Qeedji

User manual

DMB400

5.12.10 001A

Legal notice

DMB400 5.12.10 (001A_en)

Rights and Responsibilities

Product information

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

Precautions for use

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

Warranty clauses

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

WEEE Directive

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

Table of contents

Part I

Description and installation

1.1 Introduction

This manual explains how to install and configure your DMB400 device.

Recommendations and warnings

This device is designed to be used indoor.

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

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

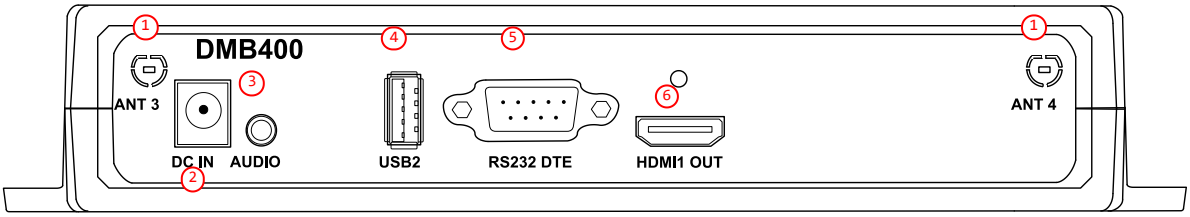
Content of the package

Items	Description	Quantity
Device	DMB400 device with Gekkota embedded.	1
Power supply unit	12 V power supply unit with cable of 1.2 m.	1
Labels	One on the cardboard packaging and another one at the back of the product. *Additional label can be present in case build-in options.*	2
WLAN antennas	To be screwed on the dedicated WLAN locations. *Provided with the device when it is supporting the `WLAN` option.*	2

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

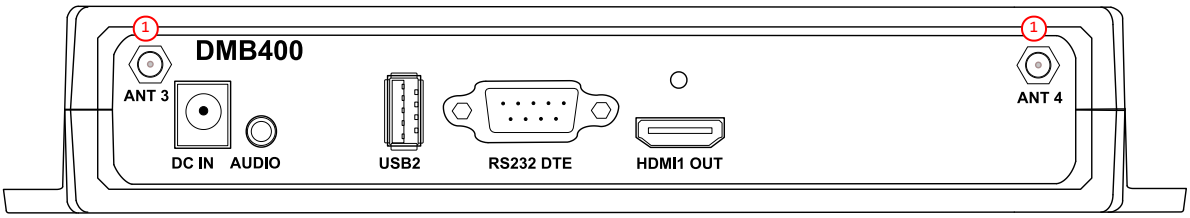
1.2 Getting started

Device front face



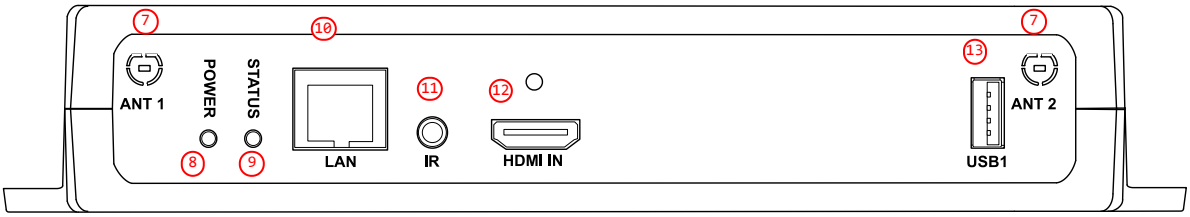
- (1) Antennas locations,
- (2) Power supply connector,
- (3) Audio connector,
- (4) USB2 3.0 connector,
- (5) RS232 DTE connector,
- (6) HDMI output connector.

Device front face with the WLAN option



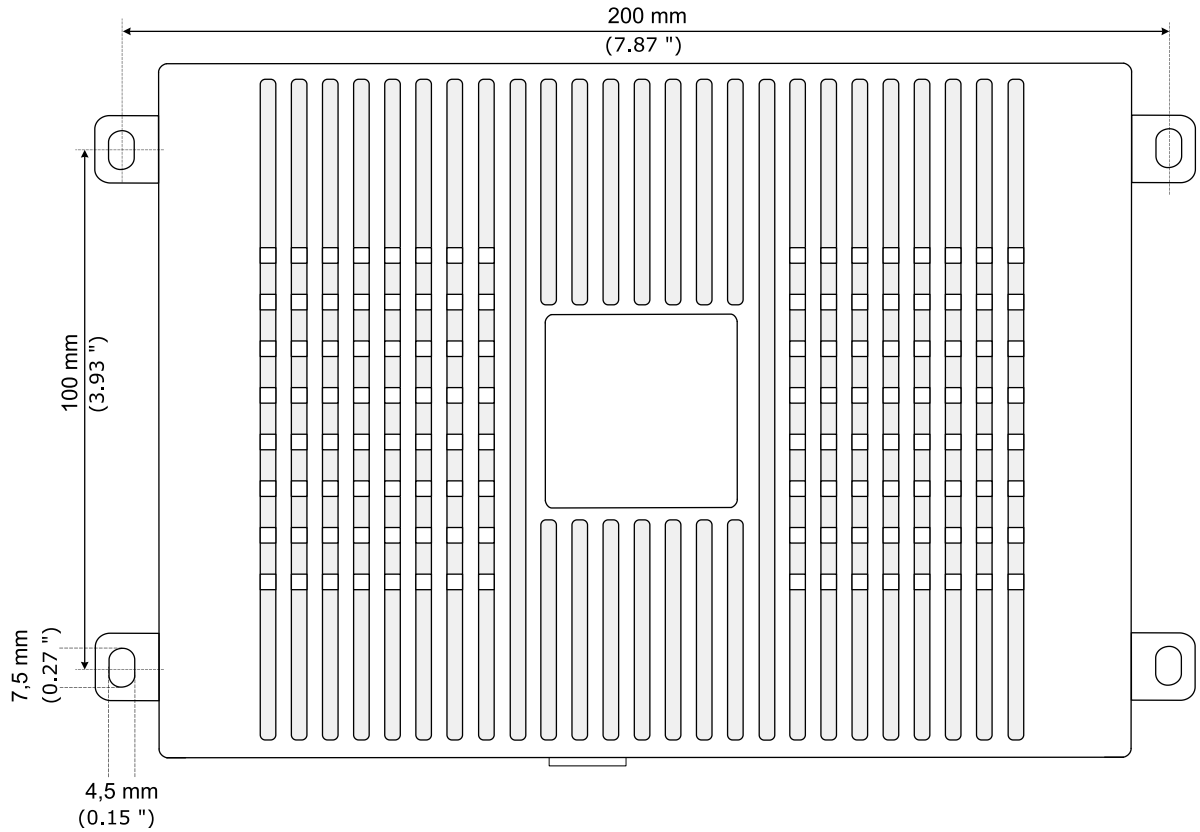
- (1) Location of the 2 WLAN antennas to screw.

Device rear face

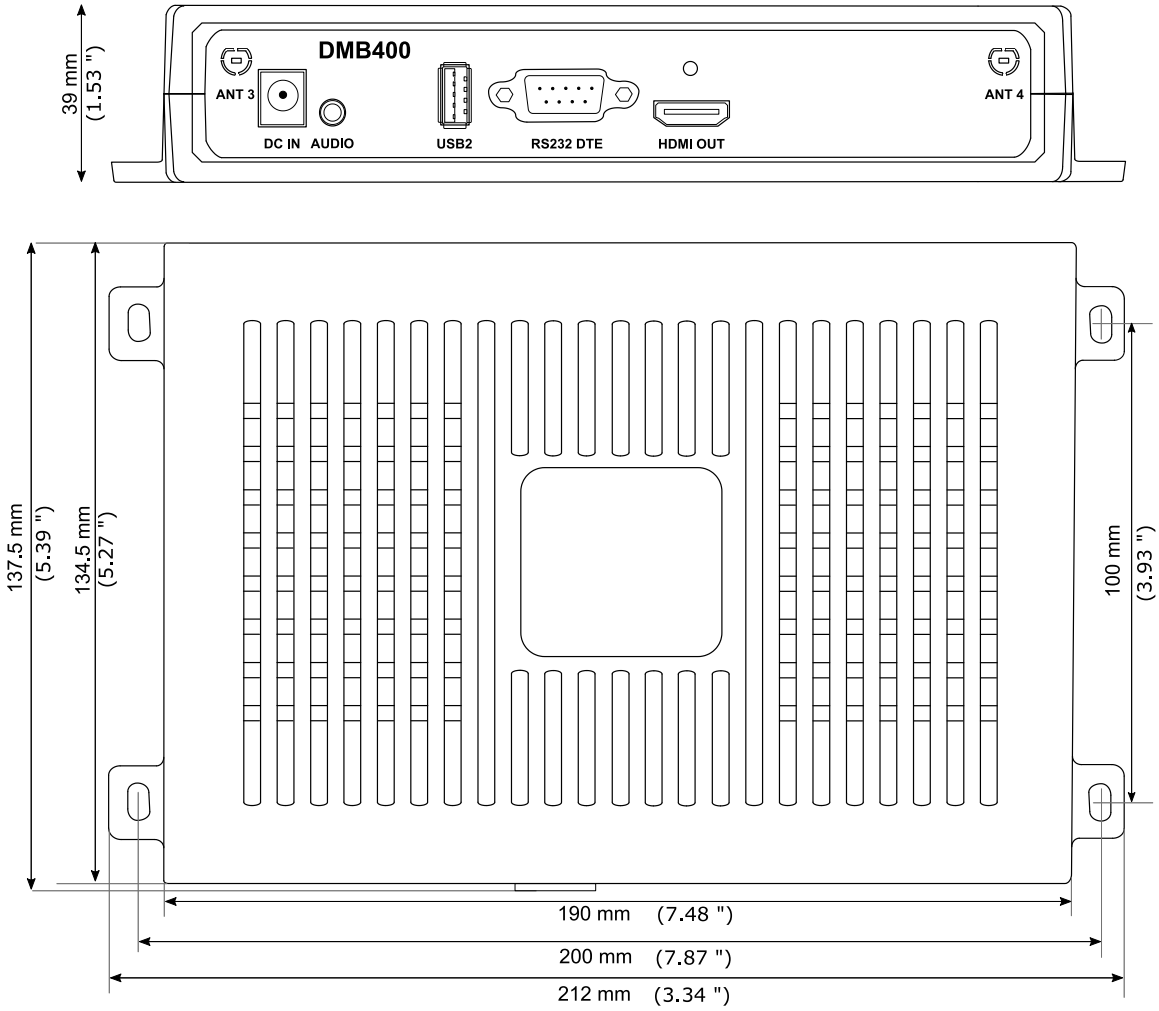


- (7) Antenna location,
- (8) Power supply red LED,
- (9) Status green LED,
- (10) LAN RJ45 connector,
- (11) GPIO/Infrared connector,
- (12) HDMI input connector,
- (13) USB1 2.0 connector.

1.2.1 Device fixture



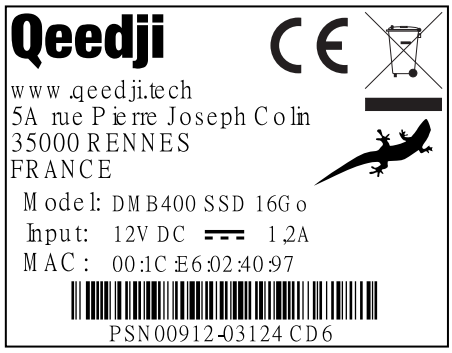
1.2.2 Device dimensions



1.2.3 Labelling

Product label

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



Packingbox label

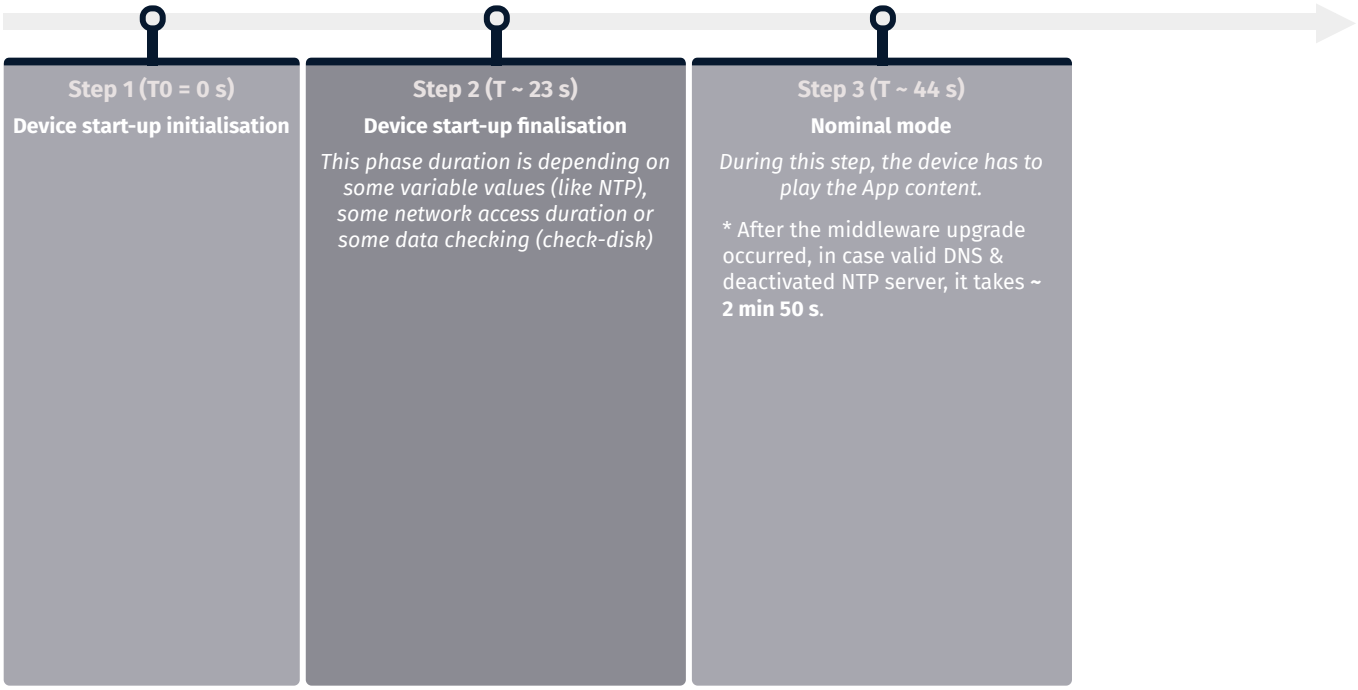
This is the label stuck also on the packingbox. It is showing information on:

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

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

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

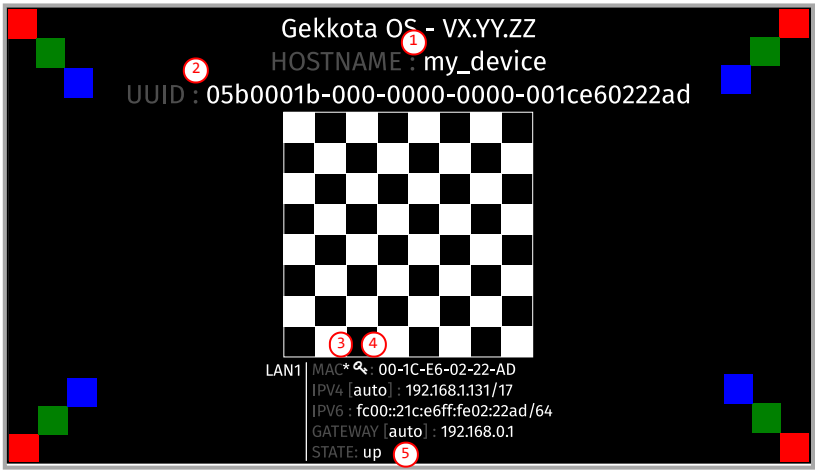
1.2.4 Device start-up steps



1.2.5 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.

This is an example of test pattern content that is displayed when the *test card* is activated.



> ☛ *The `*` star pictogram is showing the chosen identification method in the device. It can be `HOSTNAME` (1), `UUID` (2) or `MAC` (3). In the example, the star is showing the `MAC` identification method (default value).*
>
> ☛ *The key pictogram (4) is showing the MAC address value associated to the Gekkota license key.*
>
> ☛ *The `up` STATE (5) is meaning that the network interface currently showed is alive. If the STATE is `down`, the network interface is not alive.*
>
> ☛ *When the test card is activated, the content of the App is not displayed. To play the App again, you must deactivate the `Test card`.*

The `Test Card` can be deactivated by using the device configuration Web user interface.

If the CEC is activated on your display device, and the CEC pass-through feature is fully supported by your display device, the test card content can be displayed or undisplayed thanks to the display device remote control with these key sequence:

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

> ☛ *Your display device must support a remote control and supports properly the CEC.*
>
> ☛ *So that your remote control key presssing is taken into account, ensure that there is no OSD menu or OSD banner displayed over the content.*
>
> ☛ *For SAMSUNG display devices, the CEC activation is often made by activating the `Anynet` feature.*
>
> ☛ *For LG monitors, the CEC activation is often made by activating the `Simplink` feature.*
>
> ☛ *In case the key sequence is not more taken into account, some display devices may require to unselect then select again the HDMI input on which the device is connected to force a `CEC_Set_Input_Source` before applying the key sequence. Some others may require to refresh the `Anynet` peripherals with the `TOOLS` key of the remote control.*

If you have an USB keyboard connected to an USB hub, the same key sequence is supported:

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

This user preference needs to be set to *true* to support the test card displaying/undisplaying thanks to an USB keyboard:

- `innes.player.mire.key-event.*.authorized`.

These user preferences need to be set to *true* to support the test card displaying/undisplaying by CEC thanks to display device's remote control:

- `innes.player.mire.key-event.*.authorized`,
- `system.connector.*.*.cec.cec_1.enabled`.

1.3 LEDs behaviour

LED POWER behaviour (power on device)

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

LED LAN behaviour (power on device)

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

LED STATUS behaviour depending on device start-up steps

• Step 1: Device start-up initialisation

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

• Step 2: Device start-up finalisation

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

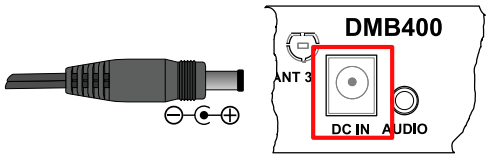
• **Step 3: Nominal mode**

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

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

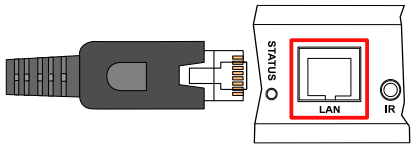
1.4 Connectors pin-out

Power supply connector (12 V DC - 1.2 A)



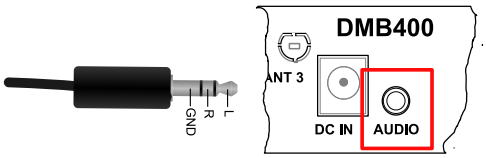
LAN connector

Ethernet RJ-45. 10/100/1000 BaseT. It is recommended to use shielded cables.



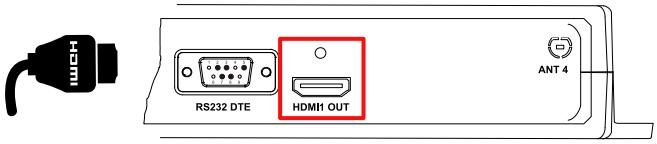
Audio Jack 3.5 mm connector (stereo L+R)

It is recommended to use cables whose length is less than 3 meters.



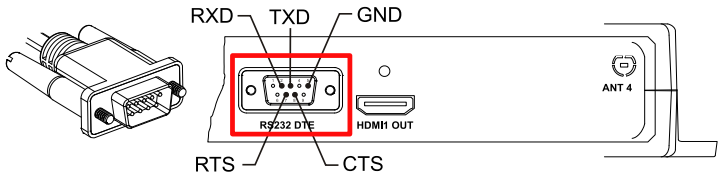
Video output connector (HDMI 2.0)

This connector is used to connect a screen or video projector.



RS232 DTE connector

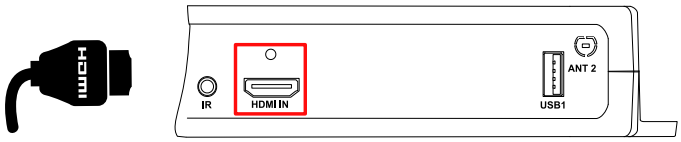
It is recommended to use cables whose length is less than 3 meters.



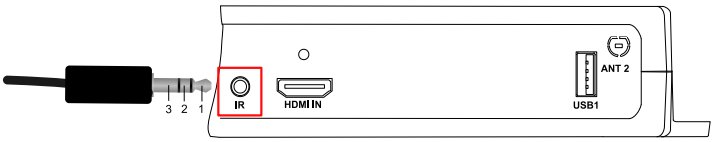
RS232 DTE connector pin-out:

N°	Function
1	CD
2	RXD
3	TXD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	-

Video input connector (HDMI 1.4)



Jack 3.5 mm connector (GPIO1/IR)



N°	Name	Write/Read	Control
1	Voltage reference 3.3 V		
2	GPIO1	IN or OUT	CPU/GPIO1
3	Ground		

Electrical features

	Vin min	Vin max	VOH min	VOL max	VIH min	VIL max
GPIO1	-0.5 V	3.6 V	2.9 V	0.4 V	2.0 V	0.8 V

The 3.3 V pin must not be used as power supply, but rather as a reference voltage.

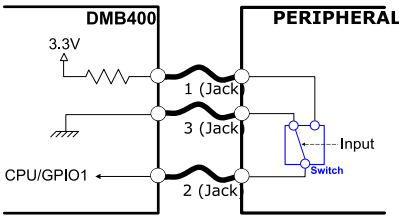
Along the device booting, the GPIO1 is configured as input during some seconds. And then after the system startup, the GPIO1 is operational.

The GPIO has a weak pull-up.

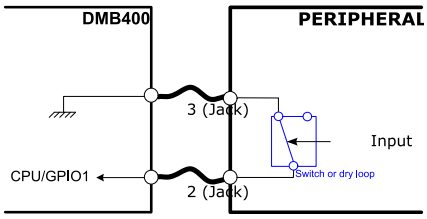
It is not recommended to hotplug/unplug the GPIO1 connector, which could damage the device.

Principle schematics for several use cases

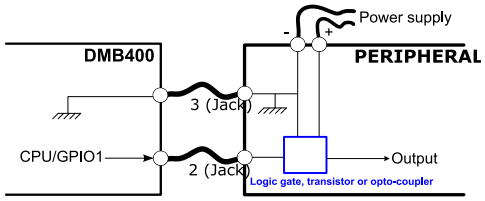
Three wires input configuration for GPIO1:



Two wires input configuration for GPIO1:



Output configuration for GPIO1:



Configuration

GPIO1 connector configuration can be done by editing the user preferences using the device configuration Web user interface or with a configuration script. The GPIO1 configuration part for this script is described here:

How to configure the Jack 3.5 mm connector:

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

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

Part II

Applicative user interface

2.1 Applicative user interface

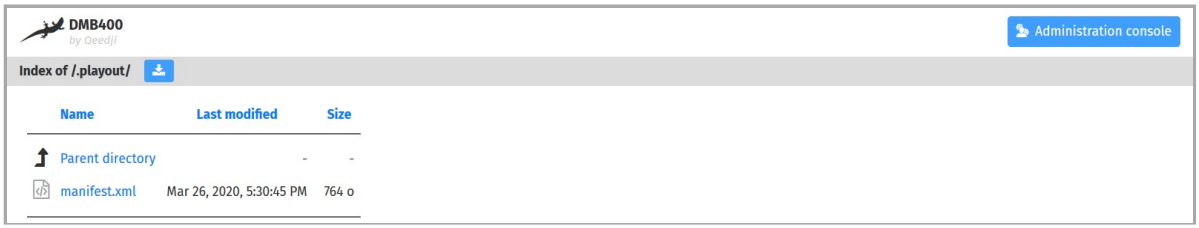
The DMB400 device supports a Web user interface that can be accessed with a Web browser. The supported Web browsers are: `Google Chrome`, `Mozilla Firefox`, `MS-Edge (Chromium)`.

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

The defaut credentials values, put at factory, to access to the device Web user interface are:

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

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



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

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

Part III

Administration console user interface

3.1 device configuration Web user interface

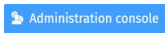
The DMB400 device supports a device configuration Web user interface that can be accessed with a Web browser. The supported Web browsers are: `Google Chrome`, `Mozilla Firefox` and `MS-Edge (Chromium)`.

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

The default credentials values, put at factory, to access to the device Web user interface are:

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

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



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

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

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

> ⚠ It is desirable that your device DMB400 device is on time. When possible, do synchronize it with an NTP server.

This is the device configuration Web user interface.

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

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

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

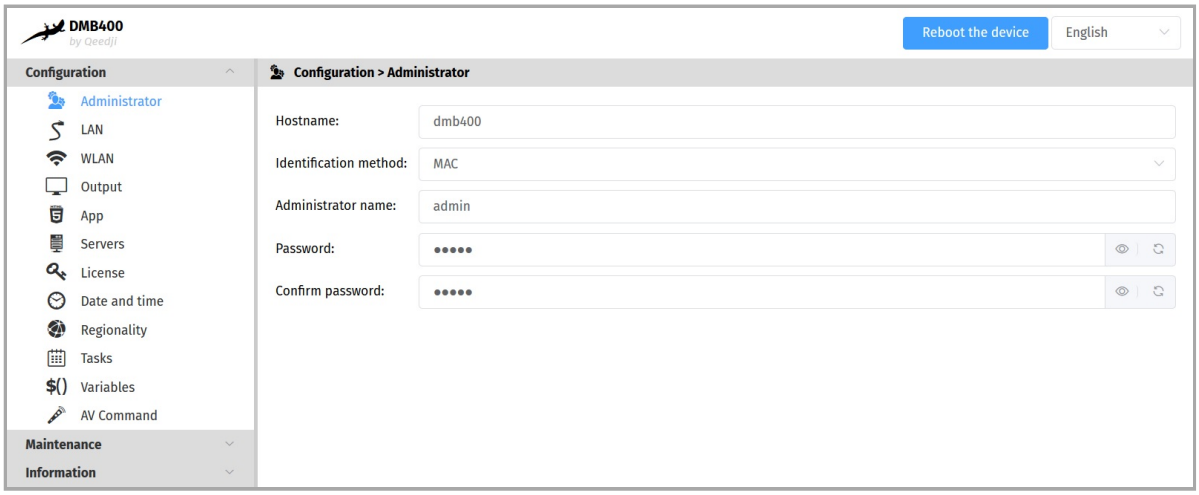
```
For example, for the MAC address value: ``00-1c-e6-02-1e-45`,
In a Web browser, enter the URL: http://[fc00::21c:e6ff:fe02:1e45]/.admin/
```

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

3.1.1 Configuration > Administrator

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

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



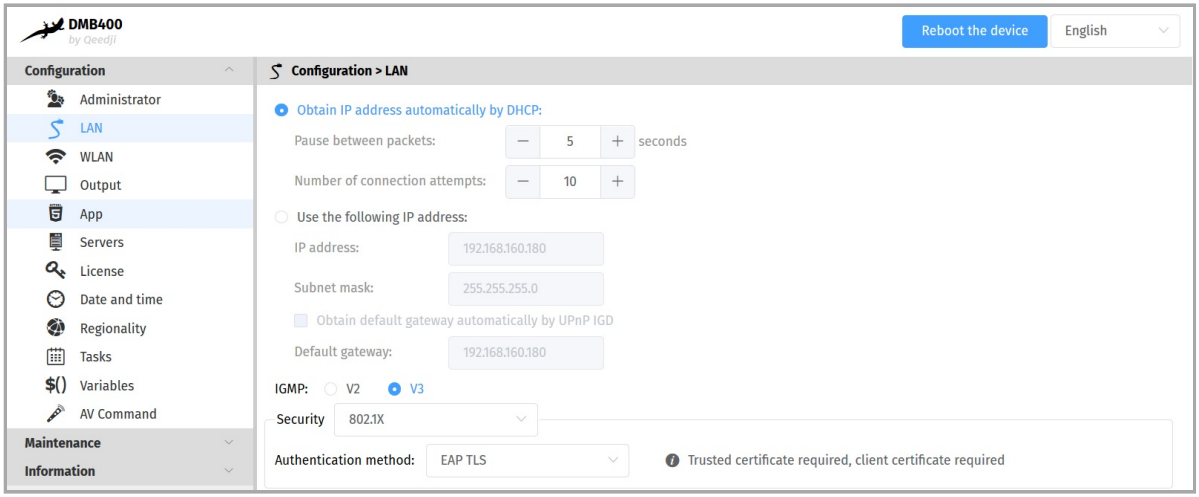
> ☛ *It is recommended that you enter one unique `Hostname` value for each device. In case several DMB400 devices are located in different buildings or geographical locations, we recommend that you enter hostname values with information about the building and the location (e.g. `Hall-RD-Paris-1`).*

For security reasons, it may be useful to change the login credentials values. Please keep them in a safe place afterwards.

> ☛ *The same login credentials are used to access to the WebDAV server and to use Web services.*

3.1.2 Configuration > LAN

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



The connection to the device configuration Web user interface with the device IPV6 address, computed from the device MAC address value, is supported. For example, if the LAN MAC address of the device is *00-1c-e6-02-27-bf*, type the URL `http://[fe80::21c:e6ff:fe02:22ad]/` or type `http://[fc00::21c:e6ff:fe02:22ad]/` in a Web browser. The routable prefix is depending on your network configuration.

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

- security: *None*.

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

- security: *802.1x*.

