contact your IT department.

■ In this AOS 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 negotiation 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 negotiation 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 deactivated through the device configuration console 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 App 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 deactivated, 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 console 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://\[fe80::21c:e6ff:fe02:27bf\]/](http://[fe80::21c:e6ff:fe02:27bf]/) or [http://\[fc00::21c:e6ff:fe02:27bf\]/](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 console 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 console 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 console web user interface.
5. connect to the device configuration console 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 console web user interface also now with its **wlan_1** IPv6 address (for example [http://\[fe80::21c:e6ff:fe02:62e3\]](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 console web user interface when your network does not support DHCP:

1. it is considered here that the TAB10b 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 console web user interface with a web browser with its **lan_1** IPv6 address (for example [http://\[fe80::21c:e6ff:fe02:5694\]](http://[fe80::21c:e6ff:fe02:5694]) get from the **MAC** value written at the back of the NAPOE109XX device),
5. deactivate **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 console 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 console 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 console web user interface also now with its **wlan_1** IPv6 address (for example [http://\[fe80::21c:e6ff:fe02:62e3\]](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 TAB10b device. And wait device reboot.
2. connect to the device configuration console 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 console web user interface also now with its **wlan_1** IPv6 address (for example [http://\[fe80::21c:e6ff:fe02:62e3\]](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 transfer¹ with an USB cable between the computer and the TAB10b device (the device must be supplied properly by the computer, by the NAPOE109kt device or by the NAPOE109ft device):

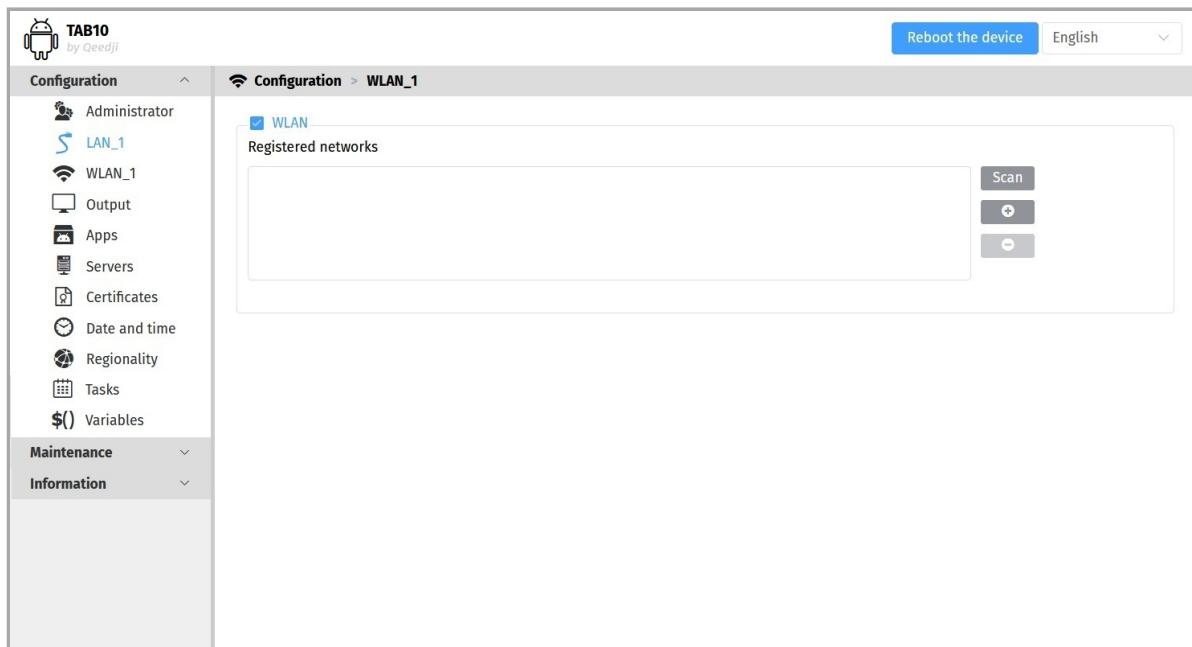
1. push a suitable configuration script on the **.configuration** directory of the device file system from a computer. And wait device reboot.
2. connect to the device configuration console web user interface with a web browser with the valid **wlan_1** IP address of the device. You can connect to the device configuration console web user interface also now with its **wlan_1** IPv6 address (for example [http://\[fe80::21c:e6ff:fe02:62e3\]](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](#).

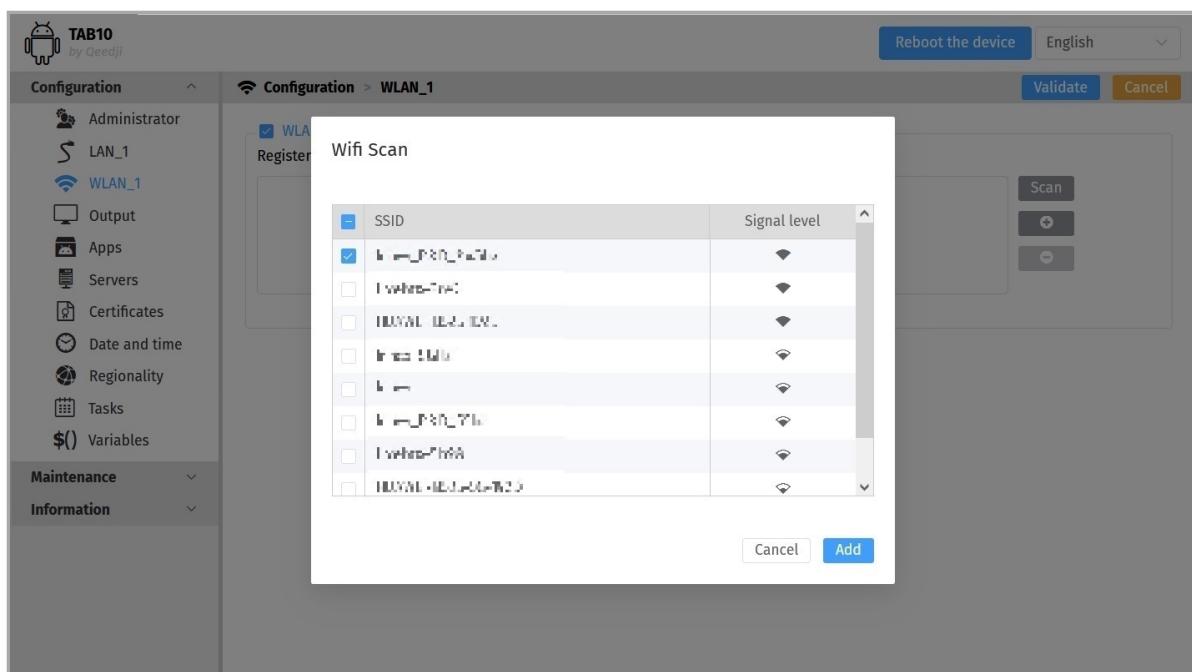
It is also possible to configure the **wlan_1** interface directly with **Android Settings App**.

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`.

The screenshot shows the configuration interface for a device named 'TAB10 by Qeedi'. The left sidebar has sections for Configuration (Administrator, LAN_1, WLAN_1, Output, Apps, Servers, Certificates, Date and time, Regionality, Tasks, Variables), Maintenance, and Information. The main panel is titled 'Configuration > WLAN_1' and shows 'WLAN' selected. It displays 'Registered networks' with a list of available networks. Below this, the 'SSID' is set to 'TAB10' and 'SSID Hidden' is set to 'Yes'. The 'Obtain IP addressing automatically by DHCP' option is selected. There are also fields for 'IP address' (192.168.2.211), 'Subnet mask' (255.255.128.0), 'Default gateway' (192.168.0.1), 'DNS 1' (8.8.8.8), and 'DNS 2' (empty). The 'Proxy server' dropdown is set to 'No proxy'. A note says 'No configuration required'. At the bottom, the 'Security' dropdown is set to 'None'.

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.

TAB10
by Qeedji

Configuration

- Administrator
- LAN_1
- WLAN_1
- Output
- Apps
- Servers
- Certificates
- Date and time
- Regionality
- Tasks
- \$() Variables

Maintenance

Information

Configuration > WLAN_1

WLAN

Registered networks

SSID:

SSID Hidden: No

Obtain IP addressing automatically by DHCP

Use the following IP addressing

IP address:

Subnet mask:

Default gateway:

DNS 1:

DNS 2:

DNS suffixes:

Proxy server: Manual proxy configuration

Address: Port: - +

Username: Password:

No proxy for:

Example: innes.pro, *.qeedji.tech, 192.168.0.1/24

Security: WPA-Personal (PSK), WPA2-Personal (PSK)

Key (8 to 63 ASCII characters):

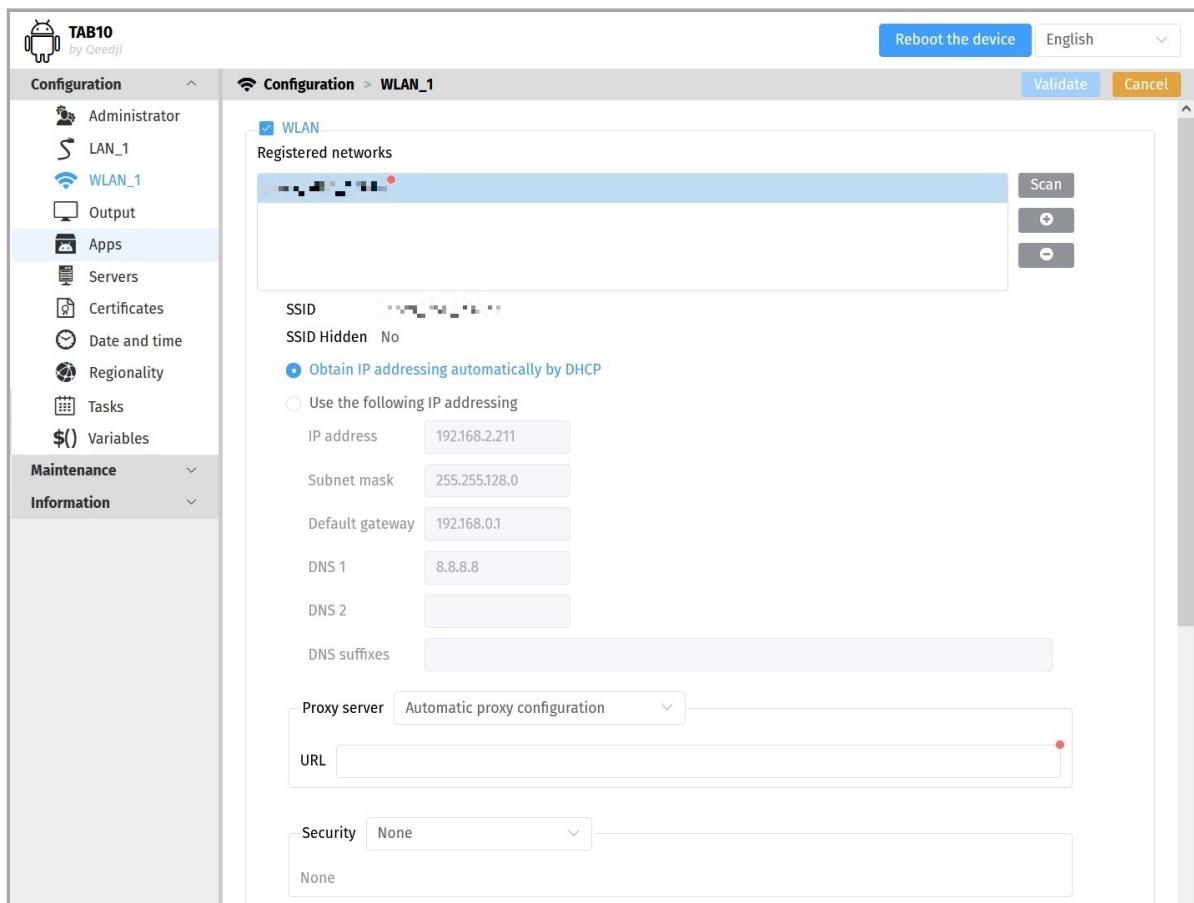
Reboot the device

English

Validate Cancel

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 securities¹ 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:

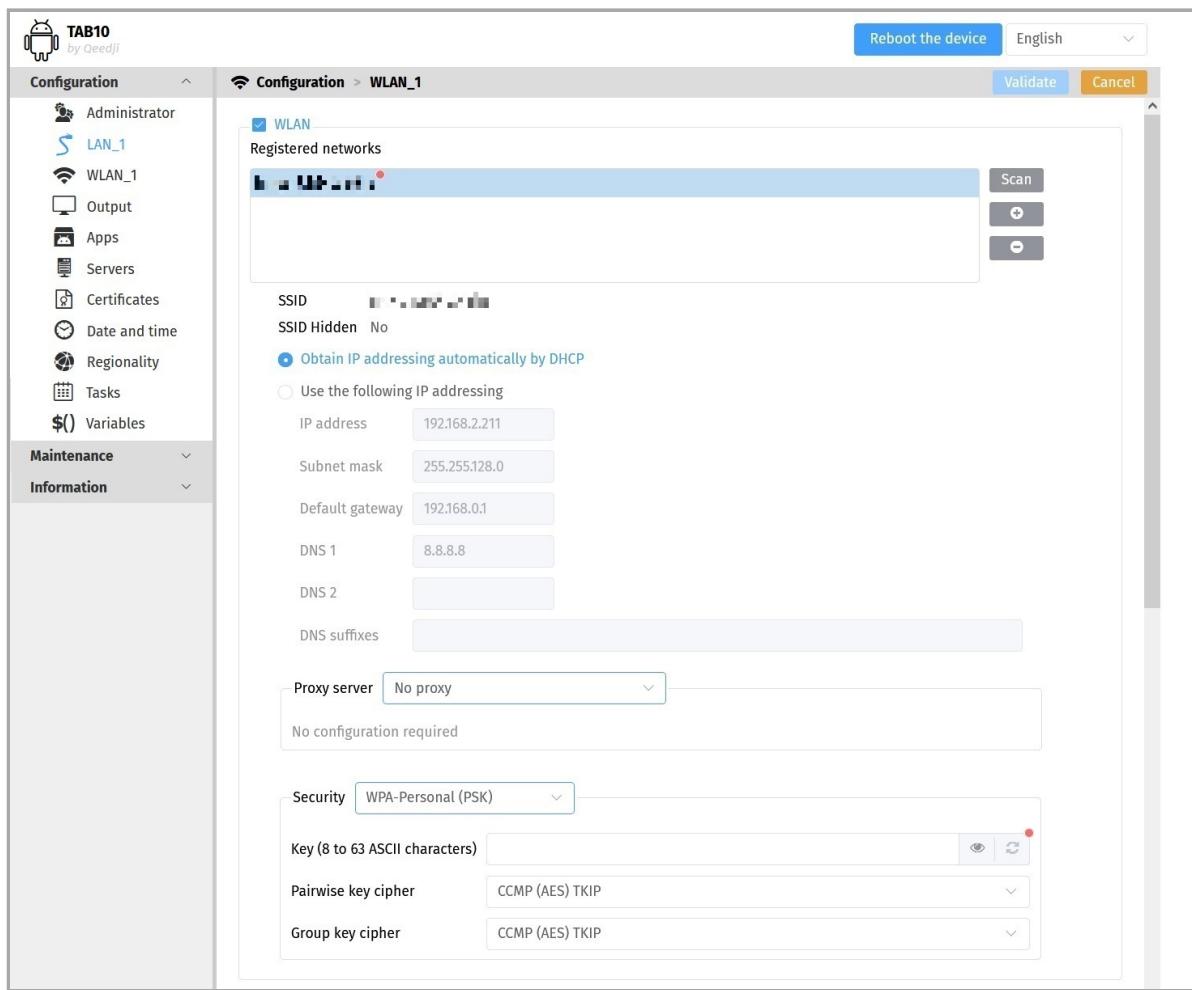
- WEP ,
- WPA-Personal (PSK) ,
- WPA2-Personal (PSK) .

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 screenshot shows the configuration interface for a TAB10 device. The left sidebar has sections for Configuration (Administrator, LAN_1, WLAN_1, Output, Apps, Servers, Certificates, Date and time, Regionality, Tasks, Variables), Maintenance, and Information. The main panel is titled 'Configuration > WLAN_1' under the 'WLAN' section. It displays a list of registered networks with one entry ('WLAN_1') selected. Below this, there are fields for SSID (set to 'WLAN_1'), SSID Hidden (set to 'No'), and IP addressing methods (radio button selected for 'Obtain IP addressing automatically by DHCP'). There are also fields for static IP configuration (IP address: 192.168.2.211, Subnet mask: 255.255.128.0, Default gateway: 192.168.0.1), DNS settings (DNS 1: 8.8.8.8, DNS 2: blank, DNS suffixes: blank), and a proxy server dropdown set to 'No proxy'. A note below says 'No configuration required'. At the bottom, there is a 'Security' dropdown set to 'WEP' and a field for the 'Key' (5 or 13 ASCII characters, 10 or 16 hexadecimal characters), which is currently empty. The top right of the interface includes buttons for 'Reboot the device', 'English' (language selection), 'Validate', and 'Cancel'.

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:

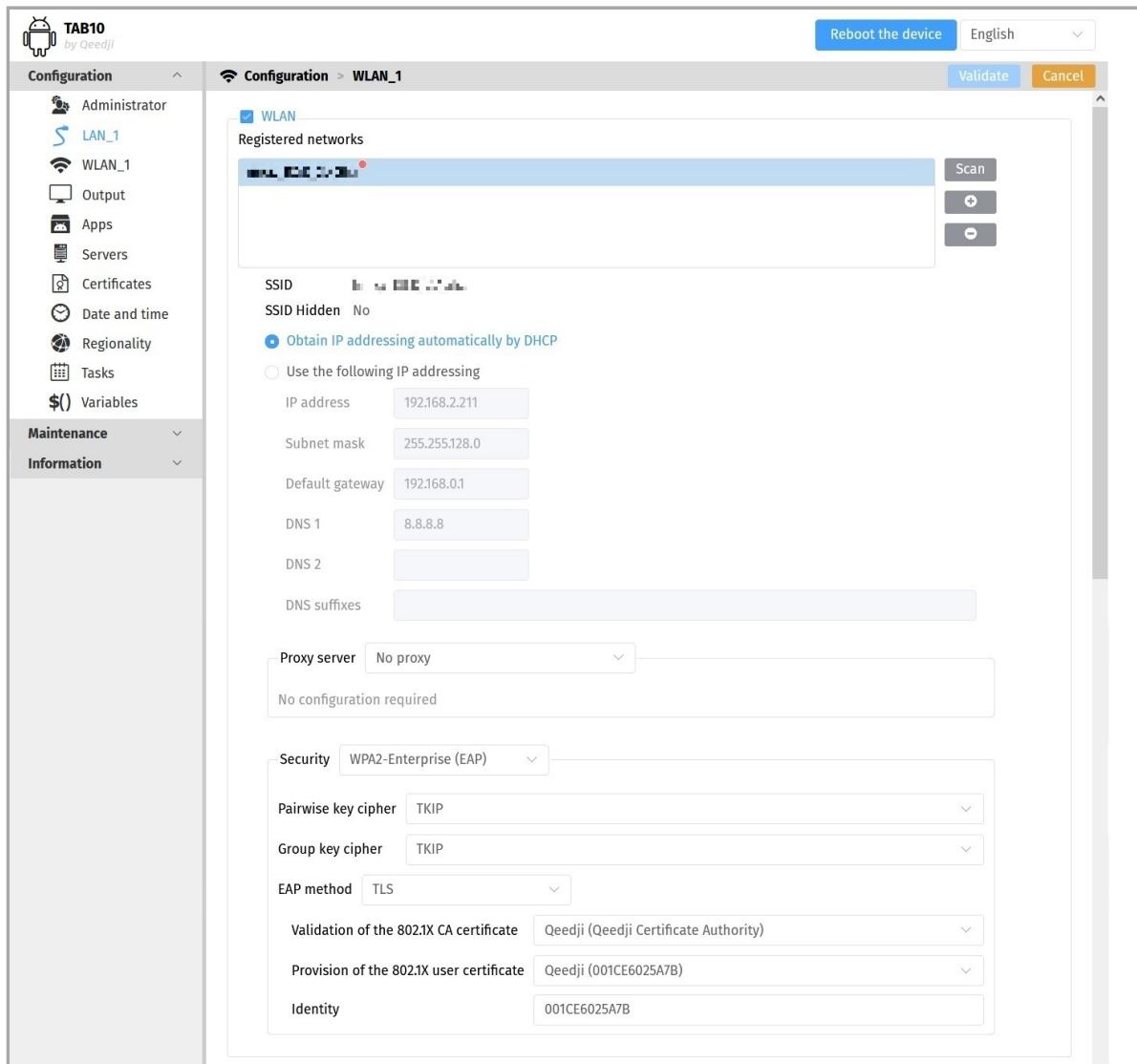
| Pairwise key cipher | Group key cipher |
|---------------------|------------------|
| TKIP | TKIP |
| CCMP (AES) TKIP | CCMP (AES) TKIP |

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 TAB10b 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 TAB10b device. For further information about certificates installation, refer to the chapter § [Certificates](#).

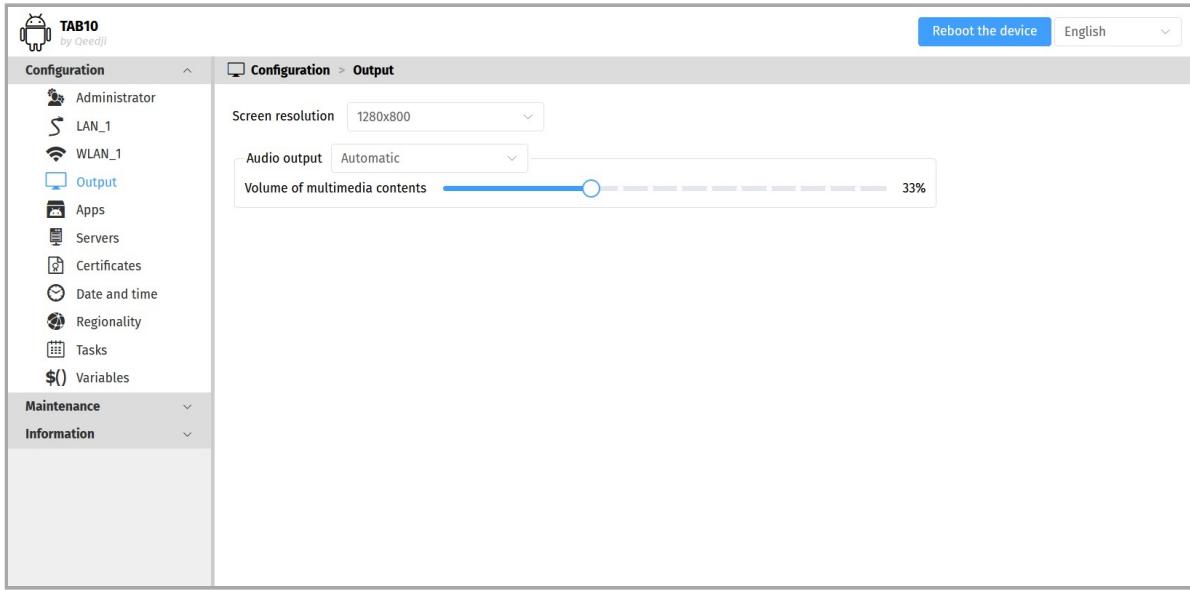
■ The **802.1X CA certificate** is the certificate with the highest authority for your RADIUS server. For further information, please contact your IT department.

■ The **Domain of the 802.1X CA certificate** input is displayed 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 90°, 180°, 270° is not supported on the tablet.
- **Audio output :**
 - audio way selection:
 - **Automatic:** if an USB-C to Jack 3.5" adapter is plugged, the audio is output in priority on it,
 - **Internal:** the audio is output on the speaker,
 - **USB Audio:** the audio is output on the USB-C to Jack 3.5" adapter.
 - **Volume of multimedia contents** bargraph: allows to tune the audio volume common to the different audio outputs (*Speaker, USB*).
 - ☞ If your TAB10b device is supplied by a NAPOE109kt device or a NAPOE109ft device, the device can support a Jack 3.5 audio output by plugging an USB-C to Jack 3.5" audio adapter on the USB-C connector.
 - ☞ Some manufacturers of USB-C to Jack 3.5" audio adaptors may apply significant attenuation to the jack output. Please check this before ordering such a device.

4.1.5 Configuration > Apps

In the Configuration tab, select the **Apps** menu to manage the Apps installed in the AQS operating system, whose launching at device start-up can be activated or deactivated.

The Apps column of the table allows to watch the Apps installed in the AQS operating system:

- the built-in Apps (App installed by default by the vendor at factory),
- all the Apps installed by the user.

☞ In this AQS version, the only built-in Apps are the Media Folder Injector (V1.10.10) App, the Power BI Online Viewer (V1.10.10) and the URL Launcher (V1.10.19) App. The activated status of the built-in Apps is unchecked by default. Consequently, they are not running by default. For further information about the built-in Apps usage, refer to the chapter § [Information on the built-in Apps form inputs](#).

| Apps | Activated |
|------------------------|--------------------------|
| Media Folder Injector | <input type="checkbox"/> |
| Power BI Online Viewer | <input type="checkbox"/> |
| URL Launcher | <input type="checkbox"/> |

This App has no configuration page

☞ The number of visible rows is five maximum. If more than five APK are installed, scroll the table to the bottom to watch the other rows of the table. The Apps are sorted in the alphabetical order.

The pane supports four buttons to manage the Apps :

- **Install the App** : allows to install an APK (.apk) on the device from a computer,
- **Uninstall the App** ¹: allows to uninstall the APK that is selected ,
- **Restart the App** button: allows to start (or restart) the APK that is selected,
- **Stop the App** button: allows to stop the APK that is selected.

An App can be installed by:

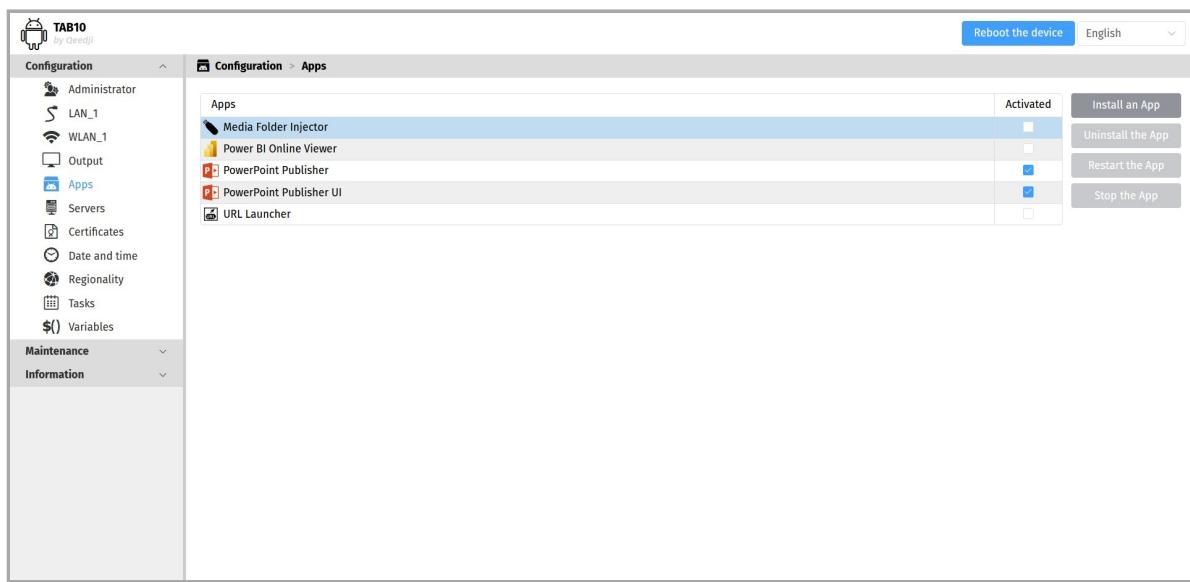
- uploading any compatible APK (.apk) with the **Install the App** button,
- pushing any compatible APK (.apk) on the .apps WebDAV directory of the device with a WebDAV client or with a third party software,
- using the **Maintenance > Files** pane of the device configuration console web user interface to upload any compatible APK (.apk),
- insert an USB-C storage device containing a compatible APK (.apk) on the device.

