CARLO GAVAZZI
Automation Components

CARLO GAVAZZI

MAIA Cloud system

MAIA Cloud system

User manual
Document revision: v. 3.0

CARLO GAVAZZI Controls SpA
via Safforze, 8
32100 Belluno (BL)
Italy
info@gavazzi-automation.com
www.gavazziautomation.com
+39 0437 355811

MAIA Cloud system

Introduction to the MAIA Cloud system

Benefits of EDGE + PaaS solution value

- **EDGE reliability**: Carlo Gavazzi UWP and EMS are the solution to separate Cloud-based services from the fieldbus. The use of a device in the middle (EDGE), it is possible to have at the same time the necessary local reliability and the leveraging effect provided by the terrific capabilities of the Cloud.
- **VPN easy to use**: the cybersecure solution allows remote user to interact with the compatible devices without common networking hassles like firewall blocks, changing public IPs and network address translation. By using a PaaS system to provide VPN access, the user does not need to install and maintain any VPN server.
- **MAIA Connect Portal**: by registering into MAIA, the user can access all the industrial-grade cloud services that Carlo Gavazzi develops as part of its product strategy.

MAIA system elements

Element	Description
MAIA Cloud	The heart of the whole infrastructure: it stores all the configuration data, the log files, the access policies, and tracks the connections to the endpoints. Any connection between MAIA Cloud and gateways or endpoints passes through the central server. *Supported browsers: latest versions of Chrome, Firefox and Safari.*
MAIA Cloud Connector plug-in	A plug-in which adds to MAIA Cloud the functions of the MAIA Cloud Connector Application. The MAIA Cloud plug-in has been designed for Windows® platforms. *Operating system requirements: Windows 7 (updated version).*
MAIA Cloud store	A dedicated page that the user can access form the main menu, which allows to install new app developed by Carlo Gavazzi, so to add functionalities to MAIA Cloud.

MAIA compatible devices

The MAIA Cloud compatible devices are:

- the UWP 4.0
- the EMS
- the UWP 3.0 Edge version **8.4.0.3 onwards**
- the XAP10RSEXX BSP version **3.1 onwards**
- the BTM family (BTM-T7-RSE, BTM-T10-RSE, BTM-T15-PLUS) BSP version **3.1 onwards**

Notes:

- MAIA Cloud allows you to access remotely also the endpoints added to the same LAN of one of the compatible devices.
- The UWP-activation key is also valid to activate the VPN service for UWP 3.0 version 8.4.0.3 backwards (see **"How to enable the VPN service for an installed UWP 3.0" on page 53**)
- To activate the VPN service for BTM Family and XAP10RSEXX BSP version 3.1 backwards you need to update the BSP on you device (click here for more info).

Ports used

Access	Port
MAIA Cloud (browser)	port 443/TCP and 1194/udp
MAIA Cloud Connector plug-in (desktop software)	port 443/TCP and 1194/udp

MAIA Cloud components

Element	Description
Node	Any object or user that is part of the MAIA Cloud architecture.
Device	Any gateway or endpoint managed by MAIA Cloud.
Gateway	A door through which MAIA Cloud can reach endpoints. This virtual network can be expanded if necessary. *The Carlo Gavazzi compatible devices are gateways.*

Element	Description
Endpoint	Any device with the following features: • It can connect via a network. • It has its own IP address (unique). *Note: the IP address is called virtual IP in the architecture and may change when the size of the network needs to be accommodated (e.g., with the addition of new endpoints to the network).* • It may connect to local network and/or to the Internet by means of a gateway • It can be connected to one gateway only. *The Carlo Gavazzi Modbus/TCP Meters and gateways TCP/IP services (such as the UWP 4.0 Web-App or the Web-API) are endpoints.*
User	Users can access and interact with MAIA Cloud, a gateway, or an endpoint according to their role. *Note: user who registers the root organization is called owner.* *The administrator defines the organization roles and assign roles to users (go to **"IAM menu" on page 30 > Roles page** for further details).*
Applications	Means to connect to an endpoint. An application specifies which software and which protocol are needed to connect. The types of application depend on the endpoint, since you can access the same endpoint in different ways (via TCP, SSH or HTTP). *You can group different applications in an application profile. Each endpoint has an application profile that defines all the available and admitted connections.*
Organization (or domain)	A collection of users, devices and applications arranged into groups. Every organization node is completely separated from, and invisible to, other organizations. *Notice: a device can belong just to one organization, and user can be added to other suborganization of the same domain.* Organizations can be arranged into a hierarchy (e.g., ***Root organization > Children > Descendants***). Within a main organization, by default users can see all the other users and devices, but not vice versa. MAIA Cloud organizations permit to perform the following tasks: • create and manage multiple domains within the same MAIA Cloud installation. • split a large enterprise into smaller departments independently managed within a single MAIA Cloud domain. • put a device or a user in the right group and give the device access to the right user. • create a suborganization invisible also to the root organization with full privacy option. *The organization structure is up to the owner of MAIA Cloud. For further details go to "What are organizations" on the facing page*
MAIA Apps	These are applications that can be activated by an administrators within their organization. MAIA Apps allow to add additional functionalities beyond the VPN (such as Fleet Management).
Resources	Users, devices, sub-organizations, month of VPN and credits are resources which composed the organization.

What are organizations

MAIA Cloud organizations are composed by:

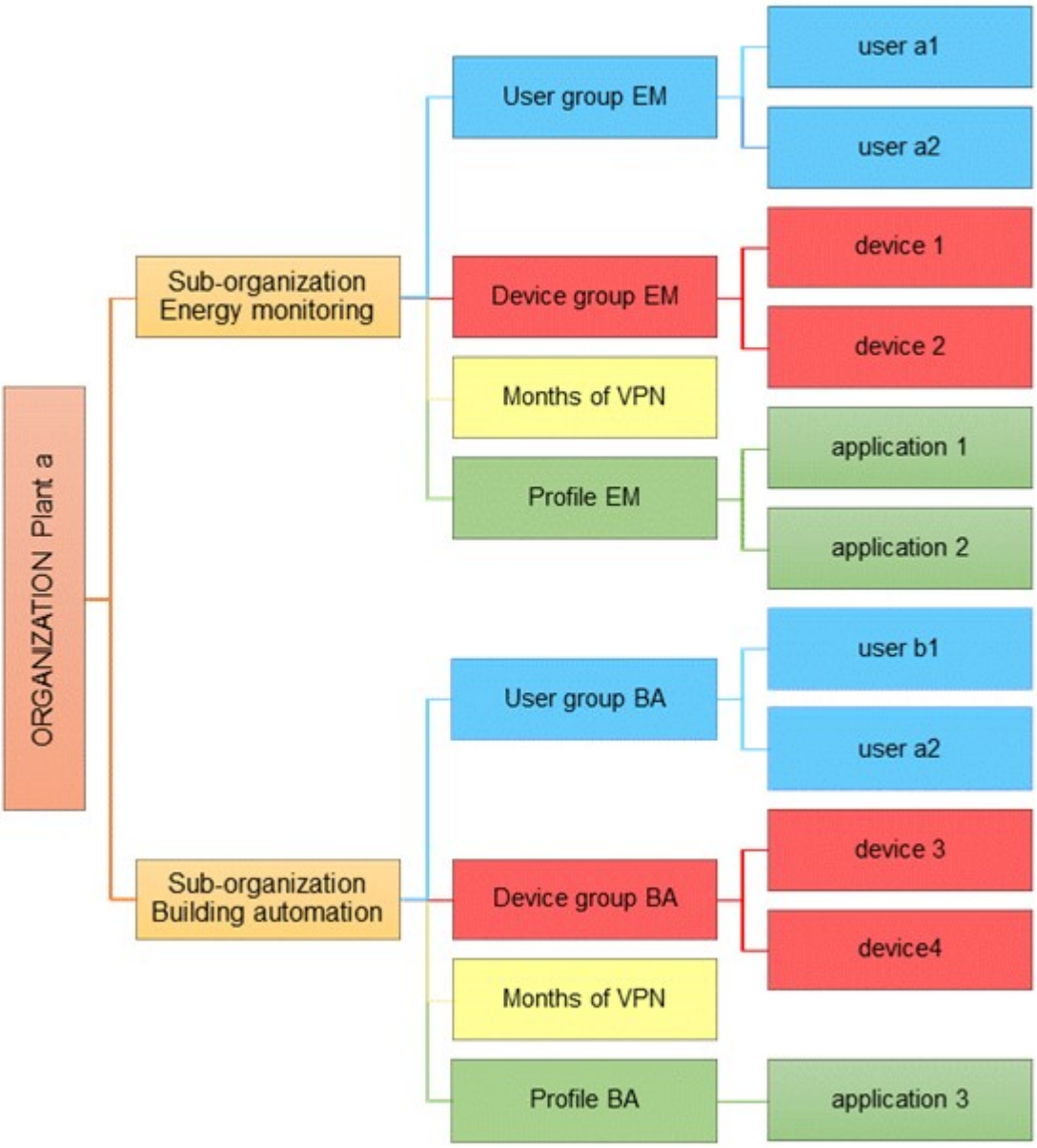
- Users that can be aggregated into user groups and connect remotely to a device through applications.
- Devices that can be aggregated into device groups.
- Applications grouped into profiles.
- Months of VPN consumed by devices
- MAIA Apps to add additional functionalities beyond the VPN
- Credits consumed by the MAIA Apps

In case of complex organizations, you can split the main organization into sub-organizations.

For further information, go to "Organization use cases" below on the facing page.

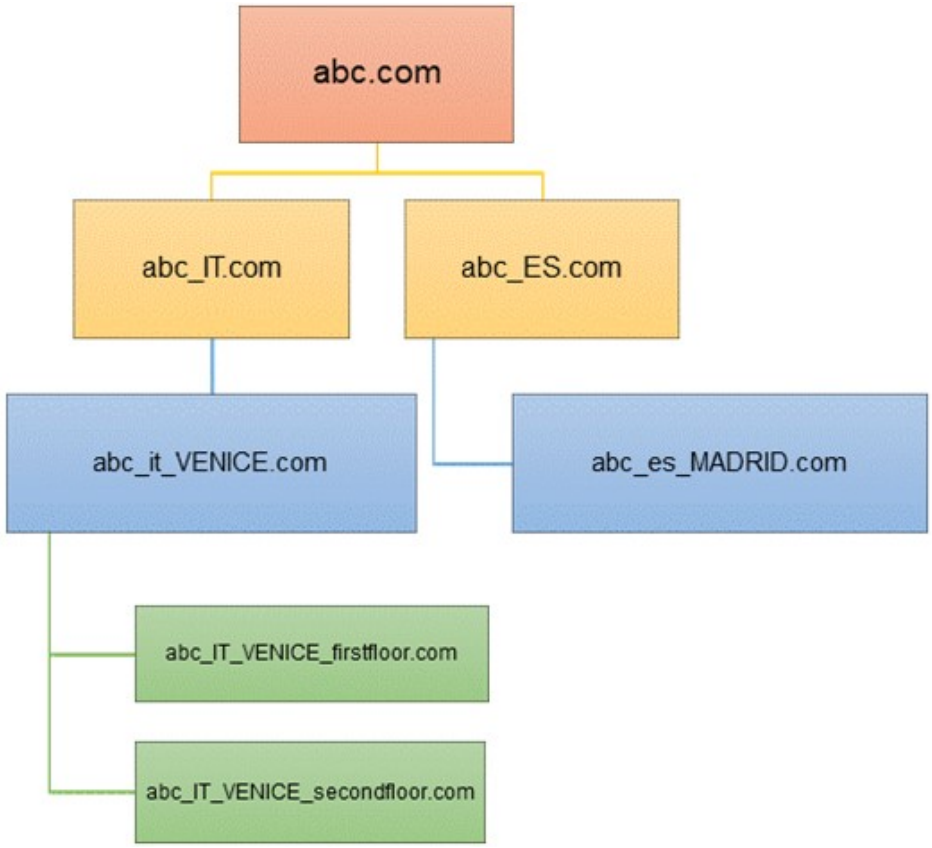
Organization use cases

1. In an office building where several meters are installed for energy monitoring and other devices are responsible for the building automation system, you should split the root organization into two sub-organizations. In this case, one sub-organization is for the energy monitoring and the other is for the building automation system.