> ☛ *In the context of a secure network, your device must be first declared in your dedicated RADIUS server with a user `login` / `password`. Given that the login credentials used by Qeedji devices for all the 802.1X authentication methods are the LAN MAC address value of the DMB400 device, any new Qeedji device entry must be registered in your RADIUS server with these specific values with the format `abcdefabcdef` / `abcdefabcdef` for a MAC address ab-cd-ef-ab-cd-ef. Some `identification methods` may require you add a `trusted certificate`, used by your RADIUS server and/or a `client certificate`, generated with the MAC address of your device, the radius users credentials and the trusted certificate of the RADIUS server; For further information, please contact your IT department.*
>
> ☛ *When using a 802.1X certificate with an expiration date, in case your device is not on time or when the expiration date has expired, the device is not able to access to the network anymore. To work around, you have to insert one USB stick containing a specific configuration script to set either a new certificate or update the device date and time.*

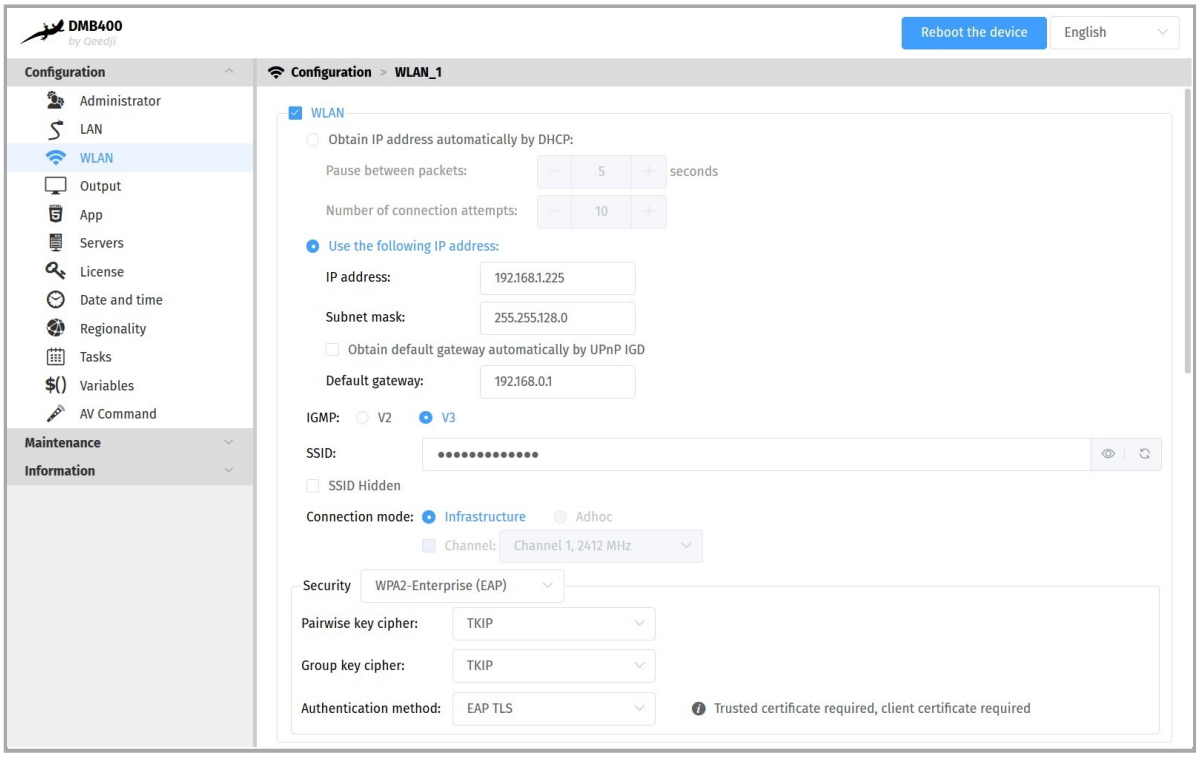
> ☛ *The device supports the UPnP and can be for example detected automatically in the local network environment of your computer.*

> ☛ *By default, the device is configured with DHCP activated. In case the DHCP server is not available, after the DHCP timeout, the device ends up using the static IP address whose default value is 192.168.0.2 when it has never been changed yet by the user. It is recommended to set an appropriate IP address, netmask and gateway if this case would happen.*

3.1.3 Configuration > WLAN

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

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



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

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

The maximum lengths for WLAN crypto keys are:

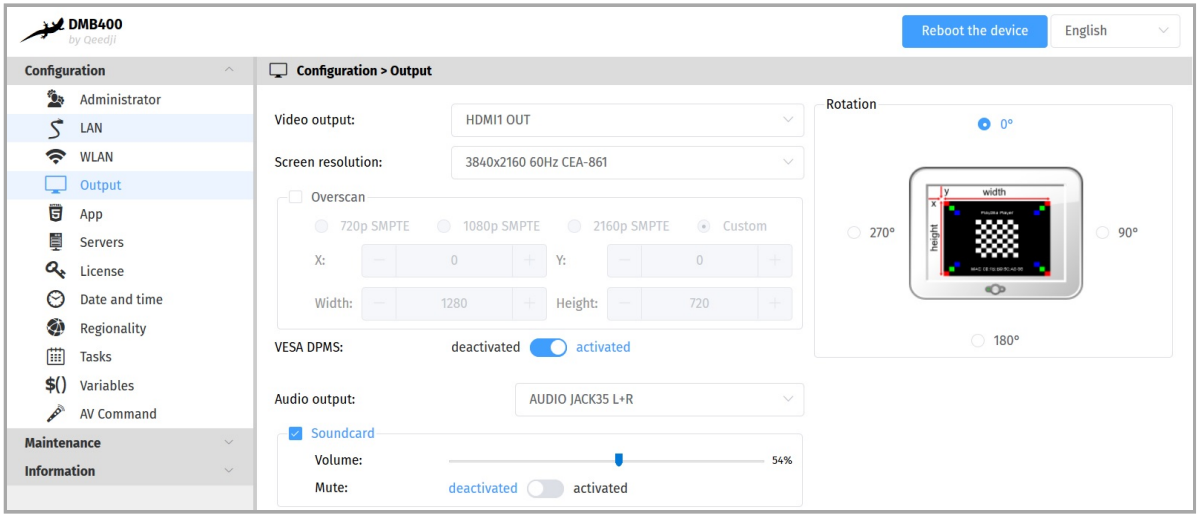
- for `WEP` key:
  - 26 hexadecimal characters max.
- for `WPA-Personal (PSK)` and `WPA2-Personal (PSK)` keys:
  - 63 ASCII characters max.

> ☛ *`TKIP` pair (or group) key encryption is not supported if the router is in `IEEE 802.11n` mode.*
>
> ☛ *Some computer OS version may not support `Adhoc` connection. For further information, contact your IT department.*
>
> ☛ *Selecting the WPA-Enterprise (EAP) or WPA-Enterprise (EAP) security implies that your device is located in a secure network, and therefore connects to a properly configured WIFI router with a dedicated RADIUS server.*
>
> ☛ *In the context of a secure network, your device must be first declared in your dedicated RADIUS server with a user `login` / `password`. Given that the login credentials used by Qeedji devices for all the 802.1X authentication methods are the LAN MAC address value of the DMB400 device, any new Qeedji device entry must be registered in your RADIUS server with these specific values with the format `abcdefabcdef` / `abcdefabcdef` for a MAC address ab-cd-ef-ab-cd-ef. Some `identification methods` may require you add a `trusted certificate`, used by your RADIUS server and/or a `client certificate`, generated with the MAC address of your device, the radius users credentials and the trusted certificate of the RADIUS server; For further information, please contact your IT department.*

The `WLAN` interface activation is not checked by default.

3.1.4 Configuration > Output

In the `Configuration` tab, select the **Output** menu to configure, among other things, the unit's video and audio output.



- `Screen resolution` :
  - `Resolution` : *96x96* to *3840x2160*.
  - `Mode` : *SMPTE*, *VESA*, *CEA-861*, *SONY*, *SAMSUNG*, *CGV CPLine AV-HD*, *PC*, *DENSITRON*, *XGA*, *LESTEL*, *LINSN*, ...
  - `Frequency` : *25 Hz*, *30 Hz*, *45 Hz*, *60 Hz*, *50 Hz*.
- `Overscan` :
  - *720p SMPTE*,
  - *1080p SMPTE*,
  - *2160p SMPTE*,
  - *Personalized*:
    - `X` : horizontal origin of the viewport in pixel,
    - `Y` : vertical origin of the viewport in pixel,
    - `Width` : width of the viewport in pixel,
    - `Height` : height of the viewport in pixel.
- `Rotation` : *0°*, *90°*, *180°*, *270°*.
- `VESA DPMS` : *on* (horizontal/vertical sync standby on) or *off* (horizontal/vertical sync standby off) [1].
- `Audio output` : *AUDIO JACK35 L+R*.
- option `Sound card` : allows to activate or deactivate the sound card:
  - `Volume` : *0..100%*,
  - option `Mute` : *on* (mute) or *off* (mute on).

> ☛ *The rotation is not supported for resolutions higher than 1920x1080.*
>
> ☛ *Some screens may not support certain display modes. In this case, try another mode with the same resolution.*
>
> ☛ *When supported by your screen and your device, if possible use a 60 Hz mode which is the smoothest mode for scrolling text.*
>
> [1] VESA DPMS sleep and standby output is performed either by a screen sleep task programmed into an App, or by a power management task with the `strongly optimized` mode.

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

3.1.5 Configuration > App

In the `Configuration` tab, select the **App** menu to select how the App must be loaded.

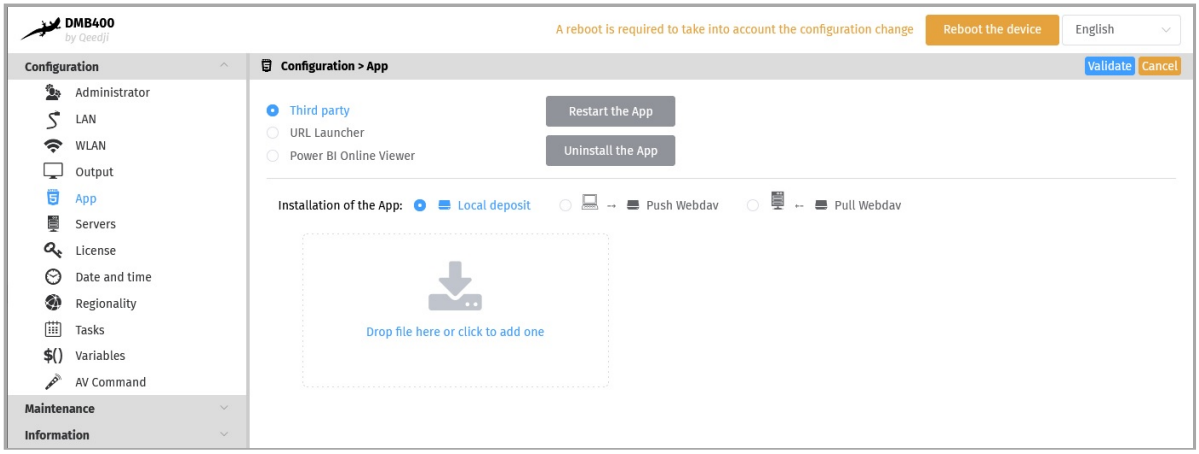
Select the `Third party` radio button to play an App:

- with the `local deposit` mode,
- with the `Push WebDAV` mode,
- with the `Pull WebDAV` mode.

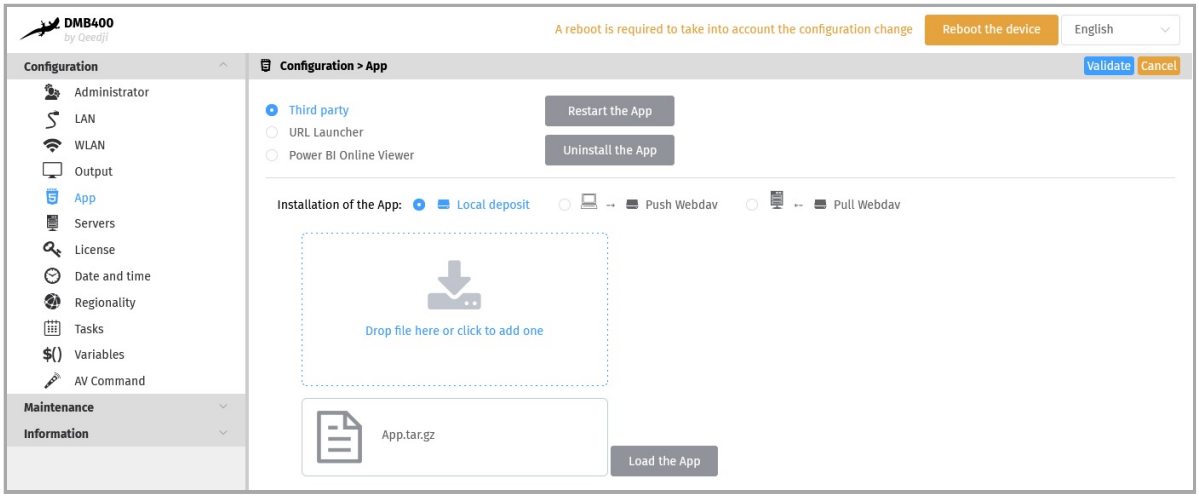
For each of these modes, you can use the `Uninstall the App` or `Restart the App` buttons at any time to remove the `App` from the device or restart it respectively.

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

- `Local deposit` : Allows to load an App from the device Web user interface. The App can start for the first time only after a device reboot.



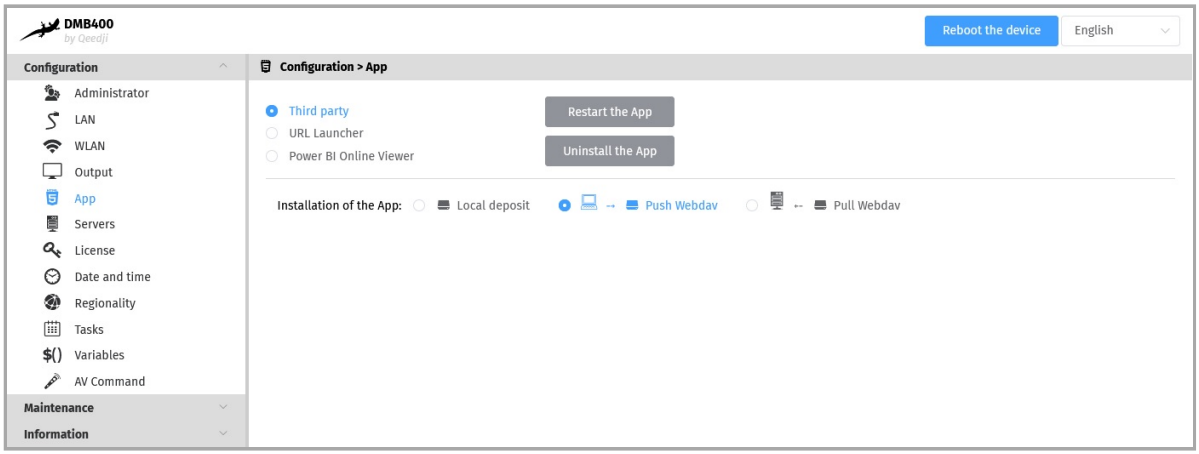
Use the `Drop file here or click to add one` box to drop your `App`.



Then click on the `Load the App` button. When the file disappears from the interface, the App is loaded. Restart the device once to start the App.

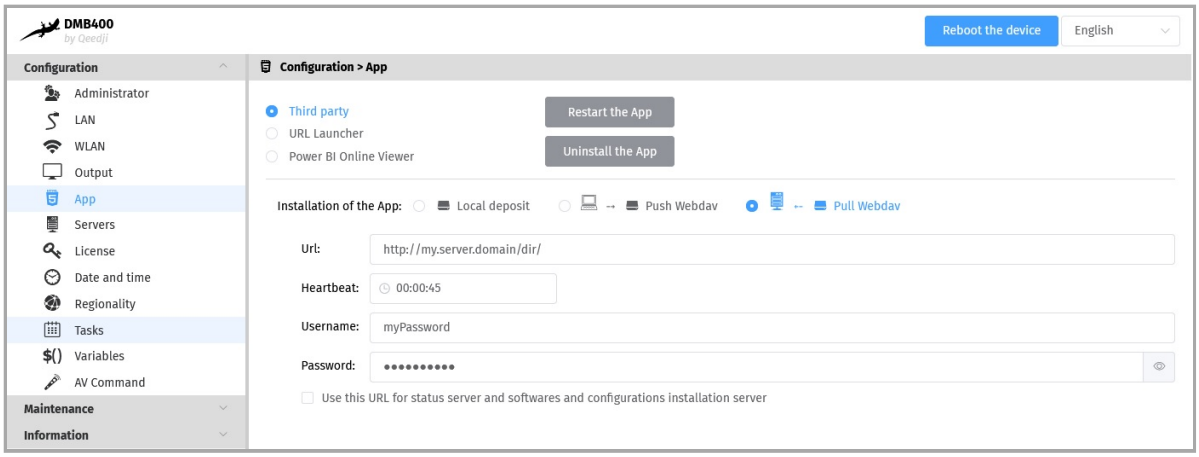
☛ *The development of App is reserved for advanced users with software development skills. The content of the App must contain at least these 2 files `manifest.xml` and `player.html`. Then archive your App in one of the supported formats: `*.tar.gz, *.zip, *.tar, *.tgz`. App examples are available at github SDK-G5 API (PDF example). For further information, contact support@qeedji.tech.*

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



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

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



Fill in the fields below properly:

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

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

Select the `URL Launcher` radio button then select a `Simple Web server` connection account to launch a Web page hosted on a Web server directory.

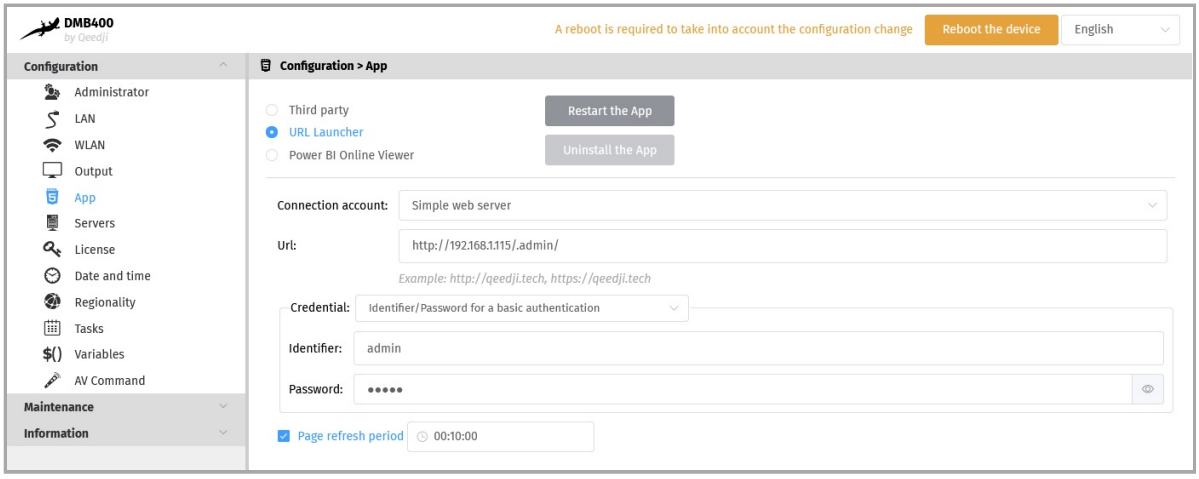
In this case, the Web page `URL` must match this syntax:

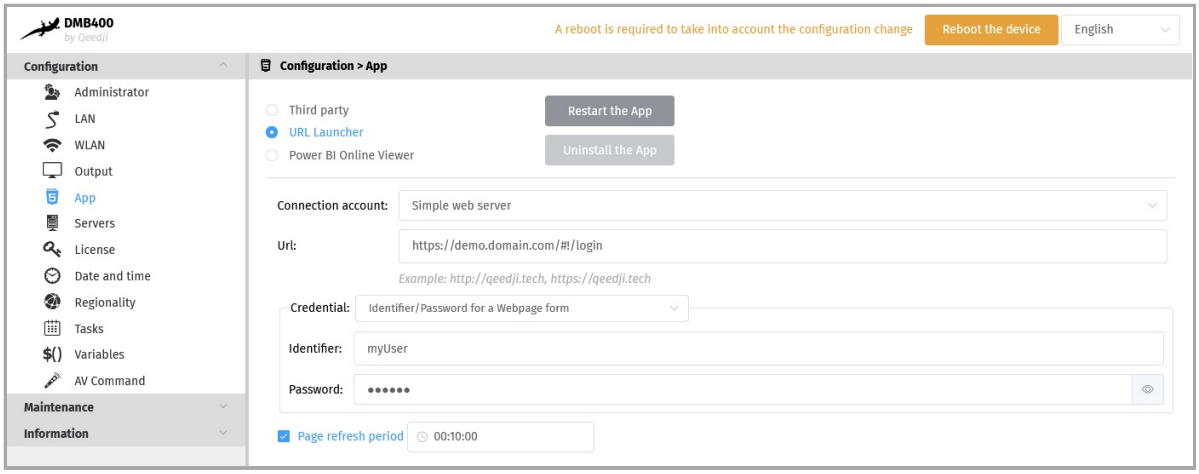
- e.g. `http://<myServer_ip_address>:<myServer_port>/<path>` (the directory must contain *index.html*),
- e.g. `http://<myServer_ip_address>:<myServer_port>/<myWebPage>.html` ,
- e.g. `https://<myServer_ip_address>:<myServer_port>/<myWebPage>.html` ,

Depending on the Web server URL, choose the appropriate `credential` type values:

- `None` : the Web page hosted on a the Web server does not requires a specific authentication,
- `Identifier/password for a basic authentication` : the Web page hosted on a the Web server requires a *Basic* HTTP authentication,
- `Domain/Identifier/password for a basic authentication` : the Web page hosted on a the Web server requires a *Basic* HTTP authentication and a domain,
- `Identifier/password for a Webpage form` : the Web page hosted on a the Web server requires is a login page with two credential input: identifier and password,

The `Page refresh period` input allows to set the duration between two Web pages refresh (default: 00:10:00).





> ☛ *This information message `Error - Unable to launch URL (error HTTP 0)` could be displayed on the display device when trying to access to a Web server with the https scheme when the appropriate server certificate is not loaded in the device.*
>
> ☛ *In case this information message `Error - Unsupported content type` is displayed on the display device, the URL is probably not consistent (e.g. the `index.html` is missing behind the URL path).*
>
> ☛ *It is advised to play Web pages suitable for the device resolution so that the entire Web page content can be watched on the display device without scrolling the Web page.*
>
> ☛ *SSO authentication is not supported in this version.*
>
> ☛ *In a next version, it will be possible to implement some user scenarii to fill the credential inputs in some specific login input placed in different places of the Web page.*

Select the `URL Launcher` radio button then select a `CIFS` connection account to launch a Web page by hosted on a CIFS server directory.

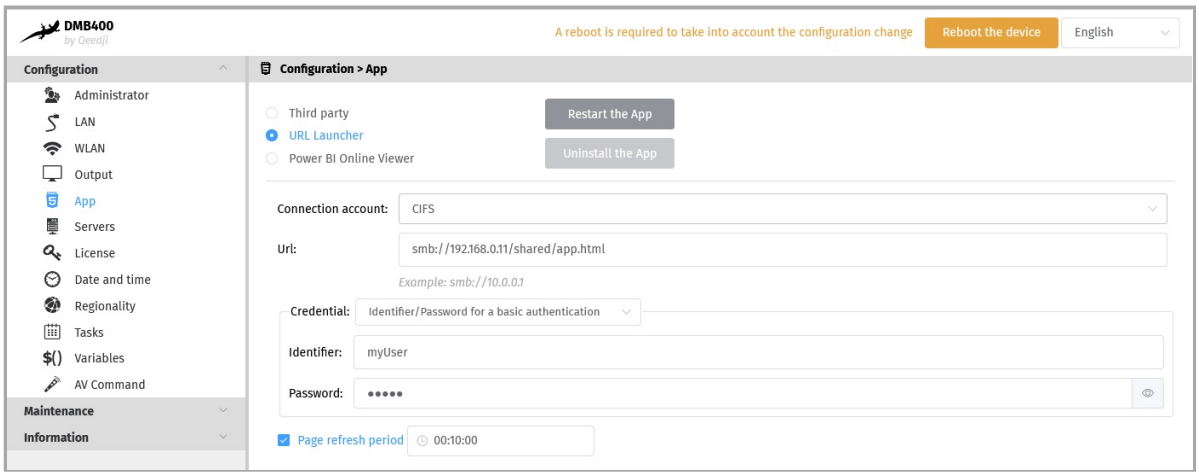
In this case, the Web page `URL` must match this syntax:

- e.g. `smb://<myServer_ip_address>/<myShareDirectory>` [1] (the directory must contain *index.html*),
- e.g. `smb://<myServer_ip_address>/<myShareDirectory>/<myWebPage>.html` [1],

[1] *The `NetBIOS` name resolution is not supported in this firmware version. Consequently, immediately after the `smb://` scheme, the URL must contain the server IP address and not a domain name.*

The `CIFS` connection account supports these `credential` type values:

- `None` : the viewing of the Web page hosted on a CIFS server directory requires no specific credential,
- `Identifier/password for a basic authentication` : the viewing of the Web page hosted on a CIFS server directory requires a *Basic* HTTP authentication,
- `Domain/Identifier/password for a basic authentication` : the viewing of the Web page hosted on a CIFS server directory requires a *Basic* HTTP authentication and a specific Windows *domain*.



> ☛ *In case this information message `Error - Unable to launch URL (error SMB 3)` is displayed on the display device, the Web page (.html) hosted in your CIFS server cannot be loaded. Please try with another Web page (.html). In case this information message `Error - Unable to launch URL (error SMB 1)` is displayed on the display device, the Web page (.html) hosted in your CIFS server cannot be loaded because the credentials are not consistent.*

Select the `URL Launcher` radio button then select a `Microsoft 365` connection account to launch a Web page hosted on your `Microsoft 365` shared folder.

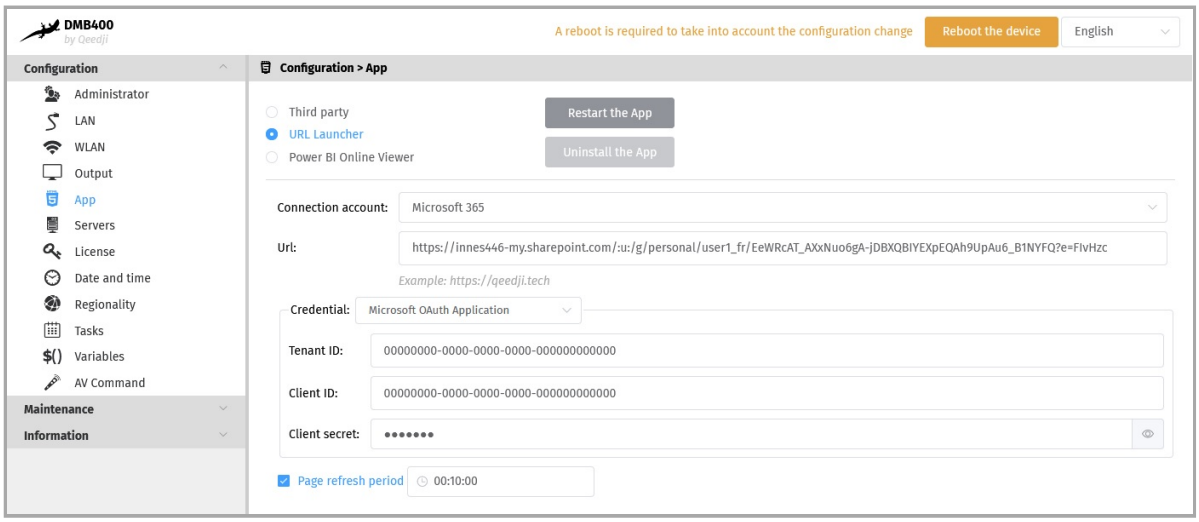
In this case, the `URL` is a link to the Web page hosted on your `Microsoft 365` folder (e.g. sharepoint URL https://innes446-my.sharepoint.com/:u:/g/personal/identifier*company*fr/ERq0Us037TdHgVh3aUf72WwBhTMrAgNjV94YPfMfA7OW3w?e=HbPwvD)

Select the `Microsoft OAuth application credential` type value then fill the following parameters with those of your Azure AD application allowing to access to your `Microsoft 365` shared folders:

- `Tenant ID` [1],
- `Client ID` [1],
- `Secret ID` [1],

[1] *An Azure AD application must be created with your `Microsoft 365` account to allow third party application to access to the Web pages hosted in your Microsoft 365 folders. For further information, refer to the chapter § Appendix: Microsoft Azure AD portal for URL launcher application.*

The `Page refresh period` allows to set the duration between two following Web pages refresh.



> ☛ *In case this information message is displayed on the display device `Error - Unable to Launch URL (error HTTP 401)`, please check the consistency of the Microsoft 365 identifier and password and the consistency of the Azure AD application `Tenant ID`, `client ID` and `secret ID`.*

Select the `Power BI Online Viewer` radio button to display your Power BI report available with these `credential` type values:

- `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],
- `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],

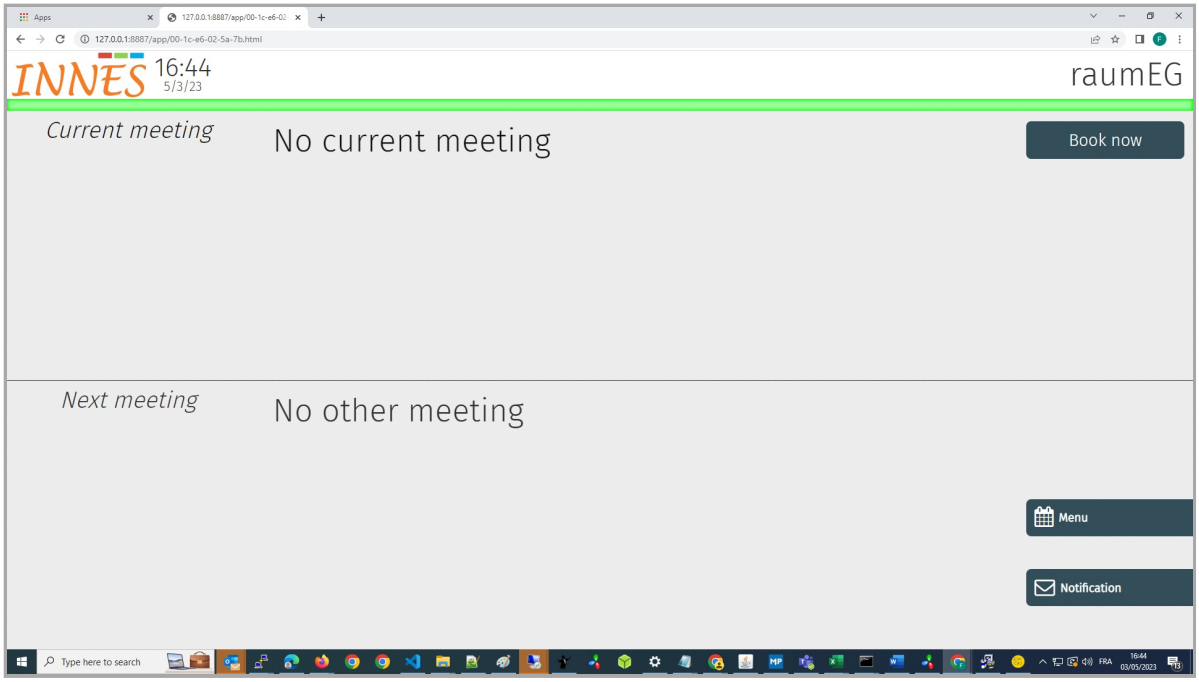
[1] *An Azure AD application must be created with `Microsoft Power BI` administration account to allow third party applications to access to the Power BI reports stored in your Microsoft Power BI workspace. For further information, refer to the chapter § Appendix: Microsoft Azure AD portal for Microsoft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

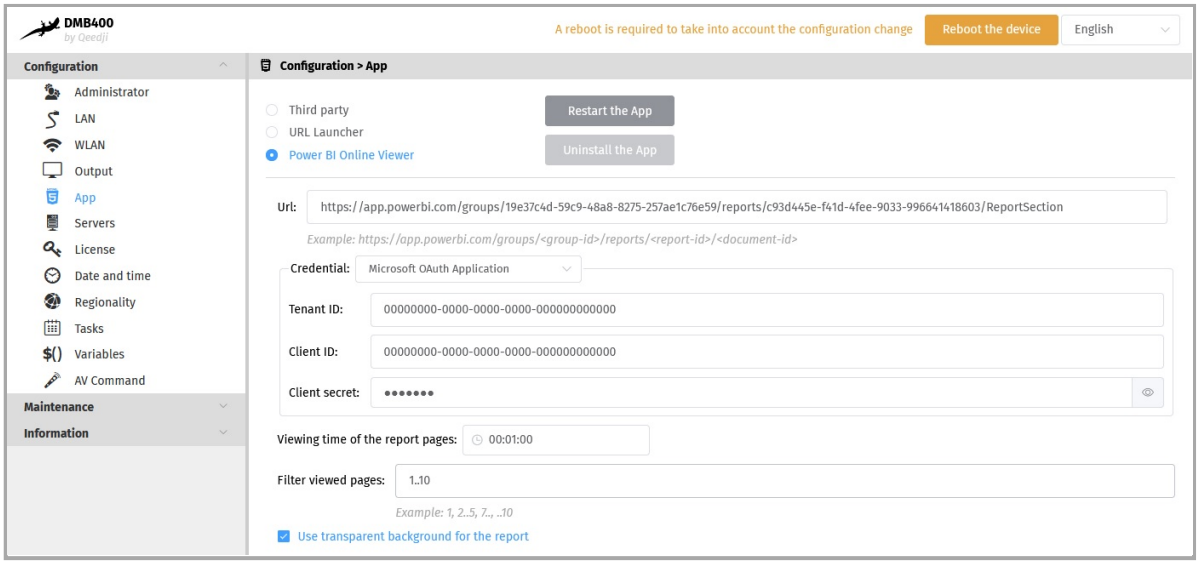
The `Viewing time of the report pages` allowqs to set the duration per report page.

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 `Use transparent background for the report` input allows to set activate or not the background transparency for the report. When the transparency is activated, the default browser background color should appear.





> ☛ *the default background color (RGB in hexa) of the device is defined in the `browser.display.background_color` user preference. Its default value is #000000 (black color).*
>
> ☛ *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 - Unable to show the Power BI report (error HTTP 404)` means that the Azure AD application can not find the workspace. The information message `Error - Unable to show the Power BI report (error HTTP 401)` means that the Azure AD application has found the report but is not allowed to access to it by leak of access rights.*

App supported

The device can support for example:

- *Linear playout App*,
- *Room booking App*,
- *GAP App*.

For further information, contact support@qeedji.tech.