Any App newly installed is activated by default, meaning that:

- its associated APK pictogram is available on the AQS desktop,
- when the APK supports the *autorestart* AOSP feature, it is started automatically after the device boot-up.

Some Apps consist in a couple of APK (*main part + UI part*). This is an example when the *Qeedji PowerPoint Publisher for Media Players App* is installed and properly activated:

- *PowerPoint Publisher* (for the main part):
 - checkbox *Activated* : checked,
- *PowerPoint Publisher UI* (for the UI part):
 - checkbox *Activated* : checked.



¹ In case an App is partially or entirely uninstalled, meaning removed from this table by clicking on the *Uninstall the App* button, the App cannot run anymore. To fix the problem, the App must be reinstalled or the App content must be published again. Then the device must reboot once.

☞ The swiping may be inactivated by some custom App.

Apps restart/stop

Any activated APK can be:

- started or restarted with the *Restart the App* button,
- stopped with the *Stop the App* button.

☞ For the *Apps* consisting in a couple of APK (*main part + UI part*), only the main part of the App can be restarted.

Flying over an App allows to know the App status showing whether the App is started or not:

- *Running*: the App is started,
- *Stopped*: the App is stopped.

Apps deactivation

☞ All the *Apps* supporting the *autorestart AOSP* feature are launched automatically after a device boot-up, but only one of them can be visually rendered on the screen. Given that the *AOS* operating system cannot choose, among the *activated Apps*, the one which must be visually rendered on the screen, and given that device resources (CPU, DDR, video decoder) are shared between the APK which are executed at the same time, it is advised to keep an only one *activated APK* at a time.

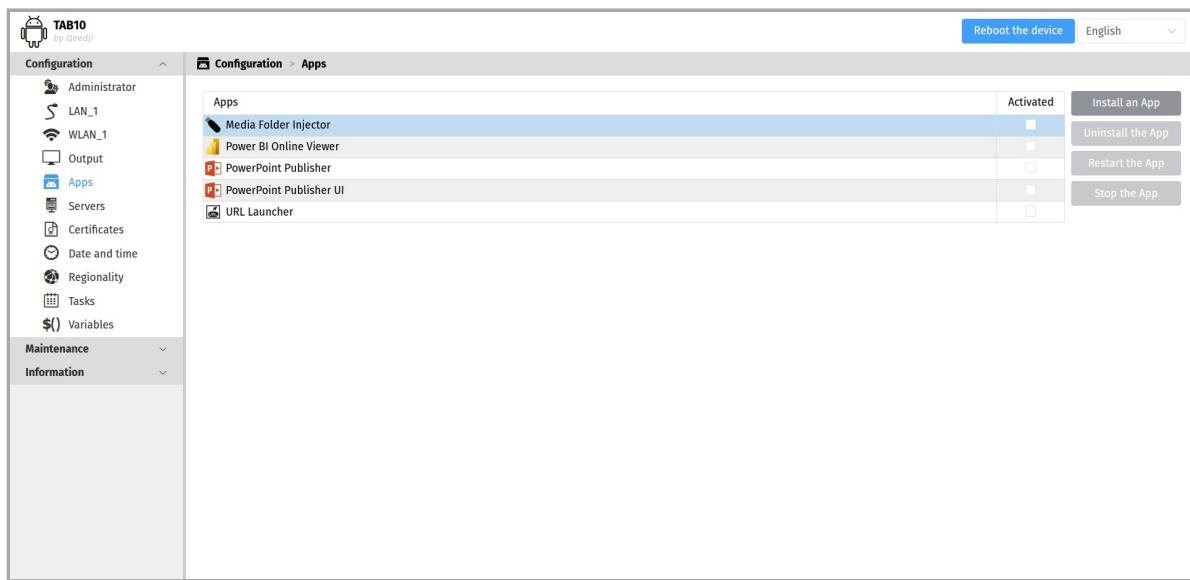
With the table of installed *Apps*, it is easy, with the appropriate checkbox in the *Activated* column, to see the *Apps* that are activated and then voluntarily choose to deactivate those that are temporarily not useful for your current need.

☞ If an *App* is not useful at all, the best is to uninstall it with the *Uninstall the App* button.

Some Apps consist in a couple of APK (*main part + UI part*). When such an *App* needs to be deactivated, the both parts of the App must be deactivated.

This is an example with the Qeedji PowerPoint Publisher for Media Players App properly deactivated:

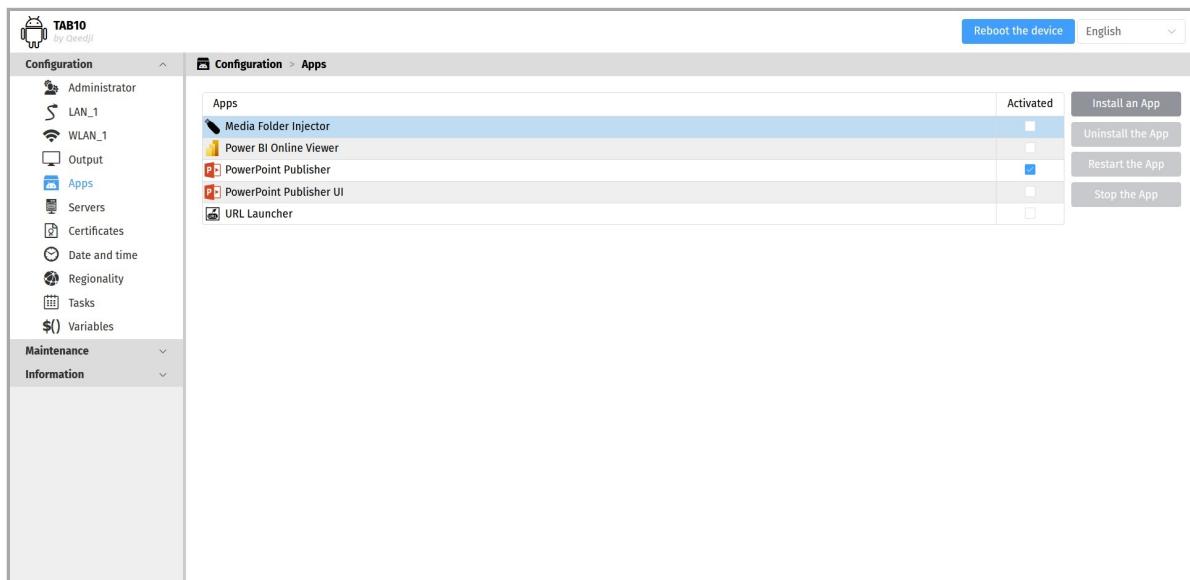
- **PowerPoint Publisher** (= the main part):
 - checkbox Activated : unchecked,
- **PowerPoint Publisher UI** (= the UI part):
 - checkbox Activated : unchecked.



⚠ If ever only the *UI* part of the *App* is not *activated*, and the *main* part of the *App* is kept *activated*, publishing the same *App* with the appropriate third party software could not lead to the automatic *App* start. To work around, activate back the *UI* part APK of the *App* then reboot the device.

This is an example with the Qeedji PowerPoint Publisher for Media Players App not properly deactivated:

- **PowerPoint Publisher** (= the main part):
 - checkbox Activated : checked,
- **PowerPoint Publisher UI** (= the UI part):
 - checkbox Activated : unchecked.



Apps reactivation

After having checked back the *activation* checkbox for an *App*, click on the *Reboot the device* button to finalize the operation.

⚠ If ever only the *UI* part of the *App* was not *activated*, and the *main* part of the *App* was kept *activated*, activate back the *UI* part of the *App* then click on the *Reboot the device* button to finalize the operation.

App form (optional)

Some *APK* can support a configuration form. To watch the configuration form for an *App*, select the appropriate *App*. If a form is supported for this *App*, the form of *Apps* appears just below the table of installed *Apps*.

☞ When the selected *App* does not support a configuration form, the additional *This App has no configuration page* information label is displayed below the table of installed *Apps*.

Custom screensaver APK

This AQS version supports the installation of custom `screensaver` APK which replaces the default AQS `screensaver com.android.dreams.basic/com.android.dreams.basic.Colors` that is displaying a colors gradient.

The `screensaver` is not activated by default. The `screensaver` can be activated by setting the user preference `system.screen.stay_on` to the value `0`.

When the `screensaver` is activated, the default user inactivity timeout before entering into `screensaver` is defined by the `system.screen_off_timeout` user preference (default value in milliseconds: `60000`).

The AQS `screensaver` stops automatically when the user touches the screen.

⚠ The AQS `screensaver` is executed when there is no user activity detected. The AQS `screensaver` can not be executed while a media with video is played in your main App (video track, web TV URI, MS-PowerPoint presentation with video). When no media with video is played anymore, the AQS `screensaver` is executed after the `system.screen_off_timeout` duration. When the AQS `screensaver` is executed, playing a media with video again in your main App doesn't stop the screensaver. In this case, the audio of the media with video may persist during the AQS `screensaver`.

⚠ Some third party APK or some built-in Apps like for example the `Media Folder Injector` APK, are designed to run with the AQS `screensaver` inactivated.

⚠ When the AQS `screensaver` is activated on your device, some third party App may be able to support either their own the `screensaver` or the AQS `screensaver`. For further information, contact support@qeedji.tech.

⚠ When the AQS `screensaver` is activated, the third party App must support properly the modification of their activities like `onPause()`, `onStart()`, `onResume()`, `onStop()` else the third party App may be not able to restart properly after exiting AQS `screensaver` and may display a black content.

A custom AQS `screensaver` APK can be installed like any other APK and is designed to be executed automatically by the AQS as the same time as:

- one built-in Apps ,
- one third party APK.

☞ When installed properly, the custom AQS `screensaver` replaces the default AQS `screensaver`. Either the default AQS `screensaver` or the custom AQS `screensaver` can run at a time.

The custom `screensaver` APK must be developed by ISV. A custom `screensaver` APK example with its configuration script is available here [github av_stream_reader_screensaver APK](https://github.com/qeedji/qeedji-tizen-apps/tree/main/applications/qeedji-qmav-stream-reader-screensaver). Once the custom AQS `screensaver` APK is installed on the device, it is by default *activated* in the table of installed APK. But the custom AQS `screensaver` APK is not yet configured. To configure it, it is advised to use the configuration script related to the custom AQS `screensaver` APK [github av_stream_reader_screensaver 000000000000.js](https://github.com/qeedji/qeedji-tizen-apps/blob/main/applications/qeedji-qmav-stream-reader-screensaver/000000000000.js). Your third party App may have to call the `goToScreen()` API and `keepScreenOn()` API to decide when the AQS `screensaver` must run or not. For further information, refer the [TAB10b developer manual](#).

☞ The custom AQS `screensaver` APK cannot be restarted through the device configuration console web user interface because the startup of the AQS `screensaver` is handled by the AQS only as soon as no user activity has been detected for `<n>` seconds (60 by default).

☞ In this version, The running/stopped status of the `screensaver` APK is not consistent.

To deactivate the custom AQS `screen saver` APK, uncheck the custom AQS `screen saver` APK in the table of installed APK. After that, the default AQS `screensaver` becomes back the AQS `screensaver`.

This is the set of `screensaver` user preferences to restore the factory `screensaver` preferences:

| User preferences name | Default value | Information |
|--|---|---|
| <code>secure.screensaver_components</code> | <code>com.android.dreams.basic/com.android.dreams.basic.Colors</code> | default AQS screensaver (color gradient) |
| <code>secure.screensaver_enabled</code> | <code>1</code> | <code>1</code> : AQS screensaver enabled, <code>0</code> : AQS screensaver disable |
| <code>system.screen.stay_on</code> | <code>1</code> | <code>0</code> : allow AQS screensaver, <code>1</code> : do not allow AQS screensaver |
| <code>system.screen_off_timeout</code> | <code>120000</code> | <code>120000</code> : timeout value in ms before going into screensaver |

TestCard App

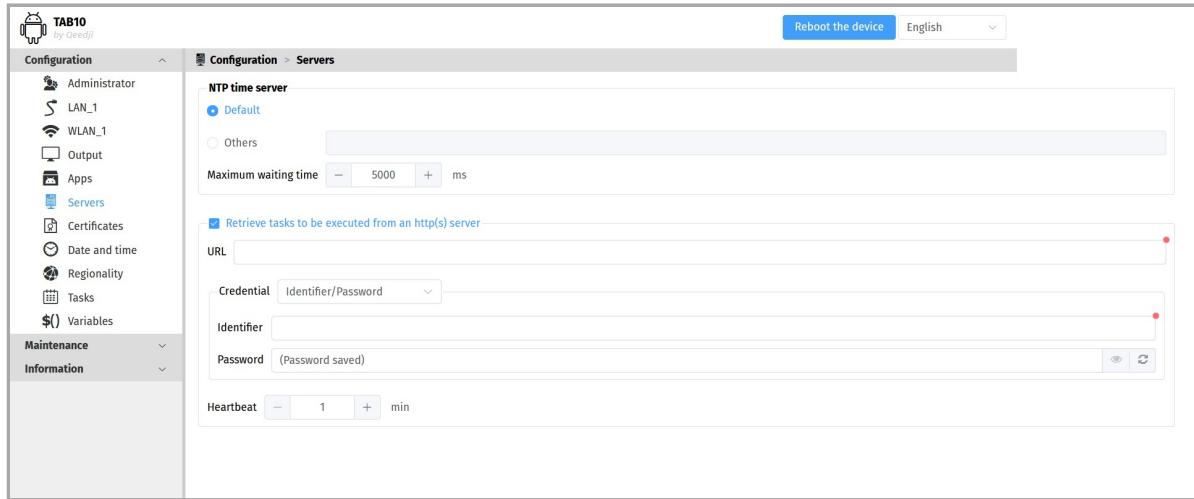
The `Test card` App, allowing to display the `Test Card` content, is not displayed in this table. To deactivate the `Test card` App launching at device start-up, refer to the chapter § [Maintenance > Test card](#).

4.1.6 Configuration > Servers

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

The NTP server input allows to either choose the default AQS NTP server¹ 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`.



In case the device must self-administrate from a HTTP server in terms of configuration upgrade, application installation or firmware update, you must activate the *Retrieve tasks to be executed from a http(s) server* then:

- enter the *URL* of your HTTP server,
 - for example:
 - `https://demo.http.server/administration/task.json`
 - `https://demo.http.server/administration?type=tasks`
- enter the *credential* type:
 - *None*,
 - *Identifier/password*:
 - enter the *Identifier* value,
 - enter the *Password* value,
- enter the *Heartbeat* value (default: 10 min), the periodic connection duration to your HTTP server.

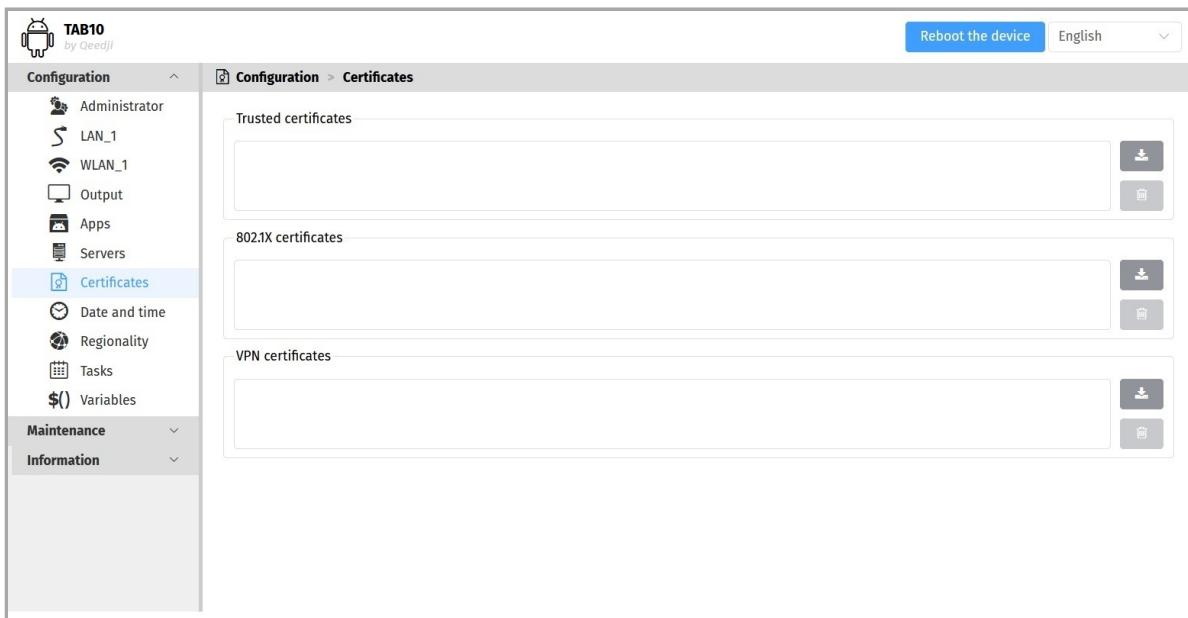
! This feature requires to own a HTTP server able to provide JSON content with appropriate tasks parameters. For further information, refer the chapter § [Appendix: HTTP server for AQS device self-administration] in the device developer manual.

4.1.7 Configuration > Certificates

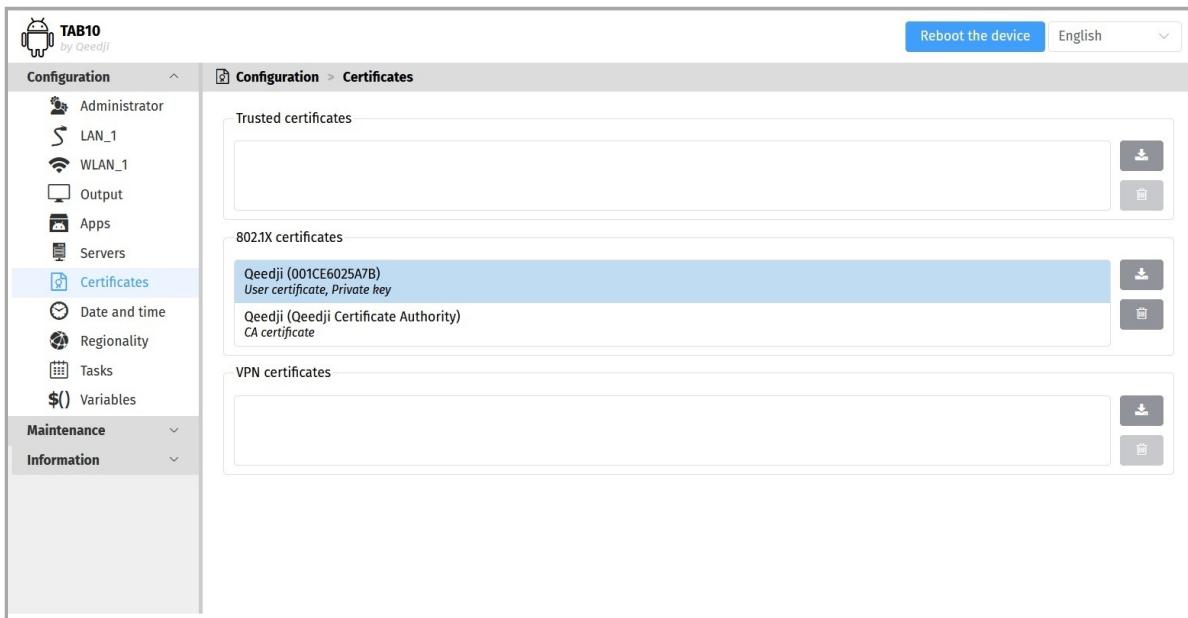
In the Configuration tab, select the **Certificates** menu to install:

- 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 TAB10b 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.

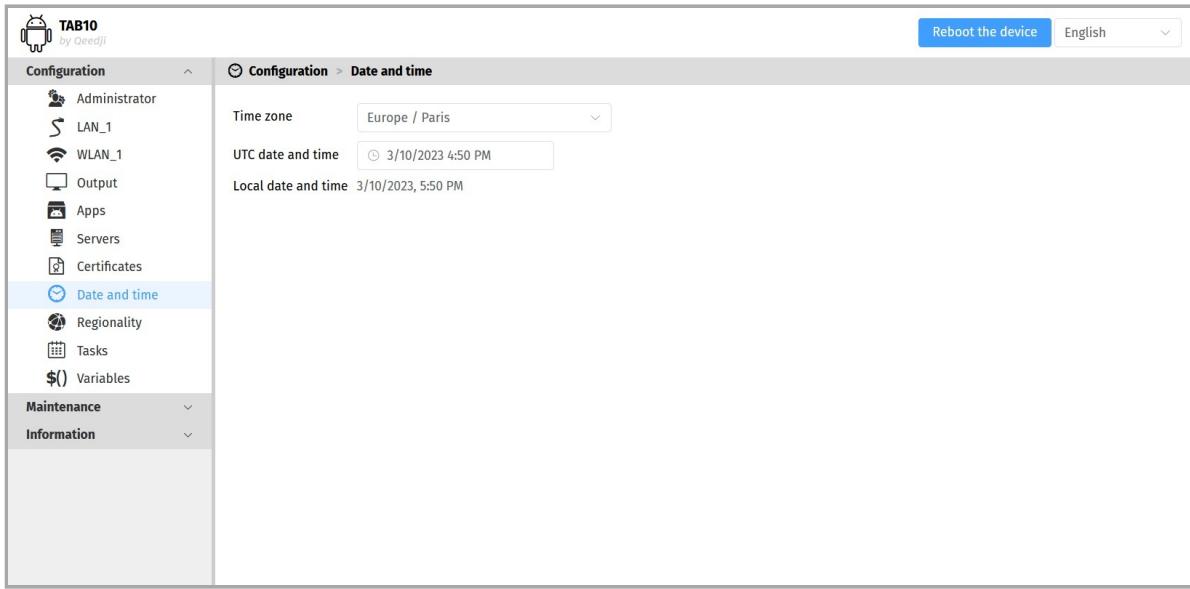
☞ When configuring EAP method with a configuration script, some of the 802.1X certificates (CA or/and user) not required anymore by the chosen EAP method will be deleted by the operating system from this pane. Consequently, when 802.1X CA certificates and/or 802.1X user certificates are required again with the chosen EAP method, it is advised to reinstall them with the configuration script as well.

☞ The autosigned certificates that must be trusted must be installed both in the Trusted certificates part and in the VPN certificates part.

4.1.8 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).



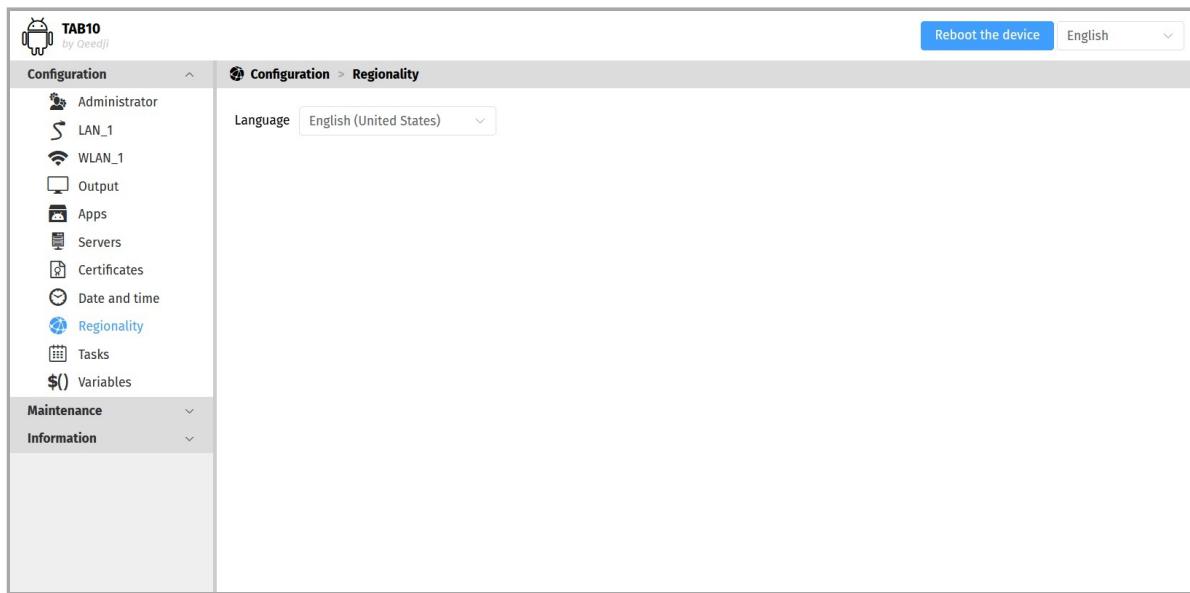
To update the date and time of your device, click on the **UTC Date and Time** value and then click on the **Now** button.

- ☞ The **Date and 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**.

If ever the device was not on time despite a right NTP configuration and right connection to the Web, check in the Android *Settings* application, in the menu *Date & time*, that the *Automatic date & time* parameter is activated. This parameter can be also set back by configuring the user preferences *global.auto_time* to 1 in the device configuration console web user interface.

4.1.9 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*.

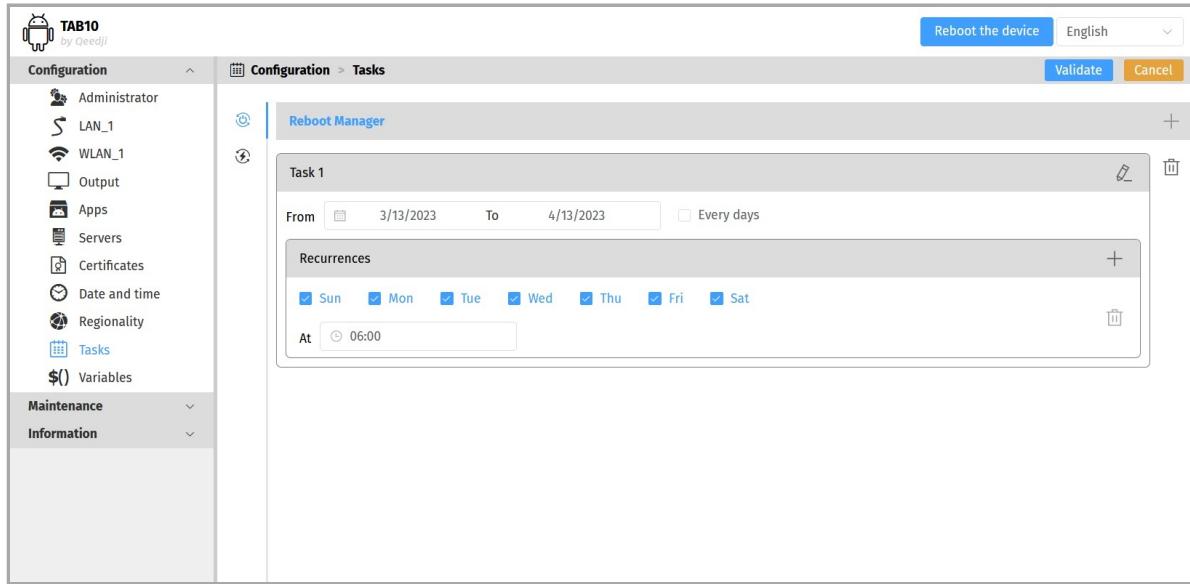
4.1.10 Configuration > Tasks

In the Configuration tab, select the **Tasks** menu to:

- program a reboot manager task,
- program a power manager task for the appliance to reduce its energy consumption.