ORGANIZATION Plant a
Sub-organization Energy monitoring
User group EM
user a1
user a2
Device group EM
device 1
device 2
Months of VPN
Profile EM
application 1
application 2
Sub-organization Building automation
User group BA
user b1
user a2
Device group BA
device 3
device4
Months of VPN
Profile BA
application 3

1. Use case 1

2. In an international retail chain called *abc.com*, with supermarkets in different Countries, every building has its system of energy-consumption monitoring.



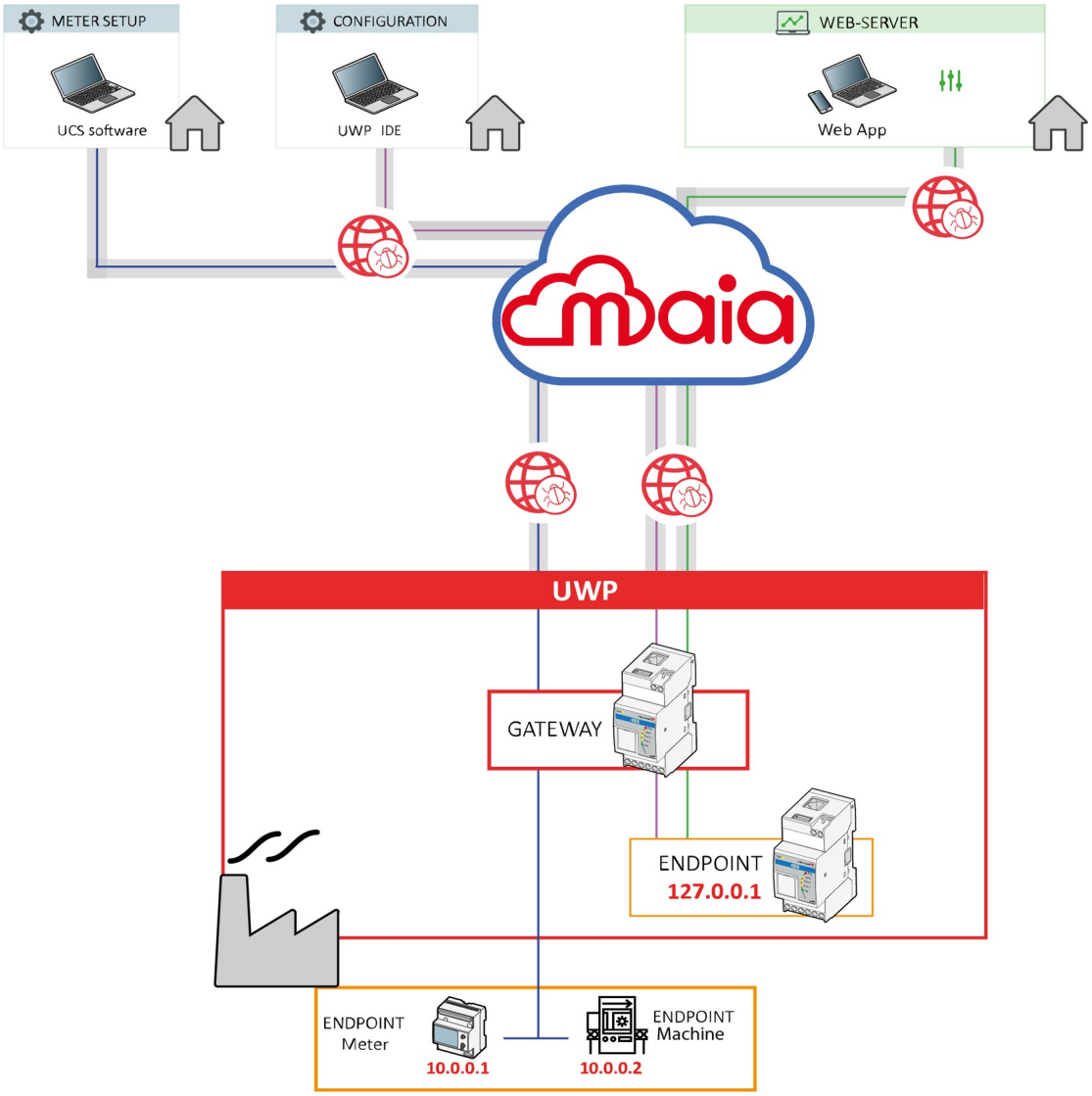
2. Use case 2

Within MAIA Cloud, every supermarket of the retail organization “hierarchy” represents a node.

> *If you want to split some buildings into different nodes, you can add other levels and create sub-organizations (for example abc_pt_porto.com, abc_pt_porto_1floor.com, abc_pt_porto_2floor.com, and so on).*

Names identifying the various sub-organizations can help the MAIA Cloud manager users: this organization hierarchy structure, in fact, reduces the chance to put devices or users in the wrong group and allows only the responsible users to access the device.

MAIA for energy monitoring and building automation



UWP and EMS are the gateways that, in a remote connection, act as end-points providing the IP address of the local host.

Following are the applications that permit a remote connection and that are compatible with the relevant controller:

- UWP 3.0 Tool/UWP 4.0 IDE, configuration software.
- UWP and EMS Web App, for viewing / exporting of data, controlling the automation functions and defining settings.
- With UWP, you can use UCS software and its modbus bridge functionality to configure or monitor the Carlo Gavazzi meters.

Is possible to access remotely also the endpoints added to the same LAN of any MAIA Cloud compatible device.

Access types

You can access our MAIA Cloud system unsing a PC or a smart-phone through the **MAIA Connect web portal** (https://app.maiaconnect.com).

You need to install and login also the MAIA Cloud Connector Plugin to set up a remote connection using a native application installed in your PC, such as UWP 4.0 IDE software or UCS software.

		Any web browser-enabled device	PC (Windows® platforms)
Perform the first login		V	V
Register into MAIA Cloud		V	V
Manage personal account		V	V
Activate devices		V	V
Manage organizations		V	V
Manage and use MAIA Apps		V	V
VPN Remote access	**built-in applications**	V	V
	native applications	X	V

MAIA Cloud licence types

MAIA Cloud services are based on licences: the ACTIVATION-KEY, the STANDARD LICENCE and the PLUS LICENCE code.

The UWP-ACTIVATION-KEY allows user to register on MAIA Cloud activate a device.

*For further details, go to **Activation code** below.*

The STANDARD and PLUS LICENCES allow user to add resources to the organization.

*For further details, go to **Standard licence and Plus licence** below.*

Activation code

The activation code is included in our UWP-ACTIVATION-KEY kit and allows user to:

- sign up for MAIA Cloud and create an organization

*For further information, go to **"MAIA Cloud licence types" above** > **How to register and create an organization**.*

- activate the device to a MAIA Cloud organization

*After the registration, the organization is created with a STANDARD LICENCE that will automatically renewed yearly. Go to **How to register and create an organization for further details** (below).*

Notes:

- *The activation code can be use once.*
- *If you use the activation code to register your organization on MAIA Cloud, you can use the same key to activate a supported device.*
- *The ACTIVATION KEY is included in the UWP and EMS package.*
- *For further information about the supported devices go to **"MAIA compatible devices" on page 6**.*

Licence

Standard licence

Standard licence allows you to add up to 50 users, 50 devices and 50 sub-organizations.

After the registration (go to How to register and create an organization for further details below), the organization is created with a Standard licence.

If you need to scale up your standard licence, please referred to your Carlo Gavazzi sales representative.

Plus licence

Plus licences are composed by resources for consumptions:

- UWP-LICENCE-MxxB allows you to add VPN months. These licences expired after 1 year.
- UWP-LICENCE-C300 allows you to add 300 Credits. These licences expired after 3 years.

Notes:

- You can combine Plus licences.
- When a Plus licence expires, unused resources expire too.
- If you need to scale up your plus licence, please referred to your Carlo Gavazzi sales representative.

Licence type	Carlo Gavazzi code	Licence Composition
Plus	UWP-LICENCE-M01B	12 VPN months
Plus	UWP-LICENCE-M02B	24 VPN months
Plus	UWP-LICENCE-M04B	48 VPN months
Plus	UWP-LICENCE-M05B	60 VPN months
Plus	UWP-LICENCE-M25B	300 VPN months
Plus	UWP-LICENCE-C300	300 Credits

Enabling VPN service for a device (for further details, go to ***"Devices menu" on page 19 > VPN page > Devices***), one month of VPN is spent, and the service is automatically renewed at the end of the month. Users with specific roles are allowed to manage VPN service (for further information, go to ***"Devices menu" on page 19 > VPN page***).

Enabling a MAIA App (see the "Applications menu" on page 41 for more details) requires credits. Once activated, the corresponding amount will be automatically deducted from the credits resources of your organization, based on the applicable payment plan.

How to register and create an organization

1. Open your browser
2. Go to MAIA Cloud login page: *https://app.maiaconnect.com*
3. Click **Register** under the **Log In** button
4. Enter the following data:
   - First name
   - Last name
   - Organization Label

     Note: this is the description of your Organization, useful to identify it. You can choose your Company or your project name. You can modify it later on.

   - Organization ID

     Note: this is your unique Organization identifier name, useful for technical support. It cannot be changed later on. Special characters are not allowed.

   - Country
   - Valid UWP-ACTIVATION-KEY for Registration. Write the Carlo Gavazzi activation code included in your UWP-ACTIVATION-KEY.

- E-mail and E-mail confirmation
- Password and Password confirmation

5. Read and accept the **Privacy policy and Terms of Use**
6. Click **Register**
7. Click the link included in the mail you received to enable your profile
8. Log in with your credential to the MAIA Cloud web portal.

Notes:

- *After the registration, the organization is created with a STANDARD licence (composed by 50 user, 50 device, 50 organization and 1 month of VPN).*
- *For further details about licences, go to MAIA Cloud licence types*
- *If you need more info about how to add licences go to How to > IAM menu > Organizations > Resources > How to add resources to a root organization.*

How to check your organization resources

Click the first arrow in the navigation bar or go to ***IAM > Organizations***.

For further details, go to "IAM menu" on page 30 > Organizations page.