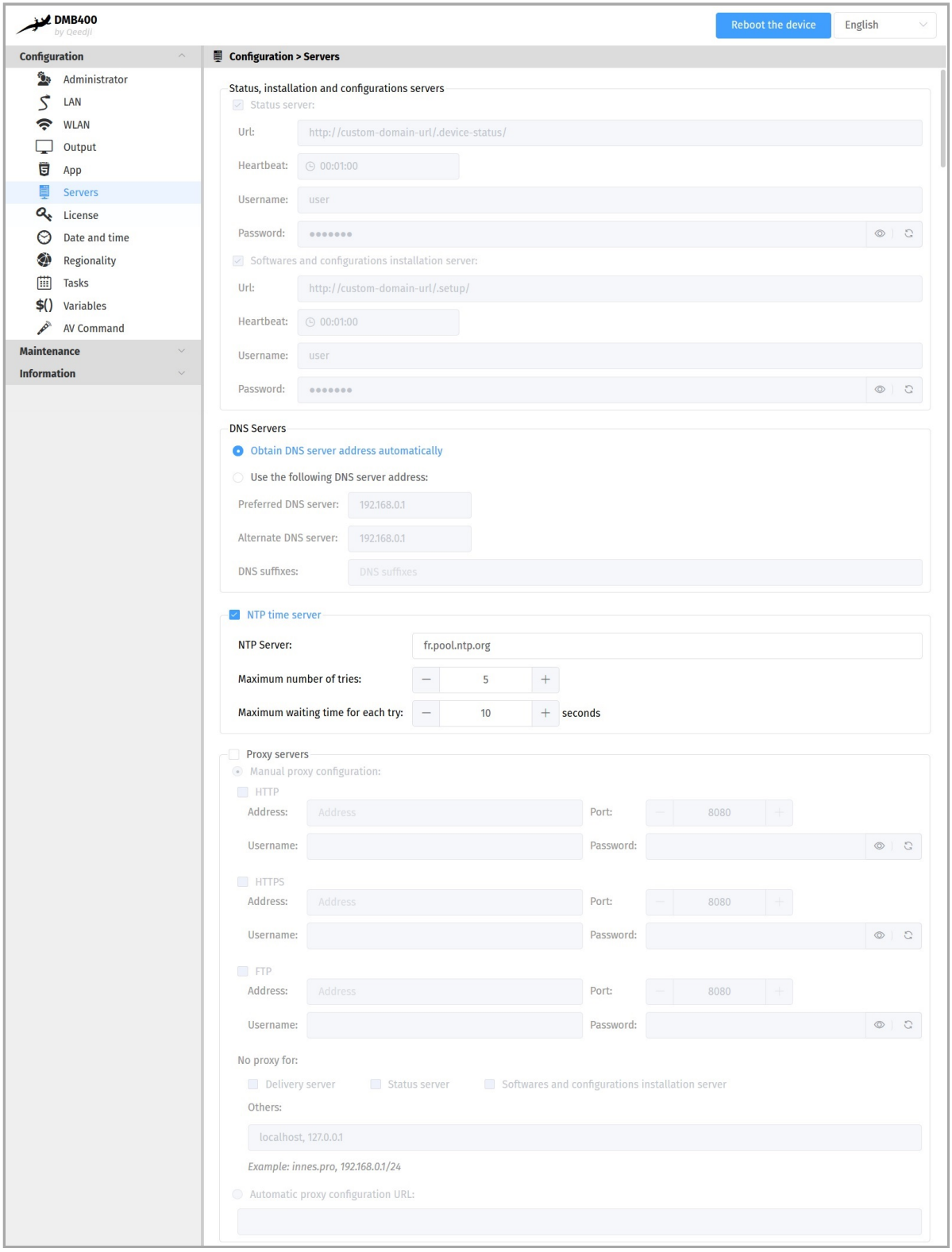
The device is supporting `GAP` App in the `Local deposit` mode and in the `pull WebDAV` mode.

> ☛ *A GAP App is a zip archive, compliant with the boot strap App (e.g. containing for example an `app.html` file and a `manifest.xml` file), which has been renamed with into a `.gap` file extension.*

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

3.1.6 Configuration > Servers

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



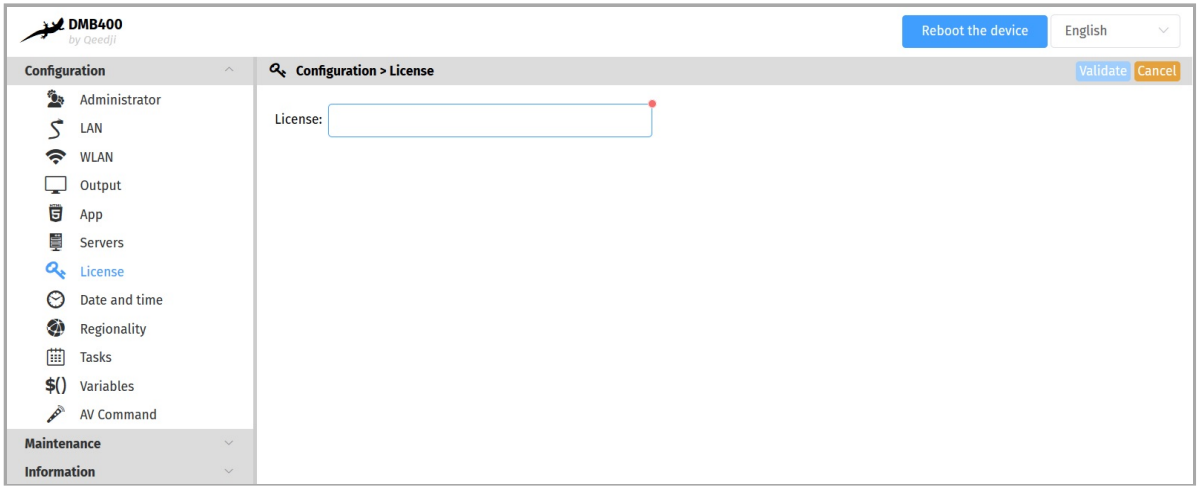
- status, software installation and configuration servers.
  - `Status server` :
    - `URL` : URL of the remote server's WebDAV frontend for the broadcast of the `.device-status/status.xml` device status file. For example: http://domain:8080/.directory/
    - `Username/password` : login and password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

- `Proxy server`.

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

3.1.7 Configuration > License

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

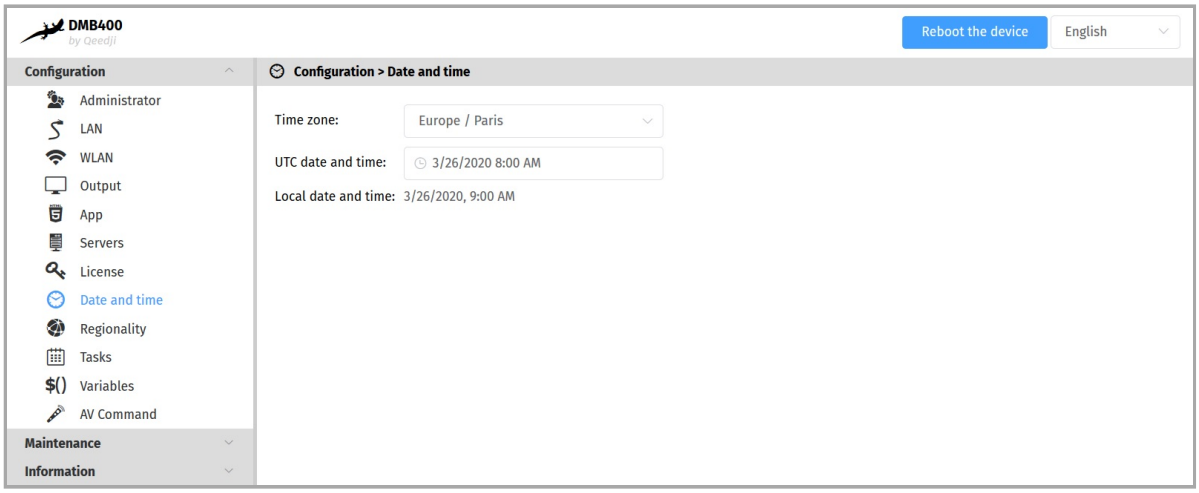


This license number is registered at the factory when the device is ordered. It is then sent to you by e-mail. If it has disappeared due to a handling error or after formatting your device, an error message indicating that the license is invalid will appear on your screen. In this case, please re-enter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

3.1.8 Configuration > Date and time

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

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



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

> ☛ *The `Date an time` set by the user can be taken into account only if the NTP server is not activated, or if the NTP server is not accessible.*
>
> ☛ *Setting a new date and time involves to restart the device immediately. If you have several configuration settings to change, it is advisable to adjust the date and time at last.*
>
> ☛ *It is advised that your device is on time. If your device is connected to the Internet, it is advised to synchronize the date and time on a Web NTP server. For further information, refer to the chapter § Configuration > Servers.*

3.1.9 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*.

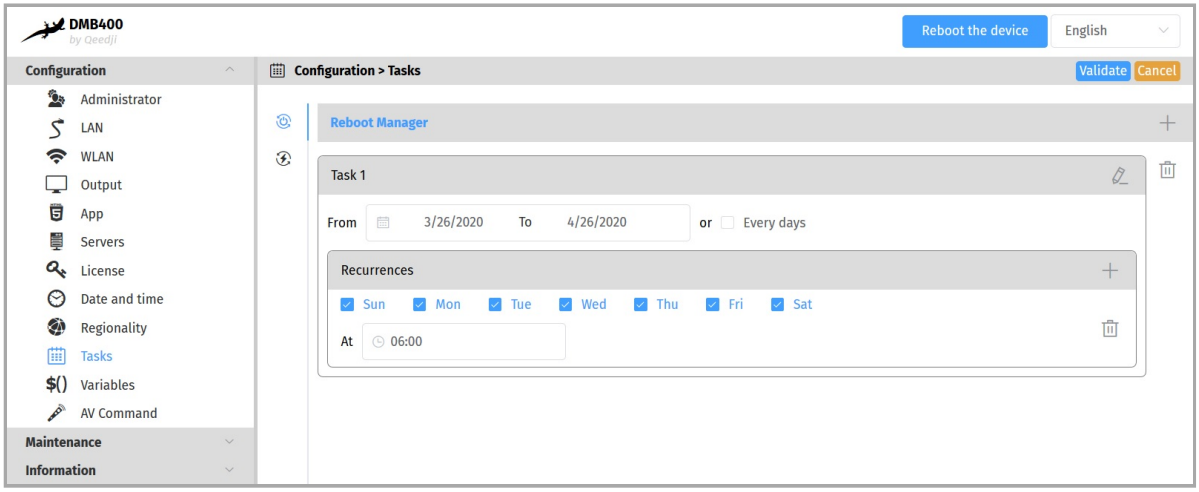
3.1.10 Configuration > Tasks

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

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

Device restart tasks

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



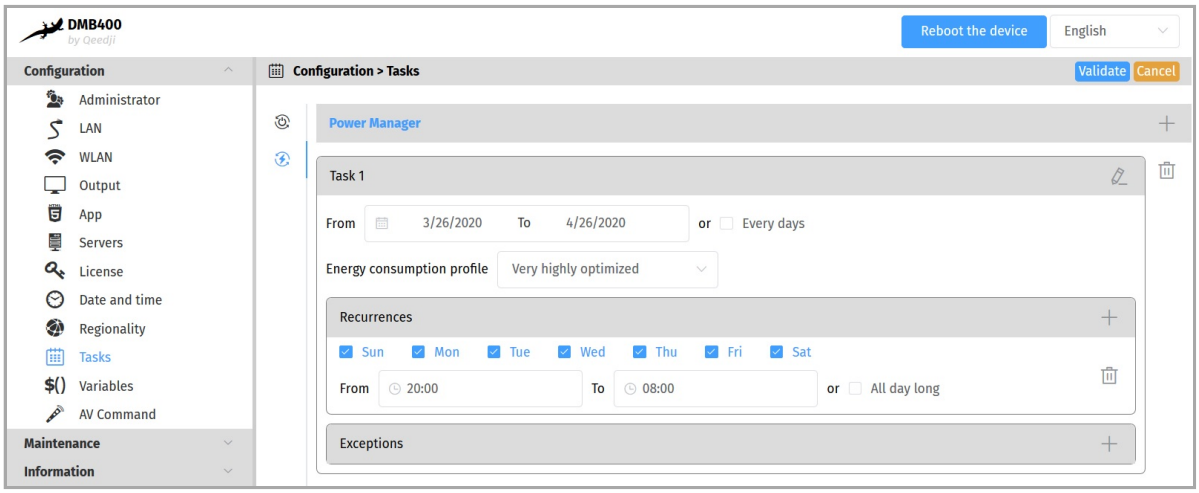
It is therefore possible to program several reboot occurrences whose parameters are stored in an ICAL format in the user preference `innes.reboot-manager.calendar`.

Example of value (ICAL format):

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

Device power manager task

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



The possible values programmable in time are

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

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

Example value (ICAL format):

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

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

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

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

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

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

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

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

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

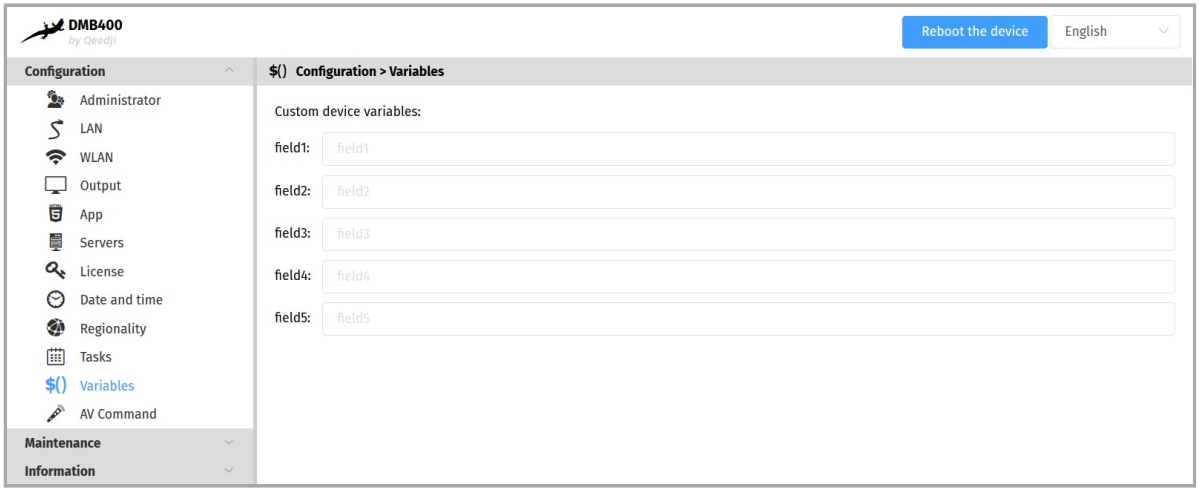
☛ *Some running App may automatically not take into account the Power manager task scheduled in the OS. In this case, only the power manager task scheduled in the App is taken into account.*

☛ *When there is no running App or when there is a system information message displayed on the display device, the Power manager task programmed in this pane is not taken into account by the middleware.*

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

3.1.11 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.

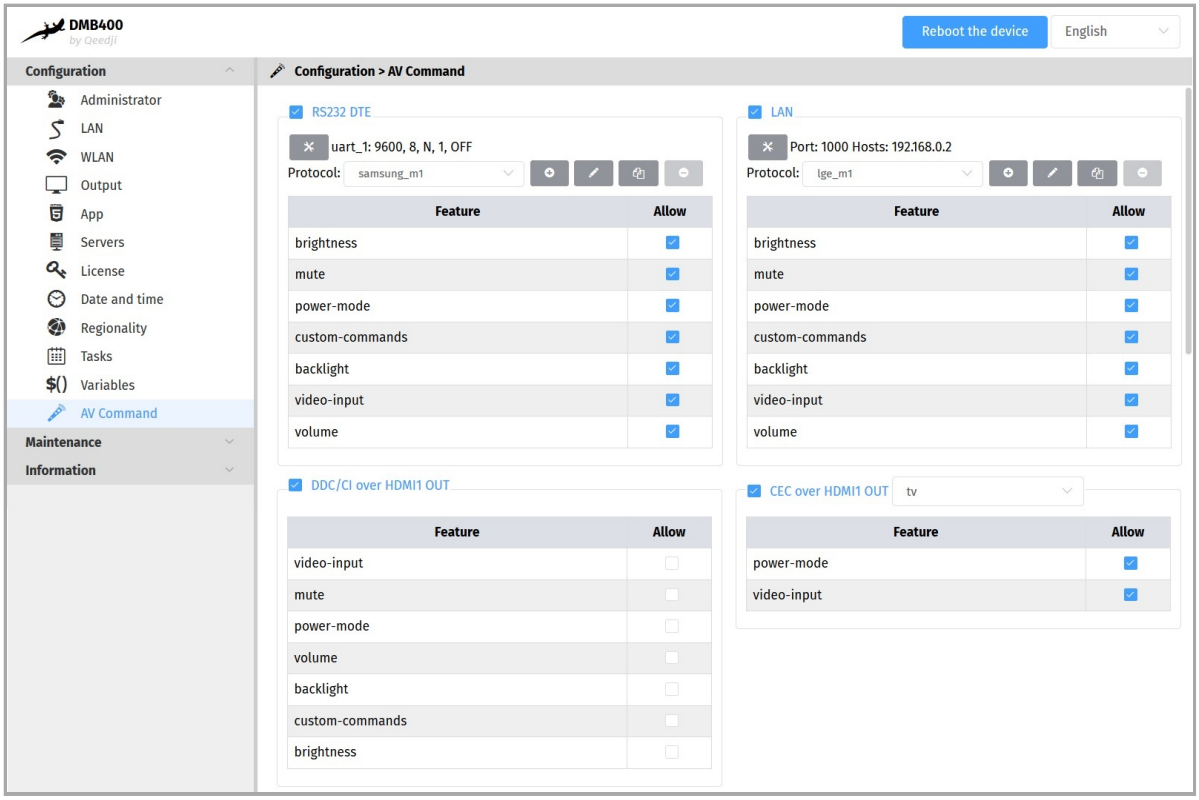
3.1.12 Configuration > AV commands

In the `Configuration` tab, select the **AV Commands** menu to enable the control of screens by AV (Audio-Video) commands through the connectors:

- `RS232`,
- `ETHERNET`,
- `HDMI`.

AV Command name	Description
brighness	screen brightness control
mute	screen mute control
power-mode	screen saver control
back-light	screen backlight control
video-input	screen audio-video source selection control
volume	screen volume control
custom-commands	control of specific display devices (projectors, ...) via support for user-implemented AV commands

> When the *power-mode* AV control is enabled through the specified connectors, it is automatically used when the App goes into screen saver mode or when a screen saver task is scheduled through the Web-based configuration interface.



> ☛ *Depending on the connectors, not all AV commands are supported.*

RS232

For screen control via AV Command RS232 DTE, select the `RS232 DTE` option.

> ☛ *First check in the datasheet that your screen supports AV Command via RS232. Using the screen configuration menu, activate the support of AV Command via RS232 on your screen (example for a SAMSUNG screen: Menu `Multicontrol` then `MDC Connection` then select `RS232 MDC`).*
>
> ☛ *In order for your screen to be able to receive AV commands, connect a crossover serial cable between your device and your screen.*

With the ✕ button, configure the RS232 interface of your device to match the RS232 configuration of your screen.

Choose the appropriate protocol according to your screen.

> ☛ *First check in the datasheet of your screen or audio-video device which AV Command protocol is supported.*
>
> ☛ *If none of the protocols are suitable, you can create your own protocol with the button ⊕ or duplicate an existing protocol with the button and adapt it with your own AV Commands.*

LAN

For screen control via AV Command LAN, select the `LAN` option.

With the ✖ button, configure the LAN interface of your device by adding:

- the IP address(es) of the screen(s) to drive,
- the port to be used (for example, port 1015) for sending AV commands.

> ☛ *Check beforehand in the datasheet that your screen supports AV Command over Ethernet. Using the screen configuration menu, activate the support of AV commands over Ethernet on your screen (for example for a SAMSUNG screen: Menu `Multicontrol` then `MDC Connection` then select `Ethernet MDC`).*
>
> ☛ *In order for your display to receive AV commands over Ethernet, make sure that your device and display are in the same local network.*

Choose the appropriate protocol based on your screen.

> ☛ *First check in the datasheet of your screen or audio-video device which AV Command protocol is supported.*
>
> ☛ *If none of the protocols are suitable, you can create your own protocol with the button ⊕ or duplicate an existing protocol with the button and adapt it with your own AV Commands.*

DDC/CI on HDMI-OUT

For AV Command DDC/CI screen control through the HDMI-OUT connector, select the `DDC/CI on HDMI-OUT` option.

> ⚠ Some displays do not support AV Command DDC/CI properly. If your screen does not exit from standby after activating AVCommand despite an App that is properly programmed, consider disabling DDC/CI AV Commands for that screen as it probably does not support standby output AV commands properly.

CEC on HDMI-OUT

For screen control by AV Command CEC through the HDMI connector, select the `CEC on HDMI-OUT` option.

> ⚠ Some screen do not properly support AV commands by CEC. If your screen does not come out of standby after activating AVCommand despite an App that is properly programmed, consider disabling CEC AV Commands for that screen as it probably does not support standby output AV commands properly.

Next, to control your screen with the AV Controls, load and play an appropriate App. It is possible to create your own App that uses the AVCommand APIs available here: github AVCommand API.

3.1.13 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 display the test pattern at device start-up, set the `Test card` toggle button to *activated*. To not display the test pattern App at device start-up, set the `Test card` toggle button to *deactivated*.

> ☛ *The test pattern content is displayed by the DMB400 device at 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 is activated, the content of the App is not played.*

Activation of the test pattern through your screen supporting CEC

If your screen supports the CEC[1][2] on HDMI, you can enable or disable the test pattern by pressing a key combination on the screen's remote control:

- [left Arrow, Right Arrow, Left Arrow, Right Arrow] key combination in less than ten seconds.

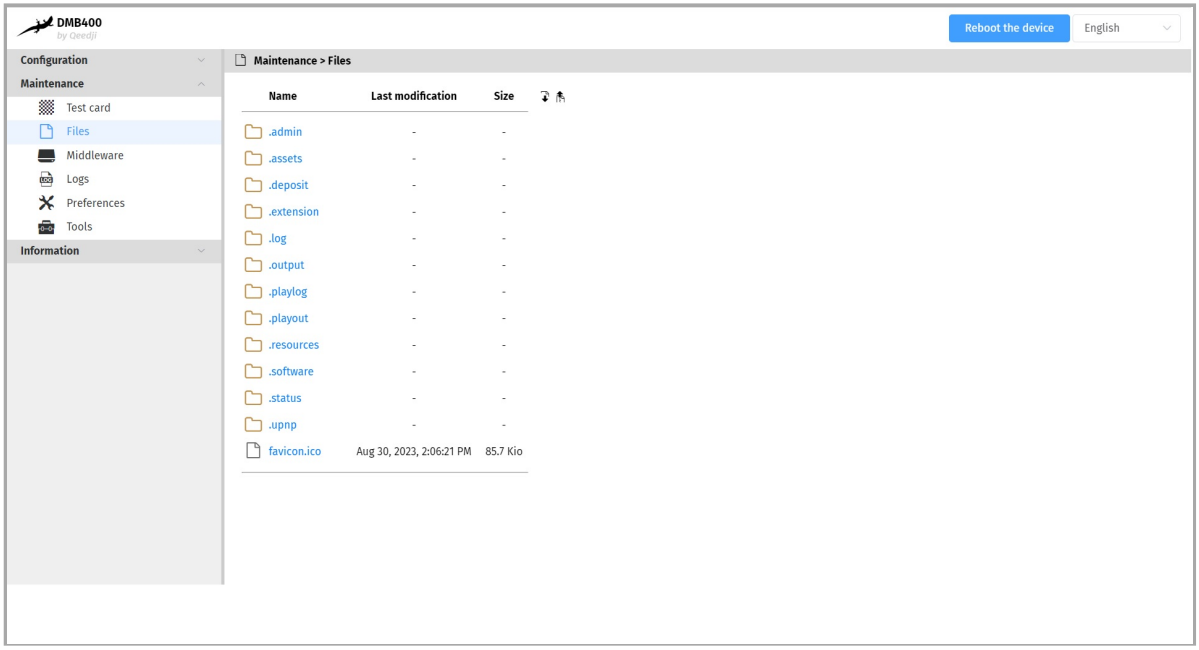
> ☛ *Make sure that no menus or banners are displayed on the screen.*
>
> ☛ *Before applying the keystroke combination, some screen requires to unselect and then select the HDMI source of the display to which the device is connected to force a CECSetInput_Source.*
>
> [1] For `SAMSUNG` screen, CEC is usually activated by activating the `Anynet` function. [2] for `LG` screen, CEC is usually activated by using the `Simplink` key on the remote control.

Function	Linked User Preference
Support for test pattern activation by key combination	`innes.player.test pattern.key-event.*.authorized` (default= true)

> ☛ *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::`).*

3.1.14 Maintenance > Files

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



These are the available WebDAV directories:

- `.admin` : location to store some resources of the device Web user interface
- `.assets` : location to store some of the resources of the device Web user interface,
- `.deposit` : location to store temporarily the App to load
- `.extension` : directory allowing to upload a configuration script to auto-configure the device,
- `.log` : location to store the application logs, when they are activated.
- `.playlog` : location to store data for mediametry
- `.playout` : location to store the App when deployed on the device,
- `.resources` : location to store some other resources of the device Web user interface
- `.software` : directory allowing to upload a `.frm` firmware and upgrade the middleware version of the DMB400 device.
- `.status` : location to store the device status file `status.xml`
- `.upnp` : location to store `device.xml` device status for UPnP detection

Middleware upgrade

The Gekkota middleware can be upgraded by pushing a new firmware file `gekkota_os-dmb300-setup-5.YY.ZZ.frm` in the `.software` directory of the device WebDAV directory (`http://<device-ip-addr>/.software`).

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>/.extension`) with the Web user interface. In this case, the file pattern must be either:

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

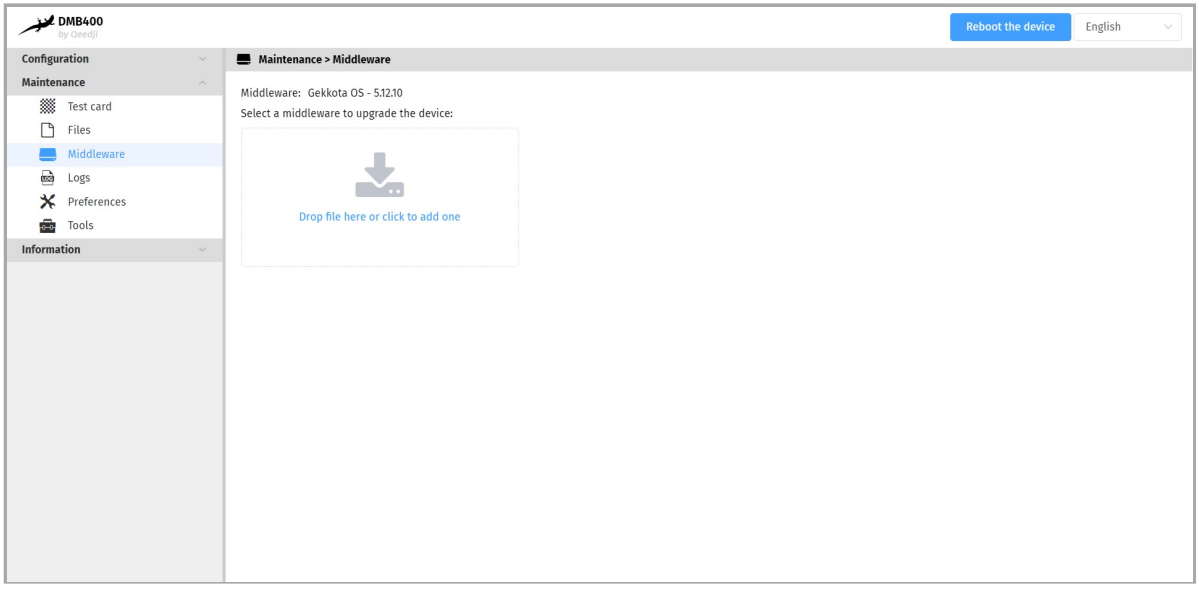
Download the configuration script example from the Qeedji Website it then:

- 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.

3.1.15 Maintenance > Middleware

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



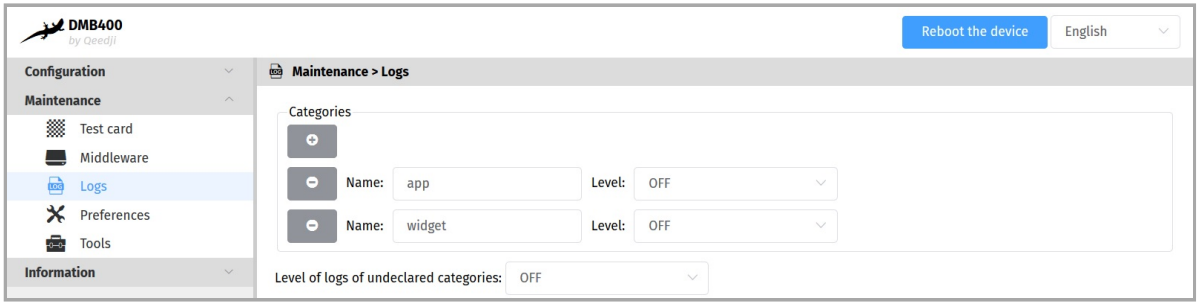
> ☛ *Corrective and evolutive maintenance software versions are regularly made available on the http://www.innes.pro/en/support/index.php?DMB400/Firmware_and_documentation_for_DMB400. It is therefore advised to regularly update the device middleware. From this website, download the latest version available for your device model. Unzip the `.zip` archive and get the `.frm` file.*
>
> ☛ *It is possible to upgrade the device from a version Gekkota OS 4.YY.ZZ to a version Gekkota OS 5.YY.ZZ. But is is not possible to downgrade the device from a version Gekkota OS 5.YY.ZZ to a version Gekkota OS 4.YY.ZZ.*

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

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

3.1.16 Maintenance > Logs

In the `Maintenance` tab, select the **Logs** menu to activate logs.



The log levels are:

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

Logs are compartmentalized according to software functions such as:

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

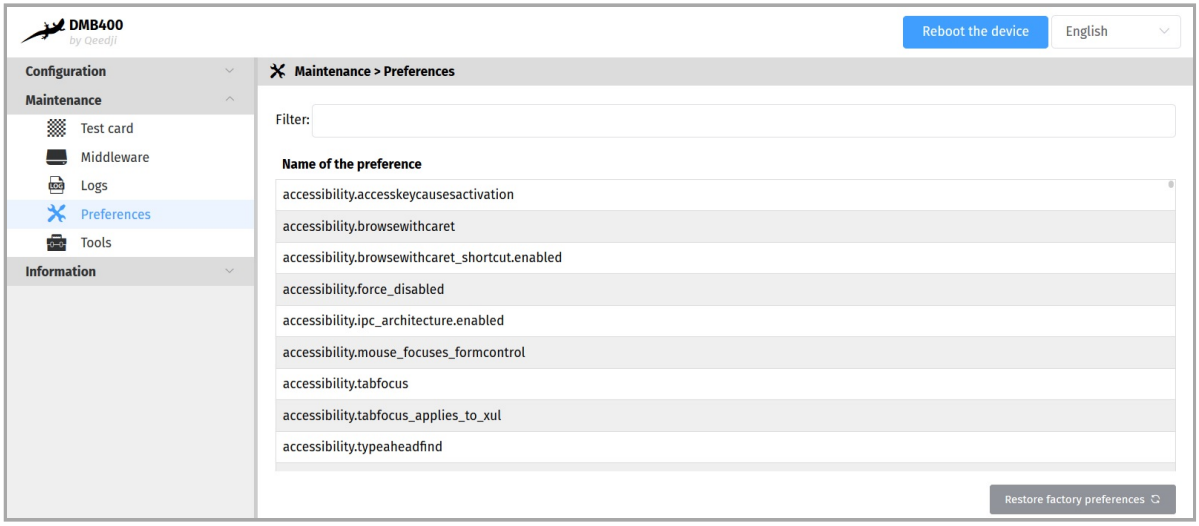
> ☛ *These logs may be activated on support request in exceptional debug cases.*
>
> ☛ *These logs can only be interpreted only by software developers who are familiar with the software bricks that have been developed.*

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

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

3.1.17 Maintenance > Preferences

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



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

Double click on a preference to change its value.