Device reboot manager task

To create a reboot manager task, click on the  button then click on the  button.

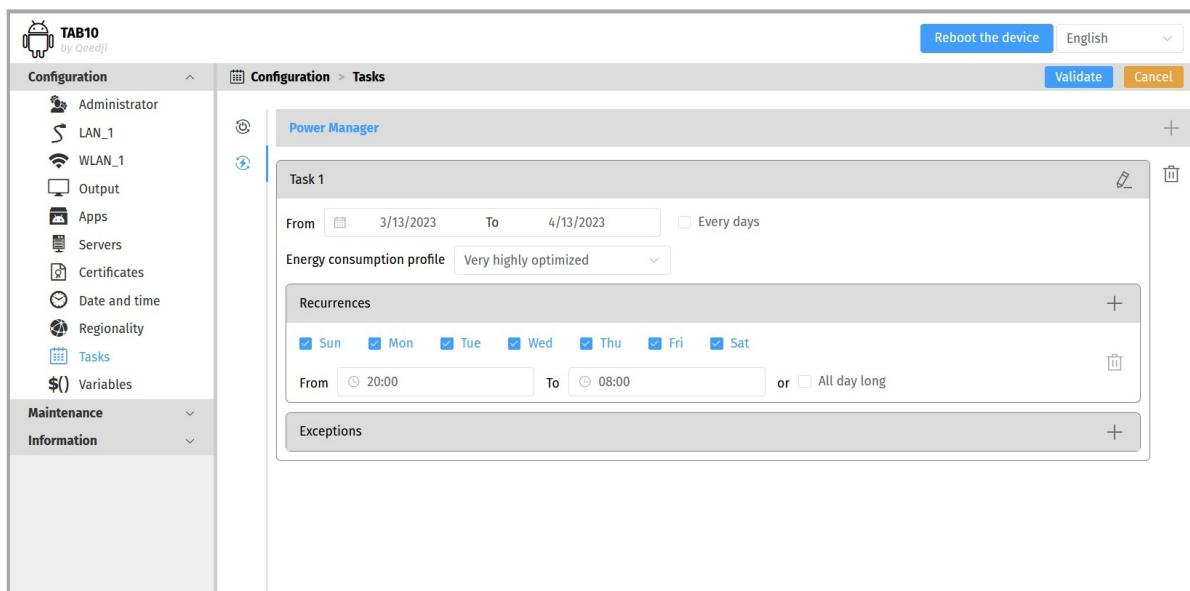


It is therefore possible to program several reboot occurrences.

 *The reboot tasks parameters are stored in an iCAL format in the `secure.reboot_calendar` user preference.*

Device power manager tasks

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



The two possible profiles values for the `power manager` task are:

- **Very highly optimized**,
- **Highly optimized**.

It is possible to create several `power manager` tasks within the same day.

- ☞ The `power manager` tasks parameters are stored into an `ICAL` format in the `secure.power_manager_calendar` user preference.
- ☞ During the device standby, the configuration upgrade through TFTP (DHCP/code 66) is effective but the associated information message cannot be seen on the screen.
- ☞ During the device standby, the device configuration update by USB storage device injection, the APK installation by USB storage device injection and the operation system upgrade by USB storage device injection keep supported. Setting the `persist.sys.power-manager.level.Low.externalstorage.copy.enable` user preference to `false` prevents the USB storage device injection to work during the device standby.
- ☞ During the device standby, at any time, making a short press on the `system` button allows to wake up automatically the device and exit the kiosk mode.
- ☞ During the device standby with the **VERY HIGHLY OPTIMIZED** profile, by default, touching the screen does not allow to wake up automatically the device. To work around, set the `persist.sys.power-manager.level.min.hid.pointer-event.enable` user preference to `true`. After a tap on the screen, if there is no user activity during the `persist.sys.power-manager.level.min.screen-off-timeout` (by default, sixty seconds), the device returns to `Device Sleep` mode. For further information refer to the chapter § [Power manager and Screen Saver modes](#).
- ☞ It is not recommended to keep two different activated Apps running with their own `Power Manager` strategy else the `Power Manager` task of the end-user App could not behave as expected.
- ☞ The `persist.sys.power-manager.device-sleep.level.default` allows to set the `Power Manager` profile that requested by the App: if its value is `min` (default value), the **Very highly optimized** value is applied for the `power manager` task requested by the App; if its value is `Low`, the **Highly optimized** value is applied for the `power manager` task requested by the App.
- ☞ In case, two `power manager` tasks with different profiles (i.e **Very highly optimized** and **Highly optimized**) are concurrents, meaning one requested by the App and one requested by the OS, the `power manager` task requested by the OS is priority.
- ☞ In case, two `power manager` tasks generated in this pane, with different profiles (i.e **Very highly optimized** and **Highly optimized**) are concurrents, meaning one requested by the App and one requested by the OS, the **Very highly optimized** `power manager` task is priority.
- ☞ When the end time of the `power manager` task is lower or equal to its start time, the `power manager` task runs automatically till the day after.
- ☞ During the device standby, the `Screen DIM` and the `Screen Saver` contents cannot be seen on the screen. For further information refer to the chapter § [Power manager and Screen Saver modes](#).
- ☞ During the device standby, the NFC tag badging and the 125KHz tag badging are deactivated.

This is the default set of `power manager` parameter values when a `power manager` task is executed:

- with the **Very highly optimized** profile:

| Function | Associated user preferences | Description |
|----------------------------------|--|-------------|
| Screen: off | system_properties.persist.sys.power-manager.level.min.display-output.power-mode = 0 | |
| Touch screen interactivity: no | system_properties.persist.sys.power-manager.level.min.hid.pointer-event.enable = false | |
| Volume mute: yes | system_properties.persist.sys.power-manager.level.min.sound-output.mute = true | |
| Volume level: 0 | system_properties.persist.sys.power-manager.level.min.sound-output.volume = 0 | |
| Backlight level ¹ : 0 | system_properties.persist.sys.power-manager.level.min.display-output.backlight = 0 | |

- with the *Highly optimized* profile:

| Function | Associated user preferences |
|-----------------------------------|---|
| Screen: on | system_properties.persist.sys.power-manager.level.low.display-output.power-mode = 1 |
| Touch screen interactivity: yes | system_properties.persist.sys.power-manager.level.low.hid.pointer-event.enable = true |
| Volume mute: no | system_properties.persist.sys.power-manager.level.low.sound-output.mute = false |
| Volume level: 50 | system_properties.persist.sys.power-manager.level.low.sound-output.volume = 50 |
| Backlight level ¹ : 50 | system_properties.persist.sys.power-manager.level.low.display-output.backlight = 50 |

 *The Very highly optimized profile with its default configuration is suitable for most of case.*

¹ The backlight level from 0 to 100 allows to adjust the screen transparency. When the transparency is at its minimum, i.e value 0, the content can still be seen by transparency.

4.1.11 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.

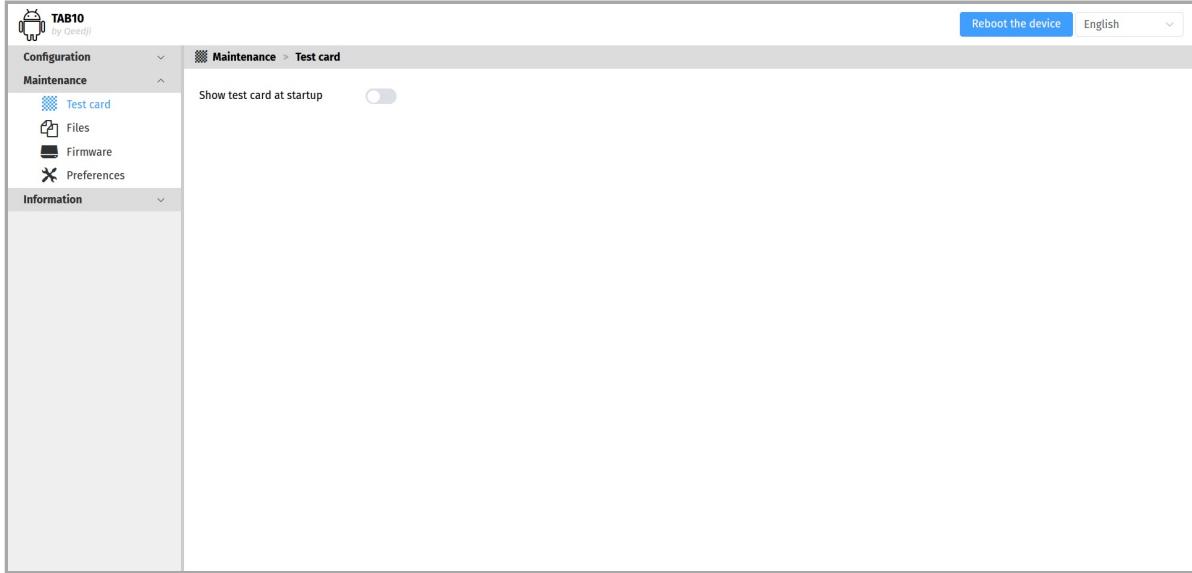
4.1.12 Maintenance > Test card

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

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

To activate the Test Card App launching at device start-up, set the **Test card** toggle button to *activated*. To not activate the **Test Card** App launching at device start-up, set the **Test card** toggle button to *deactivated*.

! The test pattern content is not displayed by default at device start-up when it is coming straight from factory. For further information about the test pattern content, refer to the chapter § [Test card](#).



! When the *Test card* App is executed at device start-up, the other activated App starts to be executed only one minute after the *Test card* content has started to be displayed. When the *Test card* content is displayed, the user cannot access to AQS desktop by pressing on the *system* button .

! The displaying of the IP V6 address value starting with the prefix `fe80::` is not supported in the Test Card content. For further information, contact your IT department so that your network is advertising the IP V6 address with another prefix (ex: `fc00::`).

4.1.13 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.

| Name | Size |
|----------------|------|
| .apps | - |
| .configuration | - |
| .data | - |
| .software | - |

These are the available WebDAV directories:

- `.apps` : directory allowing to upload APK and install it on the TAB10b 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 TAB10b device.

When an App is uninstalled from the device, the data related to it are not removed automatically. For disk space saving reasons, after an App uninstallation, it is recommended to remove the entire subdirectory related to the uninstalled App in the `.data` WebDAV directory.

Operating system upgrade

The AQS firmware can be upgraded by pushing a new firmware file `aosp_qeedji-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 console 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:

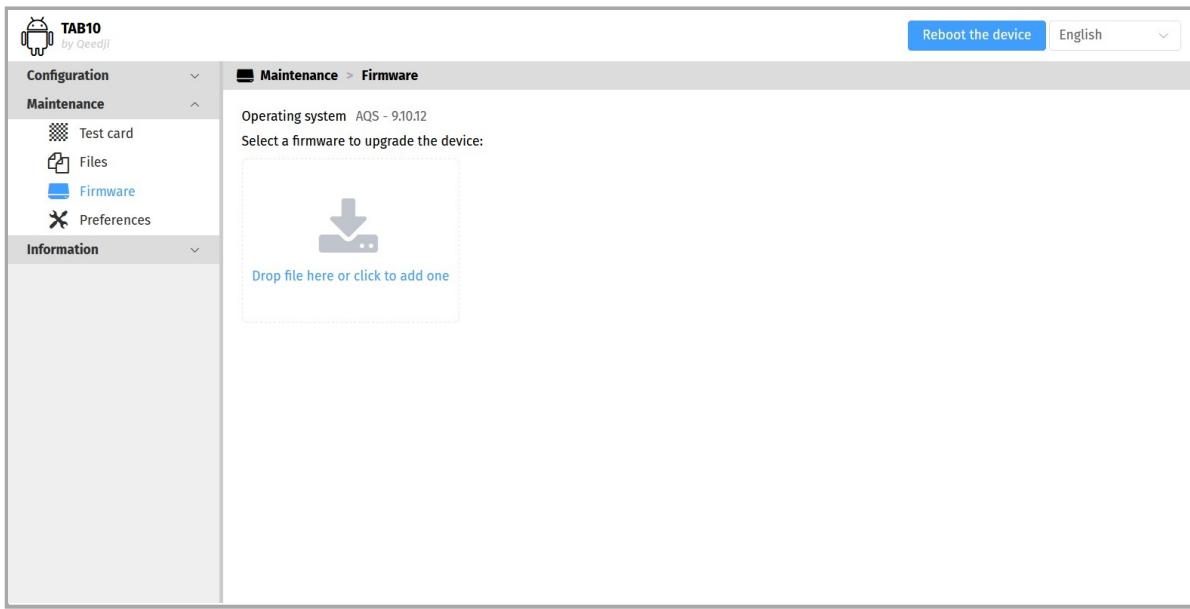
- edit the `000000000000.js` configuration script and uncomment/modify the appropriate lines according to your needs,
- rename the configuration script if required,
- once saved, drop it in the WebDAV directory like explained above,
- when suitable for your device, save it preciously for future use.

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

4.1.14 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 version of your device. Wait a few minutes, the time to install the new AQS operating system version. Go back to the device configuration console 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?TAB10/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**.

4.1.15 Maintenance > Preferences

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

The screenshot shows the Qeedo app interface with the following details:

- Top Bar:** TAB10 by Qeedo, Reboot the device, English dropdown.
- Left Sidebar:** Configuration (Test card), Maintenance (Files, Firmware, Preferences), Information (Boot count).
- Main Content:** Title: Maintenance > Preferences. A Filter input field is present. A list of preference names is shown, starting with:
 - global.adb_enabled
 - global.add_users_when_locked
 - global.airplane_mode_on
 - global.airplane_mode_radios
 - global.airplane_mode_toggleable_radios
 - global.assisted_gps_enabled
 - global.audio_safe_volume_state
 - global.auto_time
 - global.auto_time_zone
 - global.bluetooth_disabled_profiles
 - global.bluetooth_on
 - global.boot_count
 - global.call_auto_retry
 - global.car_dock_sound
 - global.car_undock_sound
 - global.cdma_cell_broadcast_emc

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.

4.1.16 Information > Device

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

The screenshot shows the Qeedji Management interface with the 'Device' menu selected under the 'Information' tab. The main panel displays the following device information:

| Information | Value |
|------------------|--------------------------------------|
| Operating system | AQS - 9.10.19 |
| Model | TAB10b |
| Device name | TAB10b |
| Hostname | TAB10b |
| MAC Id | 00:1C:E6:02:5A:7B |
| UUID | 0a200001-0000-0000-0000-001ce6025a7b |
| PSN | 01620-00001 |

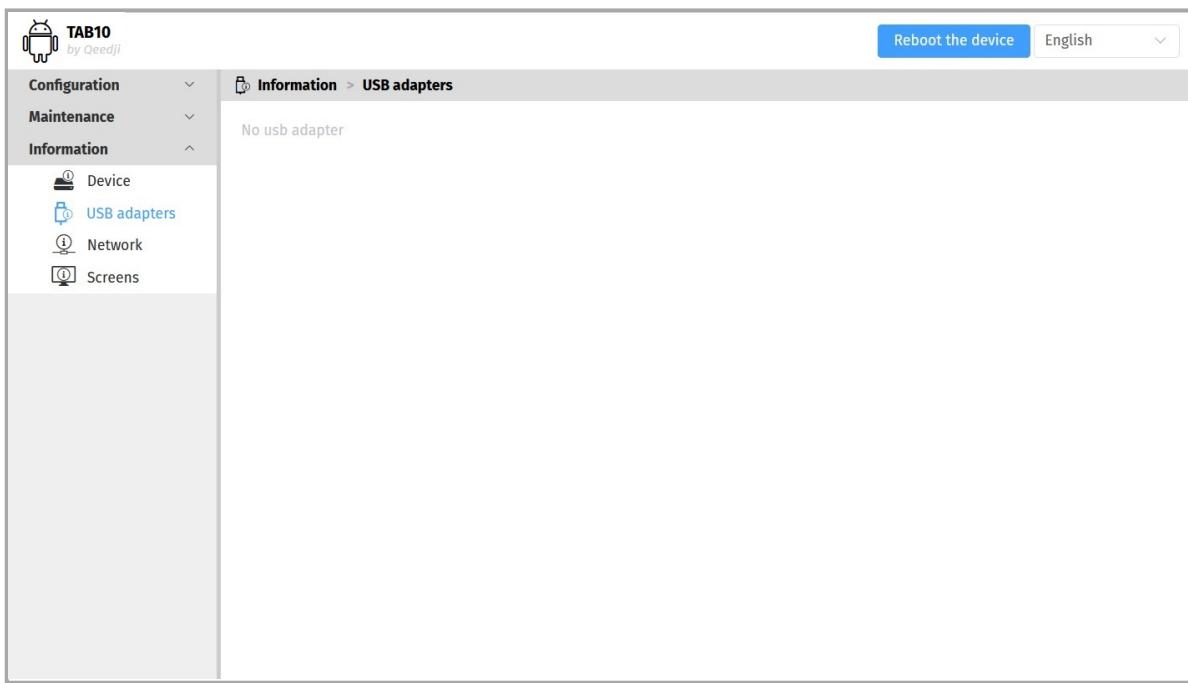
Below the information table, there is a note: "Capture video output on Friday, January 19, 2024 at 12:34:37 PM" followed by a camera icon and a blue capture button. The bottom right corner of the main panel has a watermark that says "Qeedji".

- **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.

4.1.17 Information > USB adapters

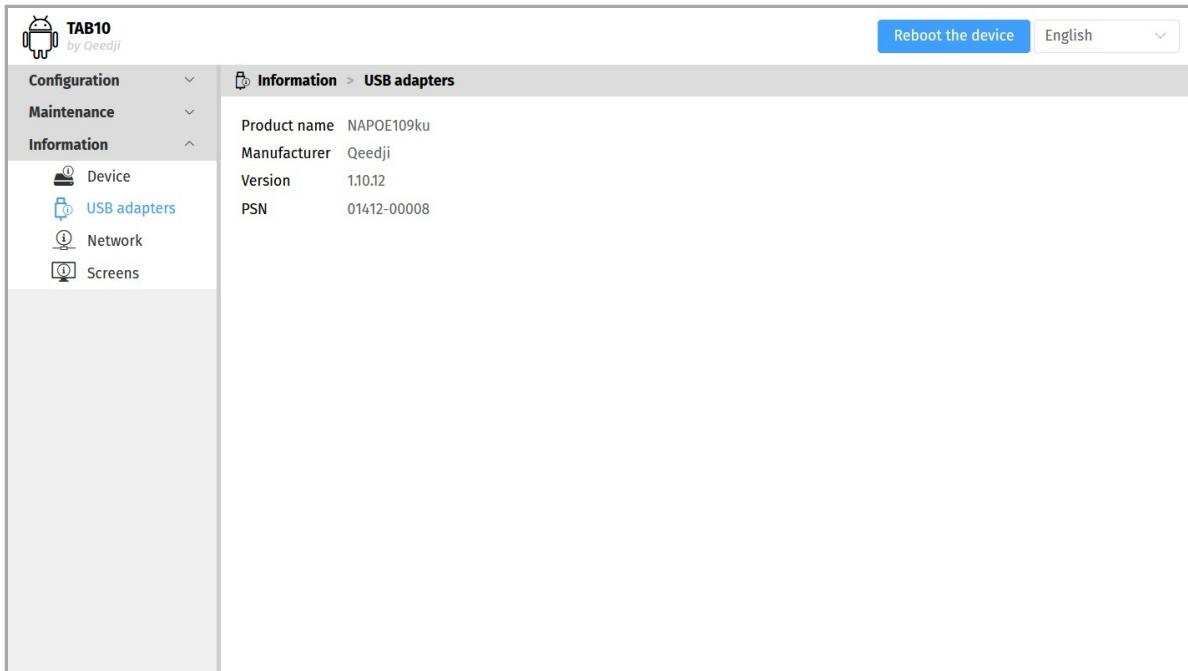
In the **Information** tab, select the **USB adapters** menu to see the product name and manufacturer name of the USB adapter devices connected to the TAB10b device.

This is an example of content when the TAB10b device is supplied by a standard USB-C wall-plug and connected to a WiFi network.



The screenshot shows the Qeedji web interface for the TAB10 device. The top navigation bar includes a logo for 'TAB10 by Qeedji', a 'Reboot the device' button, and a language selection dropdown set to 'English'. The left sidebar has a tree view with 'Configuration', 'Maintenance', and 'Information' expanded. Under 'Information', 'USB adapters' is selected, indicated by a blue icon and highlighted text. The main content area is titled 'Information > USB adapters' and contains the message 'No usb adapter'.

This is an example of content when the TAB10b device is supplied by a NAPOE109ku Ethernet adapter which is connected to a PoE switch.



The screenshot shows the Qeedji web interface for the TAB10 device. The top navigation bar includes a logo for 'TAB10 by Qeedji', a 'Reboot the device' button, and a language selection dropdown set to 'English'. The left sidebar has a tree view with 'Configuration', 'Maintenance', and 'Information' expanded. Under 'Information', 'USB adapters' is selected. The main content area is titled 'Information > USB adapters' and displays the following details:

| | |
|--------------|-------------|
| Product name | NAPOE109ku |
| Manufacturer | Qeedji |
| Version | 1.10.12 |
| PSN | 01412-00008 |

4.1.18 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 TAB10b device is supplied by a standard USB-C wall-plug and connected to the WIFI network.

The screenshot shows the 'Information > Network' pane for the TAB10b device. The left sidebar has sections for Configuration, Maintenance, and Information, with 'Network' selected. The main pane displays network settings:

| NTP time server | |
|-----------------|--|
| NTP Server | |

| WLAN_1 | |
|-----------------|---------------------------------|
| Mac address | 00:1C:E6:02:5A:7B |
| Ip v4 addresses | 192.168.1.183/17 [Auto] |
| Ip v6 addresses | fe80::21c:e6ff:fe02:5a7b/64 |
| Default gateway | 192.168.0.1 [Auto] |
| State | connected |
| SSID | Innes_R&D_2.4Ghz |
| DNS Servers | 192.168.0.4, 192.168.0.1 [Auto] |

This is an example of pane content when the TAB10b device is supplied by a NAPOE109ku Ethernet adapter which is connected to a PoE switch, which is not connected to the network. The TAB10b device is connected to the WIFI network.

The screenshot shows the 'Information > Network' pane for the TAB10b device. The left sidebar has sections for Configuration, Maintenance, and Information, with 'Network' selected. The main pane displays network settings:

| NTP time server | |
|-----------------|--|
| NTP Server | |

| LAN_1 | |
|-----------------|-----------------------------|
| Mac address | 00:1C:E6:02:56:94 |
| Ip v4 addresses | |
| Ip v6 addresses | fe80::21c:e6ff:fe02:5694/64 |
| Default gateway | |
| State | connected |
| DNS Servers | |

| WLAN_1 | |
|-----------------|---------------------------------|
| Mac address | 00:1C:E6:02:5A:7B |
| Ip v4 addresses | 192.168.1.183/17 [Auto] |
| Ip v6 addresses | fe80::21c:e6ff:fe02:5a7b/64 |
| Default gateway | 192.168.0.1 [Auto] |
| State | connected |
| SSID | Innes_R&D_2.4Ghz |
| DNS Servers | 192.168.0.4, 192.168.0.1 [Auto] |

This is an example of content when the TAB10b device is supplied by a NAPOE109ku Ethernet adapter which is connected to a PoE switch, which is connected to the network.

The screenshot shows the configuration interface for the TAB10b device. The left sidebar has sections for Configuration (Administrator, LAN_1, WLAN_1, Output, Apps, Servers, Certificates, Date and time, Regionality, Tasks, Variables), Maintenance, and Information. The main area is titled 'Information > Network'. It shows 'NTP time server' settings (NTP Server) and detailed network configurations for 'LAN_1' and 'WLAN_1'. For LAN_1, the Mac address is 00:1C:E6:02:56:94, IP v4 addresses are 192.168.1.85/17 [Auto], IP v6 addresses are fe80::21ce:6ff:fe02:5694/64, Default gateway is 192.168.0.1 [Auto], State is connected, and DNS Servers are 192.168.0.4, 192.168.0.1 [Auto]. For WLAN_1, the Mac address is 00:1C:E6:02:5A:7B, IP v4 addresses are listed but not specified, IP v6 addresses are listed but not specified, Default gateway is listed but not specified, State is not connected, SSID is listed but not specified, and DNS Servers are listed but not specified.

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::21ce:6ff: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 | |

4.1.19 Information > Screens

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

The screenshot shows the Qeedi web interface for a TAB10 device. The top navigation bar includes a logo for 'TAB10 by Qeedi', a 'Reboot the device' button, and a language selection dropdown set to 'English'. The left sidebar has sections for 'Configuration', 'Maintenance', and 'Information', with 'Information' expanded to show 'Device', 'USB adapters', 'Network', and 'Screens'. The main content area is titled 'Information > Screens' and displays 'Screen #1' with the following details: 'Screen resolution 1280X800 (60Hz)' and 'Rotation 0°'.

Part V

Built-in Apps

5.1 Media Folder Injector

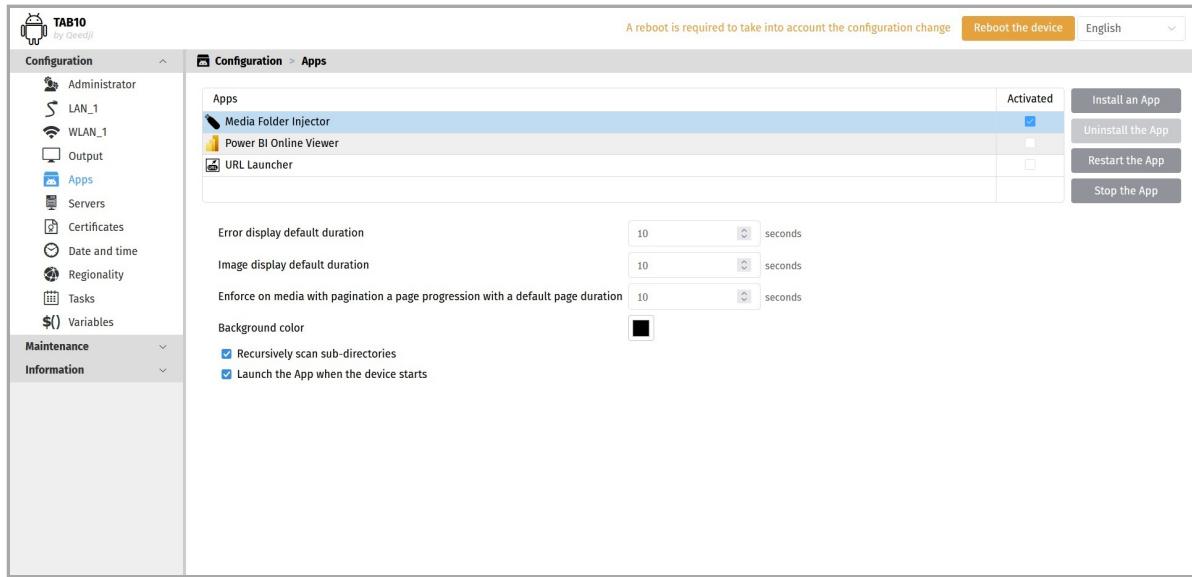
⚠ It is advised to activate only one built-in Apps or only one third party APK at a time.

| Name | Version | Description |
|-----------------------|---------|---|
| Media folder Injector | 1.10.12 | Allows to play the content copied from an USB storage device. The USB storage device must be inserted in the device then removed from the device each time the content must be updated. |

The form of the Media Folder Injector APK contains several configuration fields:

- Error display default duration : allows to configure the duration of the error message displayed for example when the media is not supported,
- Image display default duration : allows to set the display duration for images,
- Enforce on media with pagination a page progression with a default page duration : allows to set a time per page for pages that have not a defined one,
- Background color : allows to define the content background color (default value: black color),
- Recursively scan sub-directories : if not checked, this option allows to play only the media located at the root of the USB storage device. If checked, it allows to play also the medias located in the folders of the USB storage device,
- Launches the App when the device starts : if checked, this option allows to start automatically the App when the device starts.