MAIA Cloud browser

How to log in through a browser

1. Use a web browser to access MAIA Cloud (link https://app.maiaconnect.com/)
2. Enter the credentials

   Click to modify your credentials.
3. Click **Sign in**.
4. Create a new password and click submit

   Only for the first login.
5. Read and accept **Terms and Conditions** and **Privacy Policy** and click **continue**

   *Only for the first login or if **Terms and Conditions** and/or **Privacy Policy** have been updated.*

The MAIA Cloud browser allows you to perform the following tasks:

- configure the entire environment (**Organizations**, **Users**, **Devices** and **Applications**)
- monitor the endpoints through the **Dashboard** page and manage organization resources
- access devices through the built-in applications (such as SSH, HTTP, HTTPS).

Moreover, if you access the browser with the **MAIA Cloud Connector plug-in** installed (see ***"Devices menu" on page 19 > VPN page > Devices > The MAIA Cloud Connector plug-in***), you can:

- access devices also through native application (e.g. UCS).
- use the remote devices through an IP address as if they were connected to the local network.

Home page

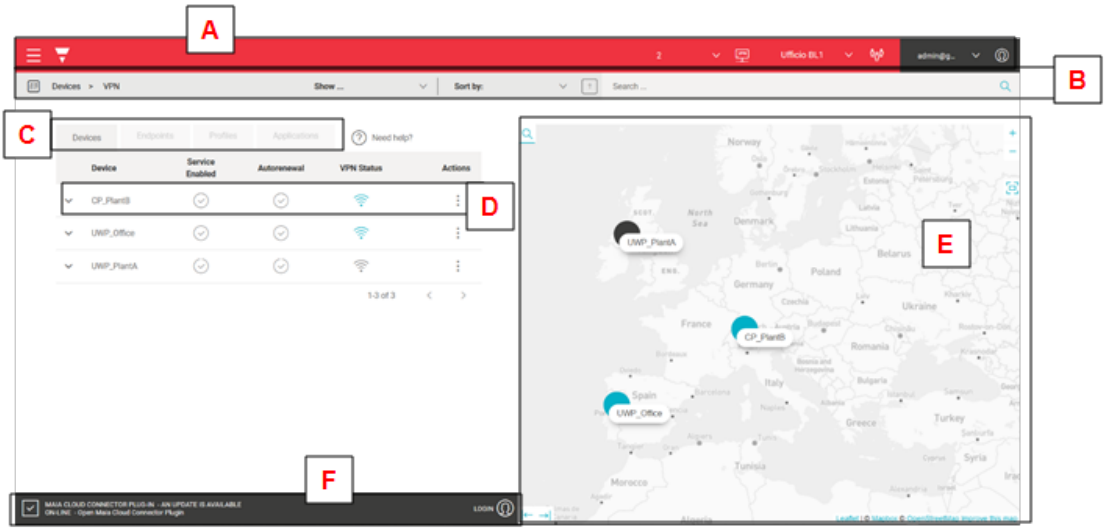
The home page is composed by the following elements:

- Navigation bar
- Secondary navigation bar
- Devices, Endpoint, Profile and Applications tabs
- Connection map

Note: the home page and the VPN page are the same.

Users with the direct access to the favourite application roles, from the Home Page only see the favourite applications.

*For more information, go to **"How to" on page 47 > IAM menu > Roles> Application roles >How to set up a direct access to favourite applications**.*



Element	Description
A	Navigation bar, common to all the MAIA Cloud pages. It contains the following options: • ☰ opens the main menu *For further details, go to "Main menu" on the next pageon the facing page.* • opens your organization resources details • 👥 represents your organization. If you click it, you can change the organization and the pages update according the selection • 👤 accesses your account details and options *For further information, go to **"Home page" on the previous page > How to manage the profile***
B	Secondary navigation bar. You can perform the following tasks: • Filter the devices choosing the status (**Show…**) • **Sort by** name the items in the list • **Search** an item. • Add another filter
C	**Devices**, **Endpoint**, **Profile** and **Applications** tabs. *For further information, go to **"Devices menu" on page 19**.*
D	The connection drop-down menu allows you to manage the devices VPN connection. *For further information, go to **"Devices menu" on page 19 > VPN page > Devices > The Connection drop-down menu and side panel**.*

Element	Description
E	The connection map showing the location of your devices. You can perform the following tasks: • Open the device action menu clicking on the relevant device *For further information, go to **"Devices menu" on page 19 > VPN page > Devices**.* • Enter a connection address (🔍) • Zoom in or out with **+** or **-** • Zoom all with ⛶ to see all the devices in the map *When you type an address, the map enlarges on the selected connection place.*
F	**MAIA Cloud Connector Plug-in** status bar allows you to manage the plug-in connection. *For further information, go to **"Devices menu" on page 19 > VPN page > Devices > The Connection drop-down menu and side panel**.*

How to manage the profile

1. Go to the MAIA Cloud browser main tab
2. Click 👤 from the navigation bar
3. Open the **Profile** menu
4. Manage the following tabs:
   - **Account**. You can change the following options:
     - Email
     - First name
     - Last name
   - **Password**. You can change the password.
   - **Authenticator**. You can improve the security of your profile.
   - **Session**. It gives you information about your MAIA Cloud session and allows you to log out.
5. From the **Authenticator** tab, download one of the suggested applications for your mobile phone, and follow the procedure.
   *This way, at the login you add a one-time code, provided by an application installed directly on your mobile phone. If you want to disable this function, go to the **Authenticator** tab and click* .

Main menu

From the **Main menu** you can manage your organization.
The following elements compose the main menu:

- Dashboard. It allows you to go back to the home page and to access the favourites page.
- Devices menu. It allows you to manage your gateways, endpoints, applications and profiles. It contains the following sub-menus:
  - Activate. It allows you to activate and add a device to your organization.
  - Manage. It allows you to manage devices and create or modify devices group.

    - VPN. It allows you to check and manage your devices connection status, manage and add endpoints, and set your remote connection up adding and managing applications and profiles.

- IAM menu. It allows you to manage your organization resources, users and users' roles.

  It contains the following sub-menus:

    - **Organizations**. It permits you to manage your organization and add sub-organizations, arrange your resources and monitoring the consumptions.
    - **Users**. It permits you to add or modify users and user groups.
    - **Roles**. It permits you to give users' custom roles, create or modify roles.
    - **MAIA Apps**. It allows you to access the app Store and the MAIA Apps that has been activated into the relevant organization

- Audit menu. It shows your organization's logs list.
- User manual. It opens the MAIA Cloud user manual.

*Note: if you select a sub-menu, you open the relevant **Options** page.*

Devices menu

This tab permits you to manage your gateways, endpoints, applications and profiles and contains the following three sub-menus:

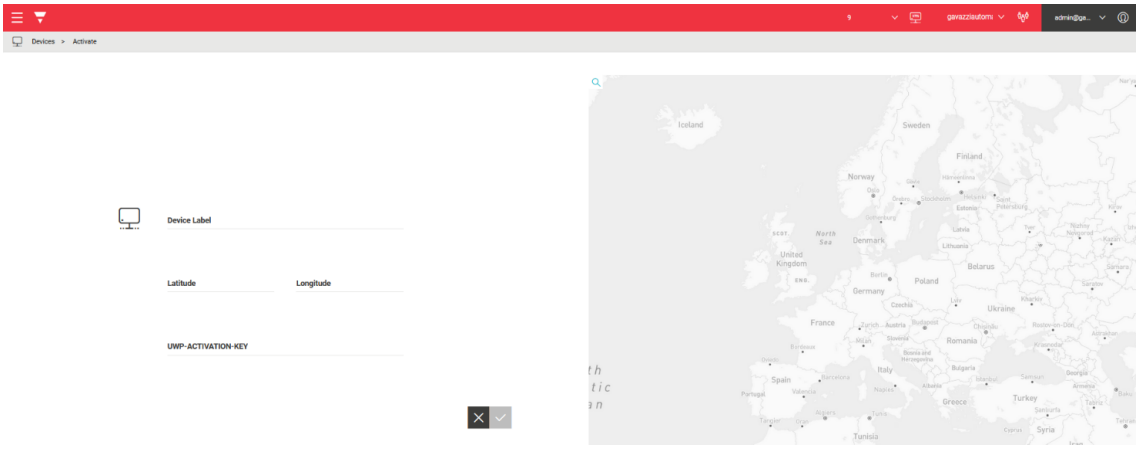
- **Activate**.
- **Manage**.
- **VPN**.

Activation page

Devices > Activate

From this page you can activate your devices and add them to your organization. You can change the organization from the top bar clicking .

*Notice: the Carlo Gavazzi **activation key** is mandatory to activate a device.*



Manage page

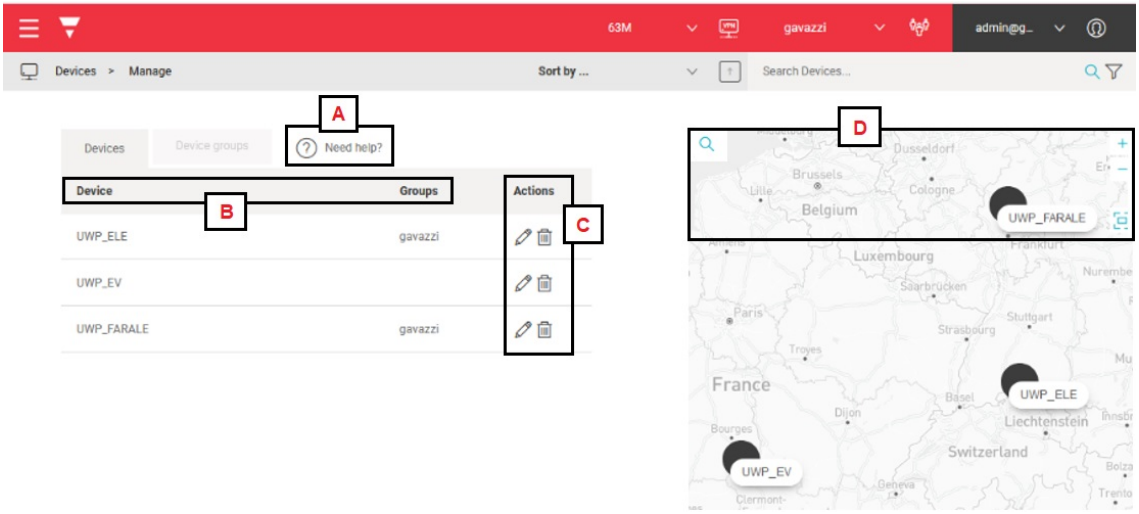
Devices > Manage page

This page allows you to manage devices and create or modify devices group.

Two tabs compose it: **"Devices menu > Manage page > Devices" below** and **"Devices menu > Manage page > Device groups" on the next page**.