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

Here are some user preferences that may be useful.

user preference	value	description
`innes.video.renderer.default`	*overlay* (default value)	Supports 1 UHD video + 1 H265 video simultaneously. This also supports the HDMI input which is treated as an additional video decoding. This allows to process the text scrolling overlay 60Hz. Allows to support video decoding at the HDMI input. Supports the enhanced hardware deinterlacing filter as well as the display of Mpeg-TS interlaced video.
`innes.video.renderer.default`	*gpu*	Allows to support 2 simultaneous 1080p video decoding + 2 simultaneous 720p decoding or to support interlaced video in very small areas.
`innes.video.decoding-group.enabled`	*true*	Allows to decode multiple videos at the same time.
`media.mediasource.enable`	*false*	Disabling the DASH MSE.
`innes.hid.pointer-event.*.authorized`	*true*	Allows to support for HDMI/USB touchscreens.
`innes.video.has.max-bitrate`	*5*	(Mbps) setting the maximum bitrate of a DASH Mpeg stream.
`media.cache_size`	*16384* (default) to *65536*	(in KB) Allows to support higher bitrate for DASH Mpeg streams.
`innes.webserver.providers.http.enabled`	*true*	Allows to support access to the device in http://.
`innes.webserver.providers.https.enabled`	*true*	Allows to support access to the device in https://.

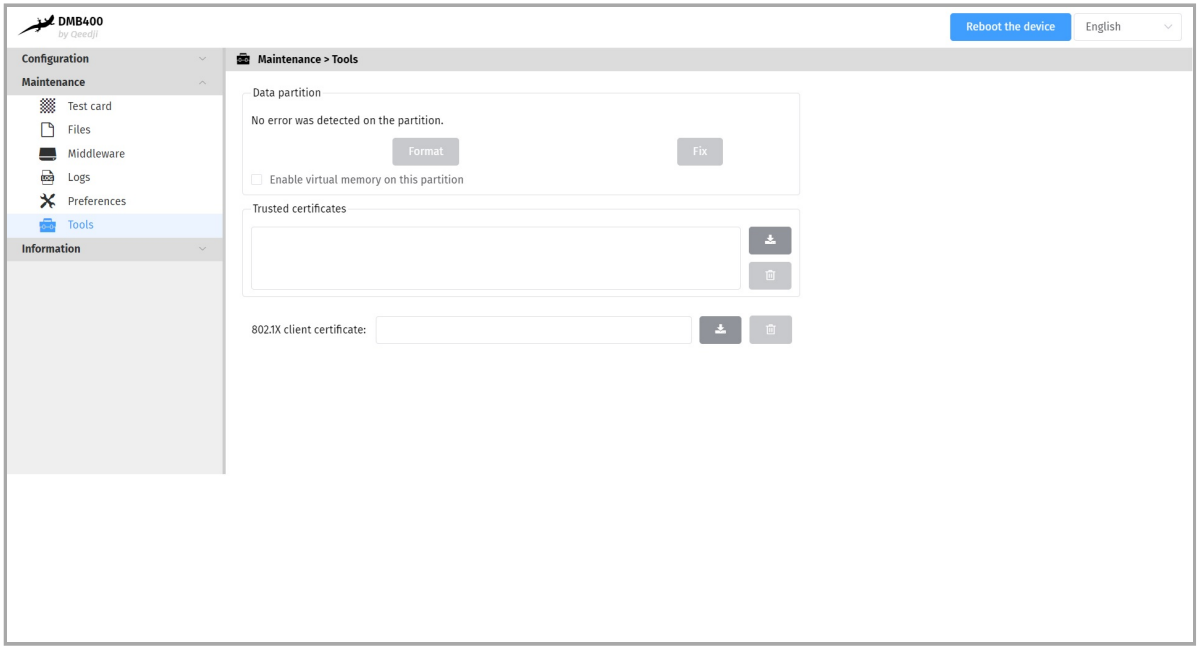
`system.clock-sync.enable`
`system.clock-sync.ptp.timeout.lock-on-master`
`system.clock-sync.ptp-domain`
`system.clock-sync.source`
	true
	30
	0
	ptp-l2
		Allows to activate the PTP/IEEE1588 synchronization on a master device,
		PTP/IEEE1588 Master device finding timeout[1] in seconds (30 by default),
		PTP/IEEE1588 domain id (0 by default),
		PTP/IEEE1588 Synchronization modes: *ntp* (default value) or *ptp-l2*.

[1] After this timeout, the DMB400 device becomes PTP/IEEE1588 master device.

3.1.18 Maintenance > Tools

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

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



Check the `Enable virtual memory on this partition` option to activate the swap disk on this device. The memory space for swap disk is 512 MB.

> ☛ *The `Enable virtual memory on this partition` option is not activated by default.*
>
> ☛ *When the `Enable virtual memory on this partition` option is changed by the user but there is not enough disk space to allocate the swap disk memory space (512 MB), the `swap` activation value in the `status.xml` device status file remains to the false value, meaning that the swap disk stays inactivated in this case. To work around, publish an App containing less medias to free up the required 512 MB memory then restart the device.*

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

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

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

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

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

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

3.1.19 Information > Device

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

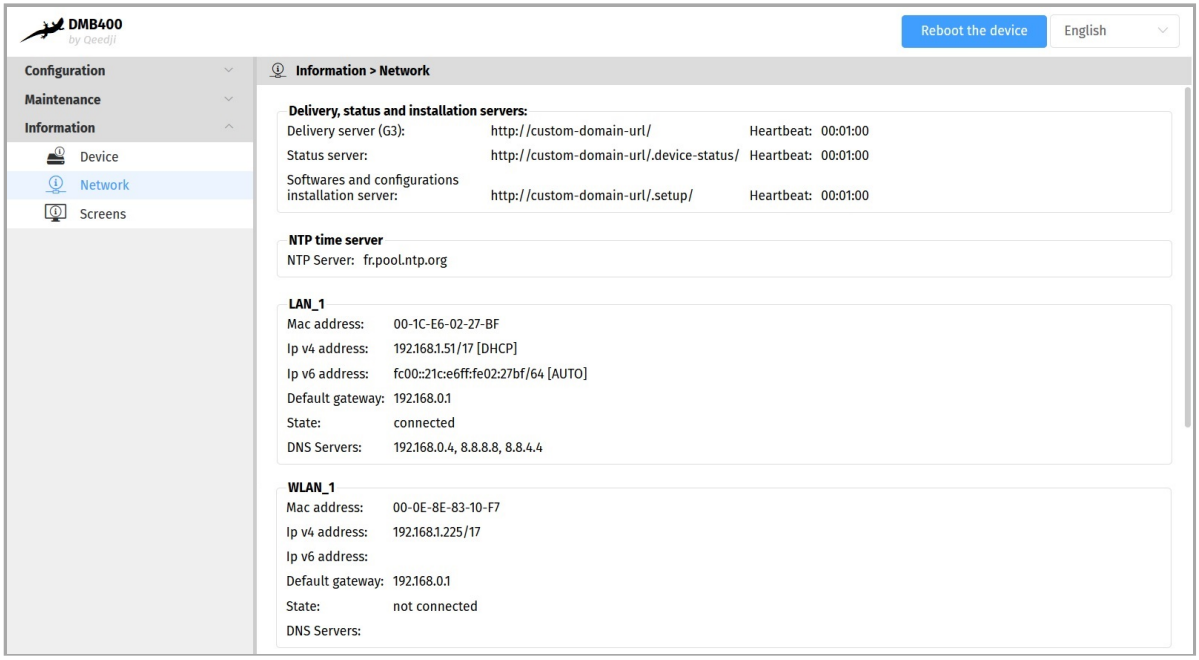
- `Middleware` : label and version of the embedded middleware,
- `Model` : model of the `Qeedji` device,
- `Hostname` : name of the device on the network,
- `MAC` : MAC address (value used in particular to generate the license key of the device),
- `UUID` : Universal Unique IDentifier,
- `PSN` : Product Serial Number.
- `HDCP` :
  - *Supported (valid key)*: Indicates that HDCP is supported by the device and that it has a valid HDCP key,
- video output capture on `<day date>` : last video output capture.

Press the button 🔄 to refresh the screenshot.

The width of the screenshot is set by the `innes.screenshot.width-max` preference (default: 960 pixel). If the width of the device's display resolution is less than this value, the width of the screenshot fits this narrower resolution width.

3.1.20 Information > Network

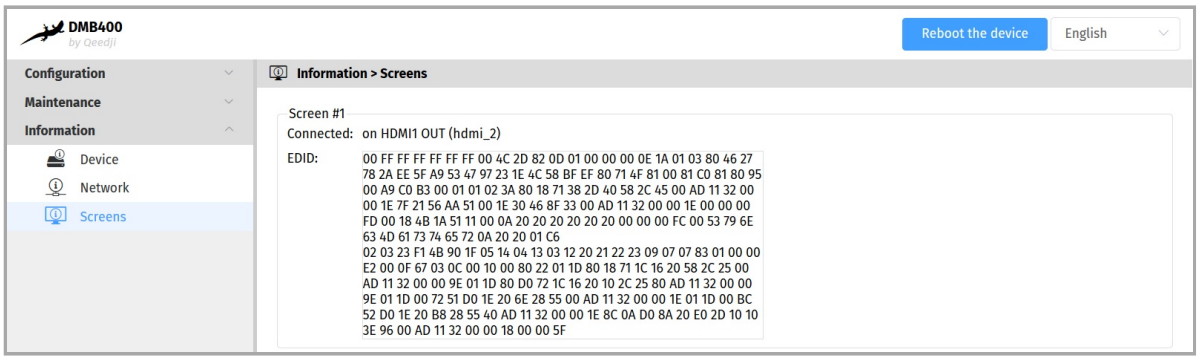
In the `Information` tab, select the **Network** menu to view a summary of the device's network configuration.



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

3.1.21 Information > Screens

In the `Information` tab, select the **Screens** menu to view information about the display device connected on the HDMI connector and the rotation angle.



Part IV

Configuration by script

4.1 Configuration by script

The DMB400 device can auto-configure with a configuration script. The configuration script can be either:

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

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

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

Part V

Technical information

5.1 Technical specifications

Model	Manufacturer
DMB400	Qeedji

Processors	
CPU	Quad core cortex-A9, 1.2GHz
GPU	MALI-400

Peripherals
1x USB 2.0 Host (Low/Full/High Speed)
1x USB 3.0 Host (Low/Full/High/Super Speed)
1x Jack 3.5 mm configurable in GPIO or Infrared
1x RS232 DTE

Storage
Internal Flash Memory for OS
SSD mSata

Middleware
Gekkota OS 4

Audio output
1x Jack 3.5 mm connector (analog stereo L+R)
Embedded with HDMI output

Video output
1x HDMI 2.0

Display resolutions[1] for video output
640x480 60Hz, 800x600 60Hz VESA, 1024x768 60Hz VESA, 1024x768 60Hz XGA, 1024x576 60Hz VESA, 1024x576 50Hz VESA, 1024x600 60Hz DENSITRON 84-0188-001T, 1280x720 60Hz CEA-861, 1280x720 50Hz CEA-861, 1280x720 60Hz VESA, 1280x720 50Hz VESA, 1280x720 60Hz SMPTE (720p), 1280x720 50Hz SMPTE (720p), 1280x720 60Hz CEA, 1280x720 50Hz CEA, 1280x720 60Hz SONY, 1280x720 60Hz CGV CPLine AV-HD, 1280x720 60Hz SAMSUNG, 1280x768 60Hz VESA, 1280x768 50Hz VESA, 1280x800 60Hz VESA, 1360x768 50Hz VESA, 1360x768 60Hz VESA, 1376x768 60Hz VESA, 1376x768 50Hz VESA, 1376x768 60Hz PC, 1920x1080 60Hz CEA-861, 1920x1080 50Hz CEA-861, 1920x1080 60Hz VESA, 1920x1080 50Hz VESA, 1920x1080 60Hz SMPTE (1080p), 1920x1080 50Hz SMPTE (1080p), 1920x1080 60Hz CEA, 1920x1080 50Hz CEA, 3840x2160 59.94Hz, 3840x2160 60Hz CEA-861, 3840x2160 50Hz CEA-861, 3840x2160 50Hz VESA, 3840x2160 45Hz VESTEL, 3840x2160 30Hz CEA-861, 3840x2160 25Hz CEA-861, 2560x1440 60Hz CEA-861, 3840x600 60Hz VESA, 1920x540 60Hz VESA, 1920x540 60Hz Samsung, 1920x360 60Hz Iiyama, 1920x300 60Hz VESA, 768x2560 60Hz LINSN, 128x96 60Hz, 112x96 60Hz, 96x96 60Hz,
[1] *The rotation is not supported for the resolution upper than 1920x1080.*

Video input
1x HDMI 1.4b

Preferred resolutions of EDID for Video input
1920x1080p 59.94Hz, 1920x1080p 60Hz, 1920x1080p 50Hz, 1280x720p 59.94Hz, 1280x720p 60Hz, 1280x720p 50Hz, 1920x1080i 59.94Hz, 1920x1080i 60Hz, 1920x1080p 29.97Hz, 1920x1080p 30Hz

Network
1x Ethernet 10/100/1000 BaseT

Options	Information
GPRS/EDGE/HSDPA Modem	Mini-SIM card (25 mm x 15 mm)
WIFI 802.11a/b/g/n (WIFI 4)	SPARKLAN WPEA-152GN(BT) module

Power supply
12 V DC (1.2 A)

Operating temperature	Storage temperature
0 °C to +40 °C	-20 °C to +60 °C

Operating humidity	Storage humidity
< 80 %	< 85 %

Weight	Dimensions (W x H x D)
With WIFI: 0,992 Kg (2,18 lb) Without WIFI: 0,971 Kg (2,14 lb)	213 x 39,5 x 137.5 mm (8,38" x 1,53" x 5,39")

Warranty
3 years

5.2 Conformities

In conformity with the following European directives:

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

Part VI

Contacts

6.1 Contacts

For further information, please contact us:

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

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

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

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

Part VII

Appendix

7.1 Appendix: Device status (status.xml)

The DMB400 device is updating regularly its device status stored in its `/.status` WebDAV directory:

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

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

Status.xml example:

```
<device-status xmlns="ns.innes.device-status">
<device>
<id-type>MAC</id-type>
<mac>00-1c-e6-02-20-e2</mac>
<hostname>dmb400</hostname>
<uuid>05c00002-0000-0000-0000-001ce60220e2</uuid>
<modelName><gekkota_os-model></modelName>
<modelNumber>4.13.12</modelNumber>
<serialNumber>00920-00002</serialNumber>
<middleware>gekkota-4</middleware>
<field1/>
<field2/>
<field3/>
<field4/>
<field5/>
<ip-addresses>
<ip-address>
<if-type>LAN</if-type>
<origin>dhcp</origin>
<value>192.168.1.119/17</value>
</ip-address>
<ip-address>
<if-type>LAN</if-type>
<origin>auto</origin>
<value>fc00::21c:e6ff:fe02:20e2/64</value>
</ip-address>
</ip-addresses>
<addons/>
</device>
<status>
<date>2020-03-31T17:40:16.055055+02:00</date>
<launcher>
<power-manager level="MAX"/>
<manifest-metadata xmlns:pzpm="ns.innes.gekkota.manifest">
<pzpm:publish-size>0</pzpm:publish-size>
<pzpm:publish-generator>gekkota_ui</pzpm:publish-generator>
<pzpm:publish-date>2020-03-30T06:45:26.759Z</pzpm:publish-date>
</manifest-metadata>
<state>NO_CONTENT</state>
</launcher>
<storage>
<total unit="byte">1912532992</total>
<used unit="byte">22161408</used>
</storage>
<display-outputs/>
<setup>
<configuration>
<metadatas/>
<version>2019-06-21T13:25:25Z</version>
</configuration>
</setup>
</status>
</device-status>
```

7.2 Appendix: Qeedji PowerPoint publisher for Media Players

This appendix explains how to publish `.pptx` MS-Powerpoint presentation on DMB400 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 DMB400 devices with the same MS-PowerPoint presentation.*
>
> ☛ *In this version, only the DMB400 devices, whose WebDAV servers are available with the `http://` scheme (default value), are supported.*

Prerequisite:

> ☛ *The DMB400 device needs to be purged from any existing App. It is advised to set the App mode to the `Push WebDAV` value. For further information, refer to the chapter § Configuration > App.*

Qeedji PowerPoint Publisher For Media Players: installation

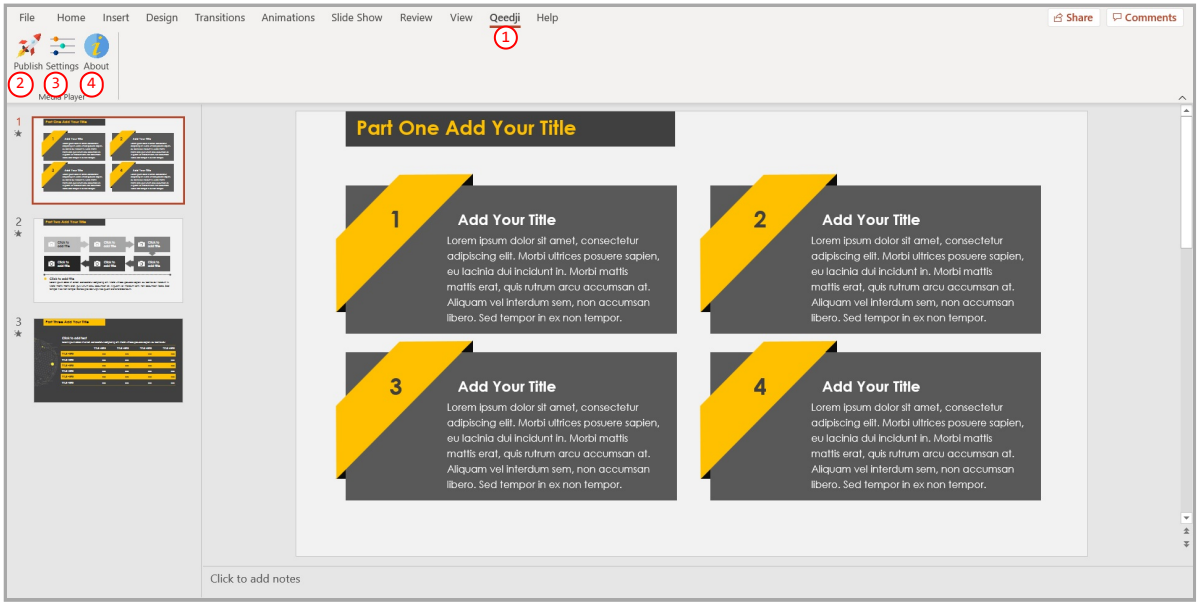
The `Qeedji PowerPoint Publisher For Media Players` PowerPoint Add In needs to be installed once:

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

> ☛ *Choosing `Everyone` may require to run the PowerPoint with the Administrator rights to be able to 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 could be requested to install first `.NET framework version 4.X.Y` before installing the `Qeedji PowerPoint Publisher For Media Players` PowerPoint Add In.*
>
> ☛ *The same language is used for `Qeedji PowerPoint Publisher For Media Players` PowerPoint Add In interface and MS-Windows.*
>
> ☛ *In case you need to upgrade `Qeedji PowerPoint Publisher For Media Players` PowerPoint Add In, it is required to close MS-Office PowerPoint and open it again to use the new version.*
>
> ☛ *In some rare cases, the warning message `PowerPoint has problems with the Qeedji complement. If the problem persists, disable this add-on and check for updates. Do you want to disable it now? (yes/no)` could be prompted when opening a MS-Office PowerPoint. In this case, do ignore the message by clicking `No`. It should not prevent the `Qeedji PowerPoint Publisher For Media Players` to work properly.*

Qeedji PowerPoint Publisher For Media Players: uninstallation

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

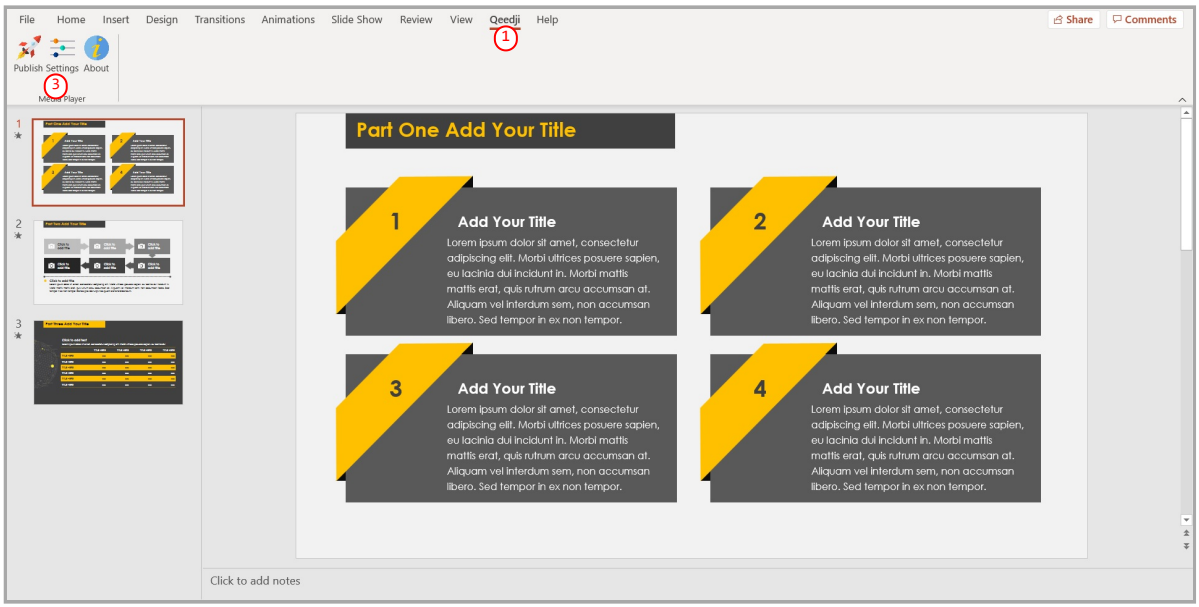
Qeedji PowerPoint Publisher For Media Players: upgrade/downgrade

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

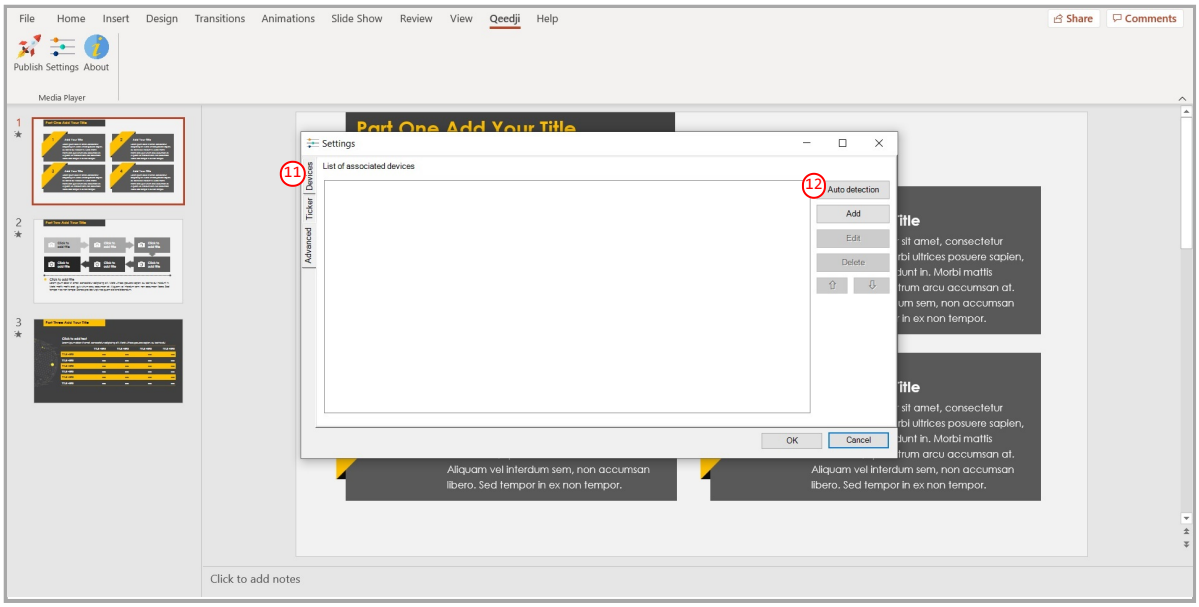


To register one or several DMB400 devices, open you MS-Office Powerpoint presentation then:

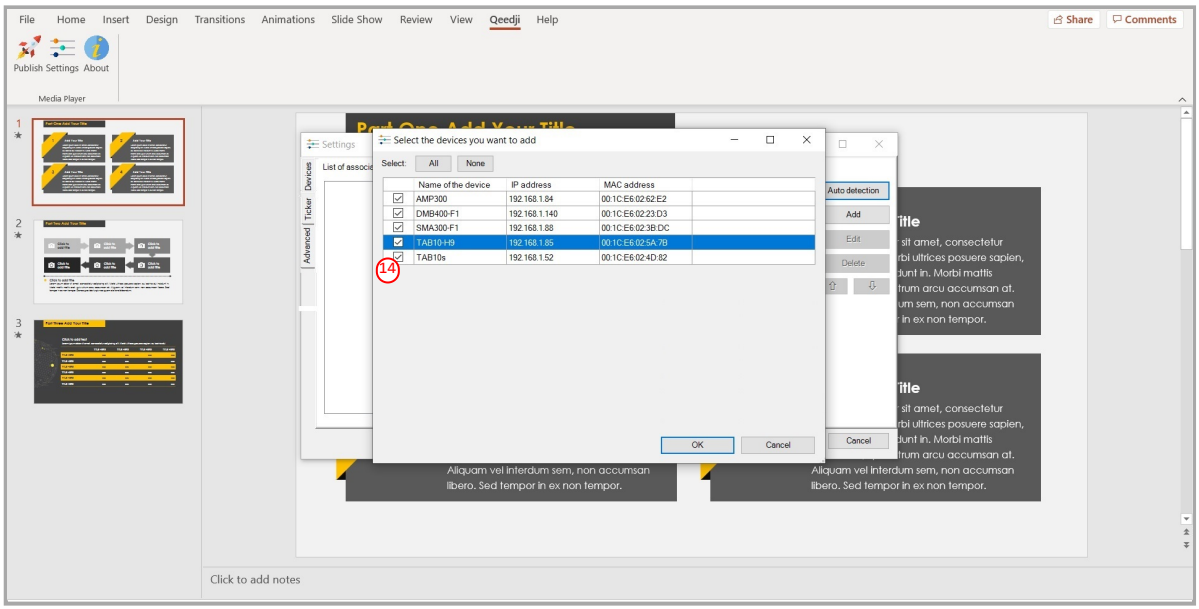
- click on the `Qeedji` (1) menu,
- on the `Qeedji` ribbon, click on the `Settings` (3) item then select the `Devices` tab.

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

On the `Devices` (11) tab, click on the `Auto detection` (12) button to detect the DMB400 devices available on your local network.



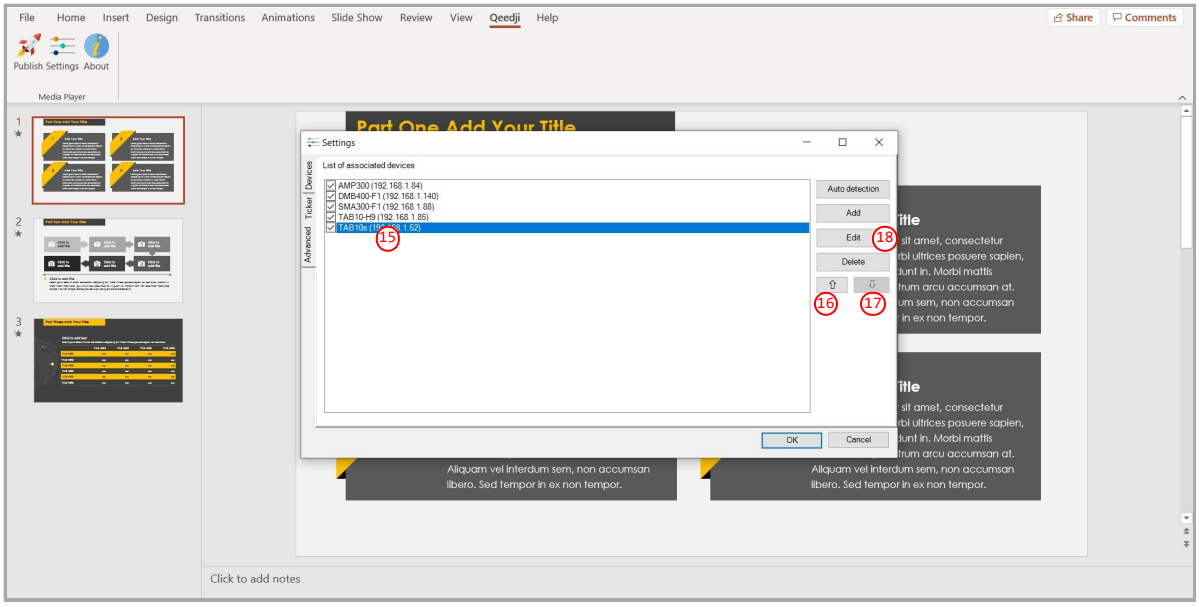
Select (14) the appropriate DMB400 devices to create a list of appropriate DMB400 devices as possible applicant for the MS-Powerpoint presentation.



Select then the only DMB400 devices on which you want to publish, by double clicking on them.

> ☛ *The DMB400 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 DMB400 device located at the top of the list. Then the publication is continuing with the next DMB400 device located immediately below, and so on.*

Select a DMB400 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.

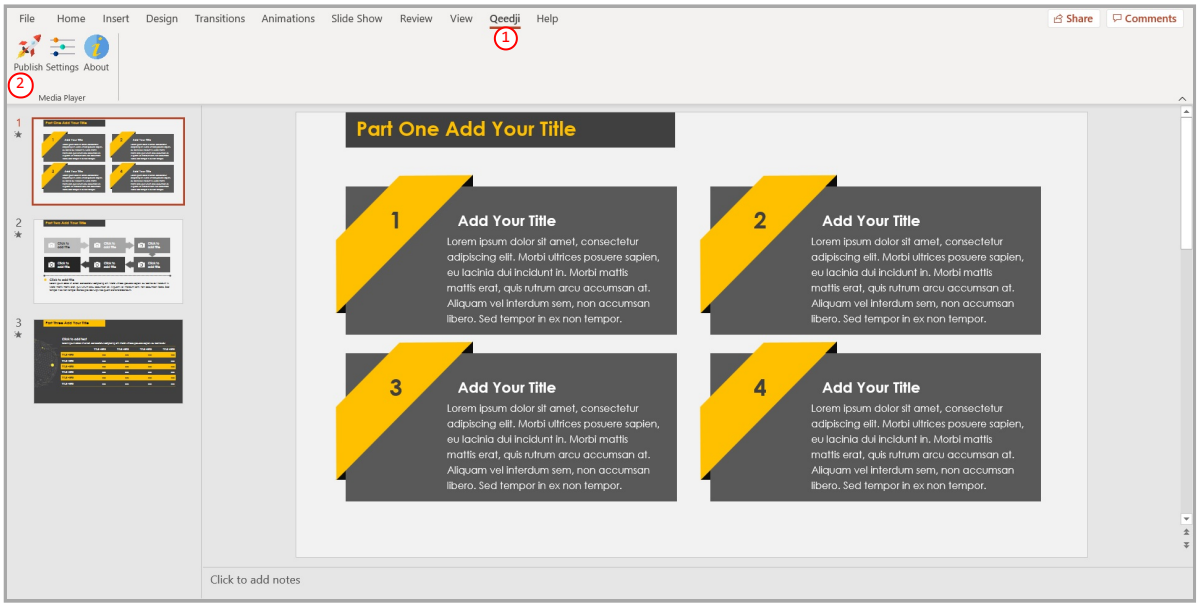


The default *administrator name/password* credentials to access to the DMB400 device's Web server is `admin` / `admin` . After an UPnP detection, the DMB400 devices are by default registered in `Qeedji PowerPoint Publisher For Media Players` with the default *user/password* `admin` / `admin` credentials to access to their Web server. If you must publish your `Qeedji PowerPoint Publisher For Media Players` App on a device with some *administrator name/password* credentials that are not the default one, select this DMB400 device in the list, press on the `Edit` button, and change the *user/password* by the appropriate *administrator name/password* credentials.