After having modified a form's parameter value, the App must be restarted or the device restarted so that the modification are taken into account.



- Only these viewable medias are supported:
 - videos: .mp4, .m4v, .webm,
 - images: .jpg, .png, .svg, .gif
 - presentations: *.pdf, *.pptx*, *.ppsx*,
 - HTML widgets: .maff, .wgt.
- Consequently, the audio medias (.mp3, .m4a) are not supported by the Media folder Injector APK.
- When the media is not supported, these errors can be raised:
 - Content temporarily unavailable (code 0): this kind of media is not supported. Remove this media from your content.
 - Content temporarily unavailable (code 4): this media not supported by your device. Remove this media from your content.
- Each viewable medias is played until it is ending. The viewable medias must have an intrinsic duration to have a determinist end time.
- Do consider that .html or .htm files are not supported. Indeed, when this kind of file is played, it never ends.
- When all the medias have been played once, the APK restarts to play the first one.
- When a new content is available in the USB storage device, all the obsolete medias and all the obsolete folders are removed from the device and the new ones are copied on the device.
- When the Media Folder Injector APK is launched, the medias located at the root of the USB storage device and the medias located in the folders are copied then played in the alphabetical order. A folder name is considered as playfolder of medias to play, consequently the names of the folders are also evaluated to define the alphabetic sorting. If you want to control the order of the medias playback, it is not advised to have a folder depth greater than one folder. When the media name has a number as prefix, the entire number prefix is evaluated to determine the alphabetical sorting.
- The viewable medias can be stored at the root of the USB storage device or in some folders. When the Recursively scan sub-directories option is deactivated, only the medias located at the root of the USB storage device are played. When there is no media to play at the root in this case, a message is displayed on the screen: *Information: no content*.
- When an empty USB storage key is inserted in the device, the medias are all removed from the device then a message is displayed on the screen: *Information: no content*.
- When a 000000000000.js or a configuration.js script, an .apk file, or a .fqs firmware file is found at the root of the USB storage device, the copy of the medias cannot be done, consequently the Media Folder Injector APK cannot update its content with the USB storage device's one.

5.2 Power BI Online Viewer

⚠ It is advised to activate only one built-in `Apps` or only one third party APK at a time.

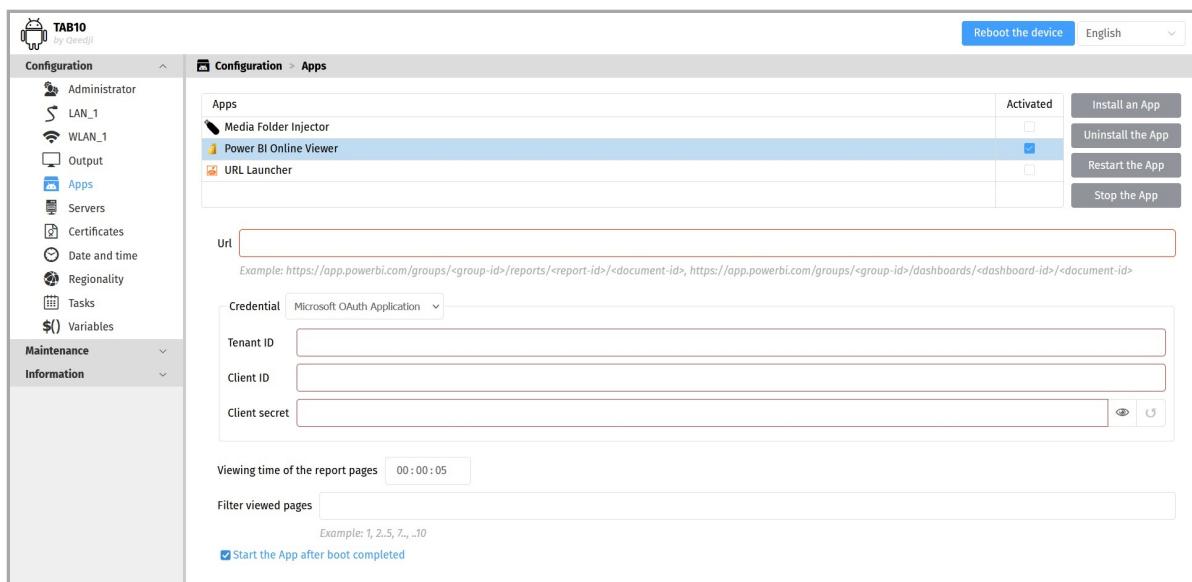
| Name | Version | Description |
|------------------------|---------|---|
| Power BI Online Viewer | 1.10.12 | Allows to view a <i>Power BI</i> report URL or a <i>Power BI</i> dashboard URL. |

The available credential type values are:

- Microsoft OAuth User : the Microsoft 365 *identifier* and *password* and these Azure AD application parameters are required to access to the resource (web page):
 - Tenant ID ¹,
 - Client ID ¹,
 - Secret ID ¹,
 - Username ,
 - Password .
- Microsoft OAuth application : these Azure AD application parameters are required to access to the resource (web page):
 - Tenant ID ¹,
 - Client ID ¹,
 - Secret ID ¹,

In the Url field, paste the URL of:

- your *Power BI* report:
 - this is a *Power BI* report URL example:
 - <https://app.powerbi.com/groups/d1119fde-7bb0-4642-b367-898a0450062c/reports/259ddad1-eec8-4003-9b43-290f40e68c5d> / (fake)
- your *Power BI* dashboard:
 - this is a *Power BI* dashboard URL example:
 - <https://app.powerbi.com/groups/d2e637a2-268e-4739-93b3-945692cd2c84/dashboards/d01ce209-87cc-4669-a864-33a5b3029b28> / (fake)



¹ An Azure AD application must be created with Microsoft Power BI administration account to allow third party applications to access to the Power BI reports and to the Power BI dashboards stored in your Microsoft Power BI workspace. For further information, refer to the chapter § Appendix: Microsoft Azure AD portal for Microsoft Power BI application.

The `Viewing time of the report pages` allows to set the viewing duration per report page.

☞ The `Viewing time of the report pages` parameter is not taken into account when visualizing a Power BI dashboard.

The `Filter viewed pages`, when matching the following syntax, allows to display only some of the report pages:

- if no filtering value is set, all the pages of the report are viewed
- e.g. 1..3: allows to display the report from the page 1 to the page 3
- e.g. 1, 5: allows to display only the page 1 and the page 5 of the report
- e.g. 2..: allows to display the report from the page 2 to the last page
- e.g. ..10: allows to display the report from the first page to the page 10

- The `Filter viewed pages` parameter is not taken into account when visualizing a Power BI dashboard.
- The viewing of reports only available on your `Microsoft Power BI Desktop` are not supported on the devices. A pro license is required for your `Power BI Desktop` to publish your report on your `Microsoft Power BI workspace`.
- The information message `Error - Invalid configuration` means that the `Power BI Online Viewer` APK has been activated but the inputs of the `Power BI Online Viewer` form have not been filled properly.
- The information message `Error - Unable to show Power BI report (error HTTP 404)` means that the Azure AD application can not find the report or the dashboard in the workspace. The information message `Error - Unable to show the Power BI report (error HTTP 401)` OR `Error - Unable to show the Power BI report (error HTTP 400)` means that either some parameter values of the Azure AD application parameters are wrong, or some rights are missing to view the report.
- The data of Power BI dashboards visuals based on the `API{}` mode of the realtime data streaming semantic model can be updated only when using the `Microsoft OAuth application` credential type.
- The information message `Error - Unable to show Power BI report (error HTTP0)` means that the device has lost network connectivity.

5.3 URL Launcher

⚠ It is advised to activate only one built-in Apps or only one third party APK at a time.

| Name | Version | Description |
|--------------|---------|--|
| URL Launcher | 1.10.20 | Allows to play a web page hosted on a simple web server. |

The form of the URL launcher APK contains several configuration fields:

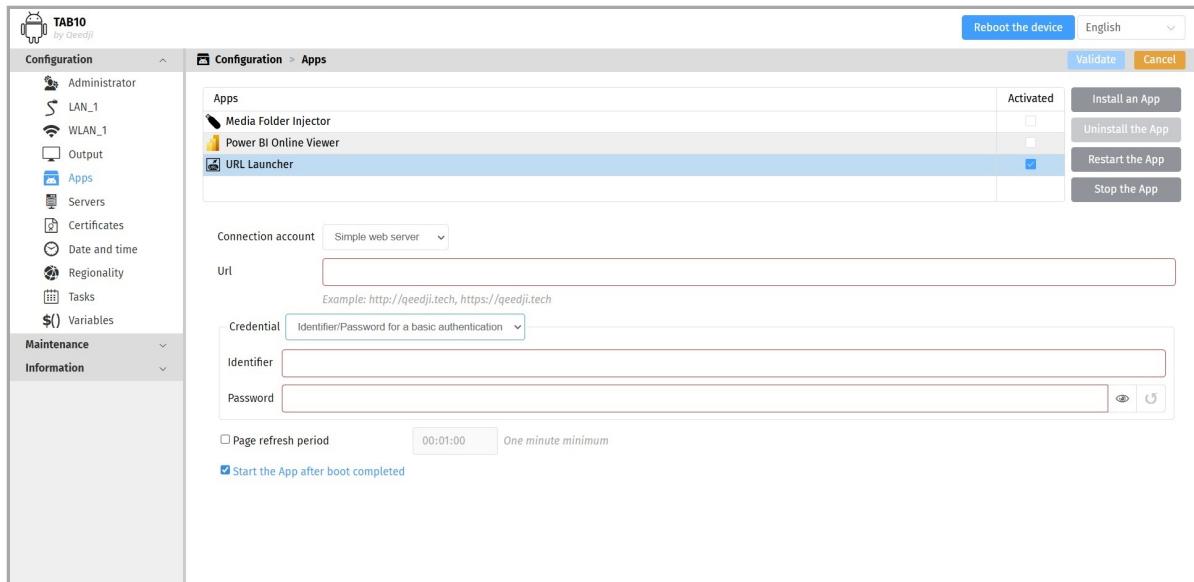
- Connection account :
 - Simple web server,
- Url : URL of the web page,
- Credential :
 - none,
 - Username/password for a basic authentication
 - Identifier : credential username to access to the web page,
 - Password : credential password to access to the web page,
 - Username/password for a webpage form
 - Identifier : credential username to access to the web page,
 - Password : credential password to access to the web page,
- Page refresh period : refresh the web page content every period value,
- Launches the App when the device starts : if checked, this option allows to start automatically the App when the device starts.

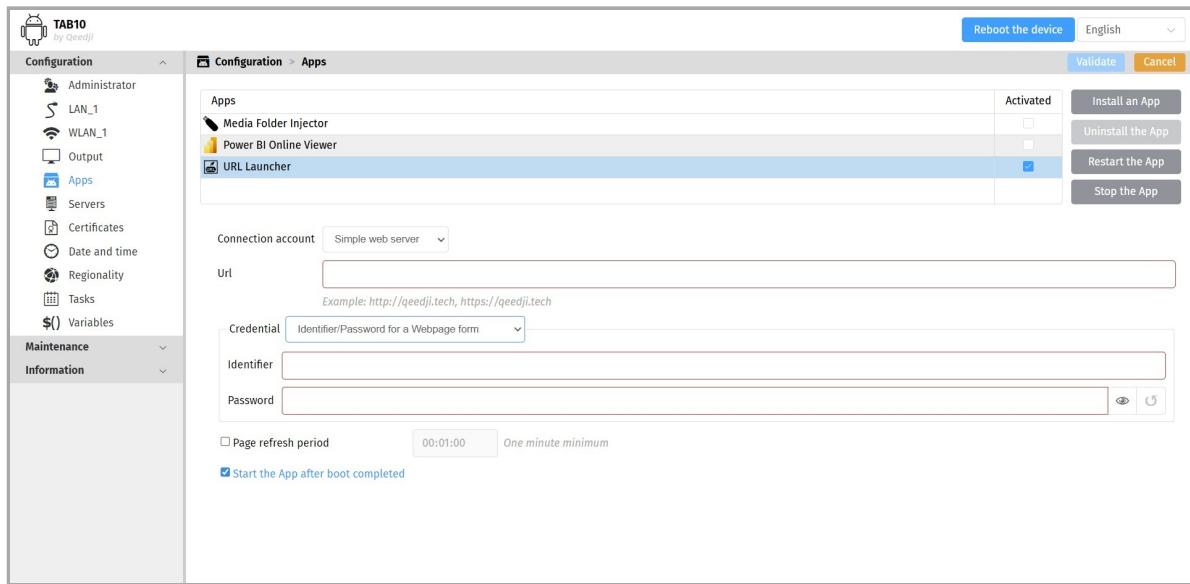
➥ Swiping is supported in the URL launcher V1.10.19 (and above version).

➥ Older version of URL launcher installed manually by the end user may be displayed as well. It is advised to remove it.

Swiping may be inactivated in some others custom App.

After having modified a form's parameter value, the App must be restarted or the device restarted so that the modification are taken into account.



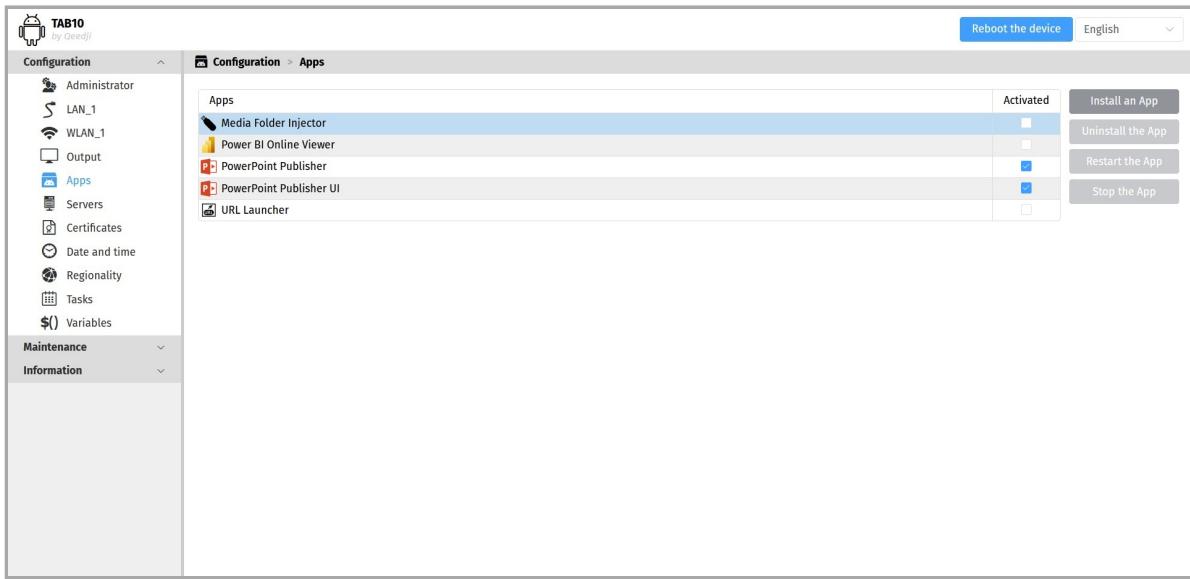


With the native `chromium Web engine` of AQS 9, the URL launcher APK is able to display properly the content of Website supporting the `X-Frame-Options` HTTP response header.

5.4 Qeedji PowerPoint Publisher for Media Players

 It is advised to activate only one built-in Apps or only one third party APK at a time.

The Qeedji PowerPoint Publisher for Media Players App is installed automatically when publishing your PowerPoint presentation from your MS-PowerPoint supporting the Qeedji PowerPoint Publisher for Media Players addin.



For further information, refer to the chapter § [Appendix: Qeedji PowerPoint Publisher for Media Players](#).

Part VI

Technical information

6.1 Technical specifications

Model Manufacturer :-- :-: TAB10b 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 NAPOE109ku , NAPOE109kt or NAPOE109ft model accessories, as it is fully qualified with the TAB10b device. For standard USB power supply adaptor, select a 5 V / 3 A capable device. |

¹ For TAB10b 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 ¹ | microSD 15 x 11 x 1 mm (0.59 x 0.43 x 0.04") |

¹ The device may support micro SD card whose memory size is upper than 16 GB. For further information, contact sales@qeedji.tech.

| 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 |

| 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 TAB10b 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 (1,585 lb) | 255 mm x 178,5 mm x 10,8 mm (10,0" x 7,0" x 0,393") |

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

| Warranty |
|-----------------|
| 1 year |

6.2 Built-in RFID reader

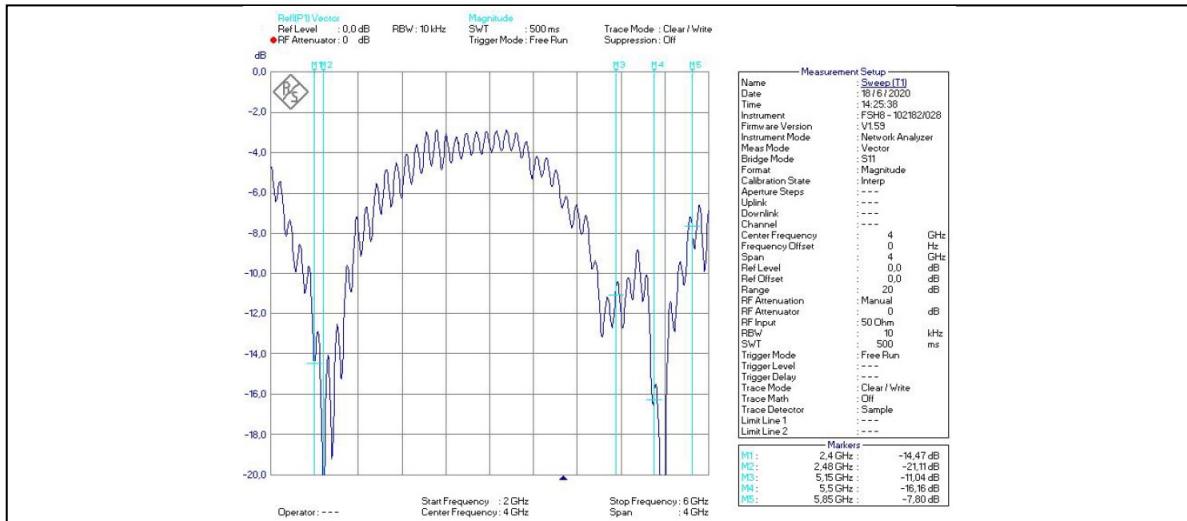
The device TAB10b has a badge reader allowing to recognize the badges supporting the RFID/NFC technology.

| 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.

6.3 Antenna return loss

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



6.4 Conformities

EUROPE

In conformity with the following European directives:

- LVD 2014/35/EU ,
- EMC 2014/30/EU ,
- RED 2014/53/EU .

Part VII

Contacts

7.1 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
INOVELEC INNES SA
5A rue Pierre Joseph Colin
35700 RENNES

Tel: +33 (0)2 23 20 01 62

Part VIII

Appendix

8.1 Appendix: Qeedji PowerPoint Publisher for Media Players

This appendix explains how to publish .pptx MS-Powerpoint presentation on TAB10b devices using your MS-Office PowerPoint, on which the Qeedji PowerPoint Publisher For Media Players PowerPoint Add In is installed.

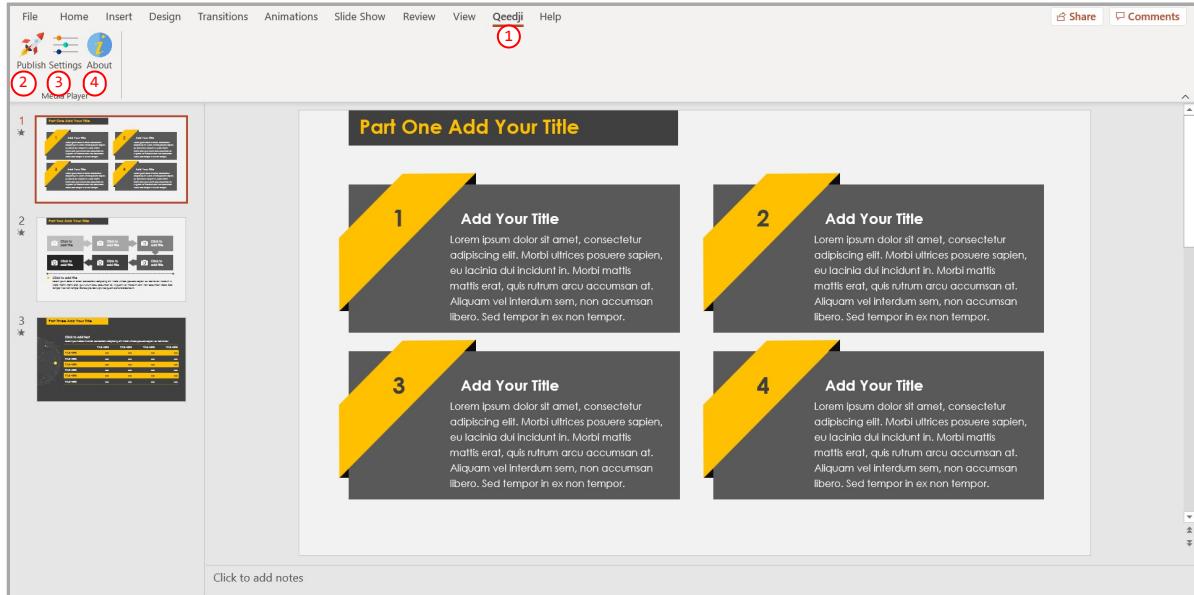
- *The Qeedji PowerPoint Publisher For Media Players PowerPoint Add In can deal with several TAB10b devices with the same MS-PowerPoint presentation.*
- *The TAB10b device needs to be purged from any other existing APK.*

Qeedji PowerPoint Publisher For Media Players: installation

- Choosing Everyone may require to run the PowerPoint with the Administrator rights to be able to deactivate 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 may 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

To remove the Qeedji PowerPoint Publisher for Media Players addin from your MS-Windows, use the Add or remove programs MS-Windows menu, then remove the program Qeedji PowerPoint Publisher for Media player.

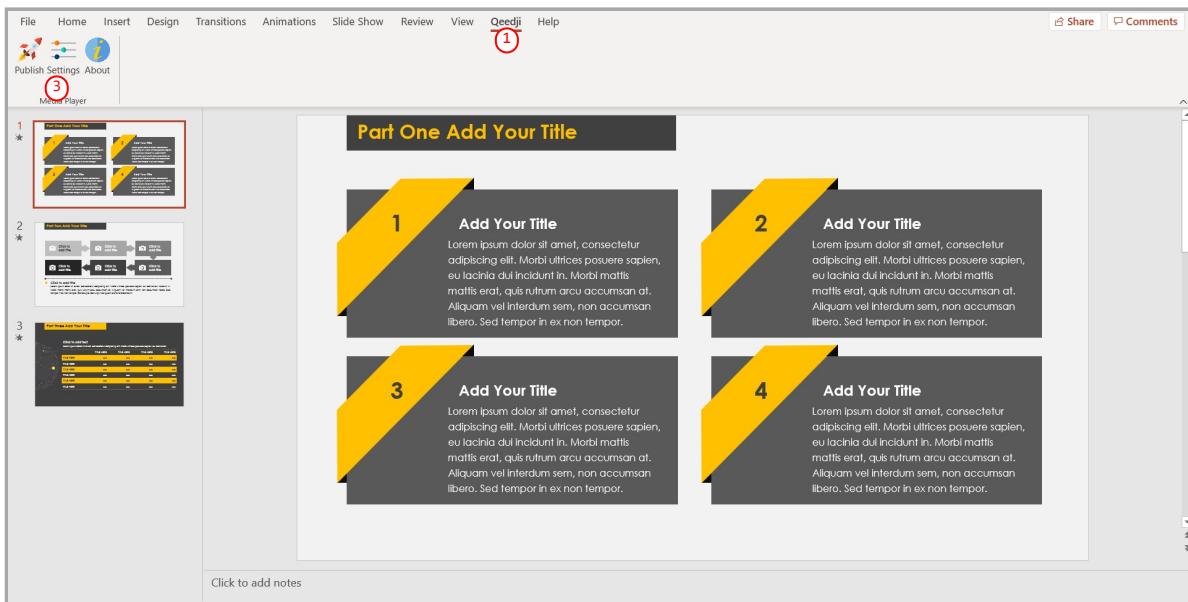
Qeedji PowerPoint Publisher For Media Players: upgrade/downgrade

Before installing a new Qeedji PowerPoint Publisher For Media Players version, it is advised to:

- close MS-PowerPoint then,
- uninstall the previous MS-PowerPoint add-in version.

- In case the version in the About pane of the Qeedji PowerPoint Publisher For Media Players is not corresponding the Qeedji PowerPoint Publisher For Media Players version just installed, disconnect from Office 365 then sign in again.