*You can change your reference organization clicking from the navigation bar. The **Manage** page is updated according to the selected organization.*

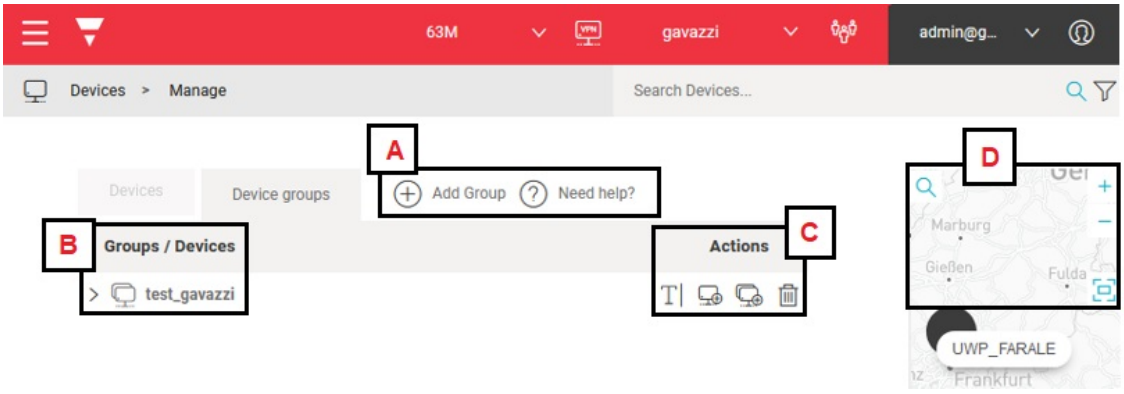
Devices menu > Manage page > Devices



Element	Description
A	Hide/Show map ? Need help: opens the context help.
B	Devices information: device label and device Group. *For further information, go to **"How to" on page 47 > Devices menu > Manage > Device groups > How to add a device group.***
C	⋮ Actions. You can edit (✎) the device information, delete (🗑) a device or move a device clicking ⋮ (for more info see **"How to move a device to another organization" on page 47**). The edit button allows you to perform the following tasks: • See the device information, such as: ◦ Label of the device, set during the activation procedure. *Note: if you want to change the device label is necessary to reset the VPN service.* ◦ ID, useful for the technical support team ◦ Activation code ◦ Description (this field is optional) ◦ Serial Number (this field is optional) • Add the device in an existing **Device Group** (**Add**) • Change the location ( )

Element	Description
D	The connection **map** showing the location of your devices. You can perform the following tasks: • Enter a connection address (🔍) • Zoom in or out (+ or —) • Zoom all (⛶) to see all the devices in the map *When you choose an address, the map enlarges on the selected area.*

Devices menu > Manage page > Device groups



Element	Description
A	+ Add Group. *For further information, go to **"How to" on page 47 > Devices menu > Manage > Device groups > How to add a device group.*** ? Need help: opens the context help.
B	Groups / Devices name. If you click > you can see the group members.
C	Actions. You can perform the following tasks:. • Rename • Add device: allows you to add device into an existing group • Add group: this tab allows you to create a group into an existing group • Delete *For further information, go to **"How to" on page 47 > Devices menu > Manage > Device groups > How to add a device group.***
D	The connection **map** showing the location of your devices. You can perform the following tasks: • Enter a connection address (🔍) • Zoom in or out (+ or —) • Zoom all (⛶) to see all the devices in the map *When you choose an address, the map enlarges on the selected area.*

VPN page

Devices > VPN page

This page allows you to perform the following tasks:

- check and manage your devices connection status.
- manage and add endpoints.
- set up your remote connection adding and managing applications and profiles.

The VPN page is composed by the following four tabs:

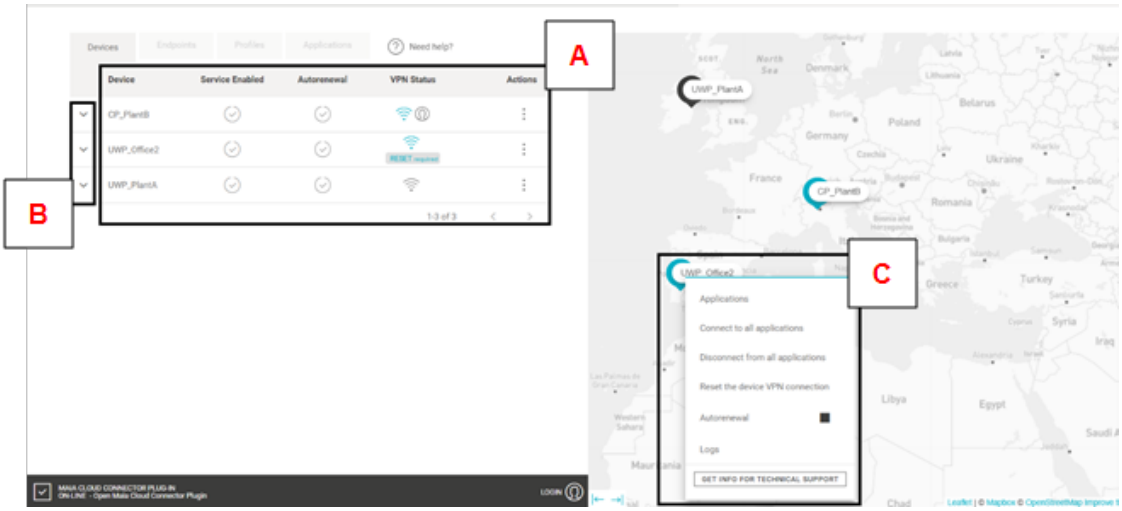
- Devices
- Endpoints
- Profiles
- Applications.

Note: you can change your reference organization clicking from the navigation bar. The VPN page is updated according to the selected organization.

Devices menu > VPN page > Devices

This tab shows the list of all the devices (gateways and endpoints) of your organization and permits you to perform the following tasks:

- View the devices location on a map
- Check the device VPN status
- Connect through VPN to the devices
- Enable/disable the VPN autorenewal
- Assign VPN credits to a device
- Access the device's Logs



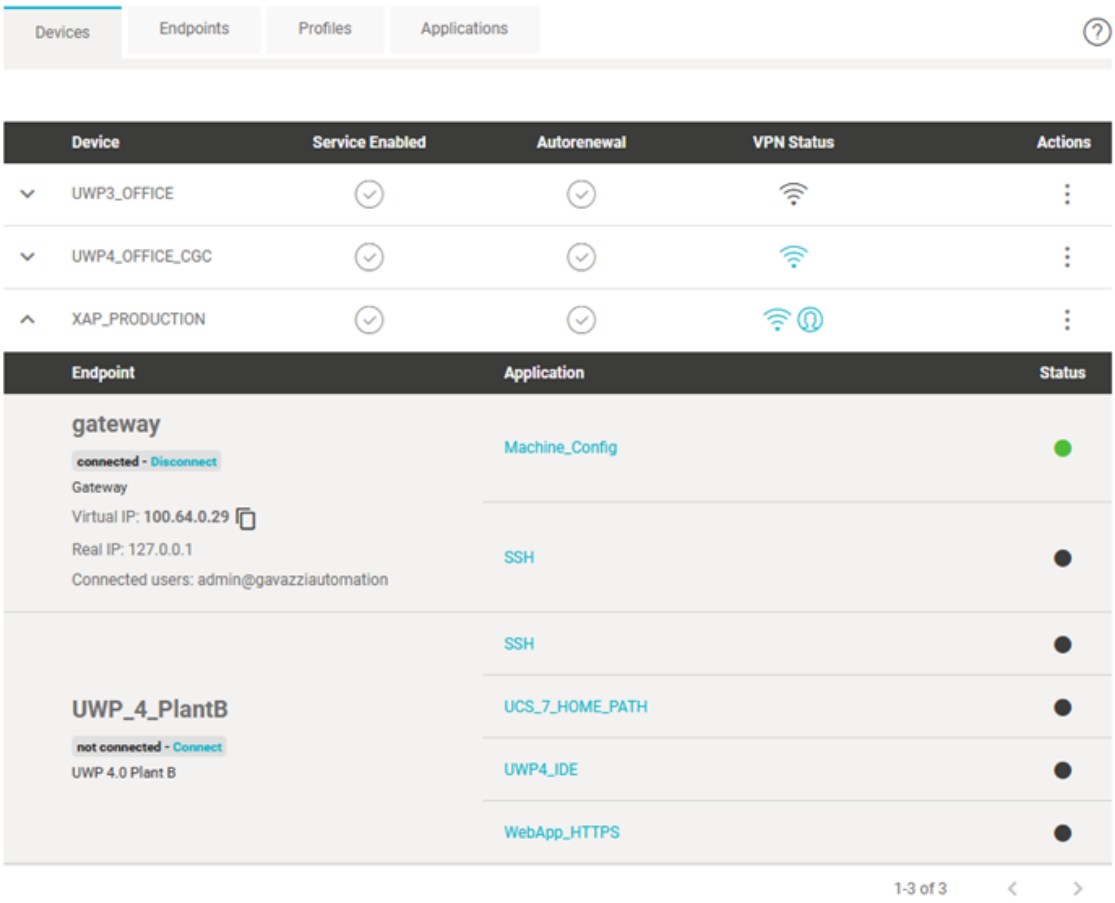
Element	Description
A	Device's information in the grid: • Device name. • Service enabled (✓). If you see this icon ○, it means that the service is disabled and you have to assign credits to enable the service from the **Actions** menu. • Auto-renewal (✓). If you see this icon ○, it means that the VPN auto-renewal is disabled. You can enabled it from the **Actions** menu. • VPN status. ◦ This icon means that the device is available and that you can connect to it through VPN. ◦ This icon is blinking, means that the device has tried to connect in the last 15 minutes. Following are the possible reasons of this condition: • You run out months of VPN resources. • No month of VPN has been assigned to the device. ◦ This icon means that the device is disconnected, and you cannot connect to it through VPN. Following are the possible reasons of this condition: • No internet connection. • No months of VPN. • VPN service disabled. • Wrong activation key. • Wrong DNS or network gateway settings. ◦ This icon means that another user is connected to this device. *Note: more users can access the device at the same time. We recommend connecting remotely only to one user at time, in order to avoid interferences while someone's working.* • **Actions**. You can access the action menu in ***Devices > VPN > Devices tab***, clicking: • ⋮ from the **Actions** column • a device in the **Connection** map • ⋮ from the **Connection** side-panel This menu allows you to perform the following tasks: ◦ **Connect**. Opens all the ports of the application which composed the device's and endpoint's profile. ◦ **Disconnect**. Logs out from all the application and closes the VPN connection. ◦ **Reset the device VPN connection**. Reboots the VPN service (not the device). ◦ **Auto-renewal**. Enables/disables the VPN service auto-renewal. ◦ **Assign credits**. After the activation or if a month of VPN resource is over, you need to assign a VPN resource to the relevant device. ◦ **Logs**. Accesses the device logs ◦ **Get info for technical support**. Downloads a .json file useful for technical support.

Element	Description
B	Click ⌄ you open the Connection drop down-menu which allows you to manage the VPN connection. *For further information, go to **"The Connection drop-down menu and side-panel" below***
C	Connection map. If you select a device and then click **Applications**, you will open the **Connection** drop down-menu which allows you to manage the VPN connection. *For further information, go to **"The Connection drop-down menu and side-panel" below***
D	MAIA Cloud Connector plug-in status bar: allows you to check and manage the plug-in connection status. *For further information, go to **"The MAIA Cloud Connector plug-in" on the next page***

The Connection drop-down menu and side-panel

You can open the **Connection** drop-down menu:

- from ***Devices > VPN > Devices*** tab clicking ⌄
- from the **Connection** map, clicking a device and then **Applications**.