Qeedji PowerPoint Publisher For Media Players: publish

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

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



> ☛ *Before publishing with the `Publish` item, it is advised to check in the `Settings` item, that the registered DMB400 devices are consistent and sorted in the right order.*

The *Publishing status report* is showing whether the publishing on each DMB400 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 DMB400.

Publishing status report example:

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

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

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

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

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

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

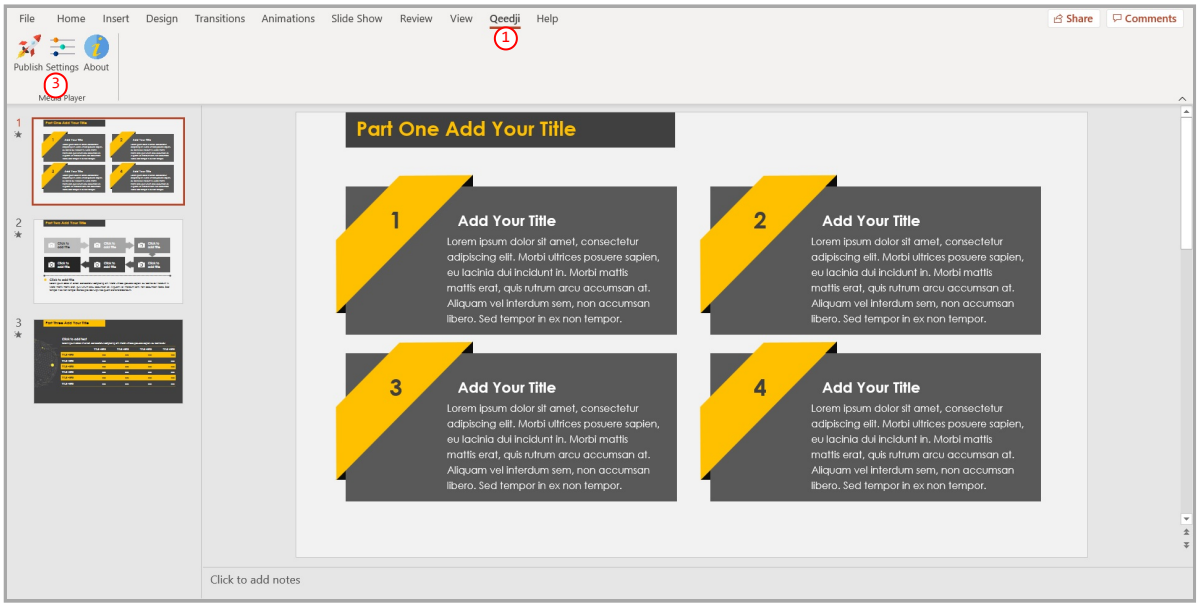
The *Publishing status report* is showing also whether the MS-PowerPoint medias can be rendered with the right fonts. In case some fonts can not be found on the Windows OS, a message `Warning - Unable to find the following fonts` is displayed followed by the missing fonts names. To solve the rendering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

The PowerPoint presentation slideshow is now running on your media player.

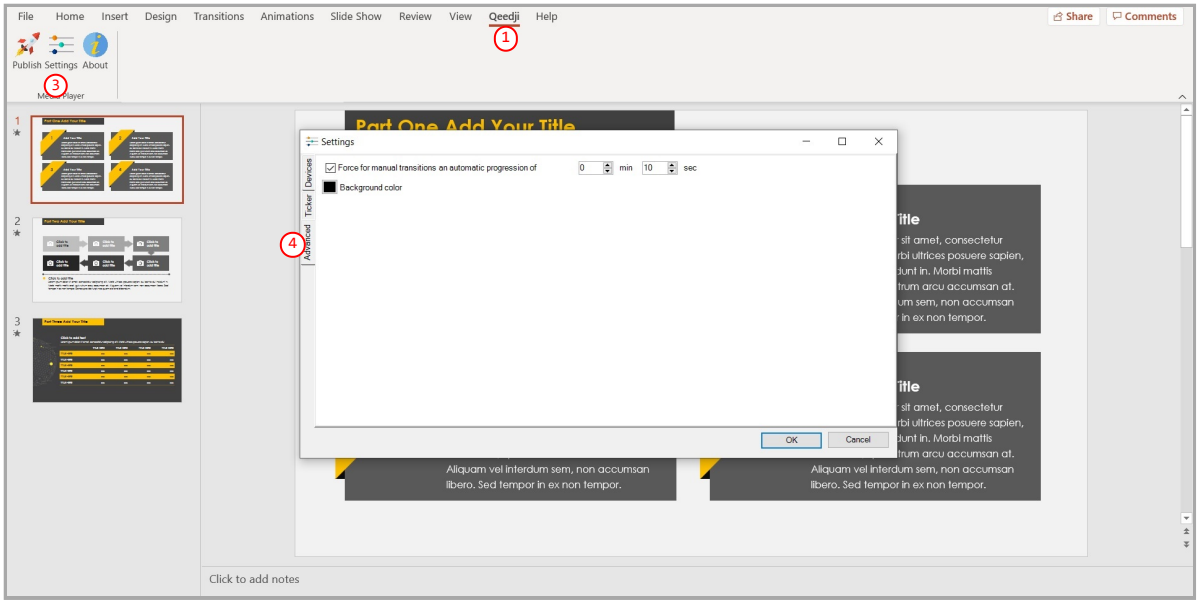
Qeedji PowerPoint Publisher For Media Players: define a default duration per page

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

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



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

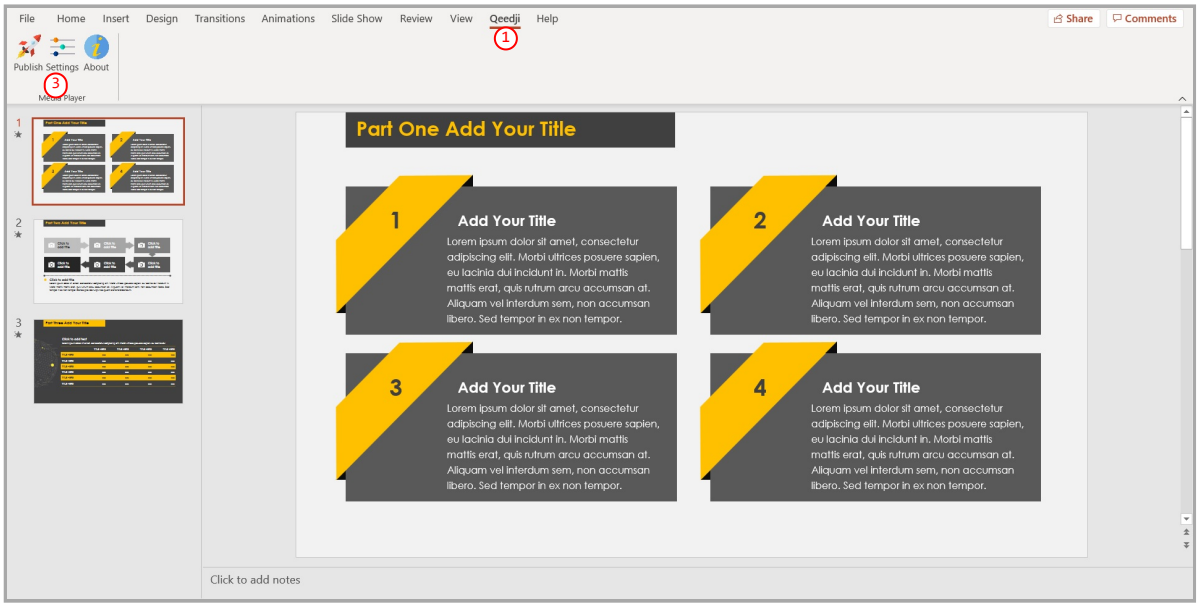


> ☛ *The `Background color` is used here only when the slide aspect ratio (`Slide Size` in MS-PowerPoint) is not 16:9.*

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

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

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



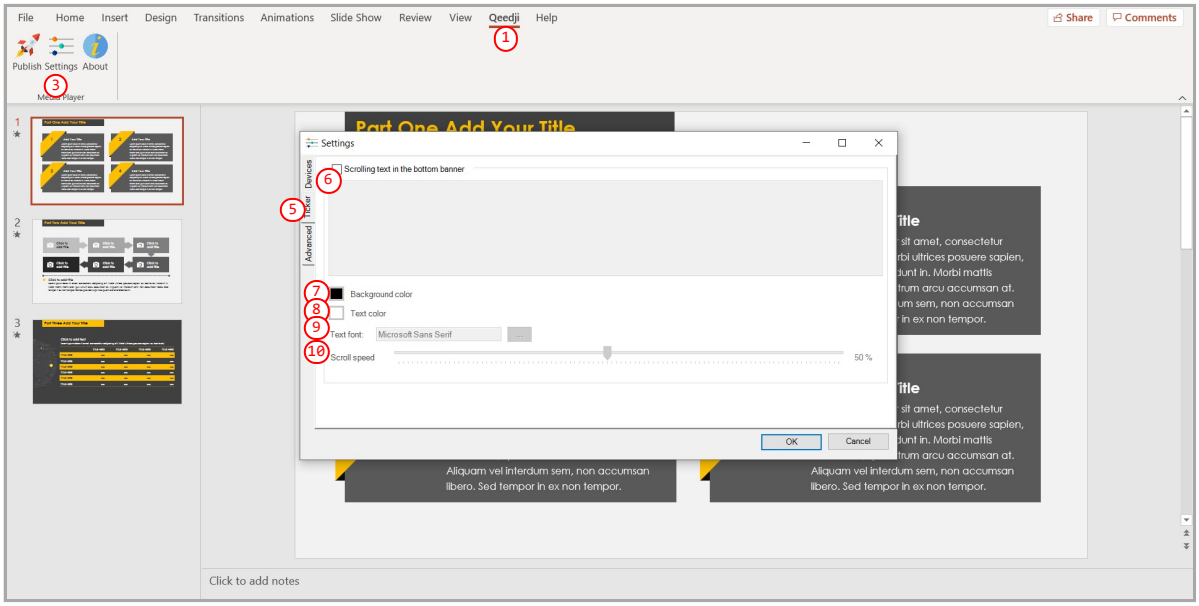
Then select the `Ticker` (5) tab.

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

These scrolling text properties can be modified:

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

> ☛ *The text is scrolled in overlay automatically.*
>
> ☛ *The banner height is 9.26% of the PowerPoint slide height.*
>
> ☛ *When the scrolling text overlay is supported by the DMB400 device, the max. number of character per line is depending on the display resolution of the DMB400 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.

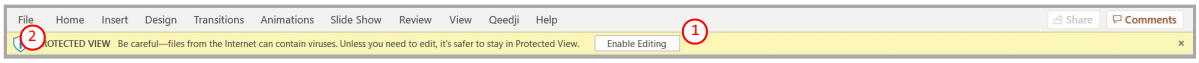
Qeedji PowerPoint Publisher For Media Players: miscellaneous

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

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

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

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



Qeedji PowerPoint Publisher For Media Players: user interactivity with USB keyboard or remote control

The user interactivity with USB keyboard and remote control key pressed is supported as soon as the PowerPoint presentation is played on the media player.

If the CEC is activated on your screen, and the CEC passthrough properly supported:

- Press on the `RIGHT ARROW` key of the screen remote control to go to the next slide,
- Press on the `LEFT ARROW` key of the screen remote control to go to the previous slide,
- Note: some screen may require to select again the video input so that the CEC works properly.

If not, you can plug an USB keyboard:

- Press on the `RIGHT ARROW` key of the USB keyboard to go to the next slide,
- Press on the `LEFT ARROW` key of the USB keyboard to go to the previous slide,
- Enter the slide number (for example: the number 4) then press `ENTER` to go ahead to a specific slide no.

> ⚠ Gekkota 4 allows to display/undisplay automatically the test card when pressing the key combination: `LEFT ARROW`, `RIGHT ARROW`, `LEFT ARROW`, `RIGHT ARROW` in less than ten seconds and could lead to unexpected along the presentation. To deactivate this feature, set the user preference `innes.player.mire.key-event.*.authorized` to false.

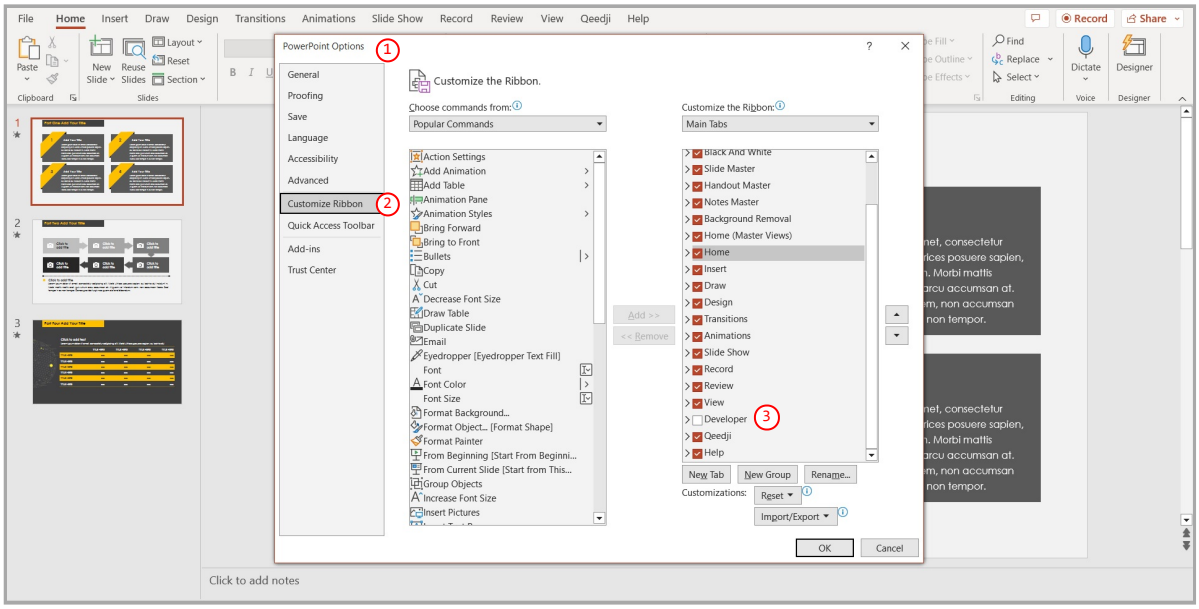
Qeedji PowerPoint Publisher For Media Players: custom script

`Qeedji PowerPoint Publisher for Media Player` (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.

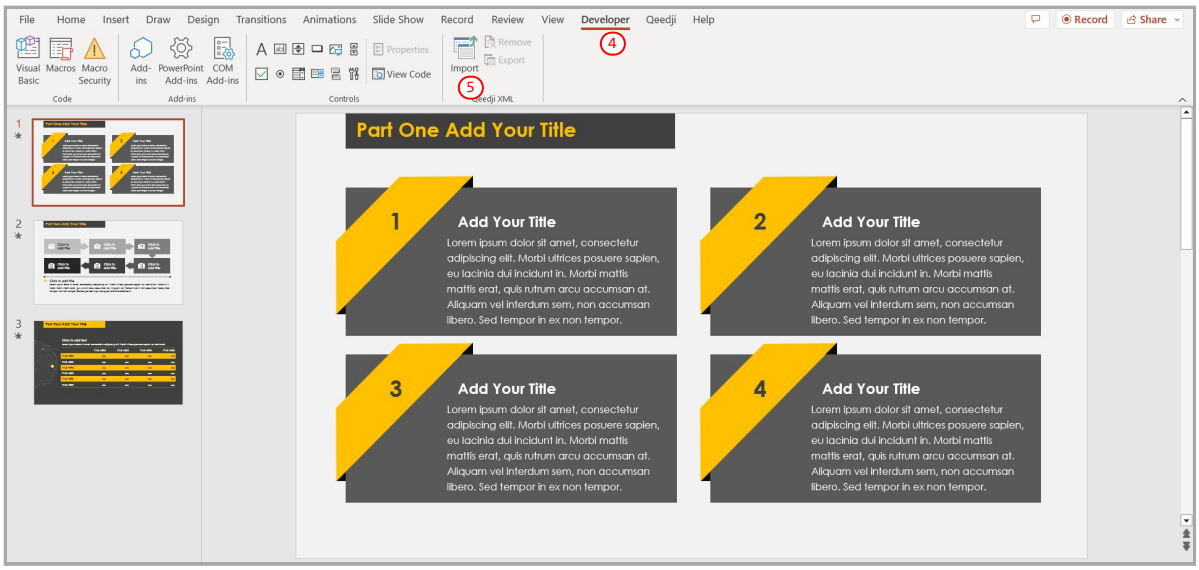
> ☛ *The `configuration.xml` can, for example, allow to navigate through your PowerPoint presentation page by sending specific UDP messages. In this case, it is advised to set a manual transition policy for slides where a user interactivity by UDP message is required. It is also advised to uncheck the option `force for manual transitions a automatic progression of <m> min <n> sec`. To get a `configuration.xml` template, contact support@innes.pro.*

Open your 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.

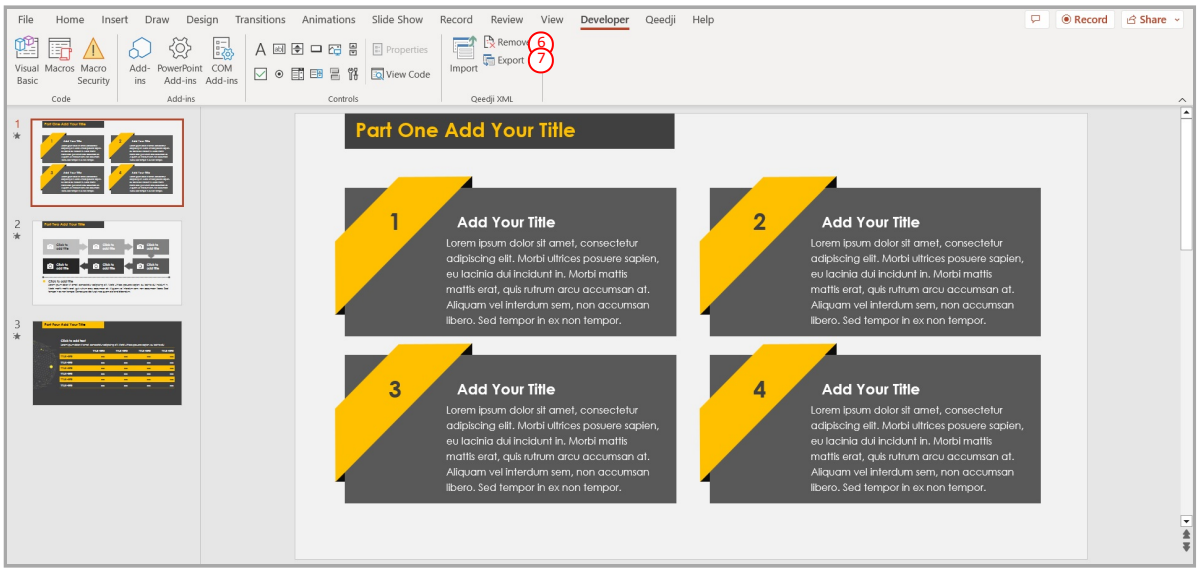


> ☛ *Each time the .xml file is modified, it must be imported again to be taken into account.*

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 16/9.

7.3 Appendix: playfolder with services account

The credential cache for `CIFS` and `Microsoft 365` service account is reset each time a new App is written in the `/.playout` WebDAV directory.

When the folder synchronization with the remote folder is broken, the playfolder continue to play the last content synchronized with success. To delete the content of the local directory, image of the remote folder content when the folder synchronization is working, you need to remove the App and publish again.

The *NetBIOS* name resolution is not supported in this OS version.

7.4 Appendix: scrolling text overlay

When the scrolling text is displayed in overlay in the full HD resolution, the device supports until 1226 characters per line (*Arial* font) in the text file.

When the scrolling text is displayed in overlay in the ultra HD resolution, the device supports until 688 characters per line (*Arial* font) in the text file.

> ☛ *When the text is scrolled in overlay, using another font than `Arial` may lead to a lower max number of characters per line.*

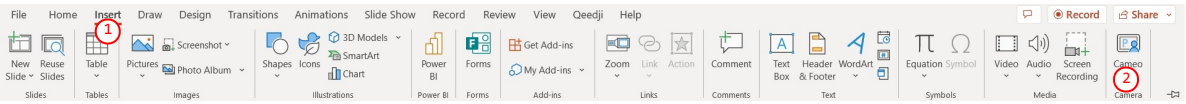
The max height for the banner in which a scrolling text is played must be lower than 20% of the screen height.

7.5 Appendix: video-input playback inside a MS-PowerPoint slide thanks to the MS-PowerPoint Cameo object insertion

The Gekkota OS (4.14.12 or above) allows to play the video coming from the HDMI-input inside a `MS-PowerPoint` slide thanks to the `MS-PowerPoint` *Cameo* object.

> ☛ *Only the recent Desktop versions of `MS-PowerPoint` support the insertion of a `MS-PowerPoint``Cameo` object type in a slide. For further information about `MS-PowerPoint` `Cameo` object, contact your `Microsoft` support.*

To insert a `MS-PowerPoint` *Cameo* object in a `MS-PowerPoint` slide, click on the *Insert* tab of the `MS-Powerpoint` ribbon then click on the *Cameo* item.



Connect a video source on the HDMI-input connector of the DMB400.

Publish the App containing the MS-PowerPoint media on the DMB400. Once done, the slide having the *Cameo* object should play automatically the video coming from the HDMI-input.

7.6 Appendix: Microsoft Azure AD portal for URL launcher application

You can create your Azure Active Directory (or AAD) 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.

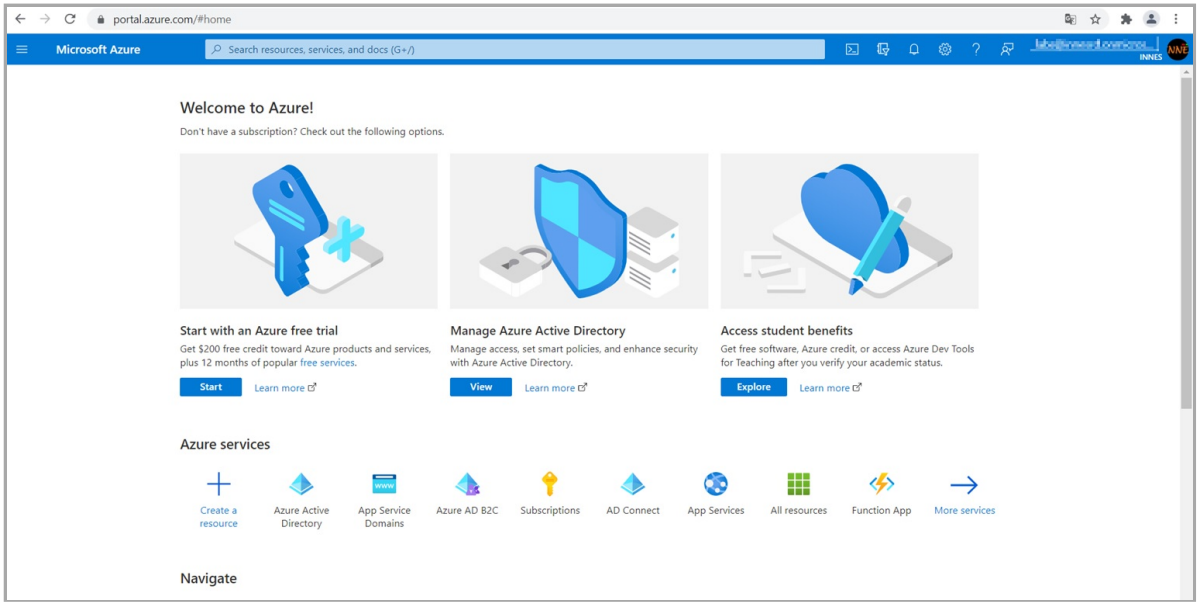
This procedure allows to generate you own client ID and client SECRET required for the `URL launcher` application with *Microsoft 365* connection account:

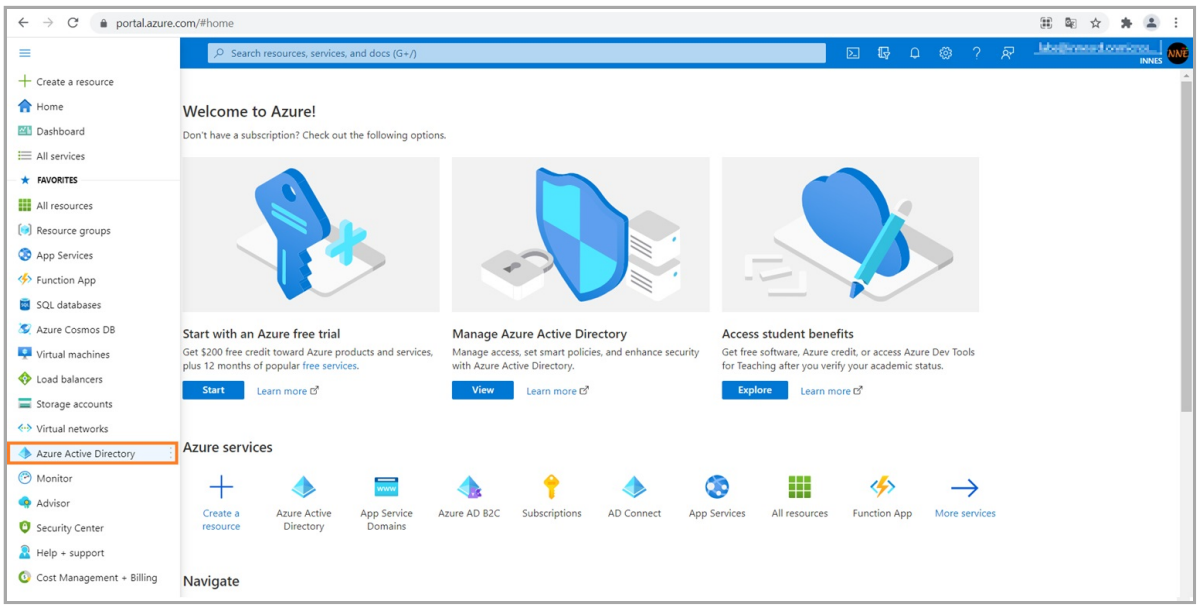
- `Application (client) ID`,
- `Directory (Tenant) ID`,
- `Client secret`.

> ☞ *If you want to follow the PowerShell scripts procedure instead of following the procedure by connecting to the `Azure AD` portal, only `PowerShell script for Azure Active Directory Application support 1.10.16 (and above)` is supported. For further information, refer to the chapter § Appendix: Azure AD Application PowerShell module.*

Connect on Microsoft Azure portal: https://portal.azure.com/ and sign in with your Office Administrator account login credentials.

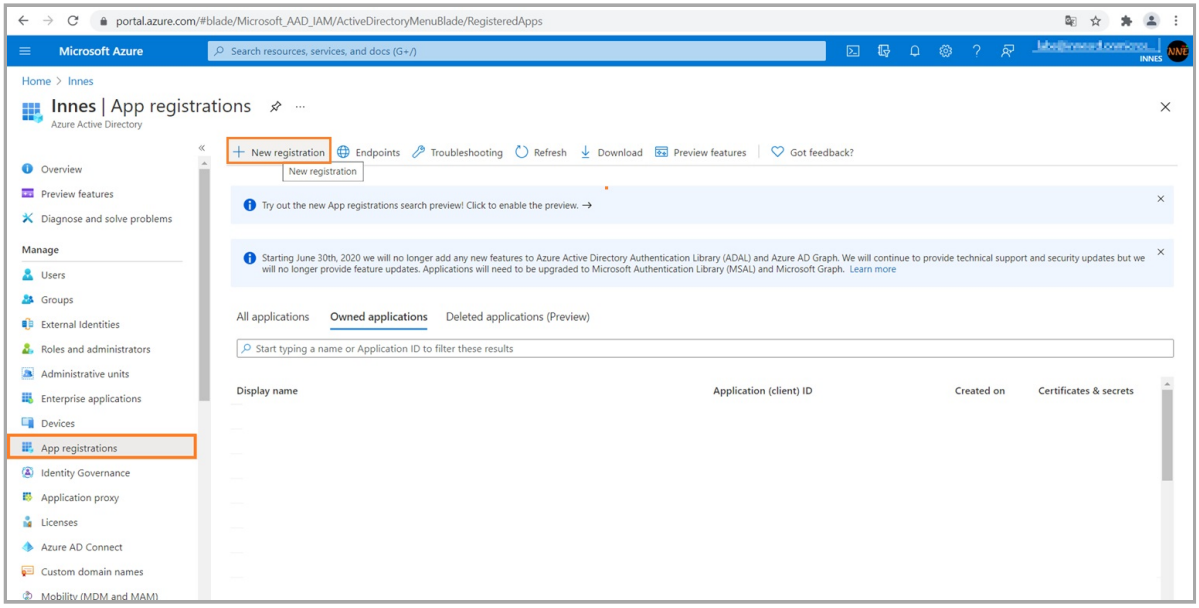
Click on the left top menu and choose the `Azure Active directory` item.



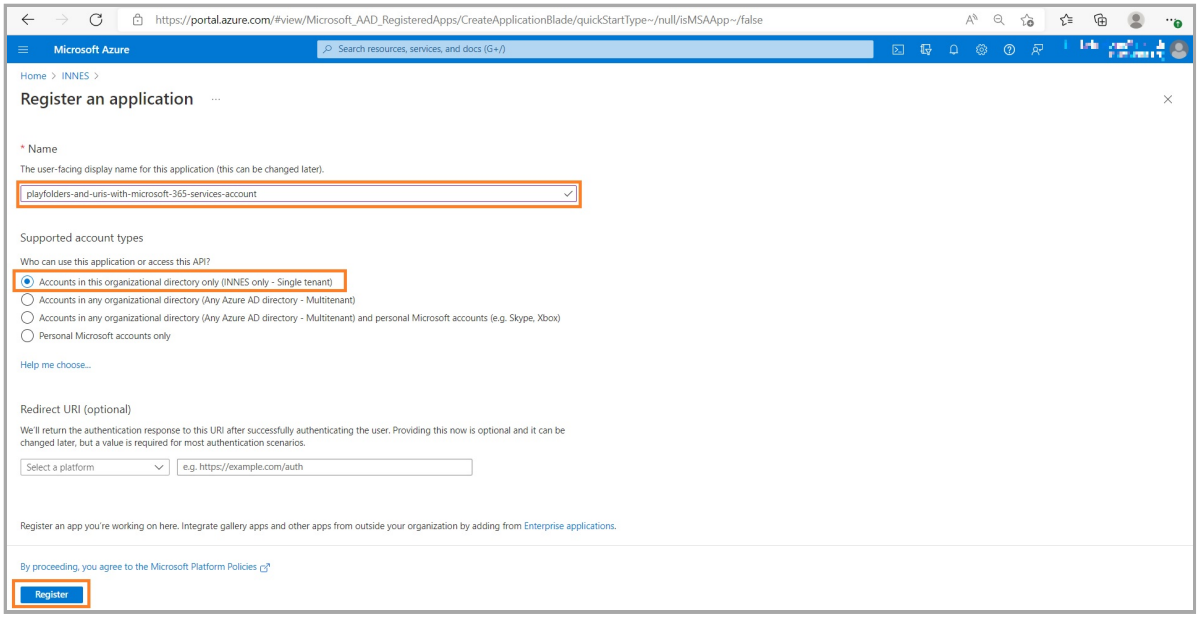


Application (client) ID and directory (Tenant) ID

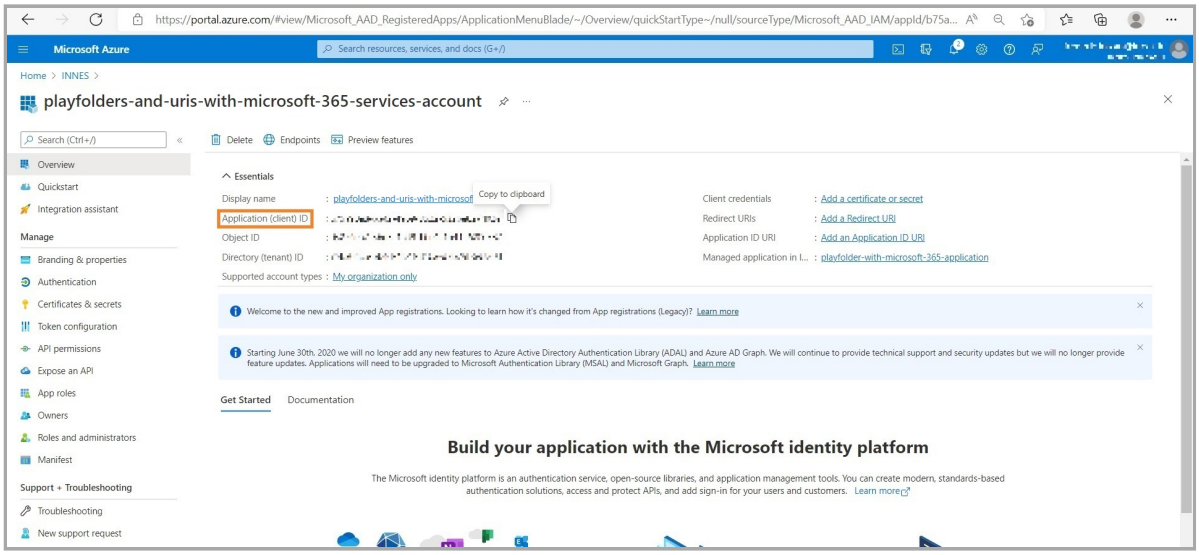
On the App registrations menu, click on *New registration*
`https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/RegisteredApps`.