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

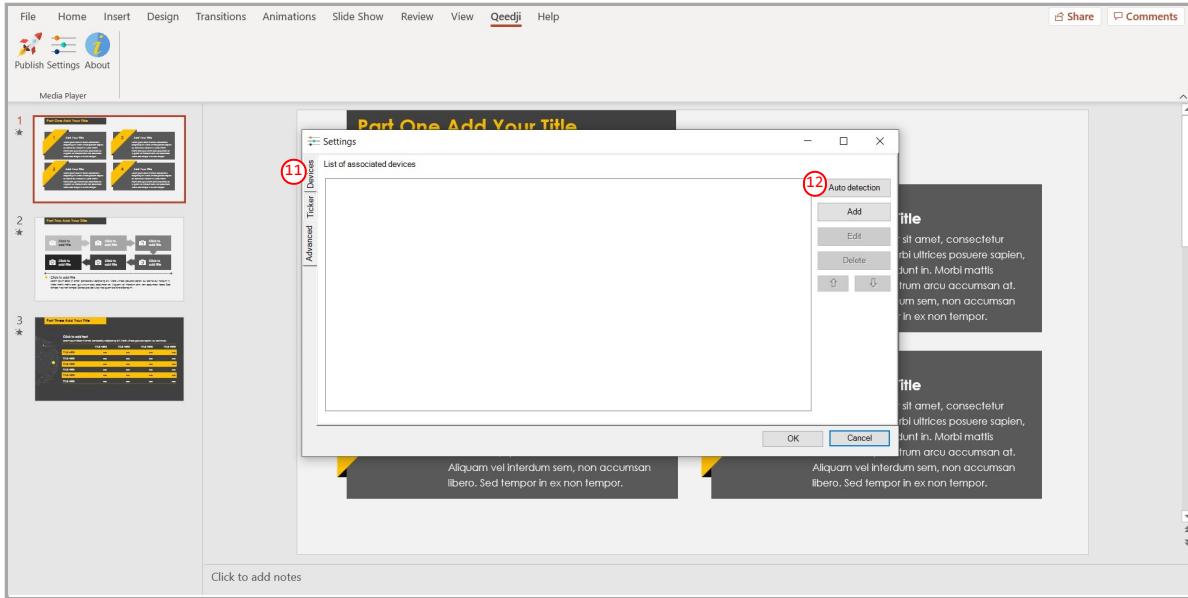


To register one or several TAB10b devices, open your MS-PowerPoint presentation then:

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

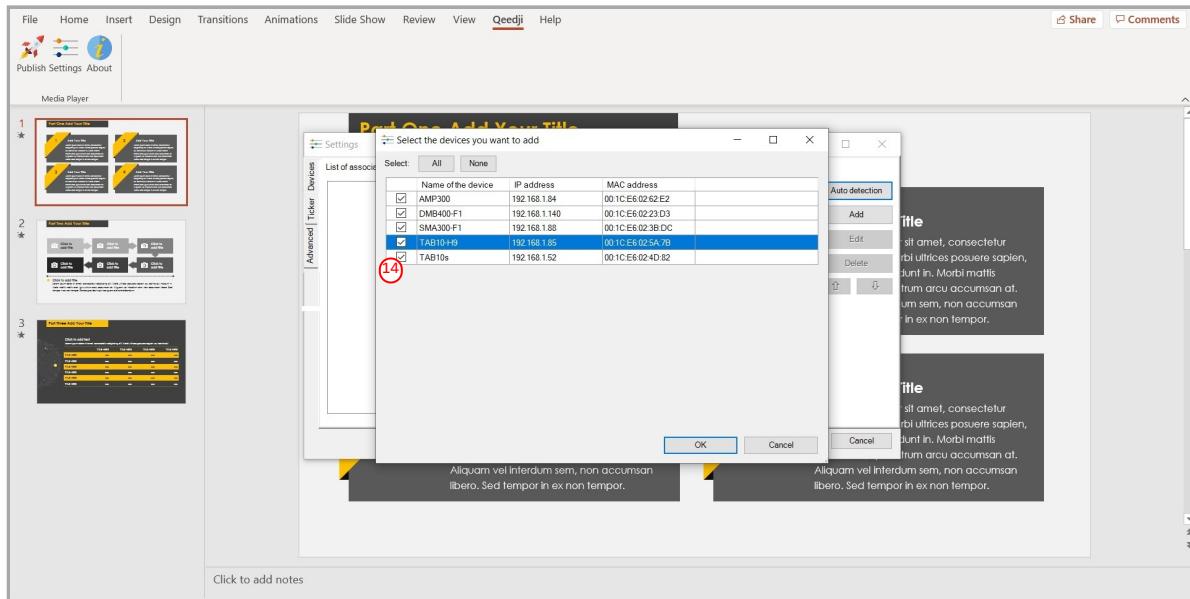
⚠ Some of the MS-PowerPoint transition effects may be not yet supported. For further information, refer to the media player release note.

On the Devices **⑪** tab, click on the Auto detection **⑫** button to detect the TAB10b devices available on your local network.



In this version, the models whose model is TAB10b can not be detected by the auto-detection function. To work around, the TAB10b device must be added manually by entering the device IP address and choosing the TAB10s model. It should be fixed in the next release of Qeedji PowerPoint Publisher for Medias players .

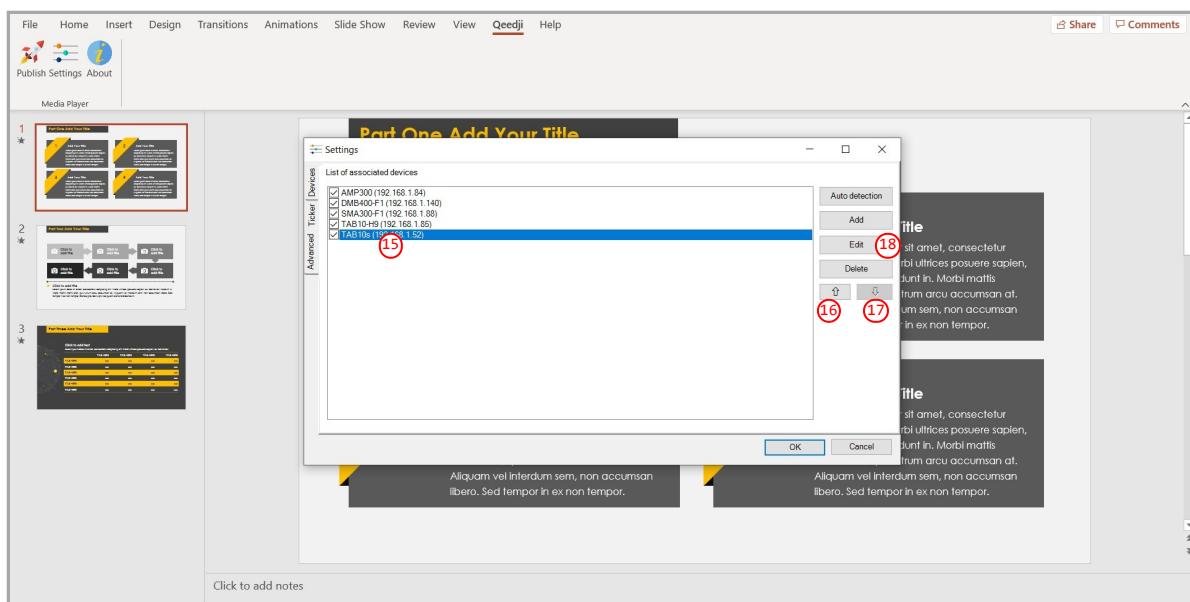
Select ⑭ the appropriate TAB10b devices to create a list of appropriate TAB10b devices as possible applicant for the MS-Powerpoint presentation.



Select then the only TAB10b devices on which you want to publish, by double clicking on them.

☞ The TAB10b 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 TAB10b device located at the top of the list. Then the publication is continuing with the next TAB10b device located immediately below, and so on.

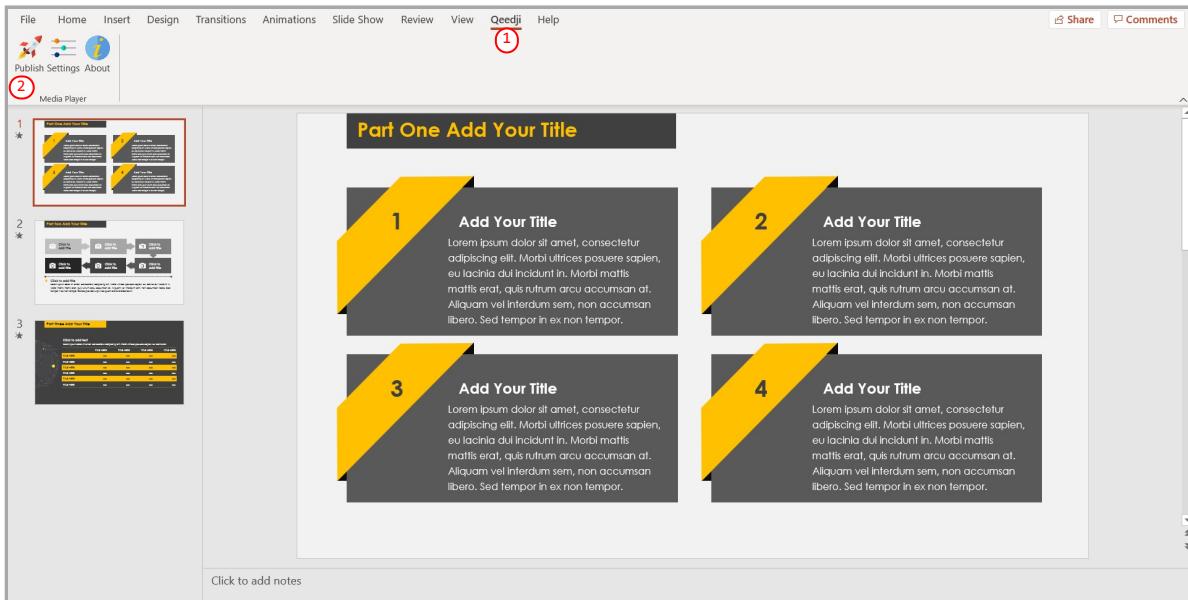
Select a TAB10b device and use the up ⑯ arrow or the down ⑰ arrow to sort them in the right order to match the MS-PowerPoint sections.



Qeedji PowerPoint Publisher For Media Players: publish

To publish a MS-Powerpoint content on your tablet, open your MS-Powerpoint presentation with MS-Office. 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 TAB10b devices are consistent and sorted in the right order.

The **Publishing status report** is showing whether the publishing on each TAB10b 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 TAB10b device.

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

5/5 - Publishing on device: TAB10b (192.168.1.53)
    Publishing succeeded

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

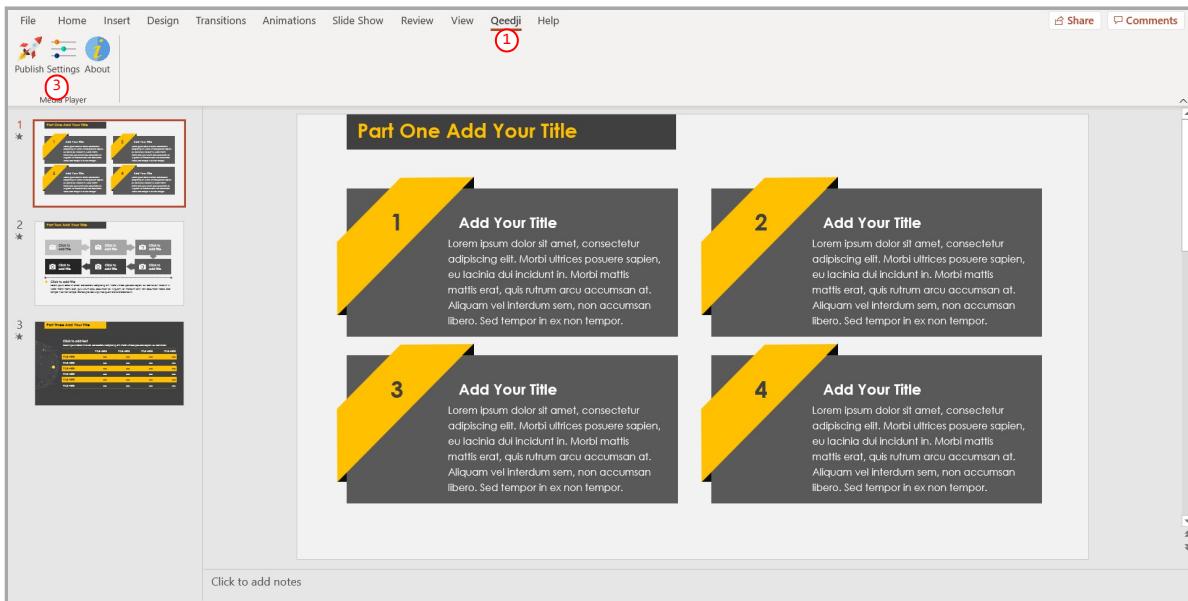
The **Publishing status report** is showing also whether the MS-PowerPoint medias can be rendered with the right fonts. In case some fonts can not be found on the Windows OS, a message **Warning - Unable to find the following fonts** is displayed followed by the missing fonts names. To solve the rendering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

The PowerPoint presentation 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-PowerPoint presentation with MS-Office then:

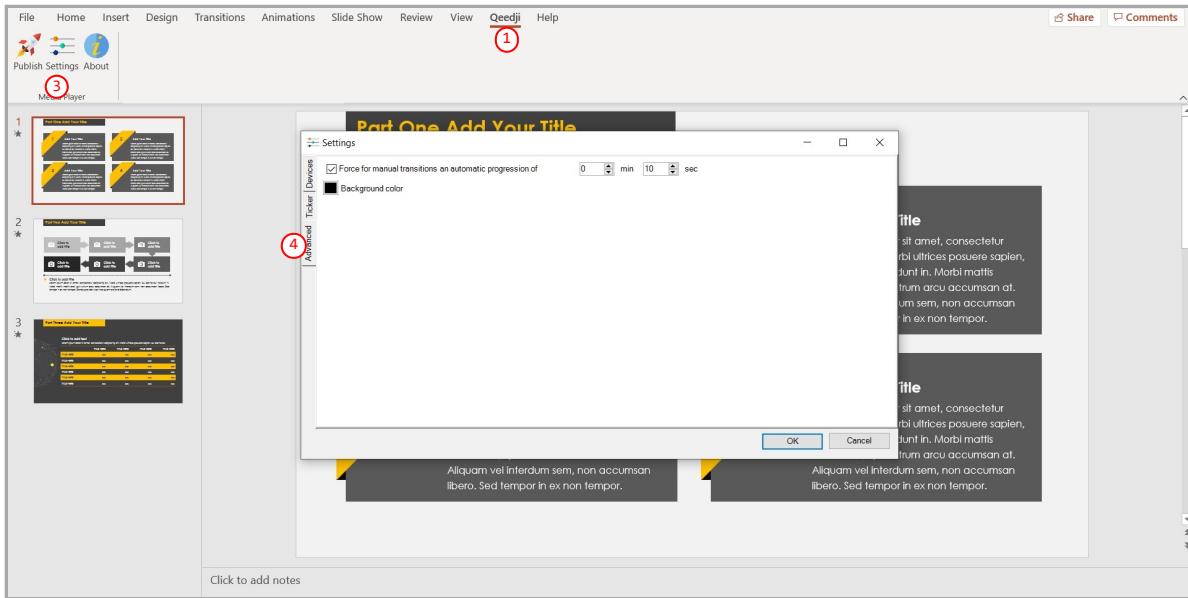
- click on the Qeedji (1) menu,
- on the Qeedji ribbon, click on the Settings (3) item then select the Advanced (4) tab.



Check the Force for manual transitions an automatic progression of option and adjust its duration:

- <m> min, <n> sec.

This default duration will be applied for slides having no duration per slide defined.



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

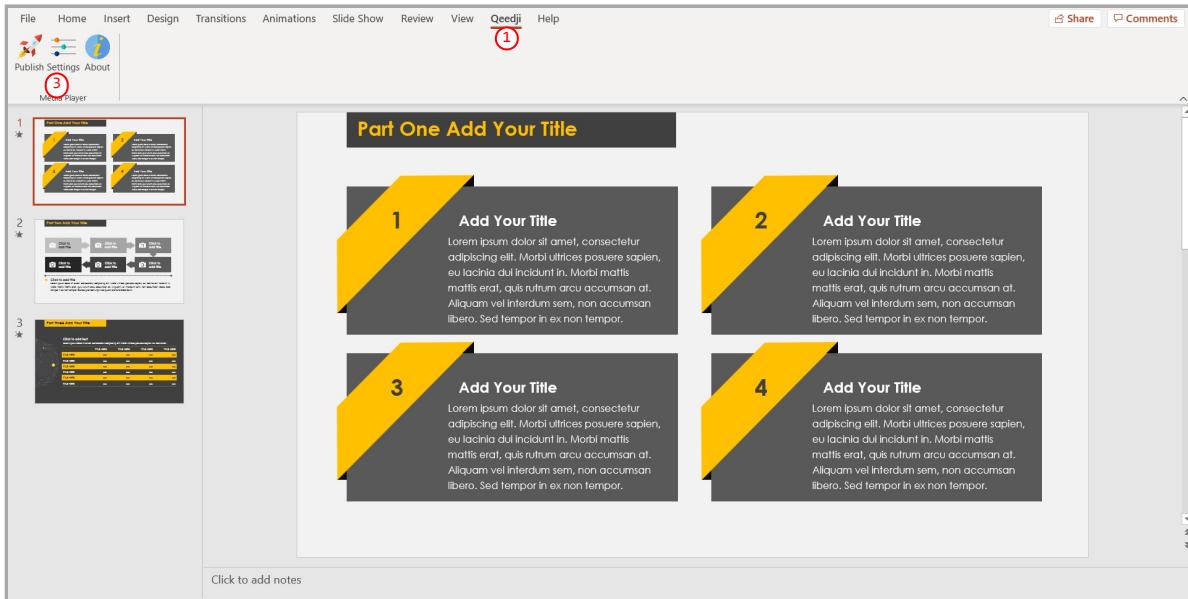
When the Force for manual transitions an automatic progression of option is not checked, to ensure a page progression, open your Powerpoint presentation with MS-Office, select the first slide, select the Transition menu. In the Transition ribbon, look at the Advance slide and check that After option is checked and check that the slide duration is more than 00:00:00. Check that point for all the slides of your Powerpoint presentation. If your slide contains a video media, check the After option and set the slide duration for this slide to 00:00:00 to automatically go to the next page when the video has ended.

Note: An PowerPoint example illustrating the last point is available in the [Qeedji PowerPoint publisher for Medias players release note](#).

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 PowerPoint presentation, open your PowerPoint presentation with MS-Office then:

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



Then select the Ticker (5) tab.

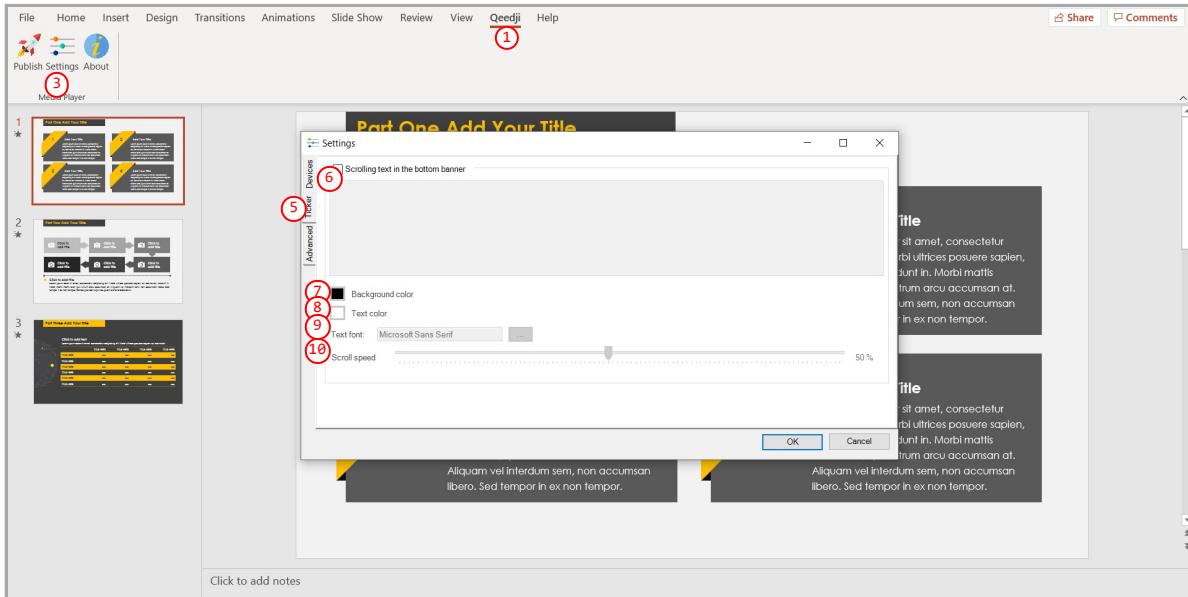
Select the Scrolling text in the bottom banner (6) option to activate the scrolling of a text at the bottom of the PowerPoint presentation.

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 TAB10b device, the max. number of character per line is depending on the display resolution of the TAB10b device and the chosen font. Outside this limit, the scrolling text cannot be displayed.



Qeedji PowerPoint Publisher For Media Players: 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.

Qeedji PowerPoint Publisher For Media Players: miscellaneous

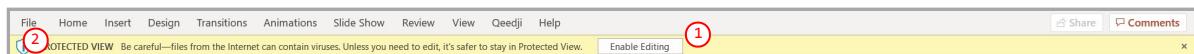
The scheme `https://` is not supported in this version.

When the App Qeedji PowerPoint Publisher for Media Players 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.

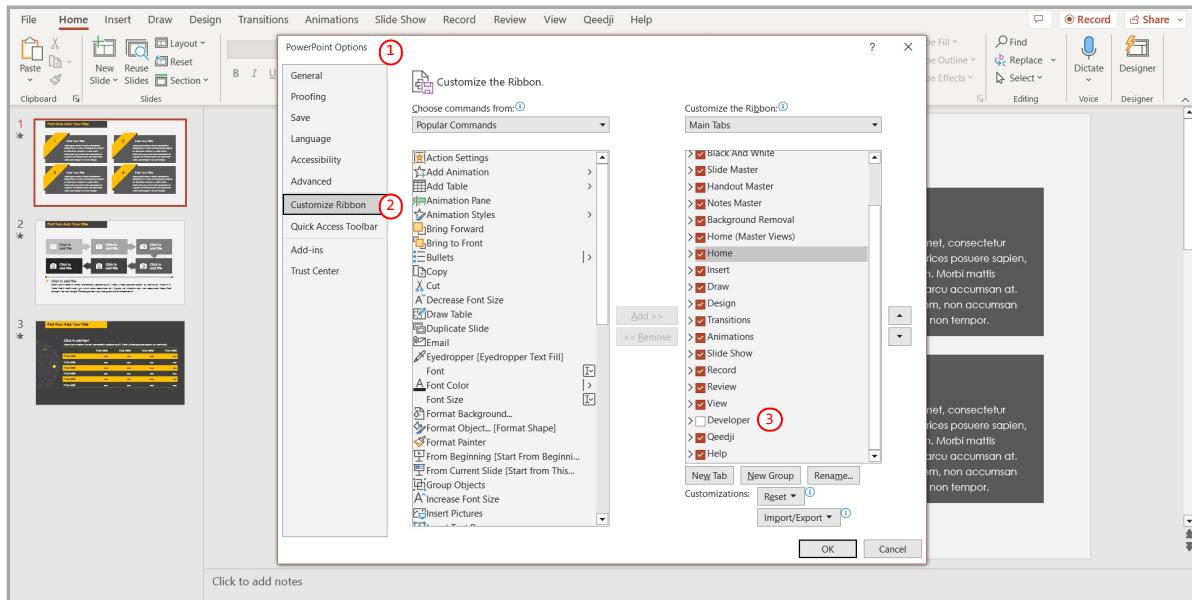


Qeedji PowerPoint Publisher For Media Players: custom script

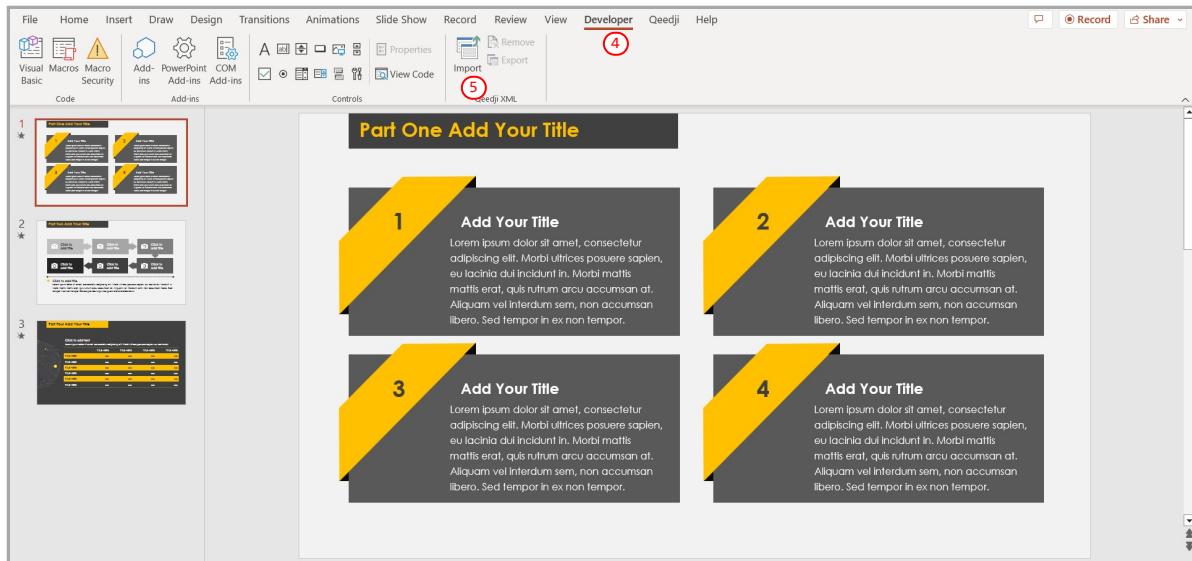
Qeedji PowerPoint Publisher for Media Players (V1.14.10 or above) allows to load a *configuration.xml* with the *Import* feature of the optional *Developer* tab in the MS-PowerPoint ribbon.

Open your MS-PowerPoint presentation (.pptx) in MS-PowerPoint and click on the *options* item of the *File* menu.

In the *PowerPoint Options* pane (1), scroll the *Customize the ribbon* (2) list to the bottom to see the *Developer* (3) option. Check the *Developer* option that is not checked by default. Then validate.



Click on the *Developer* (4) tab that has just appeared. Click then on the *Import* (5) button of the Qeedji XML ribbon part.

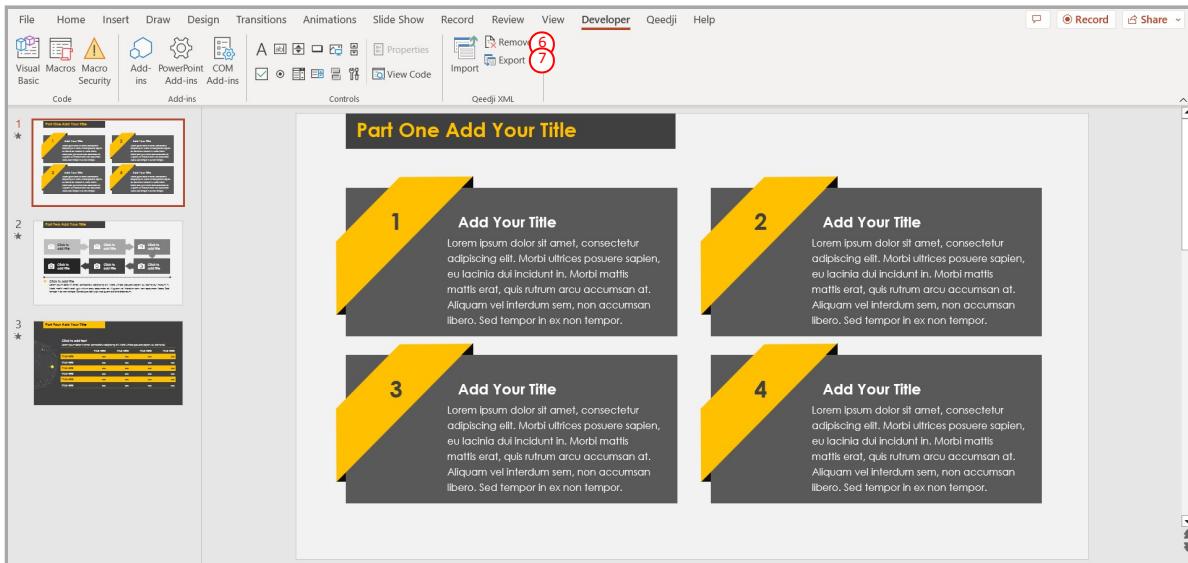


Each time the .xml file is modified, it must be imported again to be taken into account.