The **Connection** drop-down menu and the **Connection** side-panel have the same functionalities. These menus allow you to:

- Read the real and the virtual IPs of the gateway and the endpoints (only when the VPN connection has been established)
- Set up a VPN connection using a specific application clicking one of the available applications

- See if an application is a native application or a built-in application. If you see Native app pop up means that to use that application, you need to be logged in with MAIA Cloud connector plug-in
- Check the VPN status of the relevant application (if green means that you are connected to this application, if it is black means that you are not connected)

Note: each device activated in MAIA is considered an endpoint called gateway and its IP address is the local host. This endpoint is automatically created as soon as you activate the device.

The MAIA Cloud Connector plug-in

You can download the MAIA Cloud Connector plug-in directly from the status bar of the MAIA Cloud browser homepage.

The **MAIA Cloud Connector plug-in** is a desktop application that allows you to access devices through native application (e.g., UWP or UCS Software) and use the remote devices through the virtual IP address as if they were connected to the local network.

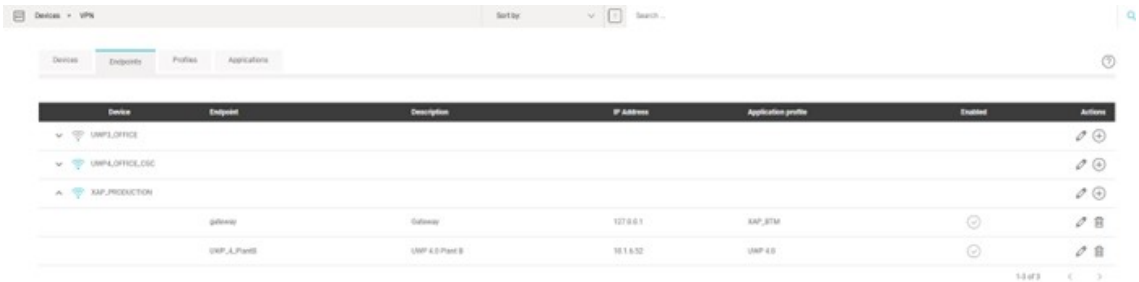
The **MAIA Cloud Connector plug-in** status bar in the MAIA Cloud browser home page allows you to check and manage the plug-in status.

Note: before login you can choose the VPN protocol (TCP or UDP)

If the bar is...	Then it means that...
Red	the application is not working or you need to launch the MAIA Cloud plug-in. It can be because you have not the plug-in installed (click ↓ to download the plug-in and follow the wizard) or because you have not launched the MAIA Cloud plug-in.
Black	you are not connected. Click 👤 to connect and click **Open MAIA Cloud Connector plug-in** to launch it. *Note: opening the app, you can access the app logs and change the path of the native applications.*
Blue	you are connected and you can see the connected users. Click 👤 to connect and click **Open MAIA Cloud Connector plug-in** to launch it. *Note: opening the app you can access the app logs and change the path of the native applications.*

Devices menu > VPN page > Endpoints

This tab allows you to manage and add endpoints to your devices.



Element	Description
A	Endpoints tab information: • the coloured icon means that the device is available and that you can connect to it through VPN • Device name • if you click it, you see the endpoints and the relevant information: ◦ Endpoint name ◦ Endpoint description ◦ Endpoint IP address *Note: each device activated using an UWP-ACTIVATION-KEY is considered an endpoint called gateway and its IP address is the local host. This endpoint is automatically created when you activate the device* ◦ Application profile assigned to the endpoint. *For further information, go to **"How to" on page 47 > Devices menu > VPN > Profiles > How to associate a profile to an endpoint**.* ◦ Enabled. If the endpoint has been correctly added and activated, it appears checked.
B	Actions. It permits you to perform the following tasks: • Edit gateway ( ). You can: ◦ Check the Do not translate real IPs into virtual IPs option to maintain the real IP used in the local network even if reached through the VPN. *Note: when a device is connected to the MAIA Cloud server, by default it gets a virtual IP address. It may be necessary for the device to maintain the real IP used in the local network even if reached through the VPN. In these use cases you can select Do not translate real IPs into virtual IPs option.* ◦ Set the Maximum number of endpoints available for the relevant gateway. *Note: 2 is the default value.* • Create an endpoint ( ). Click it to open the Endpoint Options menu. *For further information, go to How to add an endpoint.* Click ( ) to see the **Endpoints Actions** which allow you to edit ( ) or delete ( ) an endpoint.

Devices menu > VPN page > Profiles

This tab of the VPN page allows you to manage and add profiles.

Some default profiles are available and the following application compose them:

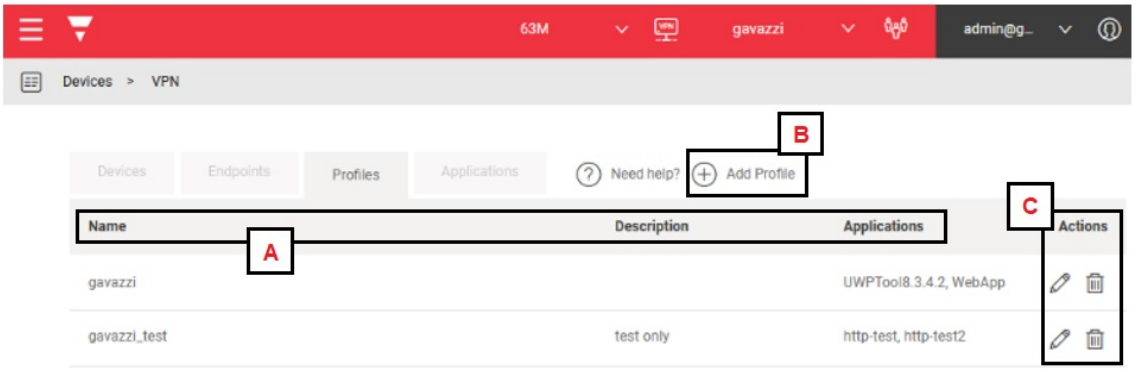
Default profile	Default applications
UWP 3.0_Default_profile	• UCS 7 Software • UWP Tool • UWP Web App • SSH remote support (only for Carlo Gavazzi Support Team).
EMS Default profile	EMS Web App SSH remote support (only for Carlo Gavazzi Support Team).
UWP 4.0_Default_profile	• UCS 7 Software • UWP IDE • UWP Web App • SSH remote support (only for Carlo Gavazzi Support Team).
BTM-XAP Default profile	• BTM XAP Web Server • System Settings

The default profiles are ready to use, just add the profile to your devices.

*For further information, go to **Devices menu > VPN > Profiles > How to associate a profile to an endpoint for further details.***

If you don't have default profile in your list you can create it following these steps:

- Create the default applications following the application settings you can find here
  *For further information, go to **"How to add an application" on page 58***
- Create the default profile adding the default applications you need.
  *For further information, go to **"How to create a profile" on page 57***



Element	Description
A	**Profiles** information: • **Profile name** • **Profile description** • **Applications composing the profile.** *For further information, go to "Devices menu > VPN page > Applications" on the facing page.*

Element	Description
B	Profiles actions. Click **+ Add Profile** to open the profile **Options** menu. *For further information, go to **Devices menu > VPN > Profiles > How to create a profile.***
C	**Actions**. You can change the profile name and/or description and add/delete the applications composing the profile ( ) or delete the profile ( ). *Note: if you delete a profile, the relevant applications are not removed.*

Devices menu > VPN page > Applications

This tab permits you to manage and add applications using a Carlo Gavazzi / third-party application installed on the client side.

Moreover, the applications allow you to access remotely and fast an end-point.

The Carlo Gavazzi default applications are the following:

- UCS 7 Software
- UWP 3.0 Tool
- UWP4.0 IDE
- UWP Web App
- EMS Web App
- BTM XAP web server
- BTM XAP System Settings
- SSH remote support (only for Carlo Gavazzi Support Team)

There are two available classes of application that you can select to set a remote connection up. The application class depends on the protocol type.

Application class	Type	Access
Built-In Application	• SSH • HTTP • HTTPS	• Browser • Desktop
Native Application	Custom	Desktop

Applications can be grouped in Profiles associated to an existing endpoint. This way, the endpoint can be reached only via some given protocols (e.g., SSH or HTTP) or services.

*For further information, go to **> Devices menu > VPN > Applications > How to add an application.***

Carlo Gavazzi default applications

Users can find the Carlo Gavazzi default applications in the **Application** tab. These applications are grouped into the default profiles by default.

Application Class	Name	Application Type	Protocol	Port
Built-In application	SSH	SSH	TCP	52325 (for technical support)
	WebApp_HTTPS	HTTPS		443
	WebApp_HTTP	HTTP		80
	CP3_WebApp_ HTTPS	HTTPS		443
	CP3_WebApp_HTTP	HTTP		80
	BTM XAP Web Server	HTTPS		443,80
	BTM XAP System Settings	HTTPS		443
Native application	UWP_Tool / IDE	Custom		10000:10002 80 443 52326
	UCS_7_PROGRAM_ PATH	Custom (Bridge Modbus)		443, 41214 *Note: it can be changed by the user*
	UCS_7_HOME_ PATH	Custom (Bridge Modbus)		443, 41214 *Note: it can be changed by the user*

Placeholders

Placeholders permit you to use the same application on every device, regardless the different configuration values of each device (for example the public IP addresses).

If you want to set up…	Then…	And…
HTTP or HTTPS applications up	Fill in the URL to open field	Define the rules to connect to the relevant application
Custom applications	Fill in the **Command Path** and, if necessary, the **Command Arguments** fields	Define the rules to connect to the relevant application. *For more information, go to* ***How to > Devices menu > VPN > Applications > Placeholders > How to use Command path and argument for native applications****.*

IAM menu

This menu permits you to manage your organization through three sub-menus:

- **Organizations**
- **Users**
- **Roles**.

Organization page

IAM > Organizations

This page permits you to perform the following tasks:

- manage your organization
- add sub-organizations
- arrange your resources
- monitor the consumptions.

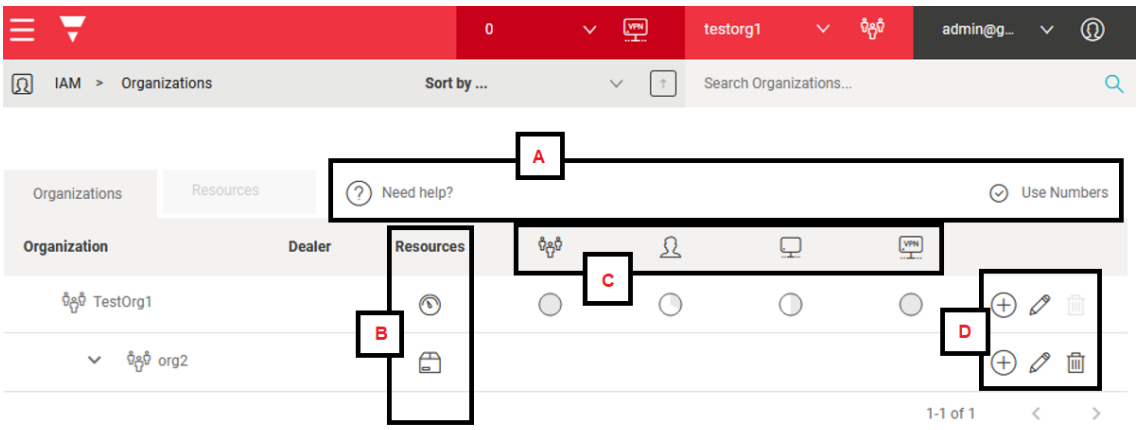
Three tabs compose it:

- **Organizations**. This section allows you to manage / add suborganizations and monitor / add suborganization resources.
- **Resources**. This tab allows you to check the available resources, the expired and scheduled licences and to add resources.
- **Consumptions**. This tab shows the consumption of your organization's devices and allows you to download this information as a csv file.