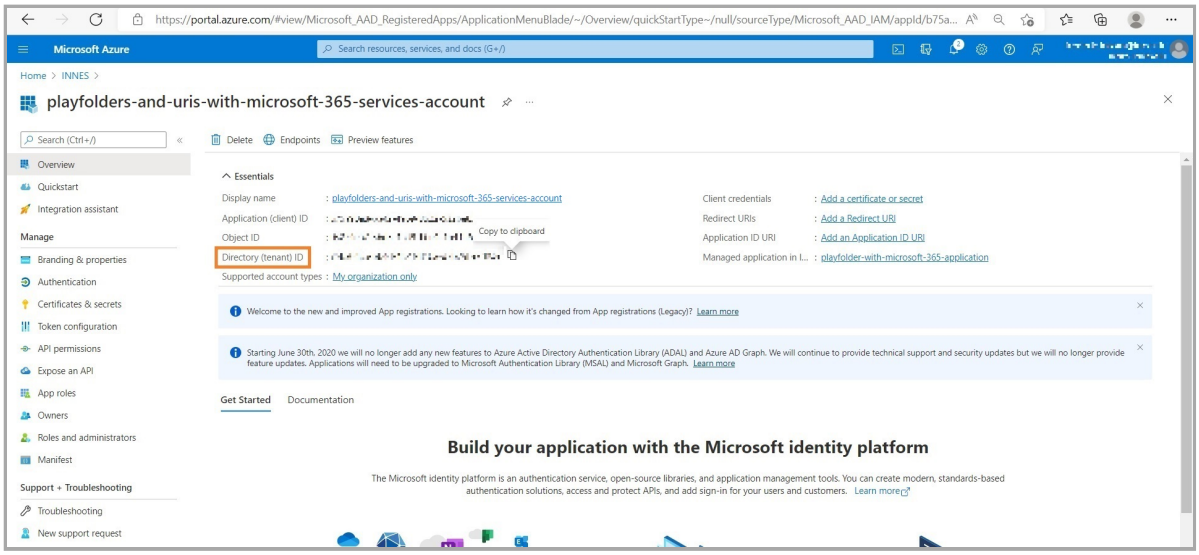
Enter an application name (e.g.: *playfolder-with-microsoft-365-application*), Select the appropriate Account in the organisation directory only (organisation only – Single tenant) radio button, and click on the *Register* button.



In the Overview menu, copy to clipboard the Application (client) ID value, the 1st value required in DMB400 App configuration tab and store it preciously.

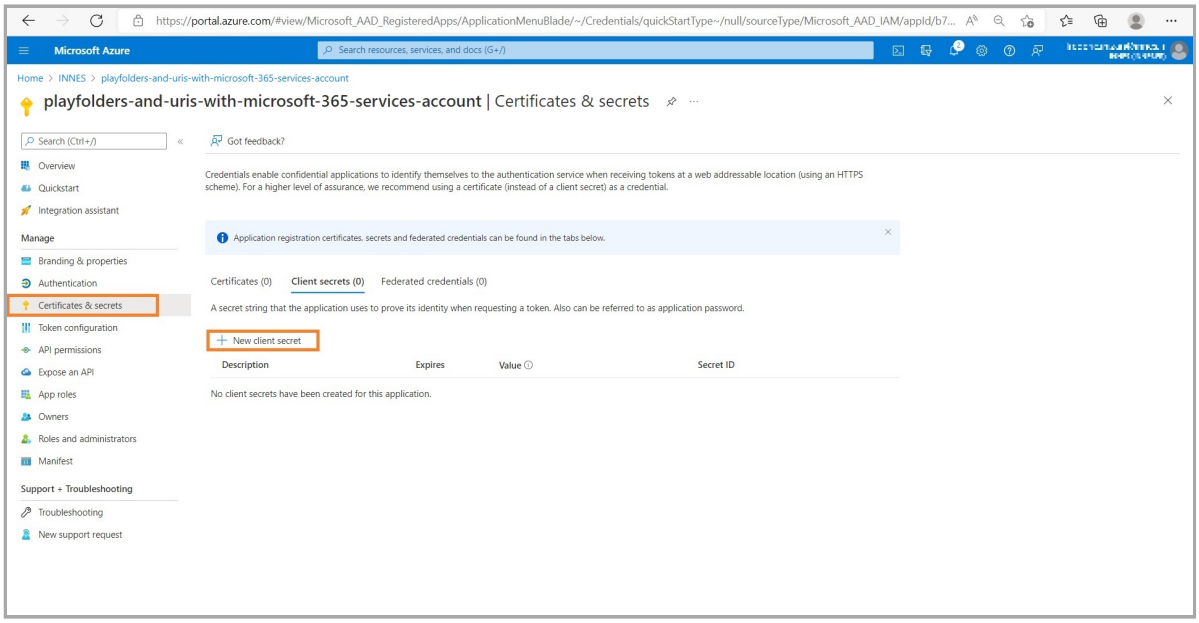


In the Overview menu, copy to clipboard the Directory (tenant) ID value, the 2nd value required in DMB400 App configuration tab and store it preciously.

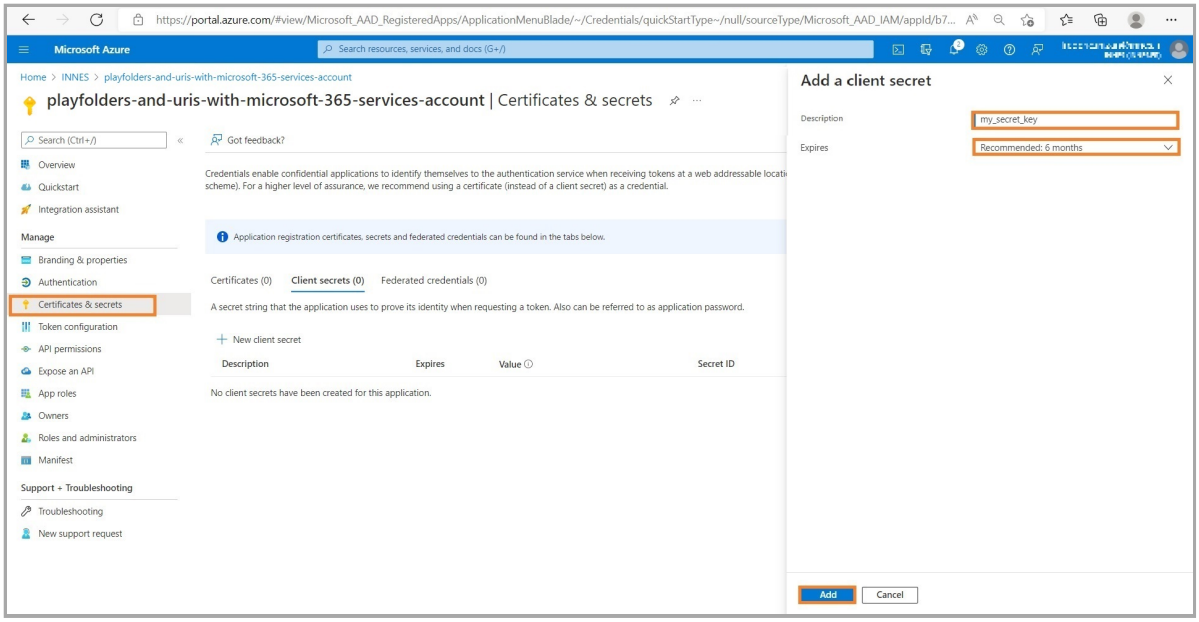


Client secret

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

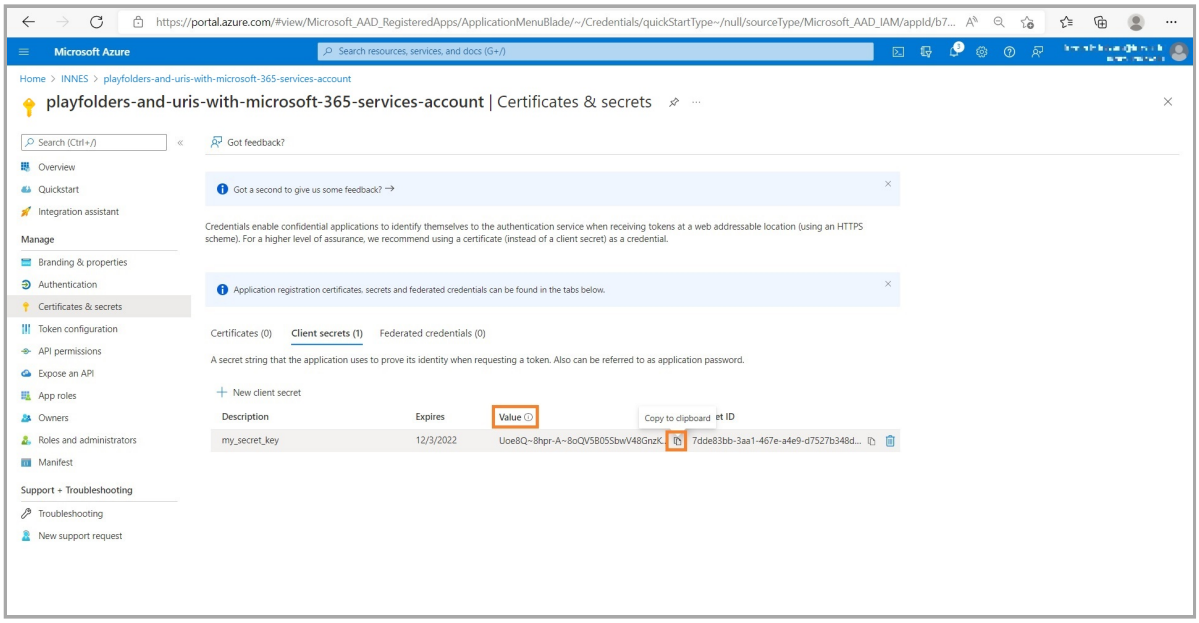


Enter a name (e.g.: *my_secret_key*) and click on the Add button.



Copy into clip board the client secret value, the 3rd input for the DMB400 App 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.


https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/Credentials/quickStartType~/null/sourceType/Microsoft_AAD_IAM/appId/b7...
Microsoft Azure
Search resources, services, and docs (G+/)
Home > INNES > playfolders-and-uris-with-microsoft-365-services-account
playfolders-and-uris-with-microsoft-365-services-account | Certificates & secrets
Search (Ctrl+/)
Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Got feedback?
Got a second to give us some feedback?
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.
Application registration certificates, secrets and federated credentials can be found in the tabs below.
Certificates (0)
Client secrets (1)
Federated credentials (0)
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.
New client secret
Description
Expires
Value
Copy to clipboard
et ID
my_secret_key
12/3/2022
Uoe8Q~8hpr-A~8oQV5B05SbwV48GnzK...
7dde83bb-3aa1-467e-a4e9-d7527b348d...

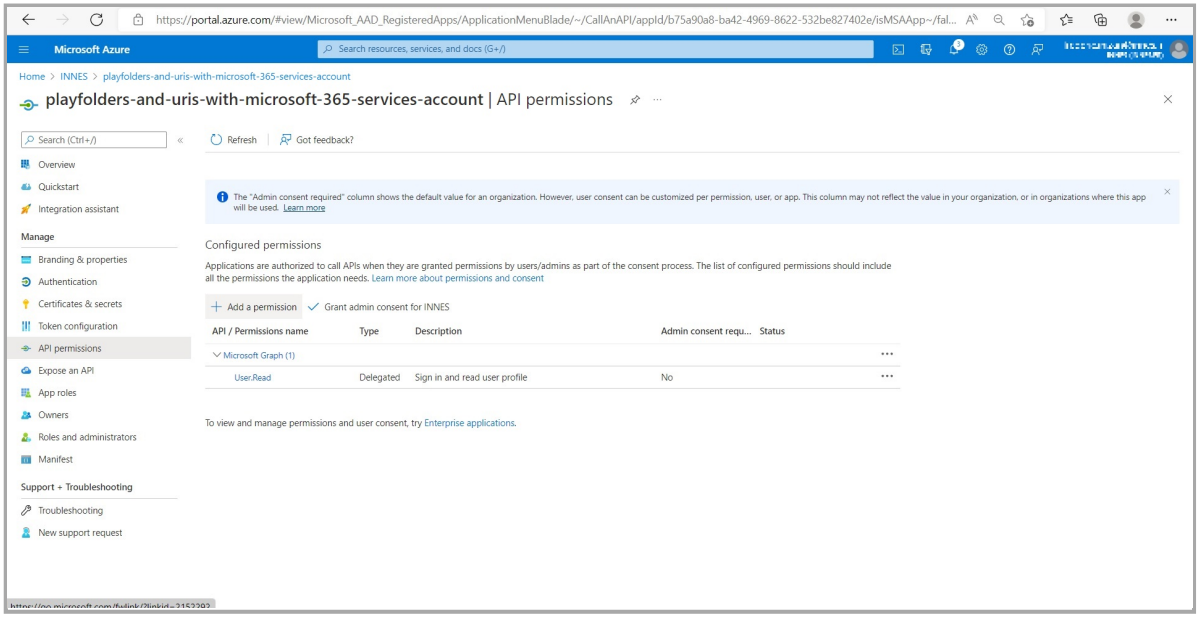
Grant permissions

For the *playfolders* and *uris* application, these permissions must be granted:

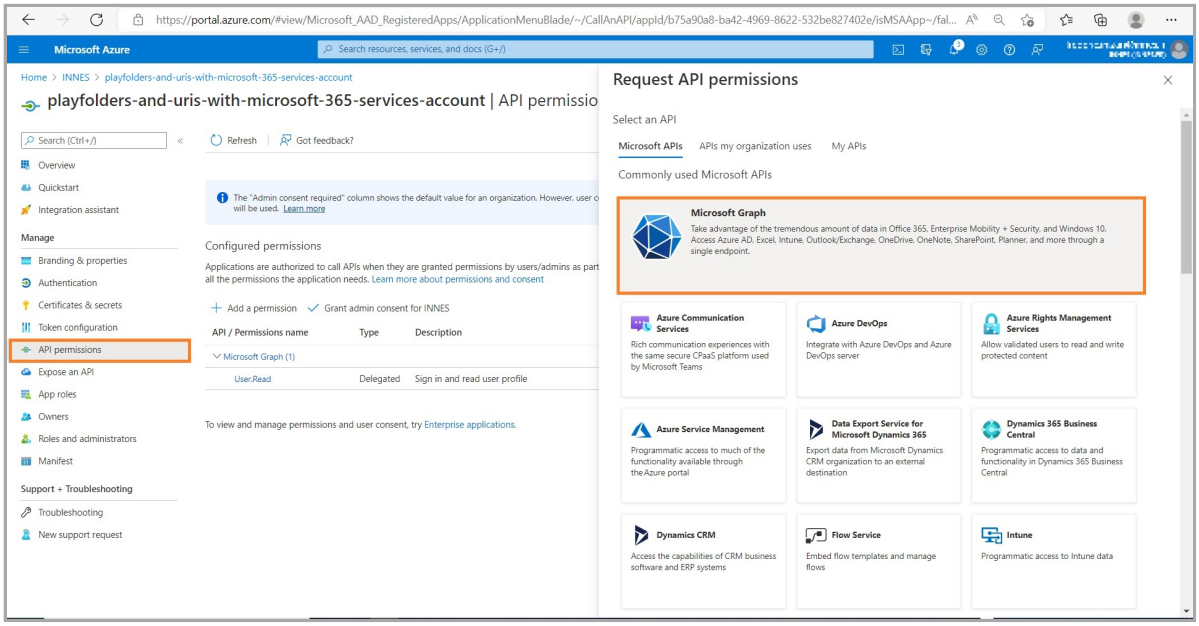
- Application permissions:
  - `Files.Read.All` ,
  - `Sites.Read.All` ,
- Delegated permissions:
  - `Files.Read.All` ,
  - `Sites.Read.All` ,
  - `User.Read` (default).

> ☛ *The `Files.Read.All` permission allows to read files or folder content on oneDrive. The `Sites.Read.All` permission allows to read the Web URL.*

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

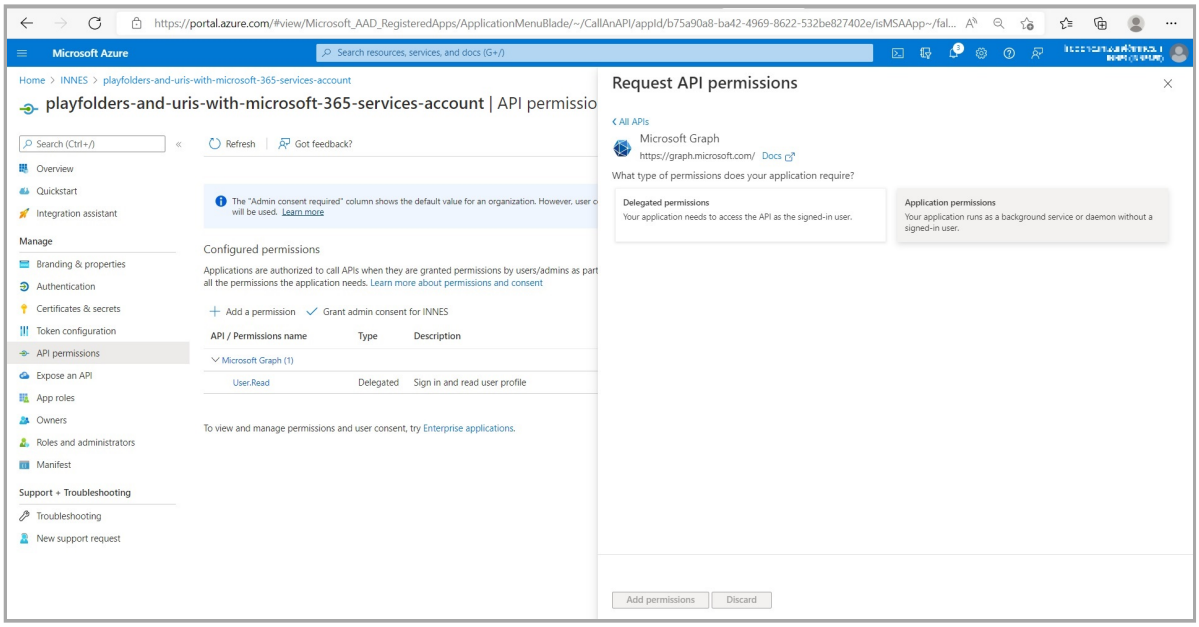


Select `Microsoft Graph` button in the `Microsoft APIs` tab.



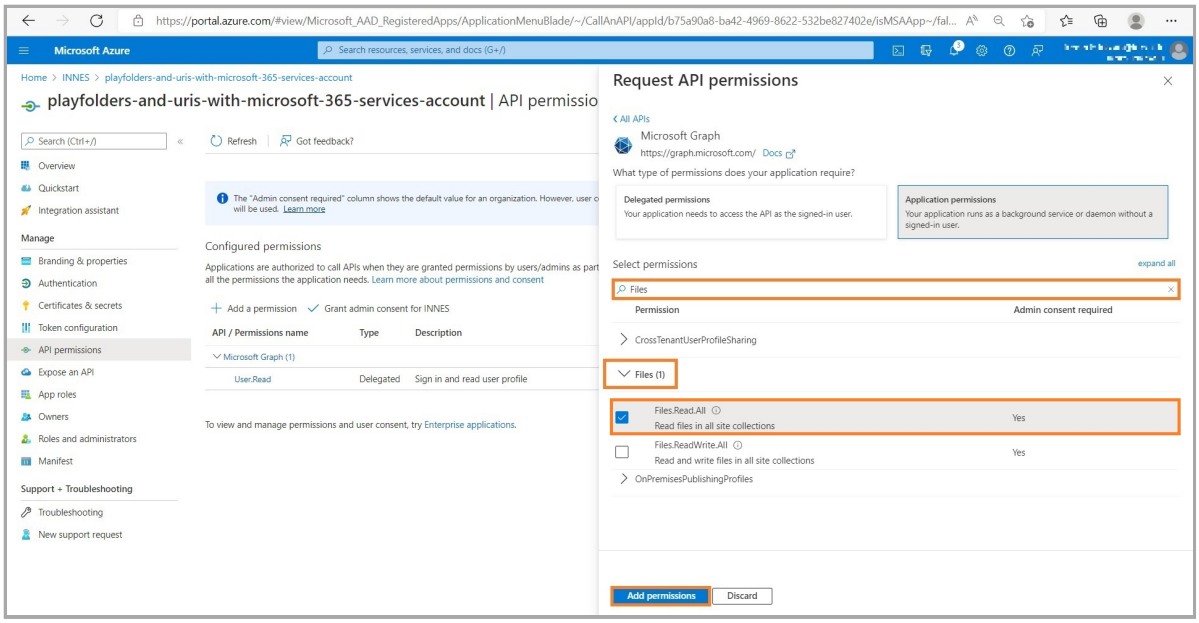
Application permission:

Select then the `Application permissions` button.

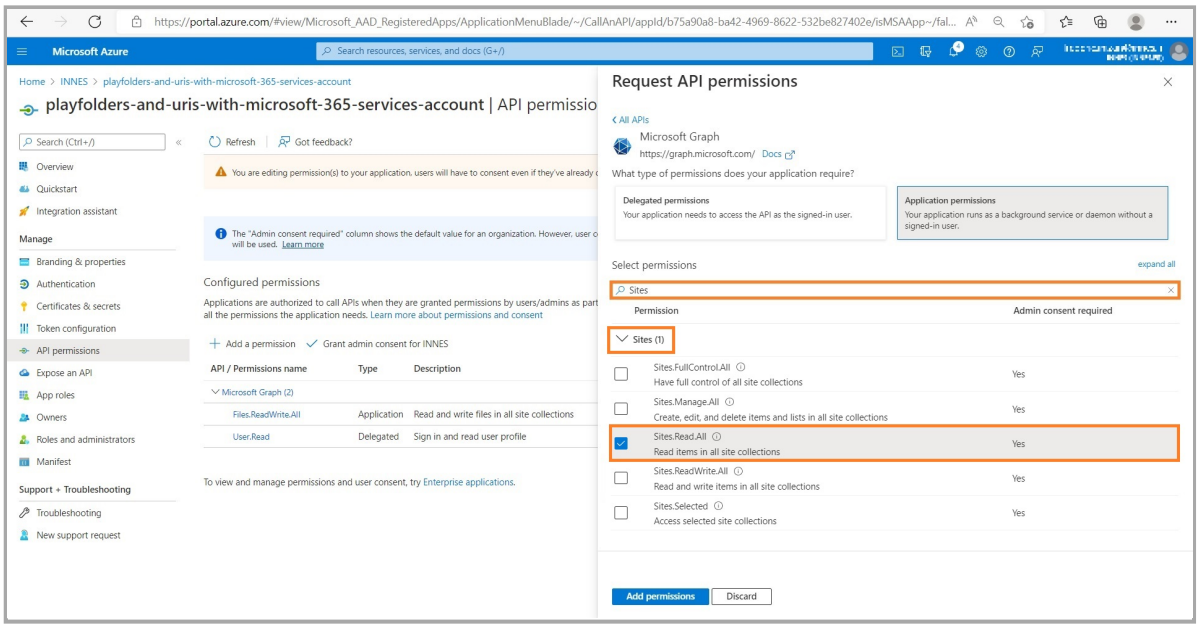


In the display filter input, enter the text *Files* and check the option `Files.Read.All` .

> ☛ *Do not click now on the `Add permissions` button.*



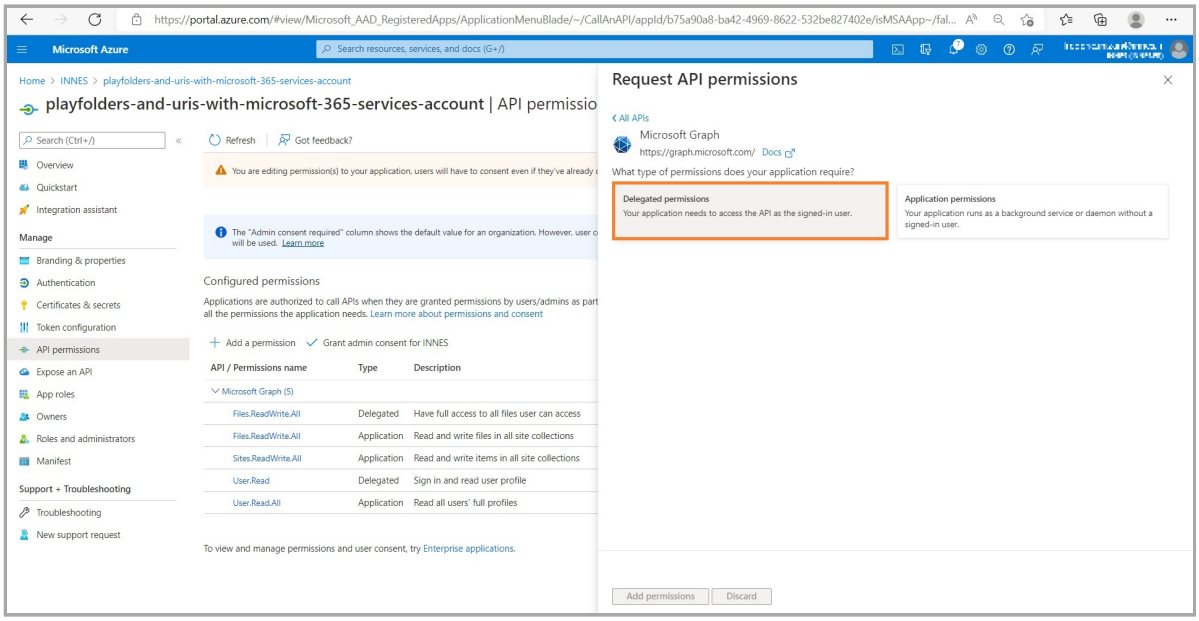
To be able to read Sharepoint Web URL or Sharepoint Web sites, in the display filter input, enter the text *Sites* then check the option `Sites.Read.All`.



Click on the `Add permissions` button.

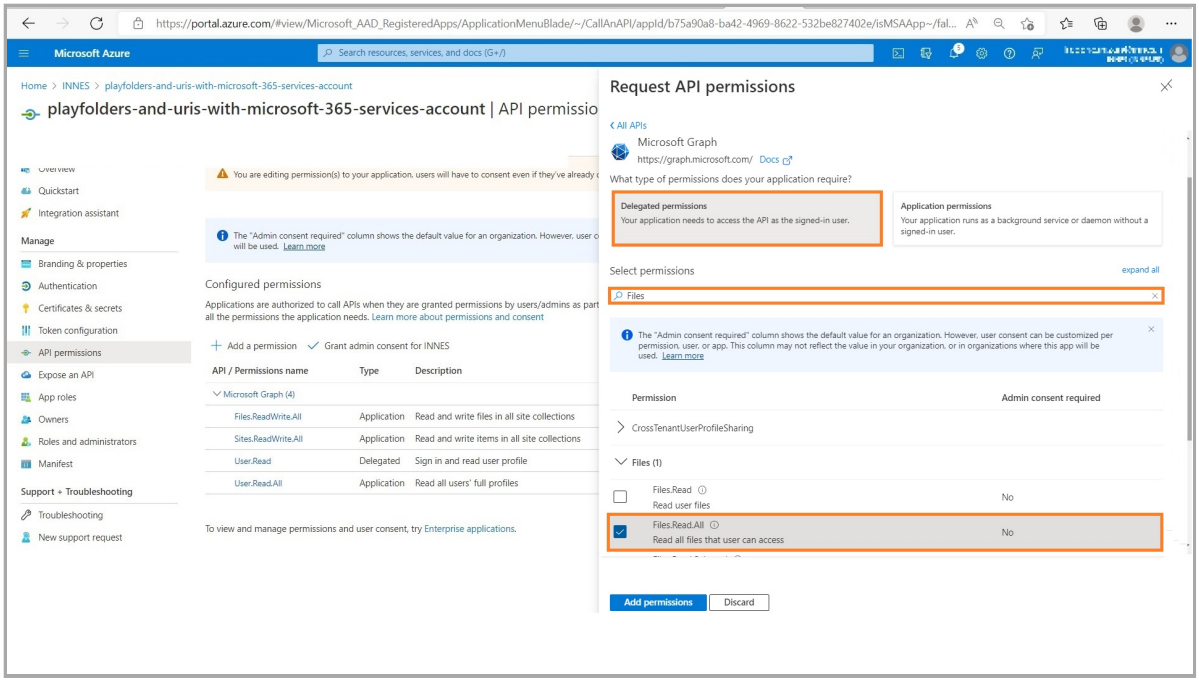
Delegated permissions:

Select then the `Delegated permissions` button.

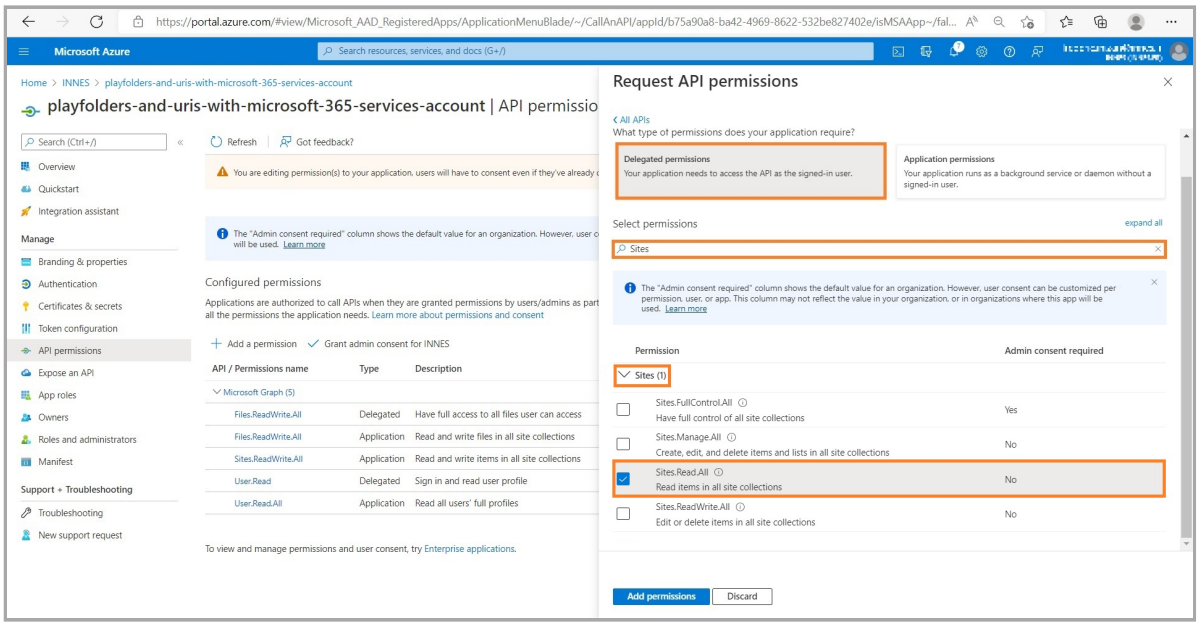


In the display filter input, enter the text *Files* and check the option `Files.Read.All` .