Select your .xml file (e.g. configuration.xml).

When the .xml file is successfully loaded, two buttons appear:

- Remove (6) allows to remove your .xml file,
- Export (7) allows to export your .xml file to check its content.



Save your MS-PowerPoint presentation and publish the [Qeedji PowerPoint publisher for Medias players App](#) on the device.

Qeedji PowerPoint Publisher For Media Players: screen standby

To program a screen standby task with recurrency, for example from 8.00 PM to 7.00 AM the day after, use the device [Power Manager](#) feature. For further information, refer to the chapter § [Configuration > Task](#).

Qeedji PowerPoint Publisher For Media Players: aspect ratio

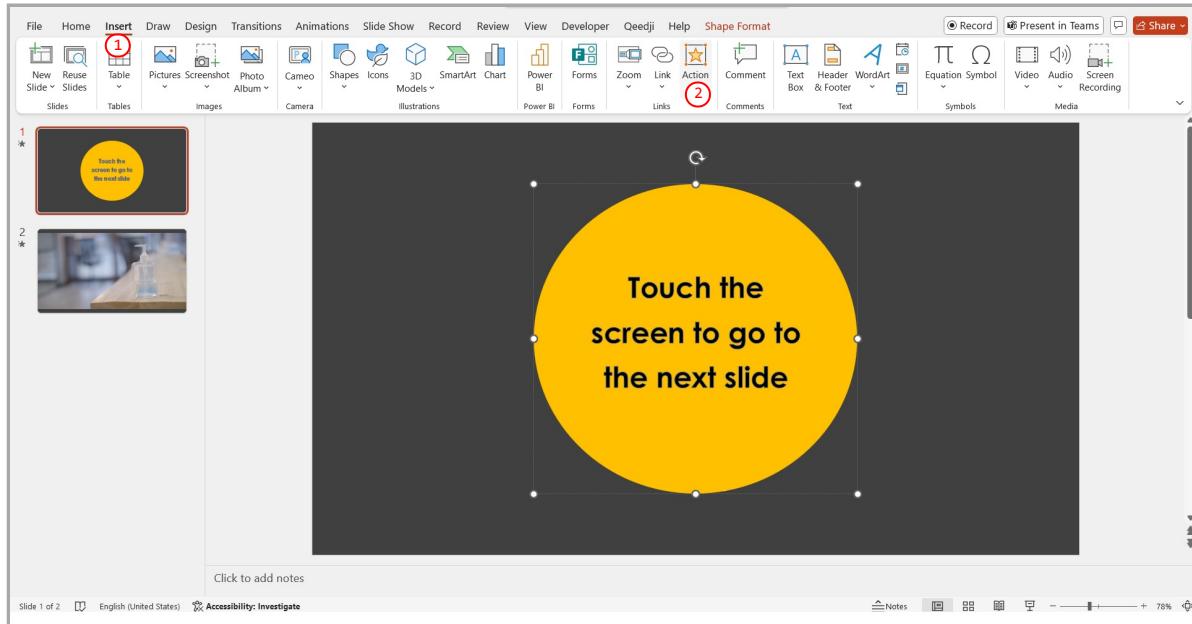
For devices, the recommended aspect ratio for MS-PowerPoint slides is 16/10.

Qeedji PowerPoint Publisher For Media Players: user interactivity with touch screen device

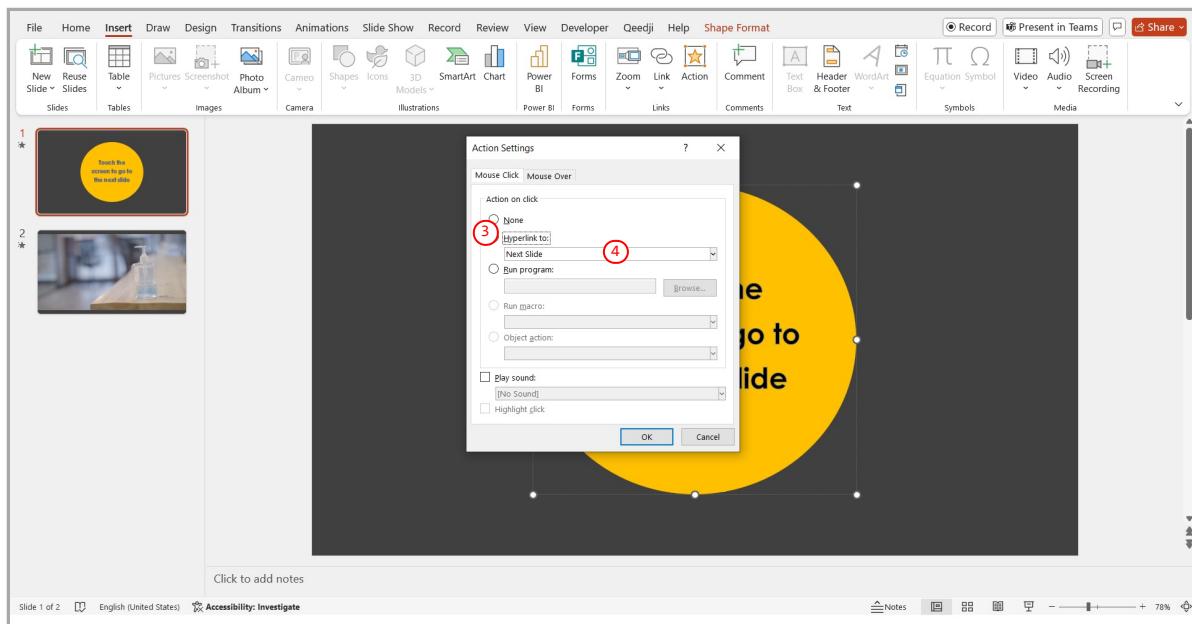
It is possible to bring touch screen interactivity to your PowerPoint presentation. This is an example to go to the next slide when the user has pressed the touch screen.

Select the slide that must support the touch screen interactivity. For this slide:

- insert an image or a text zone object whose the surface represents the interactive area,
- in this area, add a text inviting to press the screen (e.g: *Touch the screen to go to the next slide*),
- select the object of the interactive area to make appear handlers on edges and corners.
- in the ① Insert ribbon, select the ② Action item.



In the Action panel, select the Hyperlink to ③ radio button. In the drop down list, select Next slide ④.



An PowerPoint example is available in the [Qeedji PowerPoint publisher for Medias players release note](#).

For the interactive slide, to keep it displayed until user interaction, think to not define a value for the After item in the Transition menu. Think to also not check the Force for manual transitions an automatic progression of option.

8.2 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 TAB10b 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.

8.3 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_qeedji-tab10-setup-xx.yy.zz.iso`.



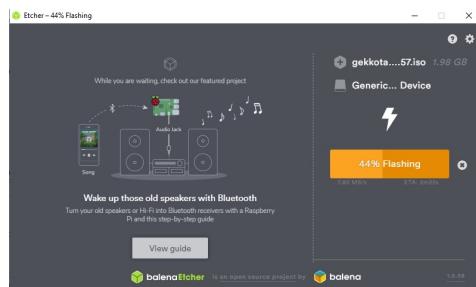
Insert the device micro SD card in the SD card slot of your computer.

- ☞ 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 TAB10b 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.



8.4 Appendix: TFTP and DHCP server configuration

To use TFTP configuration by script, you need a TFTP¹ server with a DHCP server associated to it (code 66 option).

¹ Trivial File Transfer Protocol

The network interfaces of the TAB10b 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 TAB10b device configures first its network parameters obtained by DHCP server, and then launches TFTP download.

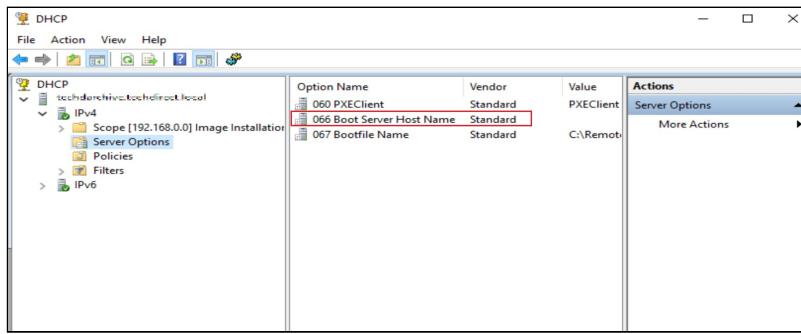
 the installation phase is launched only when the script has never been downloaded before or if its content has been modified since the last download (md5 check).

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 fully reflected.

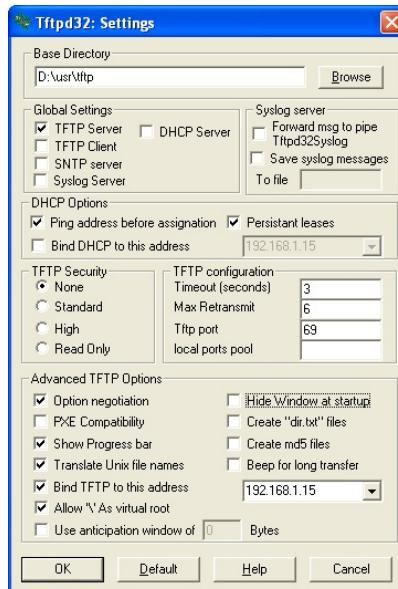


TFTP server configuration

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).

8.5 Appendix: Timezone

| Area | Country/Town pair values supported for the <code>setTimezone</code> 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 <code>setTimezone</code> 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, |

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

⚠ Do follow carefully the procedure below to mount properly the TAB10b 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:

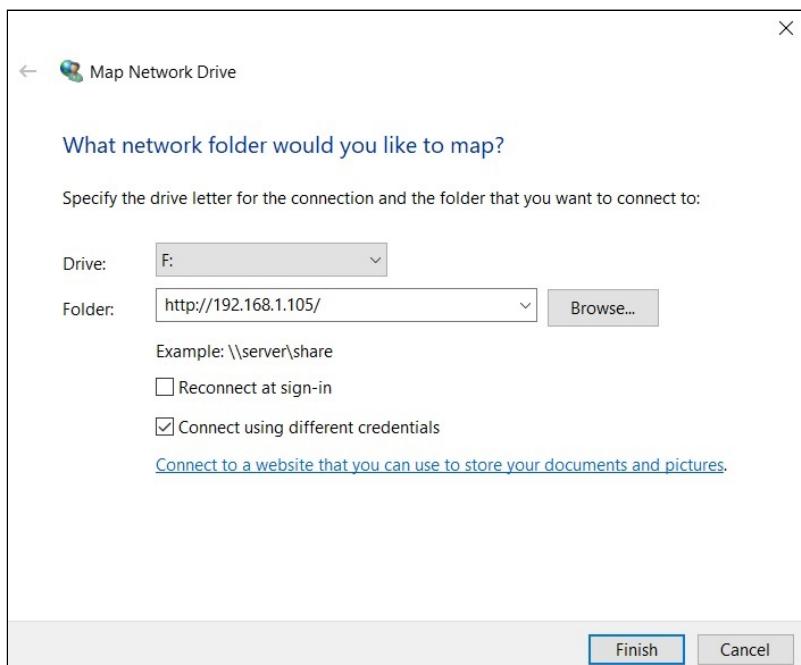
- the TAB10b is properly connected to your network with a correct network configuration (`WLAN` or `LAN` interface).

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 TAB10b device is `192.168.1.105`:



Enter the login credentials to connect to the TAB10b WebDAV server.

⚠ It is advised to double check the login credentials.

In case disk mapping success, the network drive should be mounted automatically on `\\.`

For example:



8.7 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.

8.8 Appendix: File transfer from a computer

Like any Android device, it is possible to access to the file system of the TAB10b device from a computer. That procedure can be used typically to push a configuration script or a firmware from a computer when no network is available on the TAB10b device.

Ensure that your computer is able to supply sufficient power through the USB-C connector to start the TAB10b device. Else use a NAPOE109kt device or a NAPOE109ft device to start the TAB10b device.

1. connect an USB-C cable between your computer and the TAB10b device,
2. if required, quit the Kiosk mode by pressing on the system button to access to the Android Settings App,
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 TAB10b device file system is mounted properly on your computer. These directories should be mounted on the device mass storage (e.g. `<yourComputerDrive>`):

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

To update the network configuration of your TAB10b device, push a suitable configuration script in the `\TAB10\Internal shared storage\Android\data\tech.qeedji.system\files\configuration\` directory.

To upgrade the AQS operating system, push a suitable firmware in the `\TAB10\Internal shared storage\Android\data\tech.qeedji.system\files\software\` directory.

To install an APK, push a suitable `.apk` file in the `\TAB10\Internal shared storage\Android\data\tech.qeedji.system\files\apps\` directory.

8.9 Appendix: Factory reset

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

From the AQS desktop¹,

- 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 TAB10b 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](#).

8.10 Appendix: Remove an App with Android Settings App

In case you could not have access to the device console Web user interface, it is possible to use Android Settings App to remove some App.

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.

8.11 Appendix: 802.1X security configuration with Android Settings App

In case you could not have access to the device console Web user interface, it is possible to use Android Settings App to configure 802.1X security.

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 TAB10b device generated with the CA certificate of your RADIUS server.

 When using a RADIUS certificate, it is recommended that the system date of the TAB10b 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 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
 - PAP¹,
 - MSCHAP¹,
 - MSCHAPV2¹,
 - GTC¹,
 - None¹: the AOSP uses automatically 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 TAB10b device for the WLAN interface
- Anonymous identity : identity used for the first identification phase. If the Anonymous Identity value is left empty, the Anonymous Identity value worths the Identity value set above.
- Password : client password registered in the RADIUS server for this TAB10b 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 Settings application (for WLAN interface), through the device configuration console web user interface or with a configuration script. For further information, refer to [configuration script template V1.12.13 \(or above\)](#).

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 V1.12.13 \(or above\)](#).

8.12 Appendix: Certificates installation with Android Settings App

In case you could not have access to the device console Web user interface, it is possible to use Android Settings App to configure 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 `AOS`. 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 TAB10b 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.

8.13 Appendix: Power manager and Screen Saver modes

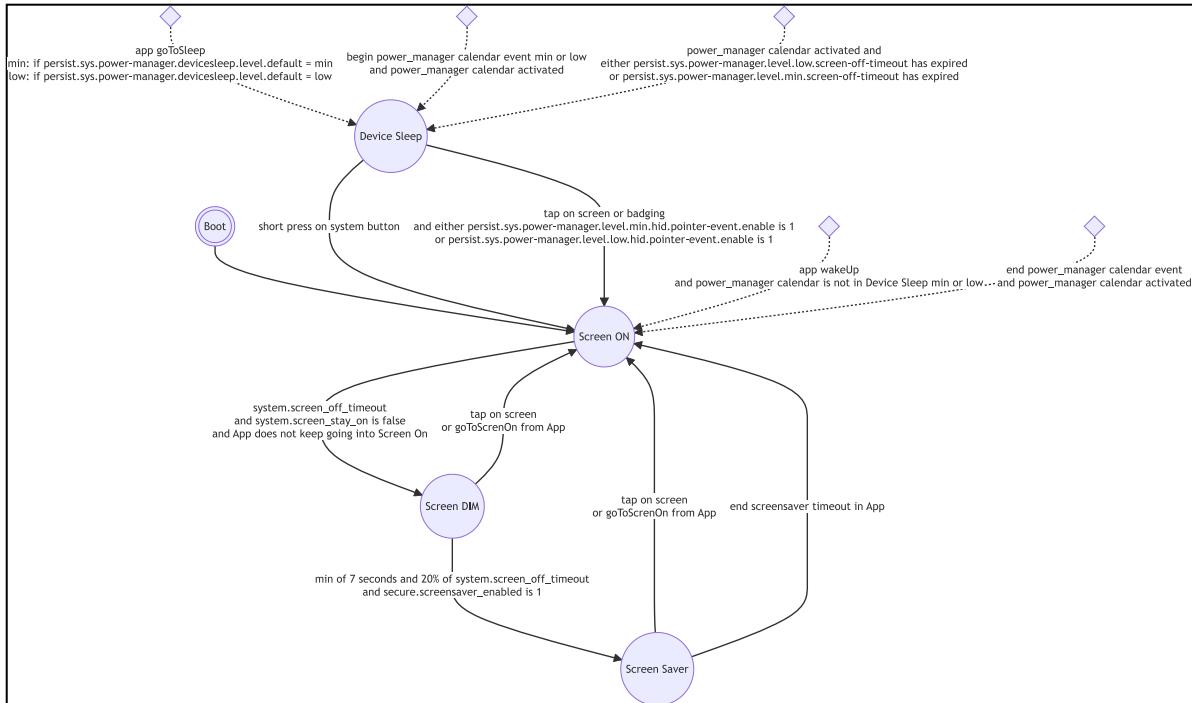
For the TAB10b device, the `Screen Saver` mode and the `Screen DIM` mode are supported. By default, the `Screen DIM` mode and `Screen Saver` mode are not activated.

| User preference name | Default value | R/W access | Possible values | Description |
|---|---------------|------------|-----------------|--|
| <code>system.screen_off_timeout</code> | 60000 | R/W | <0..n> | Duration in ms before going to <code>Screen DIM</code> mode. |
| <code>system.screen_stay_on</code> | 1 | R/W | 0 or 1 | 1 means that the device can not reach <code>Screen DIM</code> mode (default value). 0 means that the device can reach <code>Screen DIM</code> mode. When <code>secure.screensaver_enabled</code> is 1, the device reaches <code>Screen ON</code> mode after few seconds in <code>Screen DIM</code> mode. |
| <code>secure.screensaver_enabled</code> | 1 | R/W | 0 or 1 | 0: <code>Screen DIM</code> mode only, 1: <code>Screen DIM</code> mode then the screensaver is reached when there is no user interactivity. |
| <code>screen_brightness_dim</code> | 1 | R/W | 0 to 100 | When the <code>screen_brightness_dim</code> is 0, the backlight is very dark and the transparency is weak. When the <code>screen_brightness_dim</code> is 100, the backlight level is maximum. The transparency is full. |

The `Screen DIM` mode consists in the decreasing of the screen brightness by changing the backlight level. The duration of this state is the minimum value between seven seconds and 20% of the `system.screen_off_timeout` user preferences value. Once this `Screen DIM` mode is reached, tapping once on the screen allows to exit this mode and return to `Screen ON` mode (nominal screen mode).

The `Screen Saver` mode consists in displaying the `Screen saver` App, named `Colors` in the `Display` menu of the `Android settings` for the default `Screen saver` App. Once this `Screen Saver` mode is reached, tapping once on the screen allows to exit this mode and return to `Screen ON` mode (nominal screen mode); the device can also return to the `Screen ON` mode when the screen saver timeout implemented by the App has expired.

This version supports the execution of a custom `Screen saver` App instead the default `Screen saver` App.



8.14 Appendix: Identifier and password self-filling and self-confirmation in a web page form

List of supported input properties to auto-fill properly the *identifier* field

email type input

*user i name** input

email autocomplete input

*user i id** input

*login i id** input

*email i id** input

List of supported input properties to auto-fill properly the *password* field

password input type

List of supported validate button properties to self-confirm the credential values and access to the web page content

submit type input

submit type button

button type input

*sign id** input

*submit id** input

8.15 Appendix: URI for Media Folder Injector

The Media Folder Injector APK can support `.uri` medias playback. The URI media must consist in:

- a `<myName>.uri` file,
- a `<myName>.uri.xmp` file, to configure the URI media duration.

If only the `.uri` file is available, the `.uri` media is played only for 10 seconds.

A *web page* URI example can be provided by Qeedji.

1. In both files, replace the `https://www.qeedji.tech/en/` URL by your own web page URL,
2. In both files, replace the `im:userDuration` value (e.g. `00:01:00,000`) according to your need to define the intrinsic URI duration,
3. Rename the both file with a name consistent with your URL and by respecting the suffix naming,
4. Inject the USB storage device,
5. Restart the App.

A *web TV* URI example can be provided by Qeedji.

1. In both files, replace the `https://www.youtube.com/embed/18PMl7tUDIE?autoplay=1` URL by your own web TV URL,
2. In both files, replace the `im:userDuration` value (e.g. `00:01:00,000`) according to your need to define the intrinsic URI duration,
3. Rename the both file with a name consistent with your URL and by respecting the suffix naming,
4. Inject the USB storage device,
5. Restart the App.

For further information, contact support@qeedji.tech.

8.16 Appendix: Microsoft Azure AD portal for Microsoft Power BI application

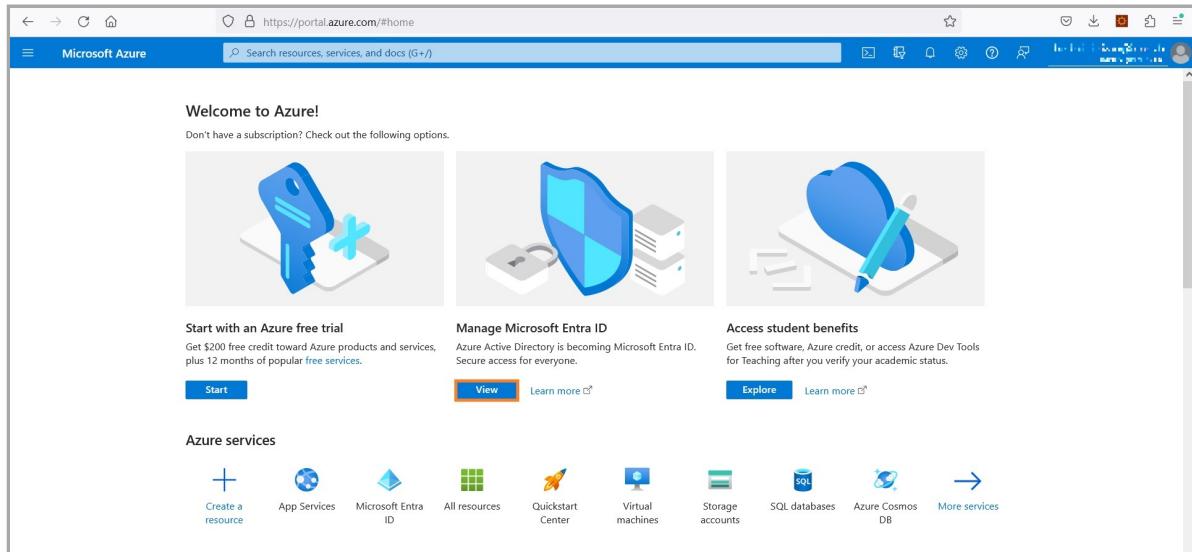
You can create your Azure Active Directory (or Azure AD) application by following this Microsoft tutorial <https://docs.microsoft.com/en-us/graph/auth-register-app-v2>.

A procedure example is shown here after by connecting to the Microsoft Azure portal.

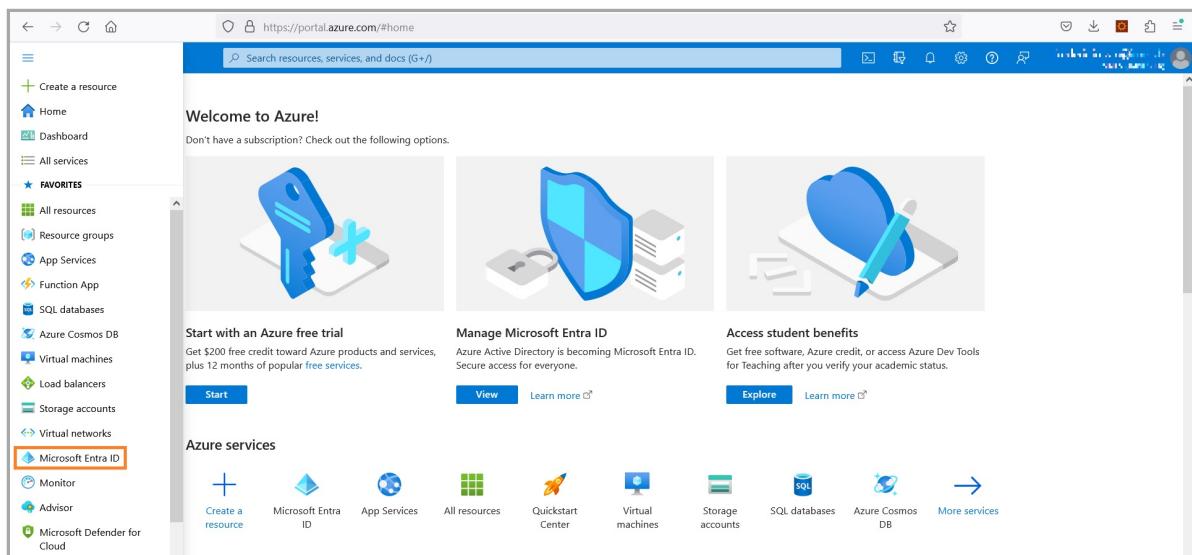
This procedure allows to generate you own client ID and SECRET required in for Power BI Online Viewer application:

- Directory (Tenant) ID ,
- Application (client) ID ,
- Client secret .

Connect on Microsoft Azure portal: <https://portal.azure.com/> and sign in with your Microsoft 365 (M365) administrator account login credentials. Click on the left top menu and choose the Azure Active Directory item.

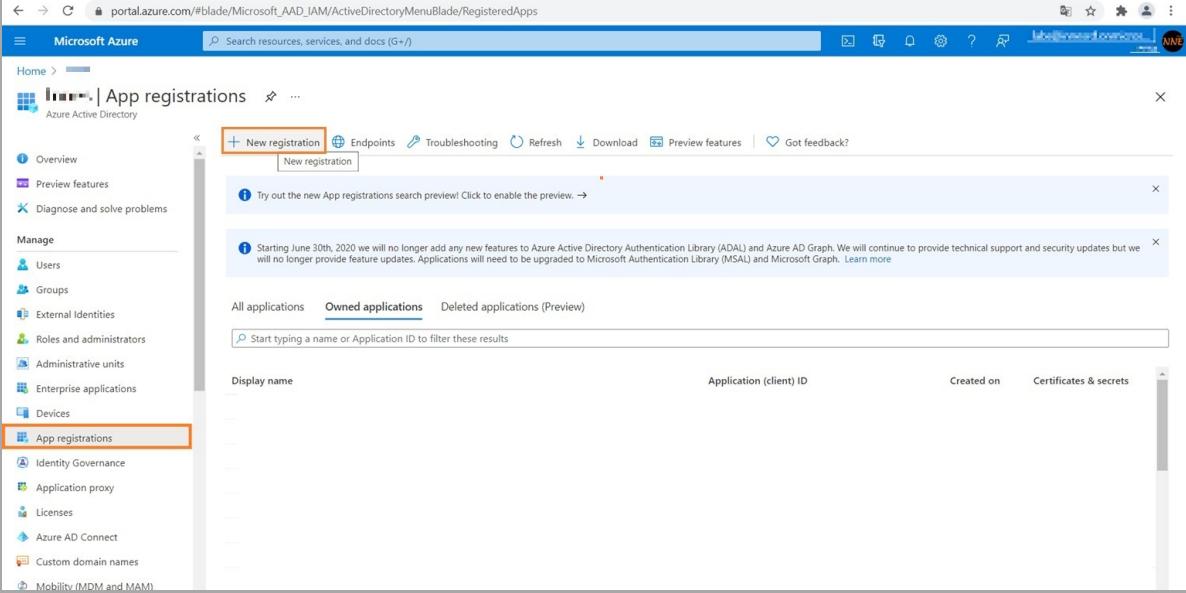


Either click on the **View** button of the the **Manage Microsoft Entra ID** section or click on the **Home** button then in the menu select the **Microsoft Entra ID** item.