Notes:

- *you can change your reference organization clicking*  *from the navigation bar. The **Organization** page is updated according to the selection.*
- *for further information about the three tabs, please refer to the descriptions below.*

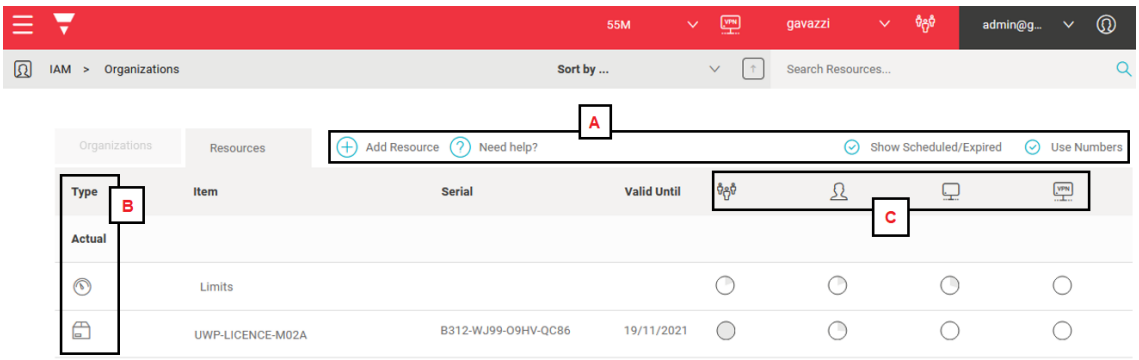
IAM > Organizations > Organizations



Element	Description
A	Need help: opens the context help. Use numbers. If you check it, you see the organization resources as number (used/total).
B	**Resources**. This column shows the following sub-organization type: if the lives on own resources option is disabled, it means that this organization receives the resources from the root organization. if the lives on own resources option is enabled, it means that in this organization the resources are added with UWP Licences. *For further information, go to* ***How to > IAM menu > How to activate a licence and add resources to an organization****.*
C	The pie charts show the following resources (according to each licence availability): • sub-organization • user • device • VPN service • © Credits *For further information, go to* ***"MAIA Cloud licence types" on page 12 > Licence code****.*

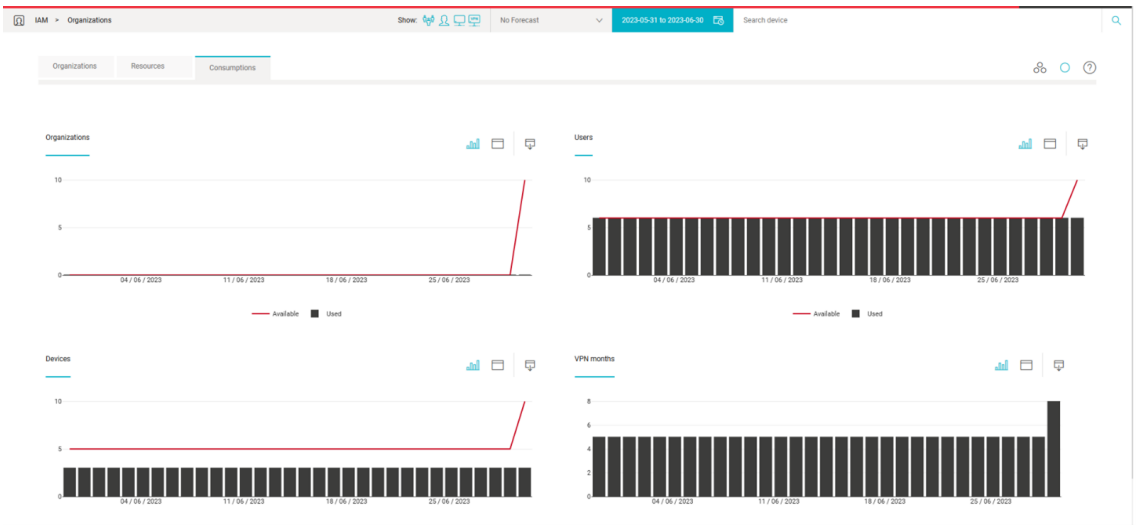
Element	Description
D	**Actions**. You can perform the following tasks: • Click  to add a sub-organization *For further information, go to* ***How to > IAM menu > How to add a sub-organization****.* • Click  to perform the following tasks: • Change the organization label • Set a host name if it is not already set *Note: once set the host name, you cannot change it or disable it.* • Enable or disabled full privacy *Note: if full privacy is enabled, you allow user to set up full privacy preventing all other users (also administrators) to see them.* • Add resources to the relevant sub-organization. *For further information, go to* ***How to > IAM menu > How to activate a licence and add resources to an organization****.* • Click  to delete an organization. • Click **Get info for technical support** to download a file useful for technical support.

IAM > Organizations > Resources



Element	Description
A	Add resource. *For further information, go to **How to > IAM menu > How to activate a licence and add resources to an organization**.* Need help: opens the context help. Show Scheduled/Expired. If you check it, you see the scheduled and/or expired licences. Use numbers. If you check it, you see the organization resources as number (used/total).
B	Type. This column shows the following sub-organization types: if the lives on own resources option is disabled, it means that this organization receives the resources from the root organization. if the lives on own resources option is enabled, it means that in this organization the resources are added with UWP Licences. *For further information, go to **How to > IAM menu > How to activate a licence and add resources to an organization**.*
C	The pie charts show the following available resources for each licence: • sub-organization • user • device • VPN service • © Credits *For further information, go to **"MAIA Cloud licence types" on page 12 > Licence code**.*

IAM > Organizations > Consumptions



Element	Description
A	From the secondary tab you can: • choose the resources to be displayed in the dashboards (by default all the resource are shown, you just need to click on the relevant icon to disabled a dashboard); • forecast: by default this option is disabled. If needed you can enabled the forecast considering a predefined period of time (1-3-6 months or 1 year) and the system automatically shows in the dashboard your consumption forecast based on the historical value; • choose the time period to consider; • search a specific device name.
B	If enabled, the suborganization's consumptions are highlight. If enabled, only the current organization consumptions are shown. Need help: opens the context help.
C	Each dashboard has the same available option: • enable/disable the chart view • shows the detailed consumption • exports a csv file

Users page

IAM > Users

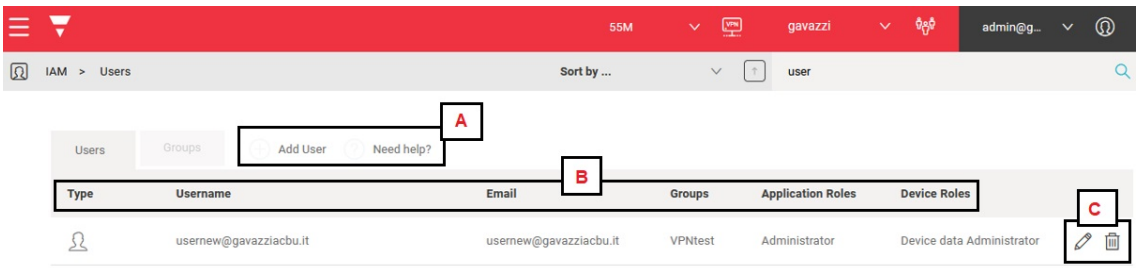
This page allows you to manage and add users / user groups. It is composed by two tabs:

Users. This tab allows you to manage the users of your organizations and add other users.

User groups. This tab allows you to add and manage user groups. User group is useful because you can assign or changed application and/or device roles to multiple users at the same time.

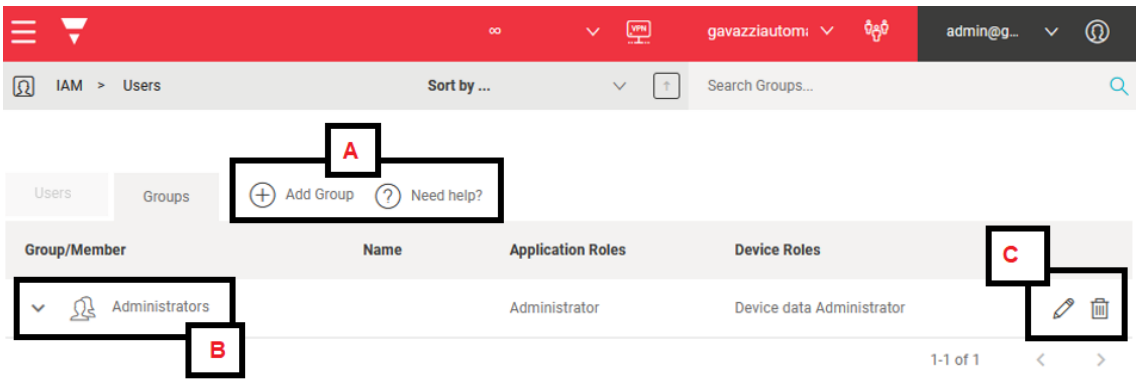
Note: you can change your reference organization clicking  *from the navigation bar. The Users page is updated according to the selected organization.*

IAM > Users > Users



Element	Description
A	+ Add user. If you click it, you are redirected to the **Options** page. *For further information, go to **How to > IAM menu > How to add a user*** ? Need help: opens the context help.
B	Information about users: • Type • Username • Email • Organization • Group (see user groups for further details) • User roles for specific fields (Application, VPN)
C	Actions. (edit) and (delete). permits you to perform the following tasks: • See user information (username, E-mail) • Add user to a group or change them (Group membership) *Go to User groups for further details* • Set or change user permissions (Application roles and Device roles) *Go to Roles page for further details* *Note: you can add more than one permission to the same user.* • Create, import or export favourite applications for user with direct access to favourite applications (Favourite Apps). • For more information go to How to set up a direct access to favourite applications. *Note: to allow user to log into MAIA Cloud, you need to set at least one Application role and one Device role. Otherwise, you can add a user to a group: this way, user inherits the users' group roles.*

IAM > Users > User groups



Element	Description
A	+ Add Group. *For further information, go to* ***How to > IAM menu > How to add a user group*** ? Need help: opens the context help.
B	User groups information: • User group name • Application roles • Devices roles If you click ⌄ , you can see the group members.
C	Actions. You can change and/or add roles and add/delete user members ( ) or delete ( ).

Roles page

IAM > Roles

This page allows you to manage and modify users' roles. It is composed by two tabs:

- **Application Roles**. The Application roles are composed by several permissions. For each MAIA organization components (i.e., users, user group, organizations, roles, devices, device group), the following four types of permission are available:
  - Create. You can add the relevant component in the MAIA organization.

    E.g., Usergroup.create allows to add new user group.
  - Delete. You can delete the relevant component from MAIA organization.

    E.g., User.delete allows to delete a user.
  - Read. You can see the relevant component in the MAIA organization.