> ☛ *Do not click now on the `Add permissions` button.*



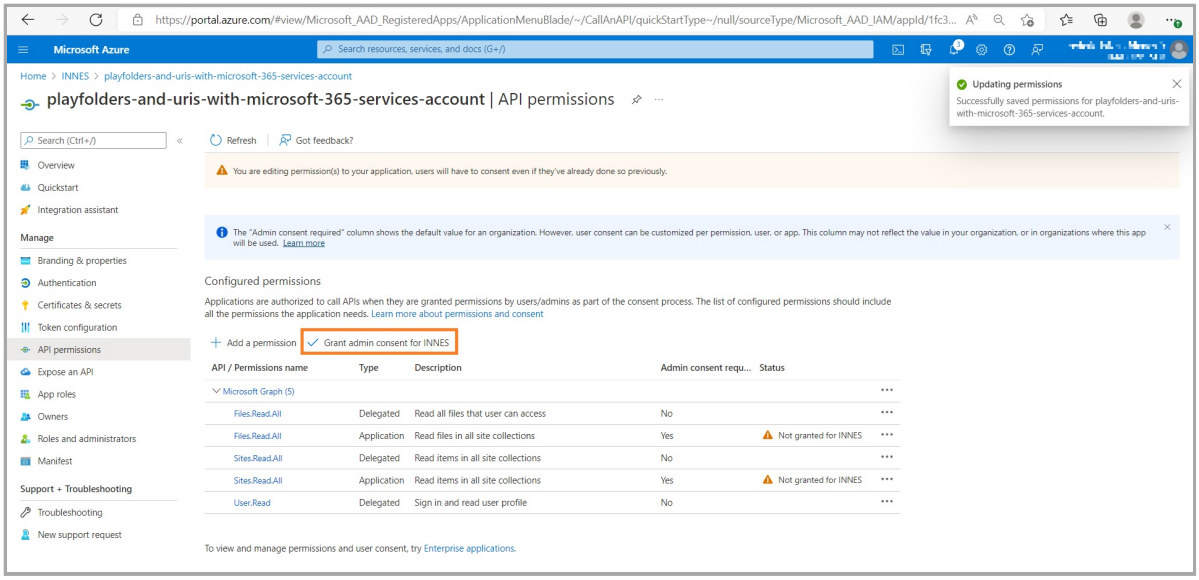
To be able to read Sharepoint Web URL or Sharepoint Web sites, in the display filter input, enter the text *Sites* then check the option `Sites.Read.All`.

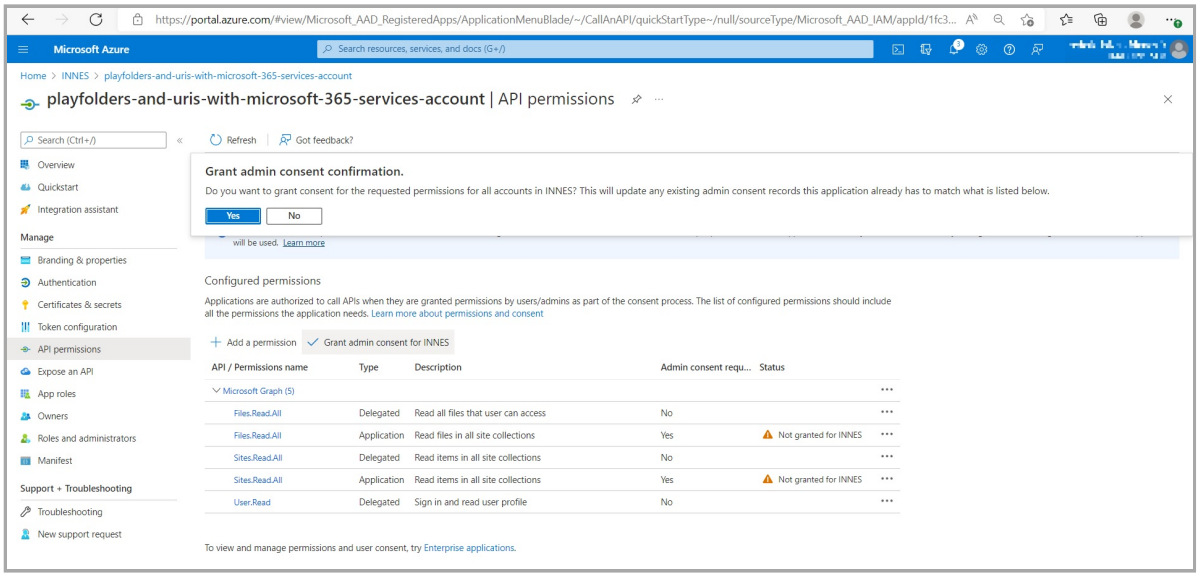


At this step, the permissions are not yet granted.

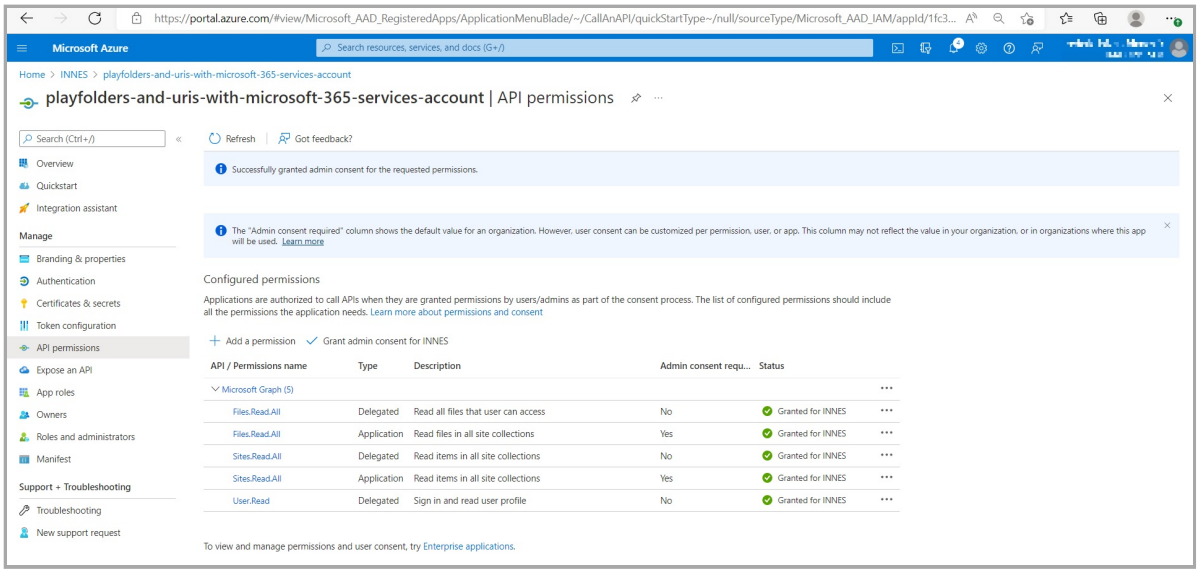
Grant permissions:

Click on the `Grant admin consent for <your_organisation> button`.





Now the permissions are granted.



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 URL launcher application.

7.7 Appendix: Azure AD Application PowerShell module for URL launcher application

This is the suitable PowerShell module to create your Azure Active Directory Application for Web page based on a *Microsoft 365* service account.

> ⚠ For Web page application, the PowerShell script for Azure Active Directory Application support (`Powershell_Innes_AAD`) must be 1.10.16 (or above).

Download the PowerShell script for Azure Active Directory Application support `Powershell_Innes_AAD-1.10.16.zip` from the Innes Site Web then follow the instructions below.

Compatibility

The `Powershell_Innes_AAD-1.10.16.zip` PowerShell script for Azure Active Directory application is compatible with `PowerShell` 5.X (deployed on Windows 10).

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 organisation 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 clic 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 AzureAD 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 theses 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 your 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 \server\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     1.10.16    PSAAD
Function        Remove-AADApplication  1.10.16    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 Web sites for SignCom application
        - "url_launcher_m365" : to access to M365 Web sites 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 report

    -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 "my-App-Label" -authorizations "Authorization type"

    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                           my-App-Label
    tenantId                       xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
    clientSecret                   xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

REMARKS
    To see the examples, type: "get-help New-AADApplication -examples".
    For more information, type: "get-help New-AADApplication -detailed".
    For technical information, type: "get-help New-AADApplication -full".
```

Example to create an Azure Active Directory application

```
PS > $result = New-AADApplication -appname "url-launcher-with-microsoft-365-service-account" -authorizations "url_launcher_m365"
```

> ☛ *Don't use space characters inside the appname else an error could be returned.*
>
> ☛ *Don't use an already existing Appname 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 (`https://www.office.com/`) login credentials having a profile with rights granted for administration of Microsoft Application.

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

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

After thirty 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 organisation* title is prompted in your Web browser.

Click 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 command :

```
PS > $result
Name                           Value
----                           -----
clientId                       xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
objectId                       xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
spId                           xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
name                           url-launcher-with-microsoft-365-service-account
tenantId                       xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
clientSecret                   xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