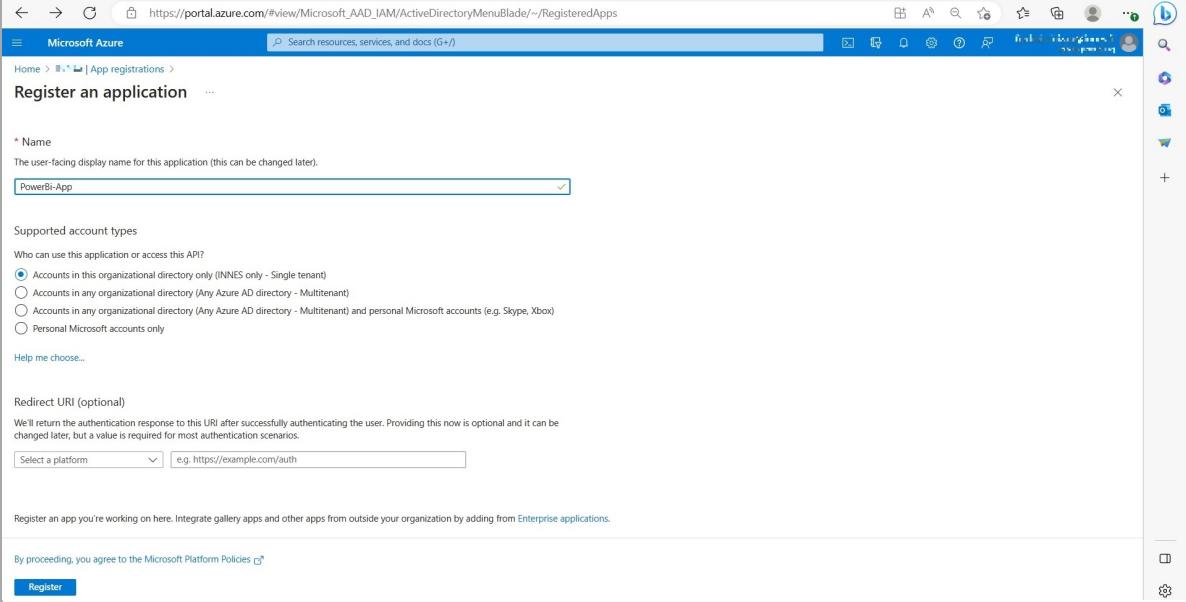
Application (client) ID and directory (Tenant) ID

On the App registrations menu, click on *New registration*.



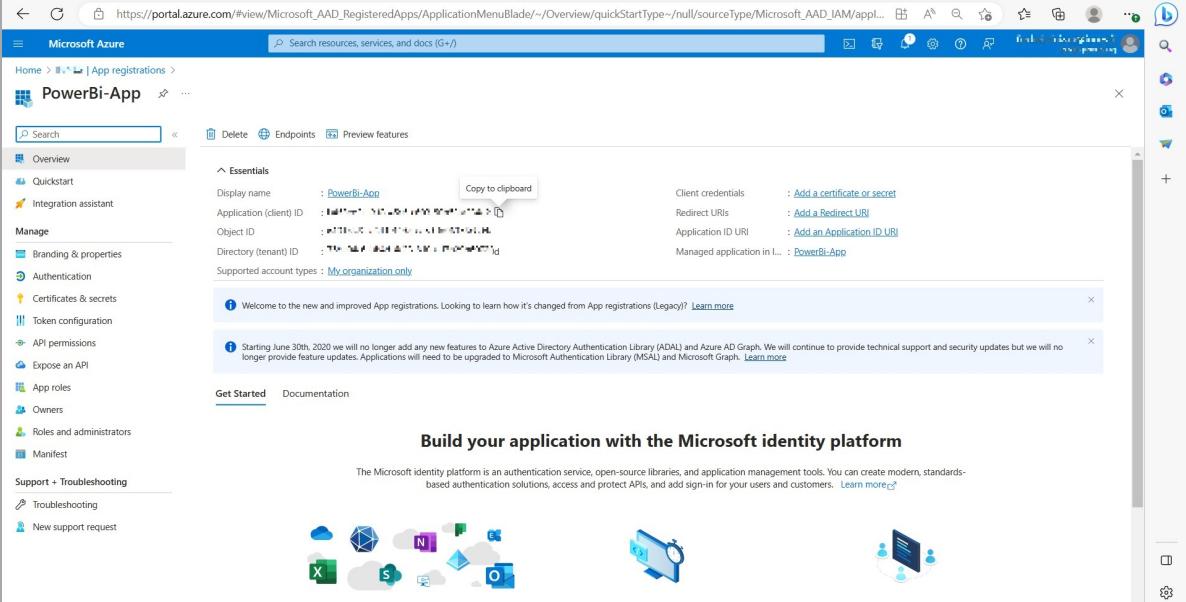
The screenshot shows the Microsoft Azure portal's App registrations blade. On the left, there's a sidebar with 'App registrations' selected. At the top, there's a search bar and several navigation links like 'Endpoints', 'Troubleshooting', 'Refresh', 'Download', 'Preview features', and 'Got feedback?'. A prominent orange box highlights the '+ New registration' button. Below it, a message says 'Try out the new App registrations search preview! Click to enable the preview.' Another message at the top right states: 'Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph.' The main area shows tabs for 'All applications', 'Owned applications' (which is selected), and 'Deleted applications (Preview)'. There's a search bar with 'Start typing a name or Application ID to filter these results'. The table below lists applications with columns for 'Display name', 'Application (client) ID', 'Created on', and 'Certificates & secrets'.

Enter an application name (e.g.: *PowerBi-App*), Select the appropriate Account in the organization directory only (organization only – Single tenant) radio button, and press on the *Register* button.



The screenshot shows the 'Register an application' wizard. The first step is 'Name', where the user-facing display name 'PowerBi-App' is entered. Below it, 'Supported account types' are listed with the 'Accounts in this organizational directory only (INNES only - Single tenant)' radio button selected. Other options include 'Accounts in any organizational directory (Any Azure AD directory - Multitenant)', 'Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)', and 'Personal Microsoft accounts only'. The 'Help me choose...' link is available. The next step is 'Redirect URI (optional)', which is currently empty. A note says 'We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.' Below is a dropdown for 'Select a platform' and a text input for 'e.g. https://example.com/auth'. A note at the bottom says 'Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.' At the bottom, there's a link 'By proceeding, you agree to the Microsoft Platform Policies' and a blue 'Register' button.

In the Overview menu, copy to clipboard the Application (client) ID value, the 1st value required in TAB10b configuration tab and store it preciously.

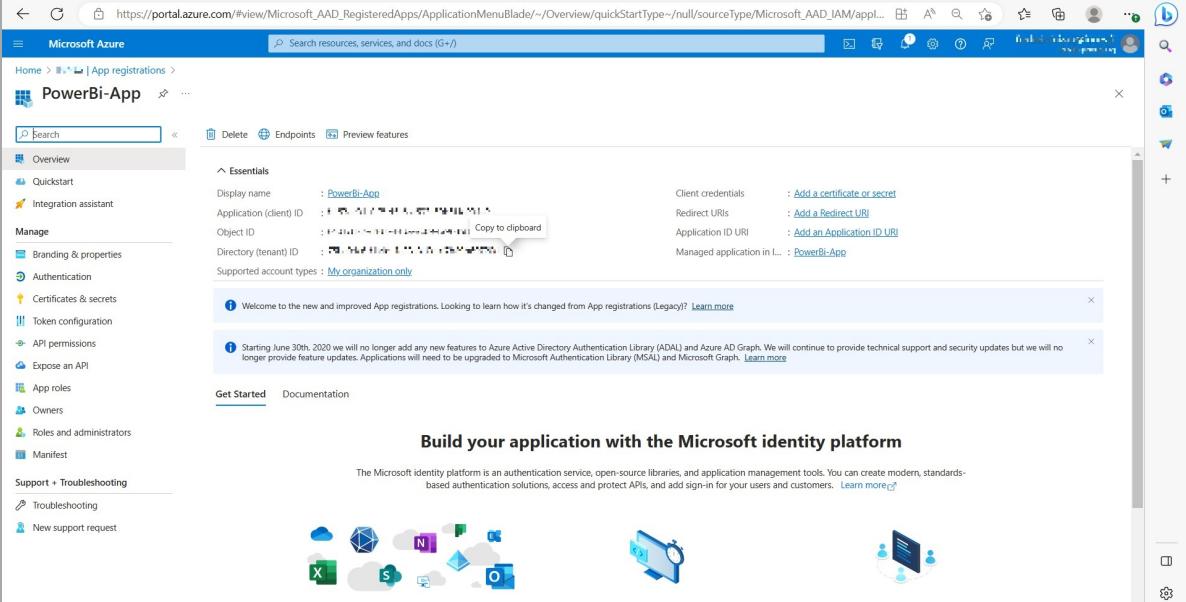


The screenshot shows the Microsoft Azure portal's App registrations section. A specific application named 'PowerBi-App' is selected. On the left, a sidebar lists various management options like Quickstart, Integration assistant, and API permissions. The main panel displays the 'Overview' tab for the app. Key details shown include:

- Display name: PowerBi-App
- Application (client) ID: (redacted)
- Object ID: (redacted)
- Directory (tenant) ID: (redacted)
- Supported account types: My organization only
- Client credentials: Add a certificate or secret
- Redirect URLs: Add a Redirect URI
- Application ID URI: Add an Application ID URI
- Managed application in L...

Below the details, there are two informational banners about app registration changes. At the bottom, there are 'Get Started' and 'Documentation' links, and a 'Build your application with the Microsoft identity platform' section featuring icons for various Microsoft services.

In the Overview menu, copy to clipboard the Directory (tenant) ID value, the 2nd value required in TAB10b configuration tab and store it preciously.



This screenshot is identical to the one above, showing the 'PowerBi-App' application registration in the Microsoft Azure portal. The focus is on the 'Overview' tab, where the 'Directory (tenant) ID' field is highlighted with a red box and has a 'Copy to clipboard' tooltip above it. The rest of the interface, including service icons and informational banners, is consistent with the first screenshot.

Client secret

In the Certificates & secrets menu, click on the New client secret button.

Enter a name (e.g.: my_client_secret) and press on the Add button.

Copy into clipboard the `client secret` value, the 3rd input for the TAB10b configuration tab and store it preciously.

⚠️ Do it right now because the `client secret` value is not visible anymore as soon as you click on a new web page.

The screenshot shows the 'Certificates & secrets' section of the Azure portal. On the left, there's a sidebar with options like Overview, Quickstart, Integration assistant, Manage, Branding & properties, Authentication, Certificates & secrets (which is selected), Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, and Manifest. The main area has tabs for Certificates (0), Client secrets (1), and Federated credentials (0). Under Client secrets, there's a table with one row for 'my_client_secret'. The table columns are Description, Expires, and Value. The Value column contains '123456'. To the right of the Value column is a 'Copy to clipboard' button. There are also 'Edit ID' and 'Delete' buttons. A tooltip above the table says: 'A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.'

When the secret is out of validity date, delete it and create a new one. Copy into clipboard the `client secret` value, the 3rd input for the TAB10b configuration tab and store it preciously.

Grant permissions

In the API permissions menu, press on the `Add a permission` button.

For powerbi application, these permissions must be granted:

- `App.Read.All`,
- `Content.Create`,
- `Dataset.ReadWrite.All`,
- `Report.ReadWrite.All`.

The screenshot shows the 'API permissions' section of the Azure portal. The sidebar is identical to the previous screenshot. The main area has a 'Configured permissions' section with a table. The table has columns: API / Permissions name, Type, Description, Admin consent req..., and Status. One row is shown: 'Microsoft Graph (1)' with 'User.Read' under 'API / Permissions name', 'Delegated' under 'Type', 'Sign in and read user profile' under 'Description', 'No' under 'Admin consent req...', and three dots under 'Status'. A tooltip above the table says: 'The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used.' Below the table, there's a note: 'To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.'

Scroll to the bottom and click on the Power BI Service button.

The screenshot shows the Azure portal interface with the URL https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/CallAnAPI/quickStartType~/null/sourceType/Microsoft_AAD_IAM/applications. The left sidebar shows the 'PowerBi-App' configuration page under 'API permissions'. The right panel displays a grid of API permission requests. The 'Power BI Service' option is highlighted with a red border, indicating it is selected.

Select then the Delegated permissions button.

The screenshot shows the same Azure portal interface as the previous one, but the 'Delegated permissions' button in the 'Power BI Service' section is now highlighted with a red border, indicating it has been selected.

In the display filter input, enter the text **calendar** and check the option **Calendars.Read**.

Do not press now on the **Add permissions** button right now.

The screenshot shows the Azure portal interface with the URL https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/CallAnAPI/quickStartType~/null/sourceType/Microsoft_AAD_IAM/app.... The left sidebar shows the 'PowerBi-App | API permissions' page with various settings like branding, authentication, and roles. The 'API permissions' section is selected. On the right, a modal window titled 'Request API permissions' is open for the 'Power BI Service'. It lists 'Delegated permissions' and 'Application permissions'. Under 'Select permissions', there is a search bar and a list of permissions categorized by app, capacity, and content. The 'Content' category is expanded, showing the 'Content.Create' permission selected with a checked checkbox. At the bottom of the modal are 'Add permissions' and 'Discard' buttons.

Expand the Content tab and check the **Content.Create** permission.

This screenshot is identical to the previous one, but the 'Content' tab under 'Select permissions' is explicitly highlighted or expanded. The 'Content.Create' permission is still selected with a checked checkbox. The rest of the interface and modal window are the same as in the first screenshot.

In the **Dataset** part, select the `Dataset.ReadWrite.All` option.

The screenshot shows the Azure portal's 'API permissions' page for a 'PowerBI-App'. On the left, the 'Dataset' section is highlighted under 'Select permissions'. In the main pane, under 'Permission', the 'Dataset' section is expanded, showing two options: 'Dataset.Read.All' (unchecked) and 'Dataset.ReadWrite.All' (checked). Both options have 'No' listed under 'Admin consent required'.

In the **Report** part, select the `Report.ReadWrite.All` option.

The screenshot shows the Azure portal's 'API permissions' page for a 'PowerBI-App'. On the left, the 'Report' section is highlighted under 'Select permissions'. In the main pane, under 'Permission', the 'Report' section is expanded, showing two options: 'Report.Read.All' (unchecked) and 'Report.ReadWrite.All' (checked). Both options have 'No' listed under 'Admin consent required'.

In the **Dashboard** part, select the `Dashboard.ReadWrite.All` option.

The screenshot shows the Microsoft Azure portal with the URL https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/CallAnAPI/appId/b463ee31-fcf8-45c6-a693-50b5f1a.... The left sidebar shows 'PowerBi-App' under 'App registrations'. The main area shows 'API permissions' with a table:

| API / Permissions name | Type | Description | Admin consent required |
|------------------------|-----------|---|------------------------|
| User.Read | Delegated | Sign in and read user profile | No |
| Power BI Service (4) | | | |
| App.Read.All | Delegated | View all Power BI apps | No |
| Content.Create | Delegated | Create content | No |
| Dataset.ReadWrite.All | Delegated | Read and write all datasets | No |
| Report.ReadWrite.All | Delegated | Make API calls that require read and write permissions on reports | No |

A modal window titled 'Request API permissions' is open on the right. It contains a note: 'Your application needs to access the API as the signed-in user.' and 'Your application runs as a background service or daemon without a signed-in user.' Below this is a search bar with 'dash' typed in. The 'Select permissions' section shows a table:

| Permission | Admin consent required |
|-------------------------|------------------------|
| Dashboard (1) | |
| Dashboard.Execute.All | No |
| Dashboard.Read.All | No |
| View all dashboards | No |
| Dashboard.ReadWrite.All | No |
| Dashboard.Reshare.All | No |

The 'Dashboard.ReadWrite.All' row has a checked checkbox. At the bottom of the modal are 'Add permissions' and 'Discard' buttons.

Click now on the **Add permissions** button.

At this step, the permissions are not yet granted. Click on the **Grant admin consent for <your_organization>** button.

The screenshot shows the Microsoft Azure portal with the same URL as the previous screenshot. The message 'You are editing permission(s) to your application, users will have to consent even if they've already done so previously.' is displayed at the top. The 'Configured permissions' table is identical to the one in the previous screenshot, with the 'Dashboard.ReadWrite.All' permission now having a checked checkbox in the 'Admin consent required' column. The status for this permission is 'No'.

Now the permissions are granted.

The screenshot shows the Microsoft Azure portal interface. The URL is https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/CallAnAPI/appId/b463ee31-fcf8-45c6-a693-50b5f1a2. The page title is "PowerBi-App | API permissions". The left sidebar shows "Overview", "Quickstart", "Integration assistant", "Manage", "Branding & properties", "Authentication", "Certificates & secrets", "Token configuration", "API permissions" (which is selected), "Expose an API", "App roles", "Owners", "Roles and administrators", "Manifest", "Support + Troubleshooting", and "New support request". The main content area has a heading "Configured permissions" with a note: "Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent". It includes a "Grant admin consent for" button and a table of permissions. The table has columns: API / Permissions name, Type, Description, Admin consent requ..., and Status. The table shows the following permissions:

| API / Permissions name | Type | Description | Admin consent requ... | Status |
|-------------------------|-----------|---|-----------------------|----------------------|
| User.Read | Delegated | Sign in and read user profile | No | Granted for everyone |
| App.Read.All | Delegated | View all Power BI apps | No | Granted for everyone |
| Content.Create | Delegated | Create content | No | Granted for everyone |
| Dashboard.ReadWrite.All | Delegated | Make API calls that require read and write permissions on ... | No | Granted for everyone |
| Dataset.ReadWrite.All | Delegated | Read and write all datasets | No | Granted for everyone |
| Report.ReadWrite.All | Delegated | Make API calls that require read and write permissions on ... | No | Granted for everyone |

At the bottom, there is a note: "To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications."

Powershell

The application can be created easily with a Powershell script. For further information, refer to the chapter § [Appendix: Azure AD Application Powershell module for Power BI Online Viewer application](#).

8.17 Appendix: Azure AD Application Powershell module for Power BI Online Viewer application

Download the `Powershell_Innes_AAD-1.10.18.zip` from the [Innes Site Web](#) then follow the instructions below.

Introduction

This set of `Powershell` functions allows to:

- create an *Azure Active Directory* application, with the `New-AADApplication` function,
- remove an *Azure Active Directory* application, with the `Remove-AADApplication` function.

These functions are defined in the `PSAAD` PowerShell module stored in the `Modules\PSAAD\` directory.

The result of the `Powershell` functions is also stored in a JSON file.

Edit the file and store preciously the values which could be required for your application:

- the `clientId` value,
- the `tenantId` value,
- the `clientSecret` value.

Security

By default, the execution of local `Powershell` scripts are not allowed. You can change their execution rights by changing the `PowerShell` security policy. This modification has to be done once with the `Set-ExecutionPolicy` `Powershell` function. Your organization may have to change it according to your security rules.

For example, to authorize the execution of all scripts, launch a `Powershell` console with administrator rights, and type:

```
PS > Set-ExecutionPolicy -ExecutionPolicy Unrestricted -scope CurrentUser
```

For further information, look at the cmdlet `Set-ExecutionPolicy` help page.

If you cannot allow the execution of unsigned local scripts, you can install the provided certificate in the list of authorized root certificates with the command:

```
PS > cd <your_path_to_the_scripts>\Powershell_Innes_AAD\Certificate\  
PS > Import-PfxCertificate -FilePath InnesCodeSigningRootCA_1.pfx -CertStoreLocation  
cert:\CurrentUser\Root -Password $(ConvertTo-SecureString "1234" -AsPlainText -Force)
```

To import the `.pfx` certificate, you can also use the MS-Windows application `certmgr.msc`, select the `Trusted Root Certification Authorities`, right click on `All Tasks`, select the `Import` item, select the file and enter the password `1234`. When ended, close the current `Powershell` console.

Prerequisite

Install the Azure AD module

Install the `AzureAD` module with the command below:

```
PS > Install-Module -name AzureAD -scope CurrentUser
```

Dependency

If this message is prompted, enter `Y`.

```
The NuGet supplier is required to continue  
PowerShellGet requires the NuGet vendor, version 2.8.5.201 or later, to interact with the repositories.  
The NuGet provider must be available in "C:\Program Files\PackageManagement\ProviderAssemblies" or ..../..  
"C:\Users\<username>\AppData\Local\PackageManagement\ProviderAssemblies".  
You can also install the provider NuGet by executing the command "Install-PackageProvider -Name NuGet ..../..  
-MinimumVersion 2.8.5.201 -Force". Do you want that PowerShellGet installs and imports the NuGet provider now?  
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"):
```

If this message is prompted, enter `Y`.

```
Unapproved repository  
You install the modules from an unapproved repository. If you approve this repository, change its ..../..  
InstallationPolicy value by running the Set-PSRepository command applet. Do you really want to install From PSGallery ?  
[Y] Yes [T] Yes for all [N] No [U] No for all [S] Suspend [?] Help (default is "N"):
```

Usage

To use one of the `Powershell` modules, you have to define the environment variable for `PSAAD`. You have 3 possibilities:

1. Either copy the directories under `Modules\` into a standard Powershell module installation directory, for example `c:\Program Files\WindowsPowerShell\Modules`. Then launch a Powershell console.
2. Or redefine the search variable for Powershell modules (the `$Env:PSModulePath` Powershell variable) each time you will use these functions. In this case, launch a Powershell console, and type the line below, adapting it to your path. Each time you launch a new Powershell console, you need to enter it again.

Example:

```
PS > $Env:PSModulePath="$Env:PSModulePath;C:\Program Files (x86)\WindowsPowerShell\Modules"
```

3. Or redefine the search variable for Powershell modules in the Windows environment variables. For that, add the path `<your_path_to_the_scripts>\Powershell_Innes_AAD\Modules` to the environment variable `PSModulePath`. Then, launch afterwards a Powershell console.

To use the functions or get help, you must then import the module(s) with the `Import-Module` function. Example:

```
PS > Import-Module PSAAD
```

Depending on how you get the scripts, you may have this following warning:

```
Security Warning Run only scripts that you trust. While scripts from the Internet can be useful,
this script can potentially harm your computer. Do you want to run \device\scripts\my.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"):
```

To avoid this message, you can unblock the script files (to do only once):

```
PS > cd <your_path_to_the_scripts>\Powershell_Innes_AAD\
PS > dir -Recurse | Unblock-File
```

The `Get-Command` function allows you to list the functions defined in a module. Example:

```
PS > Get-Command -Module PSAAD
```

Answer example:

| CommandType | Name | Version | Source |
|-------------|-----------------------|---------|--------|
| ----- | --- | ----- | ----- |
| Function | New-AADApplication | 1.10.18 | PSAAD |
| Function | Remove-AADApplication | 1.10.18 | PSAAD |

You can get help on each function of the module by using the standard cmdlet `Get-Help` with options:

- `-detailed`,
- `-full`,
- `-examples`.

Example:

```
PS > Get-Help -detailed New-AADApplication
```

NAME
New-AADApplication

SYNOPSIS
This function creates a Azure Active Directory application.

SYNTAX
New-AADApplication [[-Credential] <PSCredential>] [[-tenantId] <String>] [-appName] <String> [-authorizations] <String[]> [[-LogFile] <String>] [<CommonParameters>]

DESCRIPTION
This function creates a Azure Active Directory application.

PARAMETERS
-Credential <PSCredential>
 Credential (admin profile) used to create the Azure Active Directory application. If absent, a dialog is displayed in the browser to enter the credentials.

-tenantId <String>
 Azure Active Directory Tenant Id of the tenant in which the application has been created. This parameter is not mandatory. If absent, the tenantId is retrieved automatically after the credentials have been entered in the dialog.

-appName <String>
 Name of the Azure Active Directory application.

-authorizations <String[]>
 Authorization type:
 - "signcom_m365" : to access to M365 files and folders resources and Websites for SignCom application
 - "url_launcher_m365" : to access to M365 Websites for URL launcher application
 - "signmeeting_ews": to access to MS-Exchange room mailbox resources for SignMeeting MS-Exchange application
 - "signmeeting_m365": to access to M365 room mailbox resources for SignMeeting-M365 application
 - "briva_calendar_ews": to access to MS-Exchange room mailbox resources for Briva Calendar EWS application
 - "m365_room": to access to M365 room mailbox resource for SBL10e m365_room application
 - "m365_user": to access to M365 user presence resource for SBL10e m365_user application
 - "powerbi": to access to Power BI reports and Power BI dashboards

-LogFile <String>
 Log file path

<CommonParameters>
 This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, PipelineVariable, and OutVariable. For more information, see about_CommonParameters (<https://go.microsoft.com/fwlink/?LinkID=113216>).

----- EXAMPLE 1 -----

```
PS C:\>$result = New-AADApplication -appname "PowerBIApp" -authorizations "powerbi"
```

A consent request will be sent in 30 seconds in your browser.
You must log into an administrator account of your organization and grant the necessary permissions.

```
PS C:\>$result
Name          Value
----          -----
clientId      xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
objectId      xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
spId          xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
name          PowerBIApp
tenantId     xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
clientSecret xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Example to create an Azure Active Directory application for Gekkota

For example, to create a *powerbi* (free text) Azure AD application to view an online Microsoft *Power BI* report or *Power BI* dashboard, generate the *client Id*, the *tenant Id* and the *client secret* and store temporarily these values in the *powerbi_var* variable:

```
PS > $powerbi_var = New-AADApplication -appname "PowerBiApp" -authorizations "powerbi"
```

- ☞ Don't use an already existing app name else an error is returned.
- ☞ Don't use space characters in the app name else an error is returned.
- ⚠ Clicking on a Powershell window can suspend the command. In this case click again in the window to resume the command.

A login popup is displayed. Enter once your Microsoft 365 login credentials.

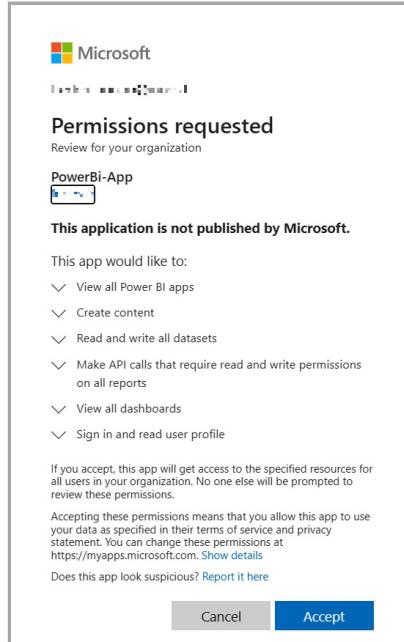
This message is then displayed in a *Powershell* context.

```
You must log into an administrator account of your organization and grant the necessary permissions.  
A consent request will be sent within 30 seconds in your browser.
```

After 30 seconds, a login popup should be prompted (<https://login.microsoftonline.com/>) automatically in your default web browser.

Enter again your *Microsoft 365* login credentials.

A new popup message with the *Permission requested, review for your organization* title is prompted in your web browser. Press on the *Accept* button. Then a message is displayed in your web browser showing that the consent is successful: *Success of the consent request*.



You can view the data of the created application by typing the following syntax

⚠ The following variable name is the same as the one you have used in the previous command above.

For example, to display the result of the previous command allowing to watch the *client Id*, the *tenant Id* and the *client secret* values:

```
PS > $powerbi_var
Name          Value
----          -----
clientId     xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
objectId     xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
spId         xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
name          PowerBiApp
tenantId     xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
clientSecret xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

The result of the *Powershell* function is also stored in a JSON file (in the example: `powerbi_var.json`).