    E.g., Organization.read allows to see organization menu and its tabs.
  - Update. You can manage the relevant component into Maia organization.

    E.g., Roles.update allows to change existing roles.
  - Iam.audit.read allows to access the Audit page

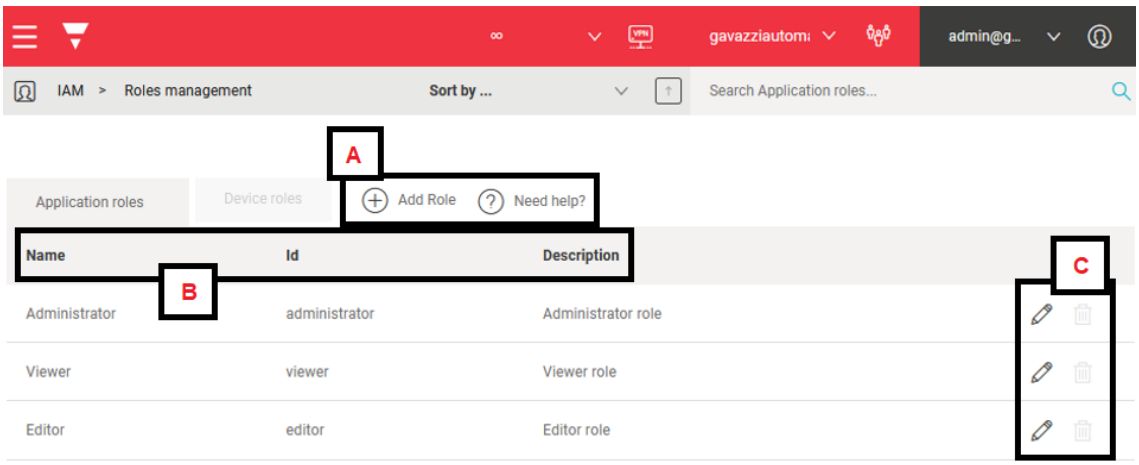
If you check the Access only favourite applications option, you can set up the Direct access to the favourite applications role. The users with this role do not access the standard MAIA Cloud portal, and can directly set up a VPN connection using one of the favourite applications.

Each favourite application is composed by a device, an endpoint and an application.

- **Devices roles**. This tab allows you to manage the device permission: this way, you can choose the users who can connect to VPN to each device and who can manage devices VPN resources.

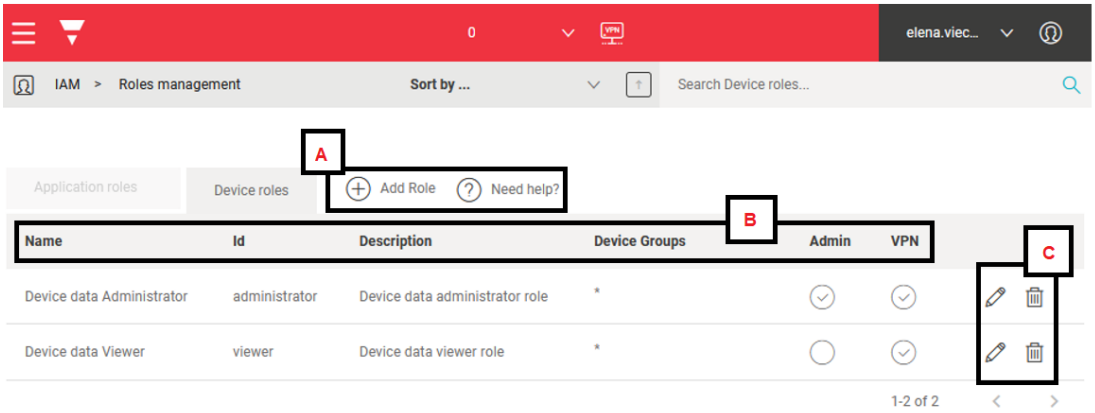
Note: you can change your reference organization clicking from the navigation bar. The Roles page is updated according to the selected organization.

IAM > Roles > Application roles



Element	Description
A	**Add roles**. If you click it, you are redirected to the relevant **Options** page. *For further details, go to **How to > IAM menu > How to add an application role**.* Need help: opens the context help.
B	Role information: • Role **Name** (administrator, viewer and editor are the standard roles) • **Role ID** • **Description**
C	**Actions**. You can change the role name, description and permission ( ) or delete ( ).

IAM > Roles > Device roles



Element	Description
A	**Add roles**. If you click **Add roles** you are redirected to the relevant **Options** page. *For further details, go to **How to > IAM menu > How to add an application role**.* Need help: opens the context help.
B	Role information: • Role **Name** *Note: administrator is the default role.* • **Role ID** • **Description** • **Device groups**. The devices which this role is related to • **Admin**: if you check it, you enable the administrator's permission. Otherwise, you will have a "standard" user. *Note: a regular user in **"Devices menu" on page 19 > VPN page** cannot assign credits to devices or enable/disable the auto renewal.* • **VPN**: if you check it, you enable the VPN access.
C	**Actions**. You can change the role name, description and the role permission ( ) or delete ( ).

Applications menu

This menu allows you to:

- Access the store to add and manage new MAIA Cloud applications
- Access and use applications already activated into your organization

Application menu > Store page

Applications > Store page

This page allows you to activate and manage MAIA Cloud applications. It is composed by two tabs:

- **Store**. Where you can find the list of available MAIA Cloud applications and access the relevant information page to read the app features and payment plan
- **Manage**. Where installed application are listed. Here you can manage the application access, upgrade or uninstall the application

Application menu > Store page >Fleet Management

This app allows you to manage and update large fleet of device, keeping your system secure and up to date.

You can perform the following actions:

- + to install the application.
  Note: to install the application you need to spend some credits
- to open the side menu with more information about the application and the relevant payment plan.
- if you want to receive news about the application

Application menu > Store page > Delegated Fleet Management

By using this app, you enable the root organization to remotely control the update process of your devices, keeping your system secure and up to date.

You can perform the following actions:

- + to install the application.
- to open the side menu with more information about the application.
- if you want to receive news about the application

How to install an application

- Open a browser
- Log in to your MAIA Cloud organization (https://app.maiaconnect.com)
- Open the **main menu** ☰
- Go to **Store**
- Click + on the relevant application window that you want to install
- Follow the wizard:
  - Payment tab: you need to accept the default payment plan to install the app

  note: if you don't have enough credits you can not proceed
  - Permission tab: you allow the application to access your organization resources
  - Enable: you define which device can be managed by the app and which user can use the app

- Recap: click finish to accept the conditions and install the app, click back to edit the previous settings

*note: typing * you can enable all the devices/uses added in your organization*

- As soon as the installation process is done, you are redirected to the Store> manage tab
- Click the arrow to access the relevant app

Fleet Management App page

This page allows you to manage, monitor and create campaign to update the fleet of devices added in your organization and/or in your suborganizations that support Fleet Management.

It is composed by two tabs:

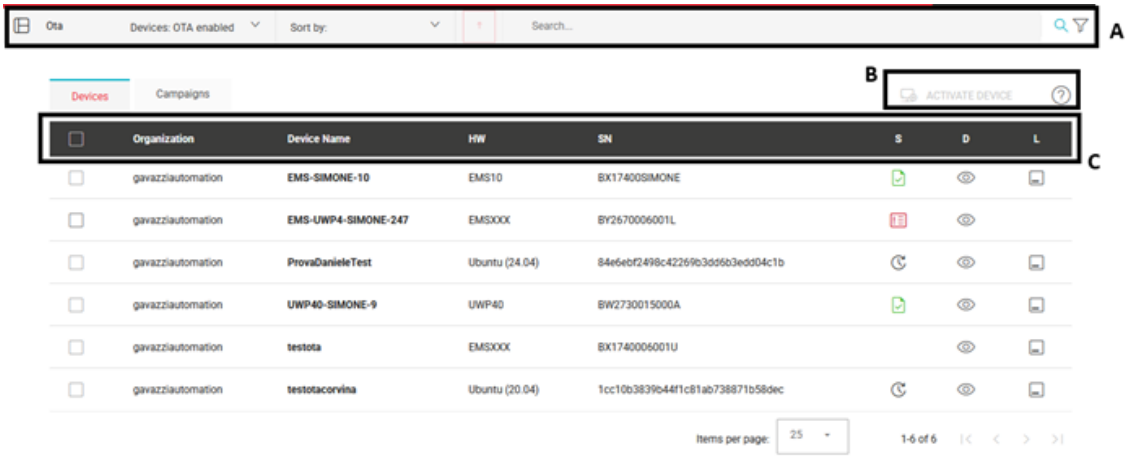
- Devices. This tab shows all the devices added in MAIA Cloud that you can manage with this application
- Campaigns. From this tab you can create, schedule and manage campaigns for device groups. A Campaign is a set or roles that is sent to devices which allows you to perform a fleet firmware update.

The fleet management app licence structure

To use the fleet management app you need:

- Standard licence to add devices and users.
  Notes:
  - as soon as you activate the fleet management app, 4 service accounts users will be added automatically
  - for more info about standard licences, go to MAIA_Cloud_licence_types > standard licence
- 250 credits to install the application (no renewal required).
  Notes:
  - For more information about credits go to MAIA_Cloud_licence_types > plus licence
  - Included in the initial plan you have the possibility to manage up to 50 devices for free during the first year
  - During the first year, if you manage more than 50 devicfes, an annual fee of 12 credits per extra device applies
- After the first year a recurrent fee of 12 credits per year applies per managed device

Applications > Fleet Management> Device page



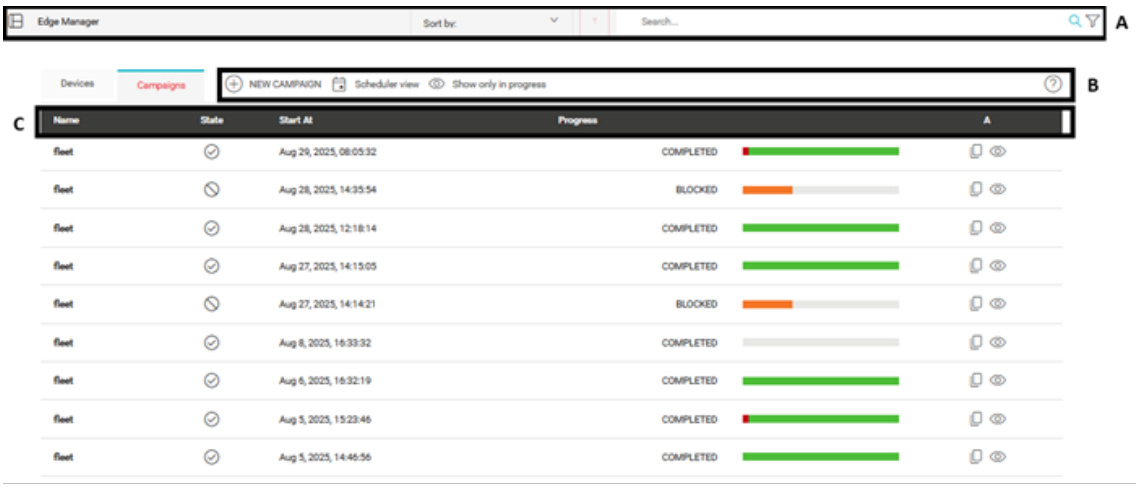
Element	Description
A	From the secondary tab you can: • choose the devices to be displayed in the table below (by default only the devices which supports the fleet management are displayed) • change the order in which the devices are displayed by clicking 'Sort by' • search a specific device in the search tab. Note clicking (▽) you can add other filters
B	Activate device Click here to enable the selected devices in the Fleet Management app. *Note: use the check box in the table to select the devices* ? Need help: opens the context help.
C	From the main tab you can access the following information: • organization: the organization where the device has been added • device name • HW: this is the HW type. When you move the cursor over the hardware type, the full part number will be displayed • SN: the serial number • FW: the firmware currently installed in the relevant device • S: the device status. When you move the cursor over the icon, a pop up will describe the status. These are the possible device status ◦ **Device not licensed**: means that the device must be activated in order to be used within the Fleet Management App. ◦ **No Campaign Applied**: this is a normal condition for newly devices not yet involved in any campaign. ◦ **Update in progress**: when the device firmware update is ongoing ◦ **Campaign correctly applied**: when the campaign has been assigned properly to the device and there is no error ◦ **Device Out-of-Sync**: when the device status does not match the campaign specification. The tooltip provides the reason why the relevant device is in this status. ◦ **Device in Error**: you can get more details about the error by checking the device logs. • D: by clicking the device detail icon you can access the relevant side menu • L: by clicking the device logs icon you can access the relevant side menu Note: all this information are available only for devices that has been activated in the fleet management app