The result of the *Powershell* function is also stored in a JSON file: `result.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 "url-launcher-with-microsoft-365-service-account"
```

A login popup is opened. Enter again your Microsoft 365 credentials. In case the values do not allow Web page with *Microsoft 365* `service account` to be launched properly, check in Azure portal that the application has been created succesfully and the rights are properly granted. If not, wait for a while, the rights granting may take several hours.

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

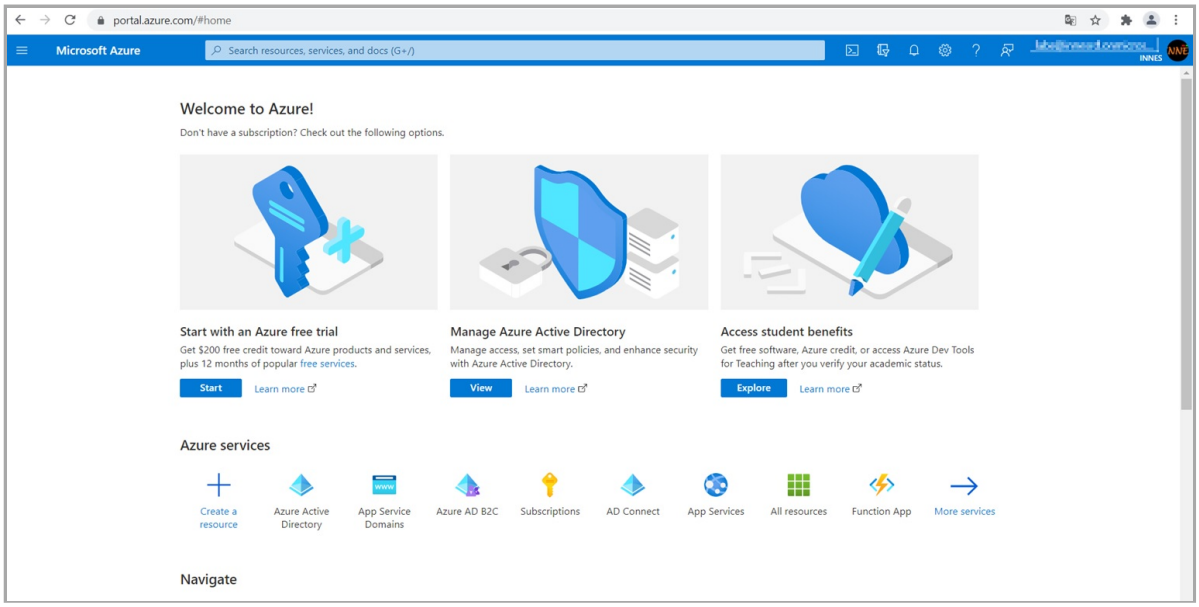
You can create your `Azure Active Directory` (or `Azure AD`) application by following this Microsoft tutorial https://docs.microsoft.com/en-us/graph/auth-register-app-v2.

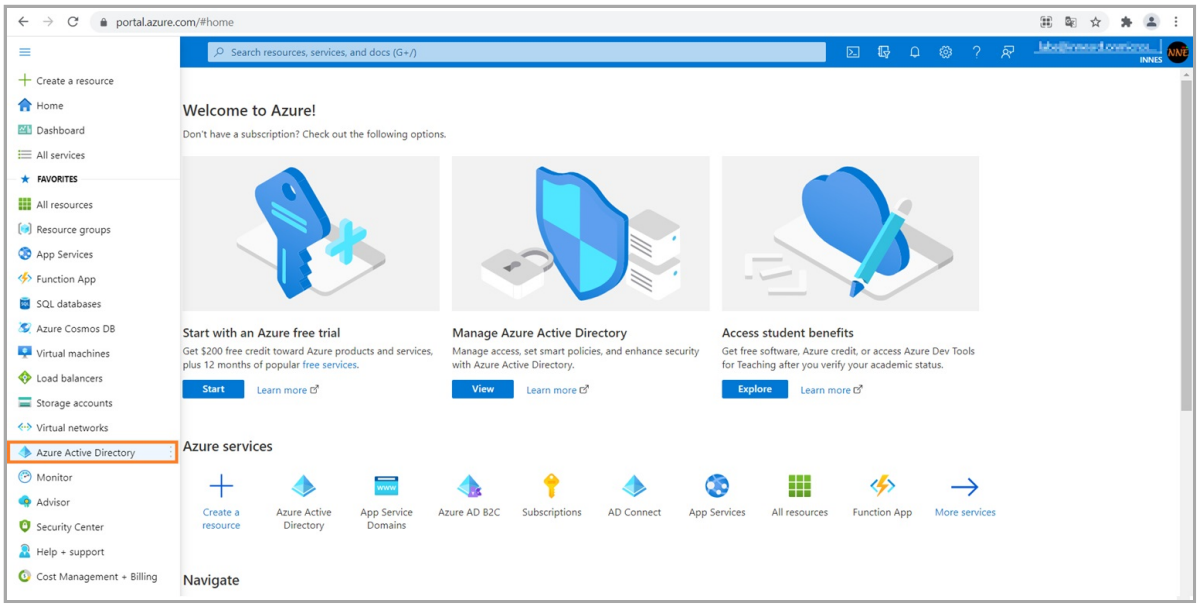
A procedure example is shown here after by connecting to the *Microsoft Azure* portal.

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`.

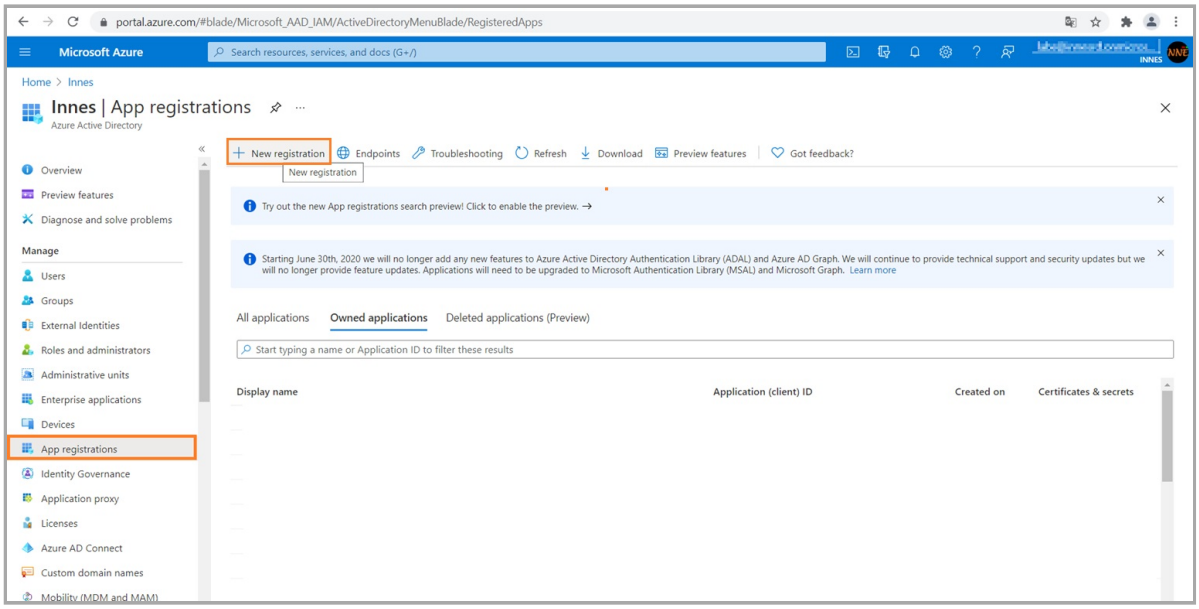
Connect on Microsoft Azure portal: https://portal.azure.com/ and sign in with your `Microsoft 365` (`M365`) administrator account login credentials. Click on the left top menu and choose the *Azure Active Directory* item.



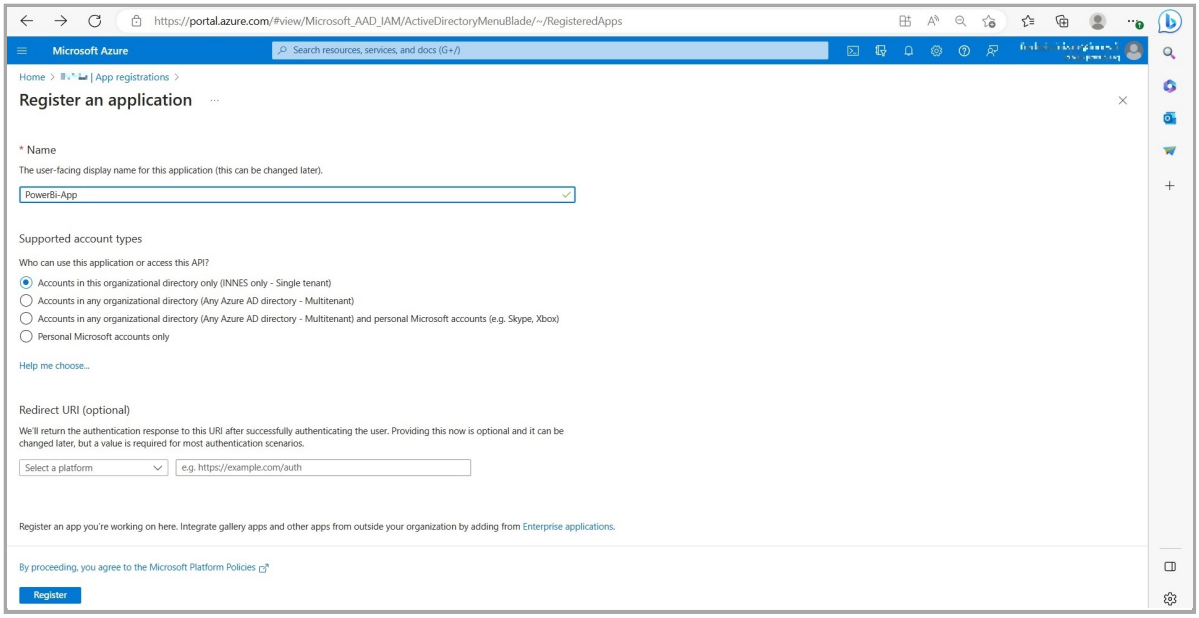


Application (client) ID and directory (Tenant) ID

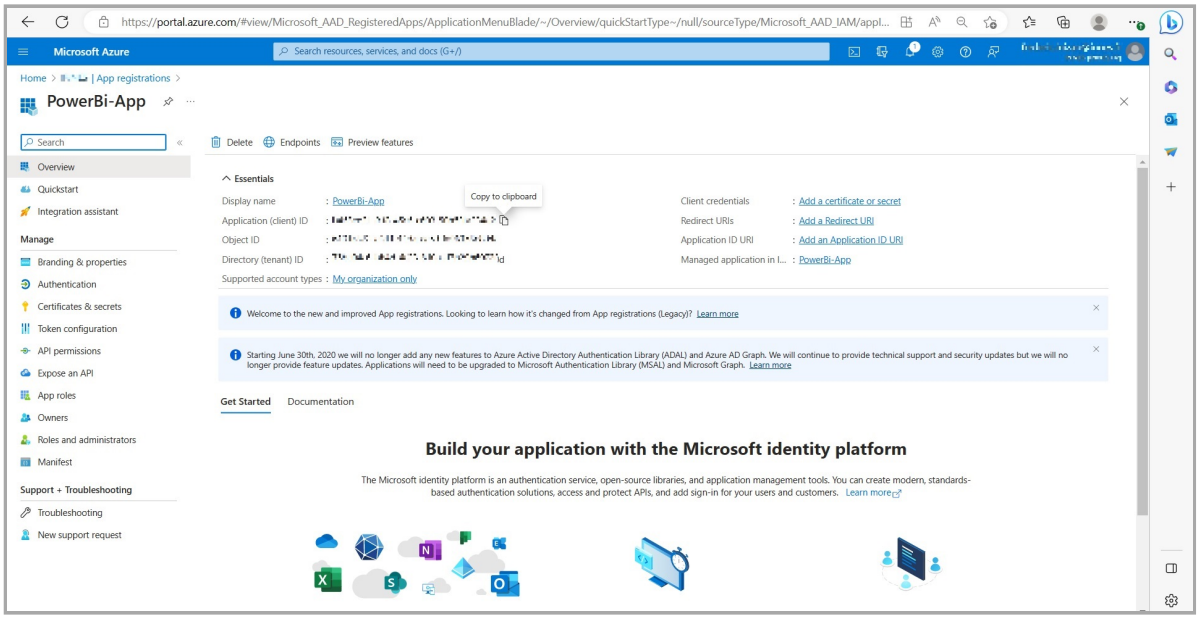
On the App registrations menu, click on *New registration*.



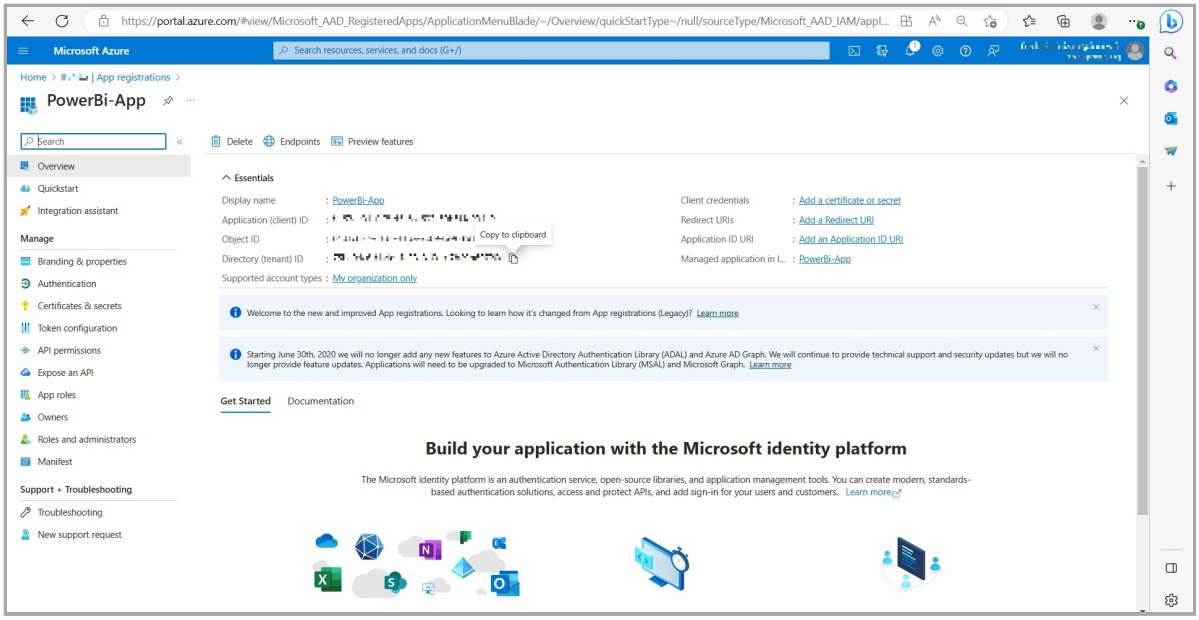
Enter an application name (e.g.: *PowerBi-App*), Select the appropriate Account in the organization directory only (organization only – Single tenant) radio button, and press on the `Register` button.



In the `Overview` menu, copy to clipboard the `Application (client) ID` value, the 1st value required in DMB400 configuration tab and store it preciously.

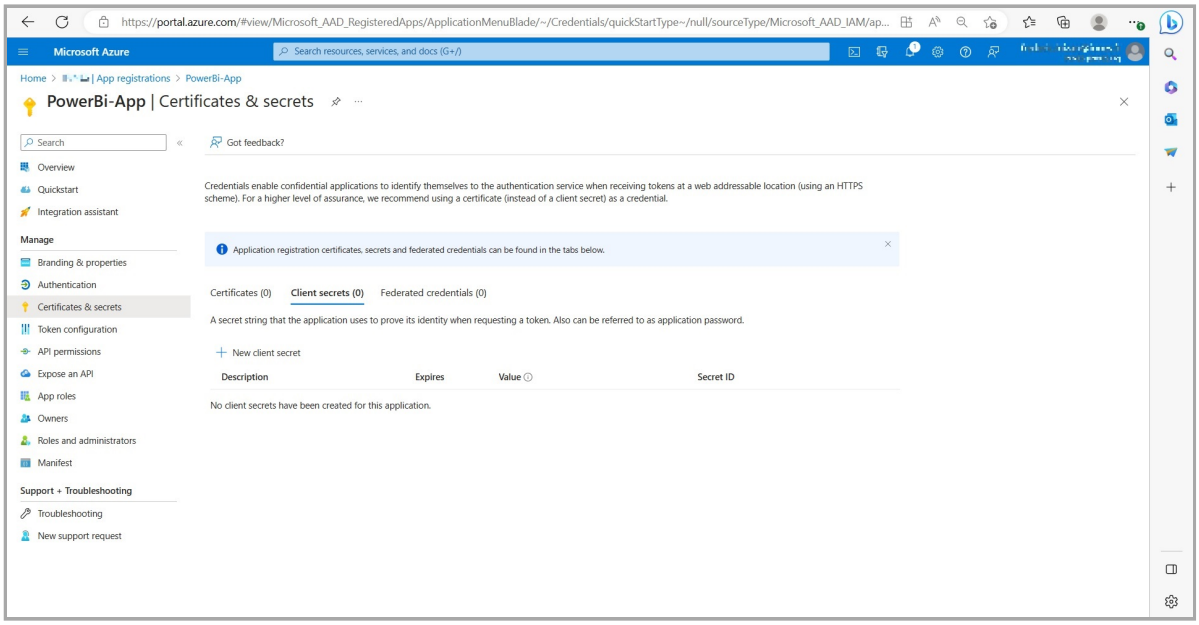


In the `Overview` menu, copy to clipboard the Directory (tenant) ID value, the 2nd value required in DMB400 configuration tab and store it preciously.

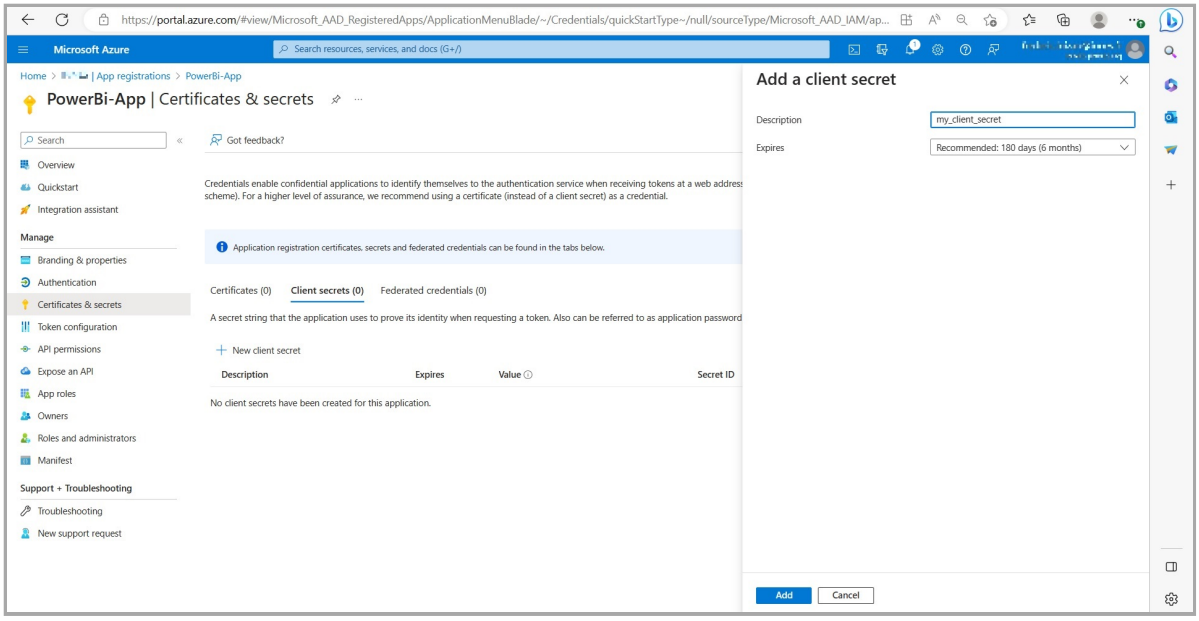


Client secret

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

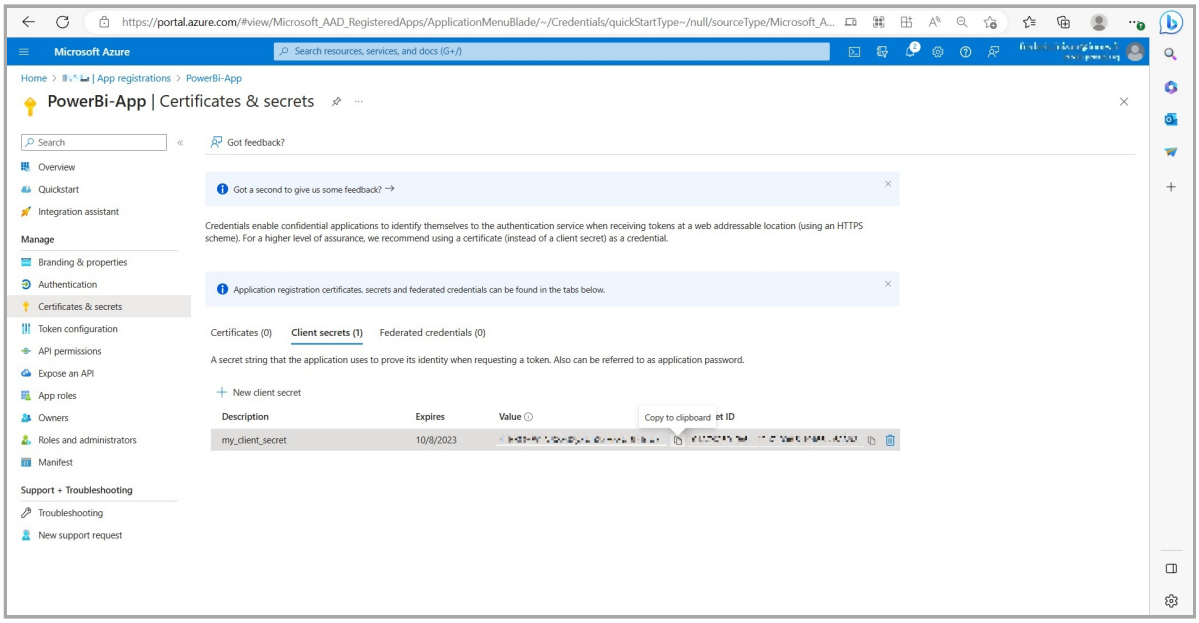


Enter a name (e.g.: `my_client_secret`) and press on the `Add` button.



Copy into clipboard the `client secret` value, the 3rd input for the DMB400 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.

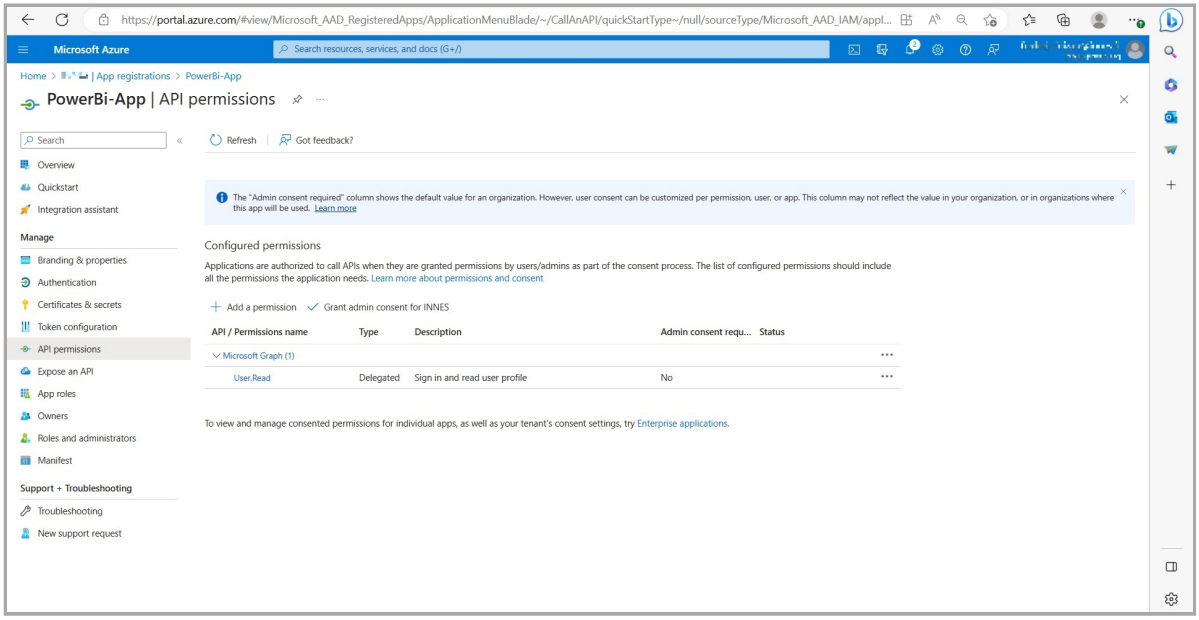

https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/Credentials/quickStartType~/null/sourceType/Microsoft_A...
Microsoft Azure
Search resources, services, and docs (G+/)
Home > | App registrations > PowerBi-App
PowerBi-App | Certificates & secrets
Search
Got feedback?
Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Got a second to give us some feedback?
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.
Application registration certificates, secrets and federated credentials can be found in the tabs below.
Certificates (0)
Client secrets (1)
Federated credentials (0)
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.
New client secret
Description
Expires
Value
Copy to clipboard
et ID
my_client_secret
10/8/2023

Grant permissions

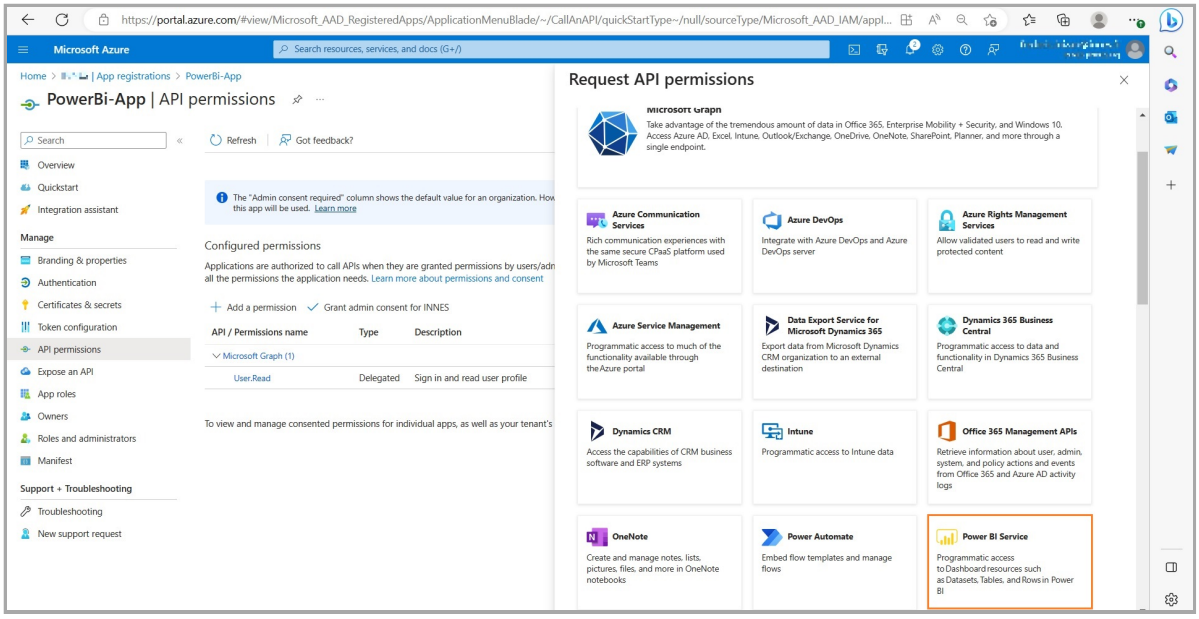
In the API permissions menu, press on the `Add` a permission button.

For *powerbi* application, these permissions must be granted:

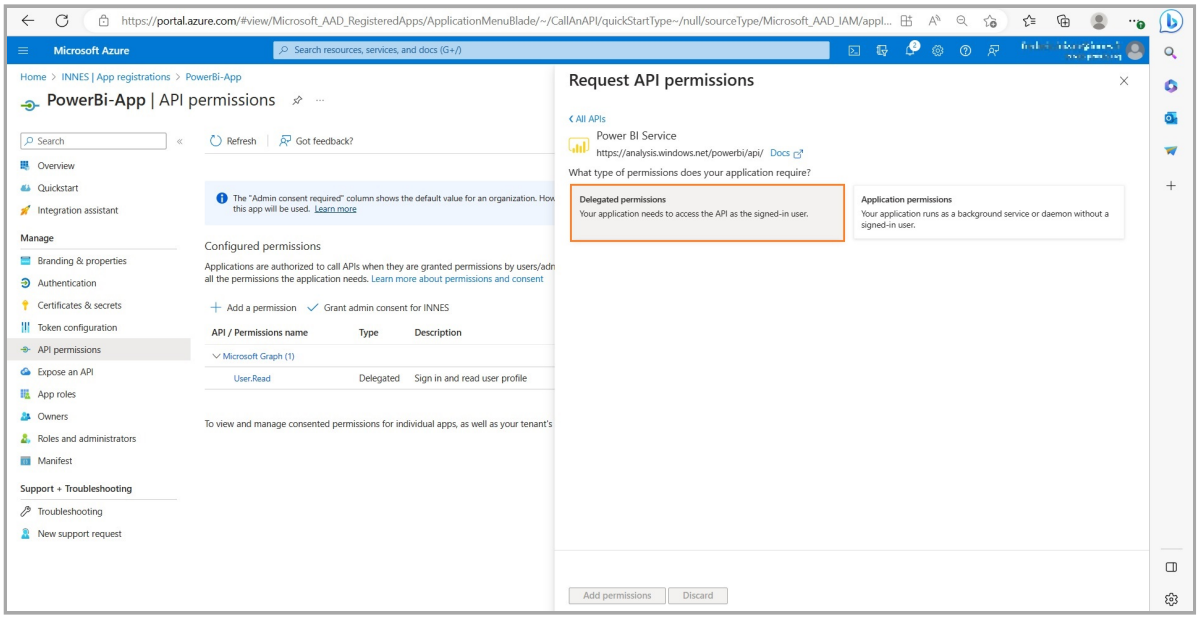
- `App.Read.All`,
- `Content.Create`,
- `Dataset.ReadWrite.All`,
- `Report.ReadWrite.All`.



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

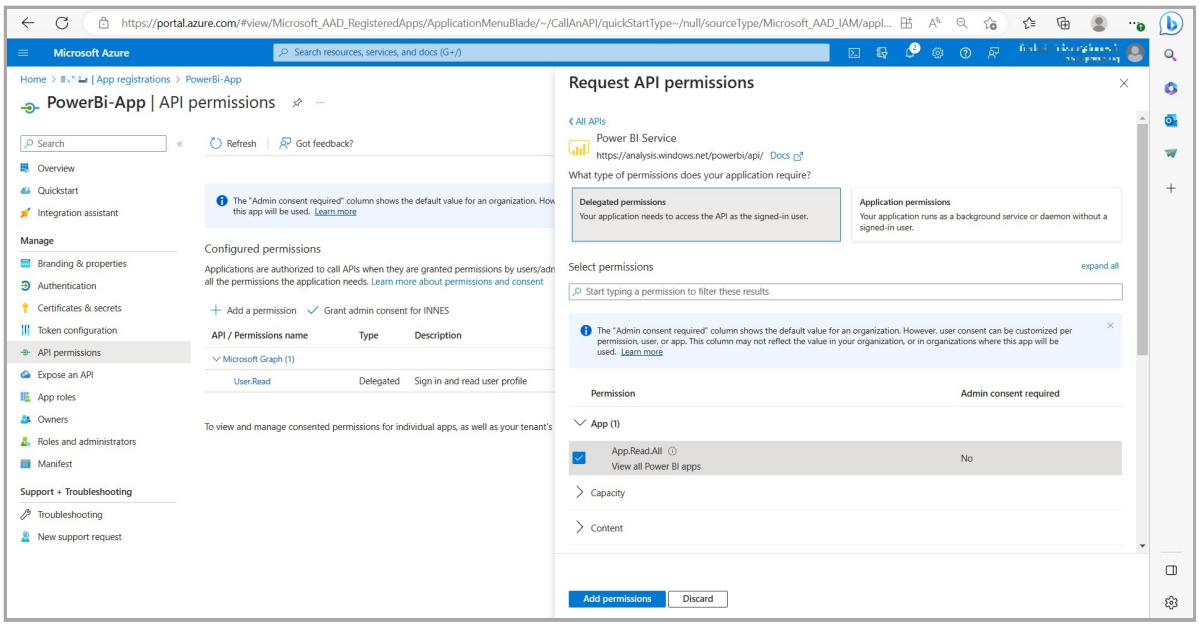


Select then the `Delegated permissions` button.

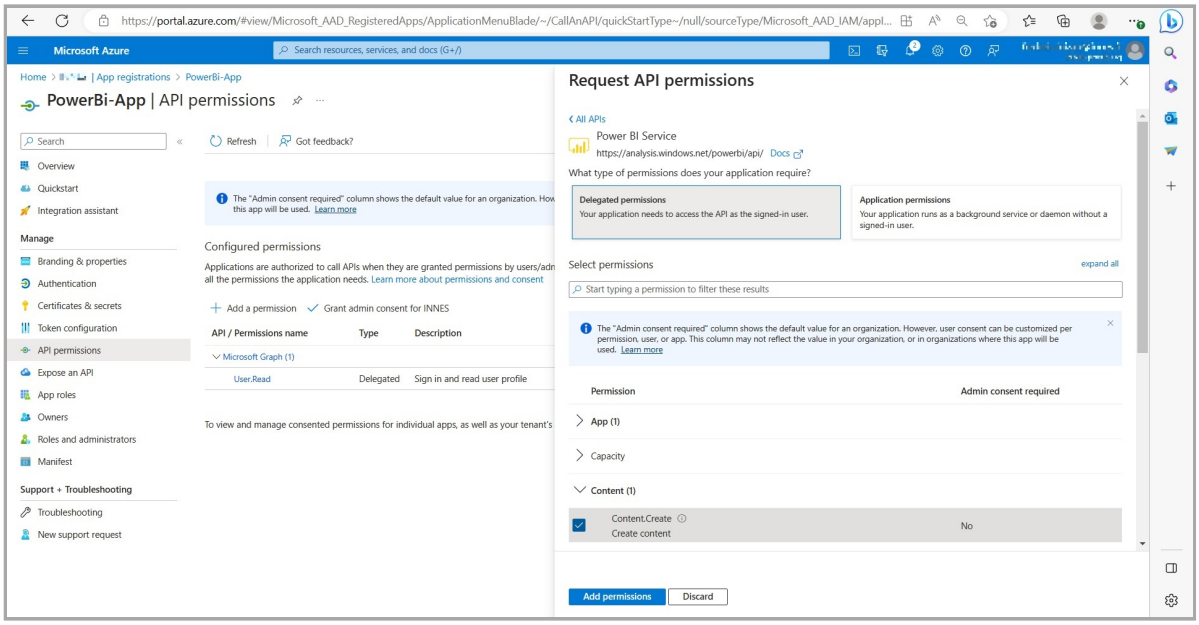


In the display filter input, enter the text *calendar* and check the option `Calendars.Read`.

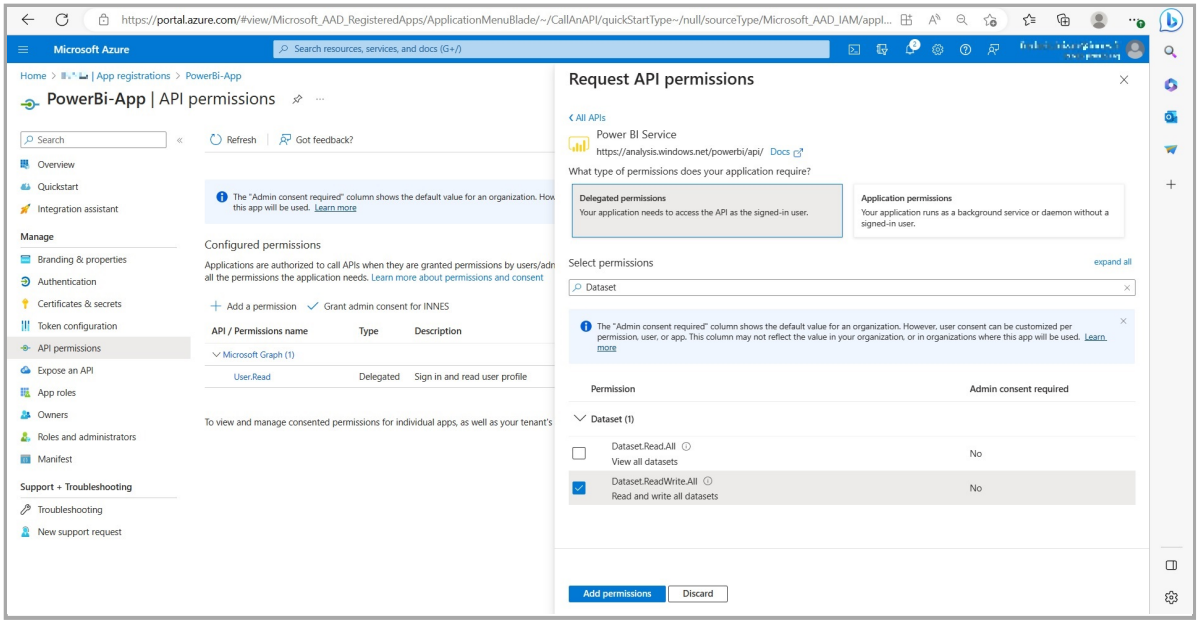
> ☛ *Do not press now on the `Add permissions` button right now.*



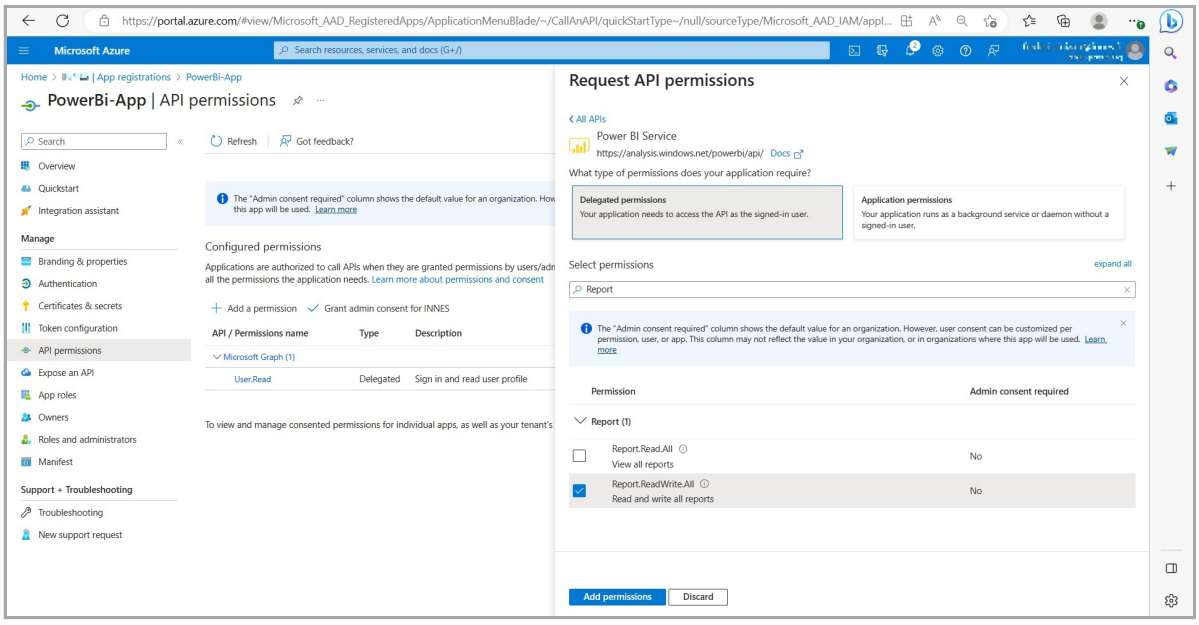
Expand the Content tab and check the `Content.Create` permission.



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

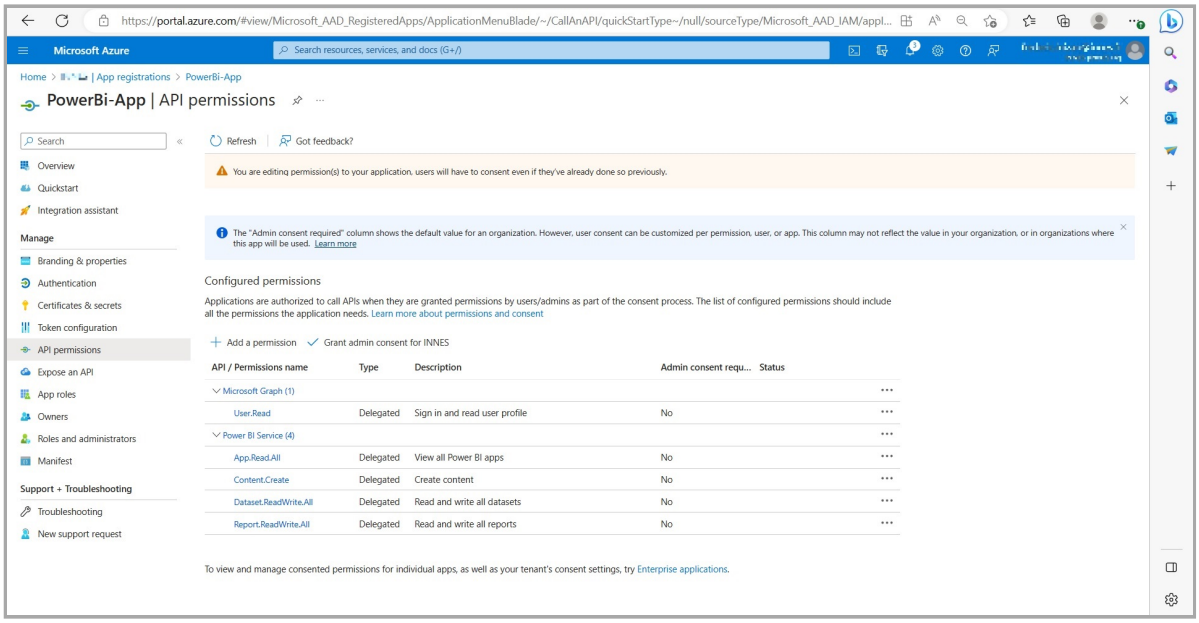


In the *Report* part, select the `Report.ReadWrite.All` option.

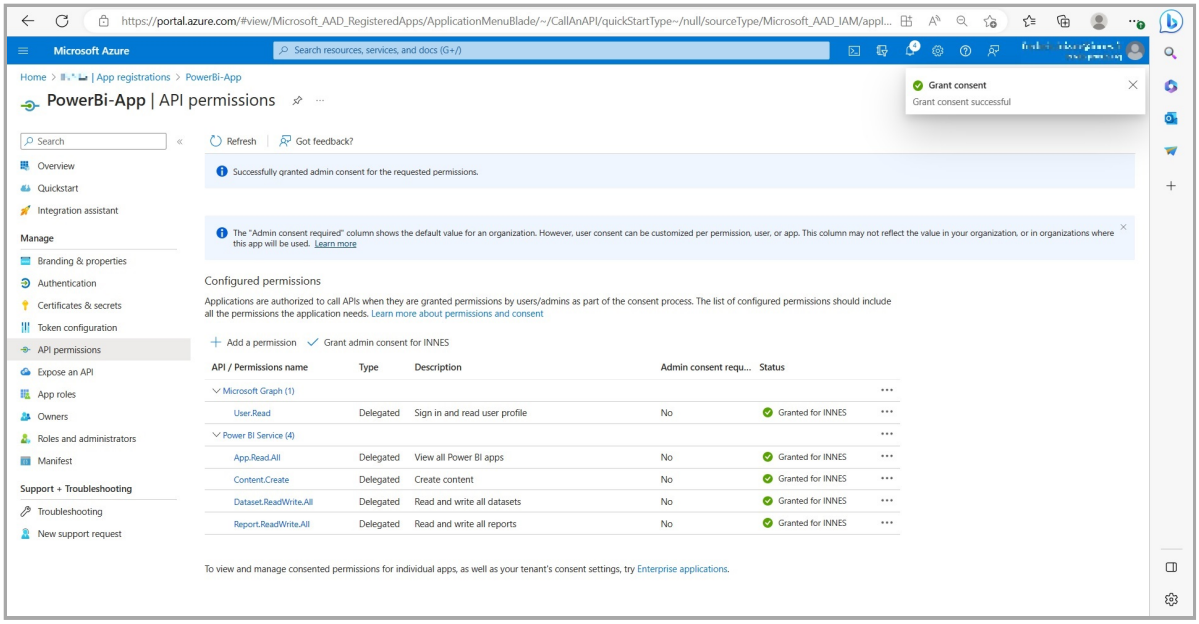


Click now on the `Add permissions` button.

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



Now the permissions are granted.



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.

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

Download the `Powershell_Innes_AAD-1.10.16.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 theses 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 \server\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         1.10.16    PSAAD
Function        Remove-AADApplication      1.10.16    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 Web sites for SignCom application
        - "url_launcher_m365" : to access to M365 Web sites 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 report

    -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                   xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

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, 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                   xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

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.

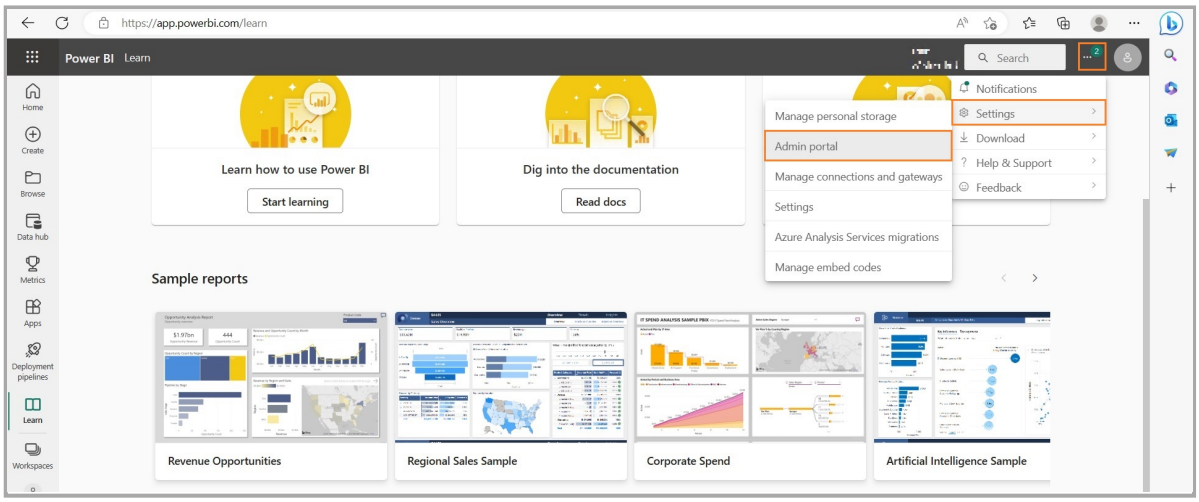
In case the values do not allow Power Bi Online viewer to work properly, check in `Microsoft Azure` portal that the application has been created succesfully and the rights are properly granted. If not, wait for a while, the rights granting may take few hours.

7.10 PowerBI Online Viewer with Microsoft OAuth application mode: additional permissions

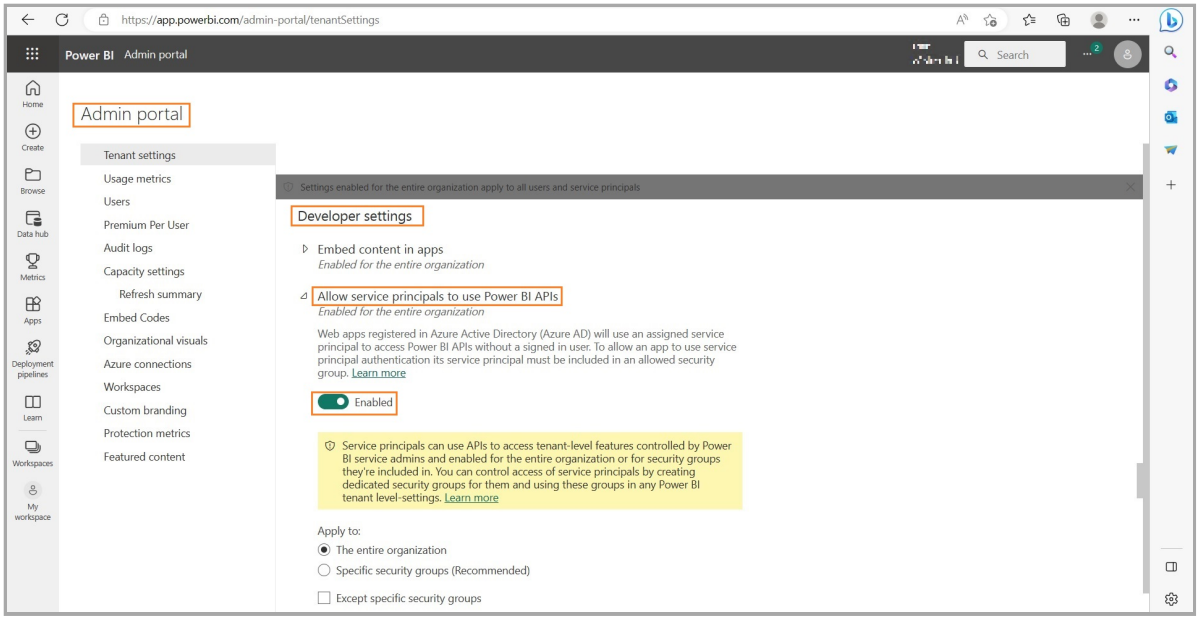
The configuration of Azure AD application does not allow to grant enough permissions to view the report when the `Microsoft OAuth application` mode is chosen. To finalize the granting of these additional permissions, follow these two steps.

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.



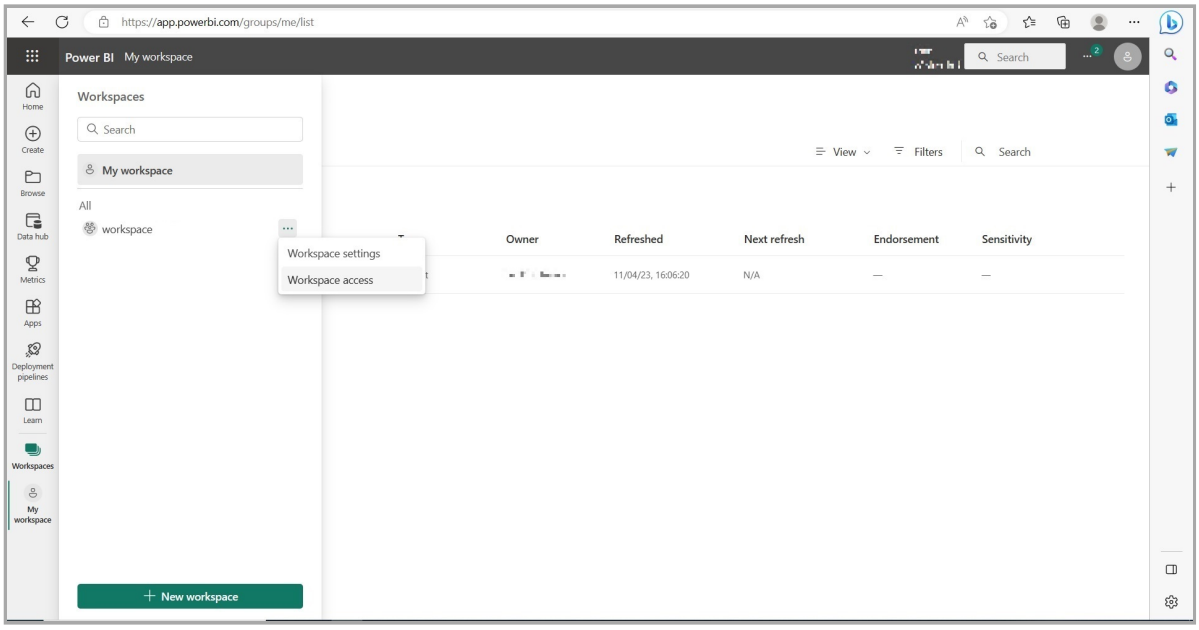
In the `Admin portal` pane, scroll to the top to find the `Developer settings` part. select `Allow service principals to use Power BI APIs`, toggle the option to the right to the *Enabled* value, check the `The entire organization` option. Click on the `Apply` button to apply the modificiation.

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

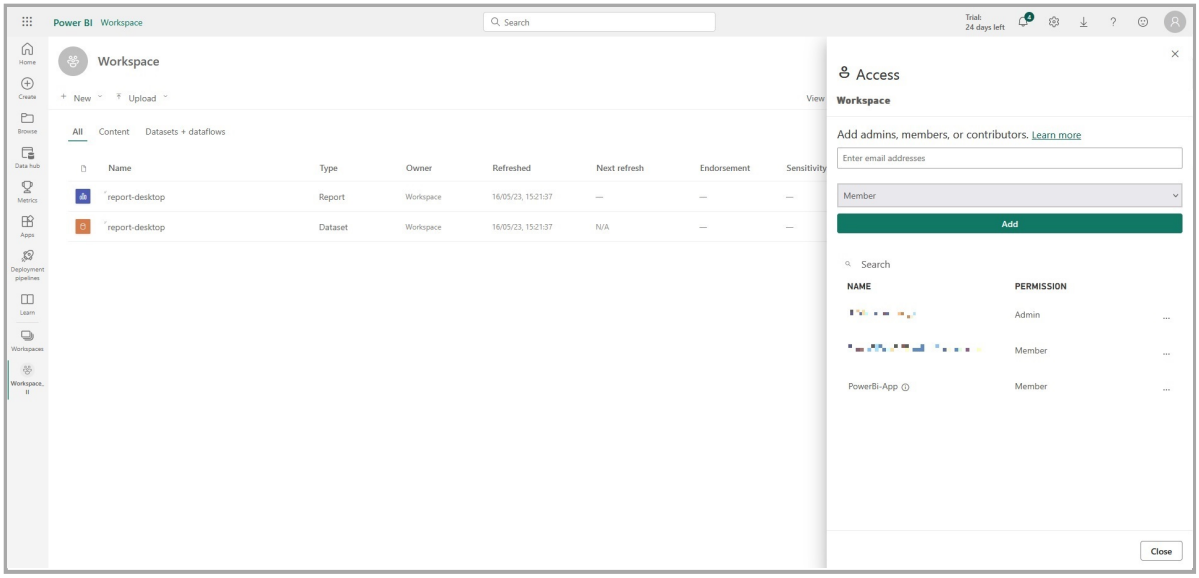
Connect to the `https://app.powerbi.com` portal with a Microsoft account having rights to modify the workspace rights.

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