Edit the file and store preciously the values required for your application:

- the `clientId` value,
- the `tenantId` value,
- the `clientSecret` value.

Example to delete an Azure Active Directory application

```
PS > Remove-AADApplication -appname "PowerBiApp"
```

A login popup is opened. Enter your M365 credentials.

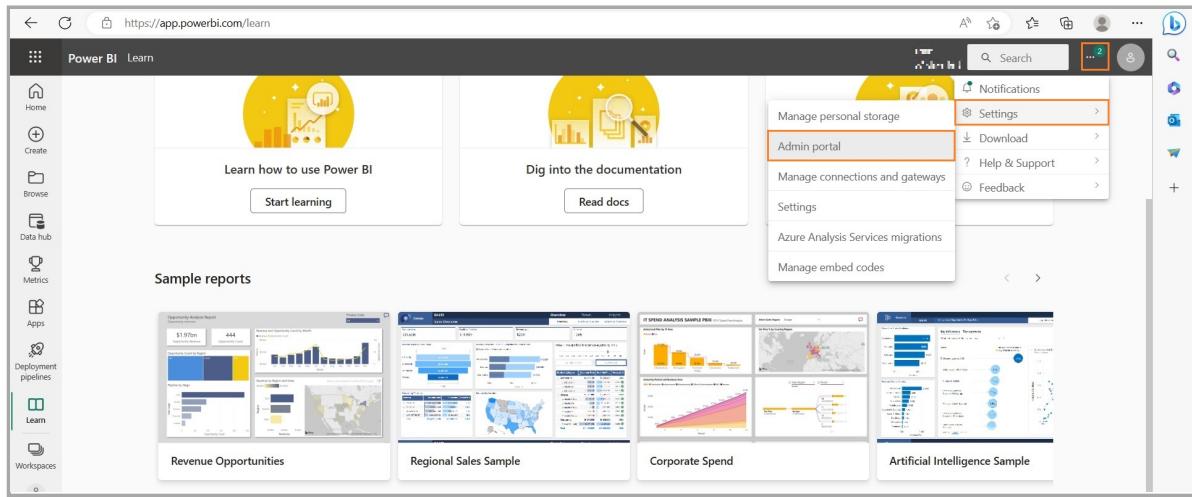
In case the values do not allow Power Bi Online viewer to work properly, check in *Microsoft Azure* portal that the application has been created successfully and the rights are properly granted. If not, wait for a while, the rights granting may take few hours.

8.18 Appendix: Power BI Online Viewer with Microsoft OAuth application mode: additional permissions

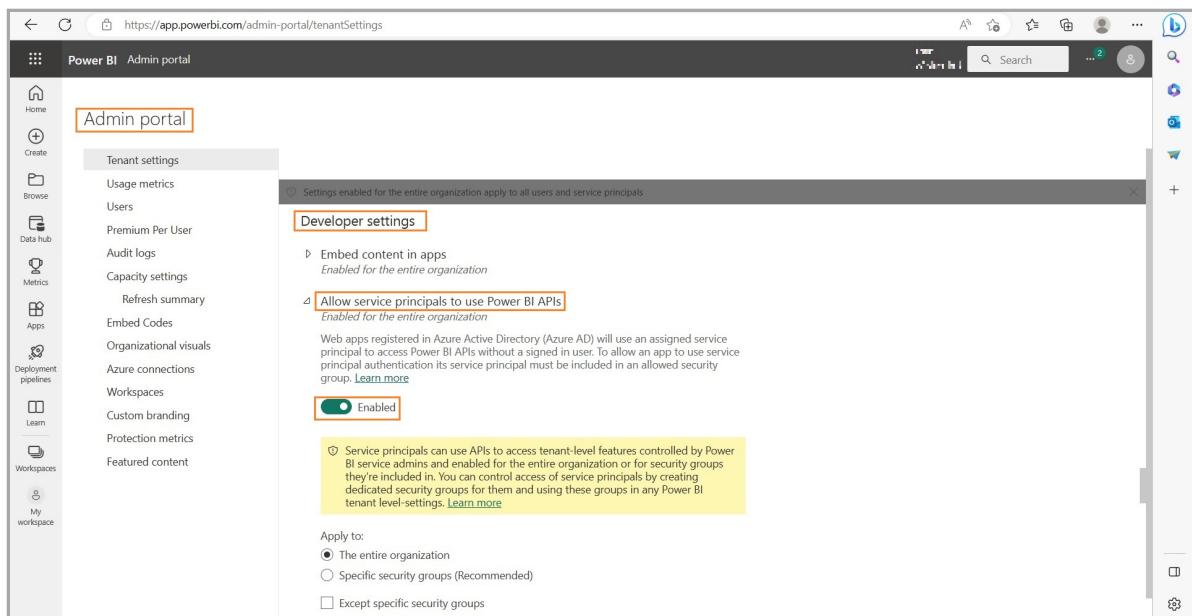
The configuration of Azure AD application does not allow to grant enough permissions to view the report when the Microsoft OAuth application mode is chosen. To finalize the granting of these additional permissions, follow these two steps.

Allowing Azure AD application to use Power BI APIs

Connect to the <https://app.powerbi.com> portal with a Microsoft 365 account having Power BI administration rights.



In the upper banner, click on the ... button then select the Settings item then the Admin portal item.



In the Admin portal pane, scroll to the top to find the Developer settings part. Select Allow service principals to use Power BI APIs, toggle the option to the right to the Enabled value, check the The entire organization option. Click on the Apply button to apply the modification.

Allowing the Azure AD application to access to the workspace hosting the report

Connect to the <https://app.powerbi.com> portal with a Microsoft account having rights to modify the workspace rights.

On the side tool banner, click on the Workspace item.

Click on the ... button of the workspace hosting your report and click on the Workspace Access item.

On the **Access** pane on the right, enter the name of the Azure AD application previously created (e.g. **PowerBi-App**) to access to the report, select the **Viewer** permission then click on the **Add** button.

Power BI reports coming from Power BI Desktop

Power BI reports published on your Power BI App workspace from Power BI Desktop are supported.

Report error 401

In case the report cannot be viewed with the **Power BI Online Viewer** App and an error 401 is raised, try with another report hosted on another workspace. To be successfully viewed, the Power BI report must consist in two part in the workspace:

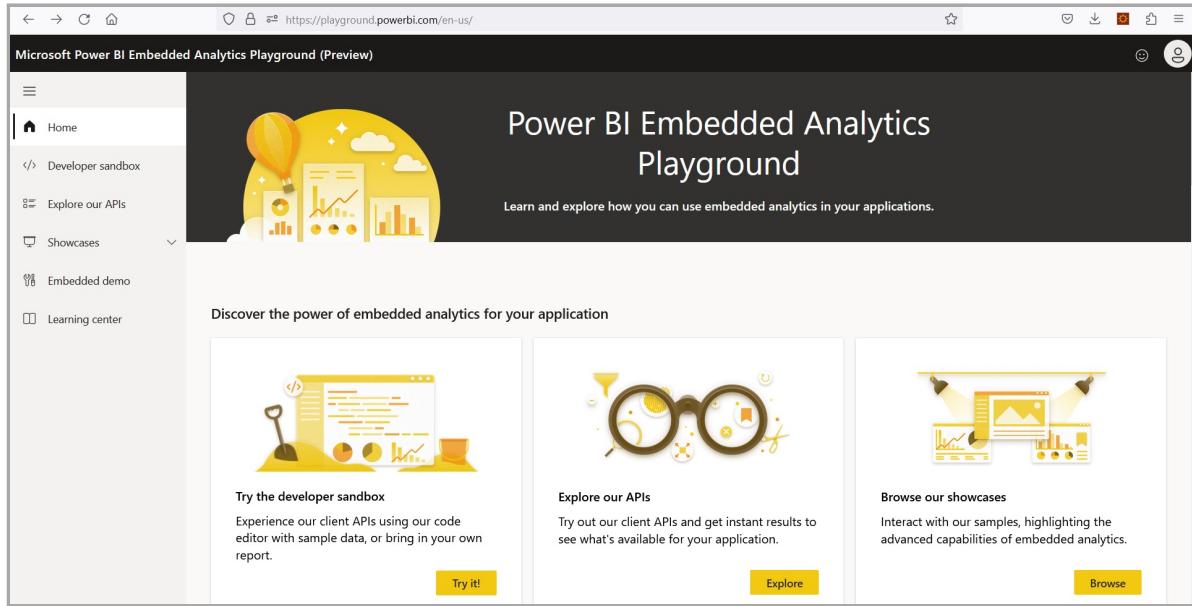
- data
- report

8.19 Appendix: Test your report with the Power BI Playground platform

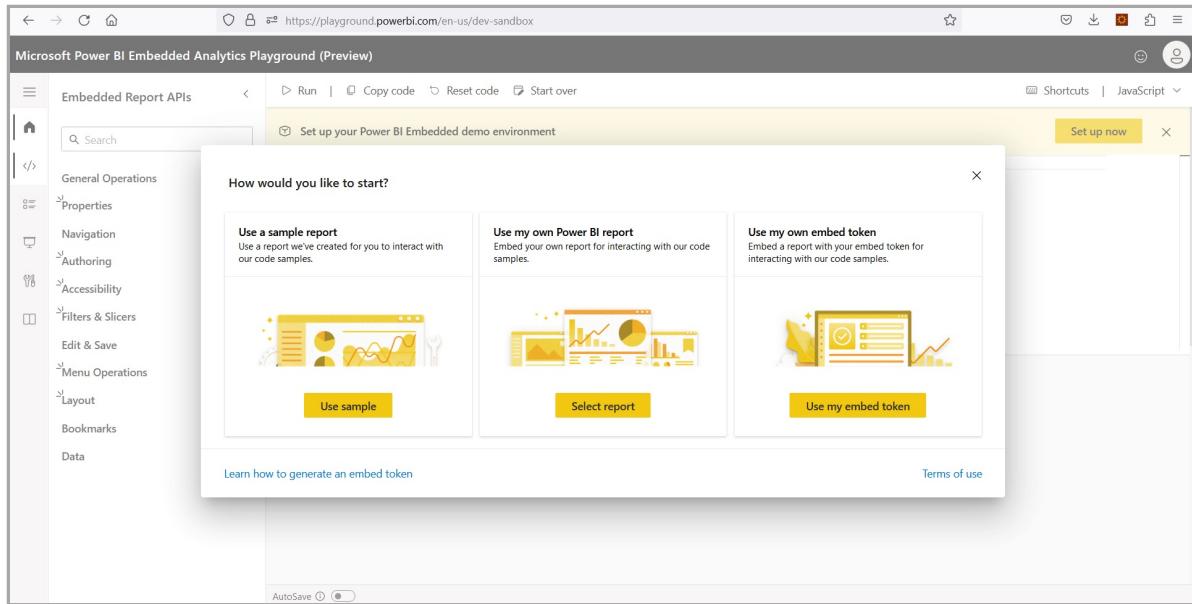
Before playing your report with the built-in *Power BI Online Viewer App*, check that your report can be embedded on device by using the *Power BI Playground* platform.

Connect to this portal <https://playground.powerbi.com/en-us/> by using your *Power BI service account*.

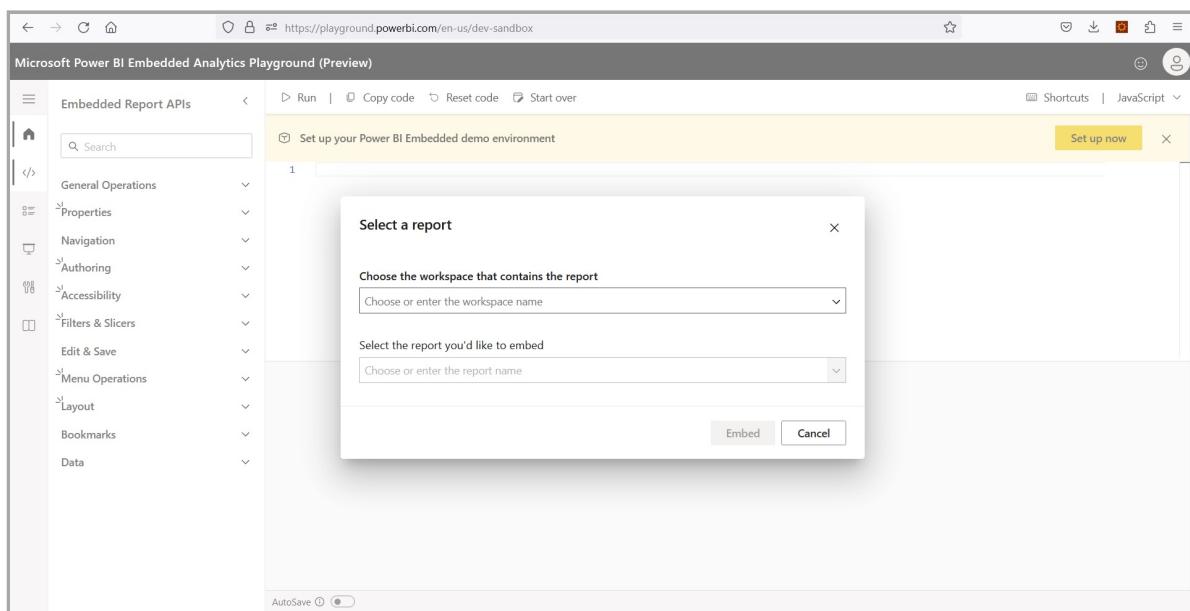
Click on the *Try it!* button of the *Try the developer sandbox* block.



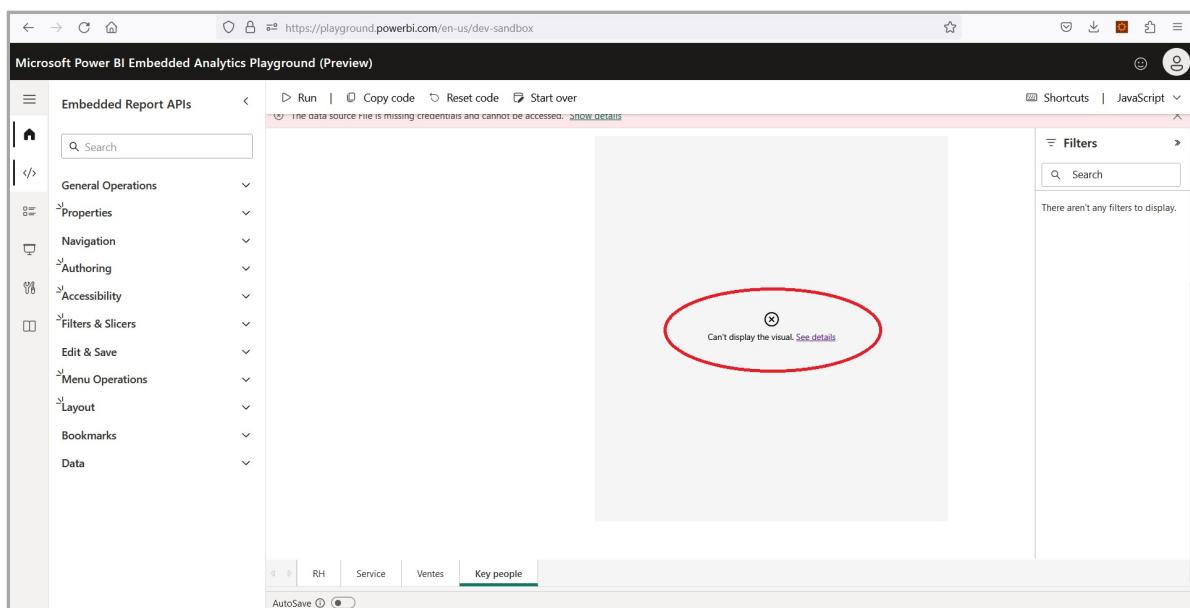
Click on the *Select report* button of the *Use my own Power BI report* block.



Select the *workspace* name where is hosted your report, then select your report in the selected *workspace*.



Navigate along all the pages of the report and check that all your data can be visualized.



In case error, try to resolve them in your *Power BI Desktop* or *Power BI service* and try again.

You can also click on the *See details* hyperlink of the vizualisation object in error. Copy the error then open a ticket on the *Microsoft Power BI* platform to raise the issue to Microsoft.

<https://admin.powerplatform.microsoft.com/newsupportticket/powerbi>

8.20 Appendix: Power BI Online Viewer known limitations

| Known limitations |
|--|
| API{} Data streaming visuals may not refresh properly by <i>Power BI Online Viewer</i> when using the <i>Microsoft OAuth User</i> credential type. To work around, use the <i>Microsoft OAuth Application</i> credential type. |
| The presence of some visualization object in the report, like the <i>Map</i> object, may prevent the report to progress to the next page. To work around, edit your <i>Power BI Desktop</i> report, remove from your report the visualization object causing the trouble then publish again your report from <i>Power BI Desktop</i> to <i>Power BI Services</i> . |
| Facing <i>HTTP 401</i> error when the report is played means that the credentials value are not consistent for this report or that a lack of <i>Power BI</i> report permissions prevent to view it. |

8.21 Appendix: Devices configuration using Powershell

Your park of Qeedji devices can be configured and maintained using the `PSDevice` Powershell module.

Introduction

This set of *Powershell* functions allows to:

for AQS devices :

- retrieve general information of device, with the `Get-AqsInfos` , functions,
- to retrieve all installed APPs, with the `Get-AqsApps` function,
- install new App with the `Install-AqsApp` function,
- remove an App with the `Remove-AqsApp` function,
- restart new App with the `Restart-AqsApp` function,
- stop new App with the `Stop-AqsApp` function,
- install a new firmware with the `Install-AqsFirmware` function.
- install a configuration script with the `Install-AqsConfiguration` function.

for Bm0032 devices :

- retrieve general information of device, with the `Get-Bm0032Infos` , functions,
- install a new firmware with the `Install-Bm0032Firmware` function.
- install a configuration script with the `Install-Bm0032Configuration` function.

for Gekkota devices :

- retrieve general information of device, with the `Get-GtkInfos` , functions,
- install a new firmware with the `Install-GtkFirmware` function,
- install a configuration script with the `Install-GtkConfiguration` function.

These functions are defined in the `PSDevice` PowerShell module stored in the `Modules\PSDevice\` directory.

Security

By default, the execution of local *Powershell* scripts are not allowed. You can change their execution rights by changing the *PowerShell* security policy. This modification has to be done once with the `Set-ExecutionPolicy` *Powershell* function. Your organization may have to change it according to your security rules.

For example, to authorize the execution of all scripts, launch a *Powershell* console with administrator rights, and type:

```
PS > Set-ExecutionPolicy -ExecutionPolicy Unrestricted -scope CurrentUser
```

For further information, look at the cmdlet `Set-ExecutionPolicy` help page.

If you cannot allow the execution of unsigned local scripts, you can install the provided certificate in the list of authorized root certificates with the command:

```
PS > cd <your_path_to_the_scripts>\Powershell_Innes_Device\Certificate\  
PS > Import-PfxCertificate -FilePath InnesCodeSigningRootCA_1.pfx -CertStoreLocation  
cert:\CurrentUser\Root -Password $(ConvertTo-SecureString "1234" -AsPlainText -Force)
```

To import the `.pfx` certificate, you can also use the MS-Windows application `certmgr.msc`, select the `Trusted Root Certification Authorities`, right clic on `All Tasks`, select the `Import` item, select the file and enter the password `1234`. When ended, close the current Powershell console.

Usage

To use Device *Powershell* modules, you have 3 possibilities:

1. Either copy the directories under `Modules\` into a standard *Powershell* module installation directory, for example "C:\Program Files\WindowsPowerShell\Modules". Then launch a *Powershell* console
2. Redefine the search variable for *Powershell* modules (the `$Env:PSModulePath` *Powershell* variable) each time you will use these functions. In this case, launch a *Powershell* console, and type the line below, adapting it to your path. Each time you will launch a new *Powershell* console, you will have to enter it again

For example:

```
PS > $Env:PSModulePath="$Env:PSModulePath;<your_path_to_the_scripts>\Powershell_Innes_Device\Modules"
```

3. Or redefine the search variable for *Powershell* modules in the Windows environment variables. For that, add the path `<your_path_to_the_scripts>\Powershell_Innes_Device\Modules` to the environment variable `PSModulePath`. Then, launch afterwards a *Powershell* console.

To use the functions or get help, you must then import the module(s) with the `Import-Module` function. Example:

```
PS > Import-Module PSDevice
```

Depending on how you get the scripts, you may have this following warning:

```
Security Warning Run only scripts that you trust. While scripts from the Internet can be useful,
this script can potentially harm your computer. Do you want to run \device\scripts\my.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"):
```

To avoid this message, you can unblock the script files (to do only once):

```
PS > cd <your_path_to_the_scripts>\Powershell_Innes_Device\
PS > dir -Recurse | Unblock-File
```

The `Get-Command` function allows you to list the functions defined in a module. Example:

```
PS > Get-Command -Module PSDevice
```

Answer example:

| CommandType | Name | Version | Source |
|-------------|-----------------------------|---------|----------|
| ----- | ---- | ----- | ----- |
| Function | Disable-AqsApp | 1.10.10 | PSDevice |
| Function | Enable-AqsApp | 1.10.10 | PSDevice |
| Function | Get-AqsApps | 1.10.10 | PSDevice |
| Function | Get-AqsInfos | 1.10.10 | PSDevice |
| Function | Get-Bm0032Infos | 1.10.10 | PSDevice |
| Function | Get-GktInfos | 1.10.10 | PSDevice |
| Function | Install-AqsApp | 1.10.10 | PSDevice |
| Function | Install-AqsConfiguration | 1.10.10 | PSDevice |
| Function | Install-AqsFirmware | 1.10.10 | PSDevice |
| Function | Install-Bm0032Configuration | 1.10.10 | PSDevice |
| Function | Install-Bm0032Firmware | 1.10.10 | PSDevice |
| Function | Install-GktConfiguration | 1.10.10 | PSDevice |
| Function | Install-GktFirmware | 1.10.10 | PSDevice |
| Function | LogWrite | 1.10.10 | PSDevice |
| Function | Remove-AqsApp | 1.10.10 | PSDevice |
| Function | Restart-AqsApp | 1.10.10 | PSDevice |
| Function | Stop-AqsApp | 1.10.10 | PSDevice |
| Function | Test-AqsDevice | 1.10.10 | PSDevice |
| Function | Test-Bm0032Device | 1.10.10 | PSDevice |
| Function | Test-GktDevice | 1.10.10 | PSDevice |

You can get help on each function of the module by using the standard cmdlet `Get-Help` with options:

- `-detailed`,
- `-full`,
- `-examples`.

Example:

```
PS > Get-Help -detailed Install-AqsApp
```

Examples

To use the examples, copy the directories `Examples\` into a standard *Powershell* module installation directory, for example "C:\Program Files\WindowsPowerShell\Modules".

In the directory `Examples`, you can find different powershell scripts which uses the functions of the modules.

You can get help on each example scripts, for example:

```
PS > Get-Help -detailed .\Examples\Example1\Get-DevicesInfos.ps1
```

Example 1: Get-DevicesInfos

The script `Examples\Example1\Get-DevicesInfos` is an example to retrieve informations about a pool of devices described in a json file. It uses the module `PSDevice`.

Example:

```
PS > cd <your_path_to_the_scripts>\Examples\Example1\  
PS > .\Get-PSDevice.ps1 -LogFile result.json
```

If any error occurs, look at the logfile (`result.json` in the example) to see what the problem may be.

This is an example of report:

```
[  
  {  
    "host": "192.168.0.74",  
    "info": {  
      "Psn": "01540-00657",  
      "Platform": "AMP300",  
      "Version": "9.10.19",  
      "Hostname": "AMP300-floor1",  
      "runningApps": [  
        {  
          "Label": "PowerPoint Publisher",  
          "Version": "1.15.10"  
        },  
        {  
          "Label": "PowerPoint Publisher UI",  
          "Version": "1.15.10"  
        }  
      ]  
    }  
  },  
  {  
    "host": "192.168.0.92",  
    "info": {  
      "Psn": "01320-00039",  
      "Hostname": "sbl10-floor2",  
      "Firmware": "bm0032_m365_user-sbl10e-1.12.10",  
      "Platform": "SBL10e"  
    }  
  },  
  {  
    "host": "192.168.0.91",  
    "info": {  
      "Psn": "00910-00216",  
      "Hostname": "DMB400-hall1",  
      "FirmwareVersion": "5.11.13",  
      "Platform": "dmb400"  
    }  
  },  
  {  
    "host": "192.168.10.91",  
    "error": "Not responding"  
  }  
]
```

Example 2.1: upgrade firmware

The script `Examples\Example1\Install-Devices` is an example to install firmware, an app, or a configuration script on a pool of devices described in a json file. The type of component to install is specified with the `-installType` option which can be "install", "app" or "configuration". The components to be installed are stored in the directory specified by the `"installDirPath"` option. Each type of device has an associated subdirectory:

- `aqs` for Aqs device,
- `gekkota` for Gekkota device,
- `bm0032` for Bm0032 device.

It uses the module `PSDevice`.

Open the `Examples\Example2\devices.json` and update with the values corresponding to the devices concerned:

- IPV4 adress,
- WebDAV server login,
- WebDAV server password.

In case you wish to upgrade the firmware of your park of AQS devices, do copy the appropriate firmware `.fqs` into the following directory:

- `Examples\Example2\install\ajs\`

In case you wish to upgrade the firmware of your park of Gekkota devices, do copy the appropriate firmware `.frm` into the following directory:

- `Examples\Example2\install\gekkota\`

In case you wish to upgrade the firmware of your park of Bm0032 devices, do copy the appropriate firmware `.bin` into the following directory:

- `Examples\Example2\install\bm0032\`

Command line example:

```
PS > cd <your_path_to_the_scripts>\Examples\Example2\
PS > .\Install-Devices.ps1
```

If any error occurs, look at the logfile (`result.json` in the example) to see what the problem may be.

Example 2.2: change device configuration

In case you wish to change the configuration of your park of AQS devices, do copy the appropriate `<MAC>.js` configuration script into the following directory:

- `Examples\Example2\install\ajs\`

In case you wish to change the configuration of your park of Gekkota devices, do copy the appropriate `<MAC>.js` configuration script into the following directory:

- `Examples\Example2\install\gekkota\`

In case you wish to change the configuration of your park of Bm0032 devices, do copy the appropriate `<MAC>.js` configuration script into the following directory:

- `Examples\Example2\install\bm0032\`

Copy the `Install-Devices.ps1` file, paste it in the same directory and rename it `Configure-Devices.ps1`. Replace in it the part `[string] $installType = "install"`, by the part `[string] $installType = "configuration"`,

Open the `Examples\Example2\devices.json` and update with the values corresponding to the devices concerned:

- IPV4 adress,
- WebDAV server login,
- WebDAV server password.

Example 2.3: install APK

In case you wish to install some APK in your park of AQS devices, do copy the appropriate `.apk` into the following directory:

- `Examples\Example2\install\ajs\`

Copy the `Install-Devices.ps1` file, paste it in the same directory and rename it `InstallApk-Devices.ps1`. Replace in it the part `[string] $installType = "install"`, by the part `[string] $installType = "app"`,

Open the `Examples\Example2\devices.json` and update with the values corresponding to the devices concerned:

- IPV4 adress,
- WebDAV server login,
- WebDAV server password.