How to activate a device in the fleet management app

1. Click ☰ to open the main menu
2. Go to **Applications > Fleet manager**
3. Go to the **Devices page**
4. Use the checkbox to select the devices you need to activate in the application

5. Click Activate device
6. A pop up will inform you about the devices that you are going to activate and the relevant credits that you are going to spend.
   If you do not have enough credits, you can not finish the procedure and you need to go back to point 4.
   If you have credits, you need to authorize the transaction to finish the procedure.

Applications > Fleet Management> Campaign page



Element	Description
A	From the secondary tab you can: • change the order in which the campaigns are displayed by clicking 'Sort by'. You can sort by name or by start time • search a specific campaign using the search tab Note clicking (▽) you can add other filters
B	• + to create a new campaign *For more info go to **"How to create a campaign" on the next page*** • to change the page view from the default one to the calendar • to filter the campaign and see only the one which is in progress • ? Need help: opens the context help.
C	From the main tab you can access the following information: • name: the name of the campaign • State: campaign status. When you move the cursor over the icon, a pop up will describe the status • Progress: the progress bar displays a summary of the campaign status. When you move the cursor over the colored bar, a pop up will show the number of update with the relevant status • A: from the action menu you can: ◦ clone a campaign ◦ access the campaign details

How to create a campaign

1. Click ☰ to open the main menu
2. Go to **Applications > Fleet manager**
3. Go to the **Campaigns page**
4. Click + New campaign to open the campaign side menu
5. Define the campaign Name
6. Choose the Hardware type to which the update has to be sent from the drop-down menu

   Note: as soon as the hardware is selected, it will be automatically added as a filter in the Devices section. To remove the filter, simply click EDIT DEVICE LIST
7. Choose the Firmware upgrade policy that has to be followed
   a. Last available: if you want the system to automatically check for the latest release available on the Gavazzi servers and install it.

      Note: auto-update can also be enabled for this policy. The system will then regularly check the server and apply updates, if available, according to a user-defined interval in days.
      To stop the auto-update procedure you need to create another campaign with this setting disabled

   b. Select from list: you can choose the target release from the drop down menu

      Note: the dropdown will show the five most recent releases relevant to the hardware selected earlier.
8. define the campaign target Devices: clicking EDIT DEVICE LIST the dedicated page will open.

   From the table you can select or deselect a device or a group of devices. You can also use the filters available in the top part of the page.

   Notes:

   - you can use One-by-one mode if you want to perform an individual selection.
   - you can use Filters mode if you want to add a group of devices with a specific policy to the list
9. if needed, you can configure a Device maintenance window: this window defines the time interval during which the devices are allowed to start the firmware update process.

   Note: by default is disabled, you can set daily, weekly, monthly, or yearly intervals.

   By default, a campaign starts as soon as the settings are saved (Launch now mode setting). The Scheduler allows you to set a different start time: choosing Planned mode, you can define when the Campaign has to be sent to the relevant devices.
10. Click ✔ to save

Note: if you add devices not already activated in the fleet management app an adictional pop up will open to inform you about the devices that you are going to activate and the relevant credits that you are going to spend.

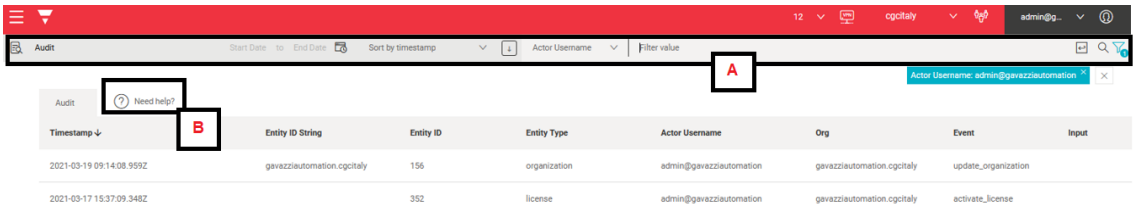
If you do not have enough credits, you can not finish the procedure and you need to go back to point 6.

If you have credits, you need to authorize the transaction to finish the procedure.

Audit menu

This menu shows you the organization logs with useful information to check which user did an action and the relevant timestamps.

Note: you can change your reference organization clicking 👥 *from the navigation bar. The **Audit** page is updated according to the selected organization.*



Element	Description
A	From the secondary tab you can: • choose the time period to consider ( ) • sort by allows you to sort the log list by a specific category • filter by a specific category ( )
B	Need help: opens the context help.

How to

IAM menu

IAM menu > Organizations > Organizations

How to add a sub-organization

1. Open the **main menu** (☰)
2. Go to ***IAM > Organization***
3. Go to the **Organization** tab
4. Click **Add Organization**
5. Enter the organization name
6.

If you want to…	Then enable…
set a host name to the sub-organization	**Has hostname**
create a sub-organization and allow user to set up full privacy preventing all other users (also administrators) to see them	**Allow full privacy**
create an organization which lives on own resources	**Lives on own resources** *For further information, go to* ***"How to activate a licence and add resources to an organization" on page 49***

How to move a device to another organization

1. Open the **main menu** (☰) of the organization where you want to move the device
2. Go to **IAM > Organization**
3. Go to the **Organization** tab
4. Click **other action** ⋮
5. Click **Generate import KEY**

   Note: the key will automatically saved in your clipboard and will be valid for 10 minutes)
6. Access the organization where the device is currently activated
7. Open the **main menu** (☰)
8. Go to Devices > Manage
9. Click **other action** ⋮ from the action menu of the relevant device
10. Click move device
11. Copy the key generated in point 5 to the side menu

    Note: once the device has been moved, any associated resources are not lost.

IAM menu > Organizations > Resources

How to add resources to root organization

1. Open the **main menu** (☰)
2. Go to ***IAM > Organization***
3. From the **Resources** tab, click **Add Resource**
4. Enter your **Licence Code**

   Note: if your code is valid, you automatically see the licence type (standard or plus), the licence expiration date, and the resources composing the licence.

5. Click ✔ to add the resources to your organization

For more information about resources, go to ***"MAIA Cloud licence types" on page 12 > Licence code****.*

How to activate a licence and add resources to an organization

The procedure depends on the lives on own resources option.

If “lives on own resources” is…	Then…
Disabled	1. Open the **main menu** (☰) 2. Go to ***IAM > Organization*** 3. Open the **Organization** tab 4. Click **Edit** from the **Actions** column of the sub-organization you want to manage 5. From the settings menu, you can add Users, Devices, Suborganization and Month of VPN 6. Click ✔ to save *This way, the root organization resources go to the sub-organization.*
Enabled	1. From the top bar, select the sub-organization where you want to add resources 2. Open the **main menu** (☰) 3. Go to ***IAM > Organization*** 4. Open the **Resources** tab 5. Click ✚ **Add Resources** 6. Write the UWP licence code *Note: if your code is valid, you see automatically the licence type (standard or plus), the licence expiration date, and the resources composing the licence.* 7. Click ✔ to save

*For more information about organizations and organization type, go to **IAM menu > Organizations page***

IAM menu > Users > Users

How to add a user

1. Open the **main menu** (☰)
2. Go to ***IAM > Users***
3. Go to the **Users** tab
4. Click **Add User**
5. Fill in the options page
6. Choose a user group (not mandatory)
7. Set the user’s roles
8. If you want to set a user with the direct access to favourite applications, click ✚ to define at least one application.

For more information, go to ***"How to set a direct access to favourite applications " on the next page***

9. Click ✔ to add user to your organization

   For more information about user roles, go to ***IAM menu > Roles page****.*

IAM menu > Users > User groups

How to add a user group

1. Open the **main menu** (☰)
2. Go to ***IAM > Users***
3. Go to the **User groups** tab
4. Click **Add group**
5. Enter your user group name
6. Choose an application and/or device role from the list
7. Select the users to add from the list
8. Click **Enter** to save

How to add a user to a user group

1. Open the **main menu** (☰)
2. Go to ***IAM > Users***
3. Go to the **User groups** tab
4. Click ✎ to edit the group
5. Select the users to add
6. Click **Enter** to save

IAM menu > Roles> Application roles

How to add an application role

1. Open the **main menu** (☰)
2. Go to ***IAM > Roles***
3. Go to the **Application roles** tab
4. Click ➕ **Add roles**
5. Enter a role name
6. Write a description (not mandatory)
7. Choose the permission for your role

If you want your user to access…	Then…
the standard MAIA Cloud portal	8. Disable the **Access only favourite applications** option 9. Choose the permissions from the list
Only the favourite applications	8. Enable the **Access only favourite applications** option 9. Check the *iam.device.read* permission

10. Click ✔ to save

How to set a direct access to favourite applications

1. Enable the **Access only favourite applications** option to create a specific application role and the *iam.device.read* permission.

   *For further information, go to **"How to add an application role" above***

2. Go to ***IAM > Users > Edit user*** or ***Add user***
3. Set the application role for the relevant user
4. Set a device role
5. Click ➕ to add to **Favourite Applications**
6. Choose the device, the endpoint and one of the available applications

   Note: you can also import favourite applications from a database (⬇).

7. Click ✔ to save

IAM menu > Roles> Device roles

How to add a device role

1. Open the **main menu** (☰)
2. Go to ***IAM > Roles***
3. Go to the **Device roles** tab
4. Click ➕ **Add roles**
5. Fill in the option page with role name
6. Write a description (not mandatory)
7. Choose the devices
8. Set the permission

   *Notice: a regular user cannot assign credits to devices or enable/disable the autorenewal from **Devices > VPN page > Action** menu. An administrator has the full control of devices.*
9. Check the VPN access to allow users to use VPN
10. Click ✔ to save

Devices menu

Devices menu > Activate

How to activate a Device

1. Open a browser
2. Log in to your MAIA Cloud organization (https://app.maiaconnect.com)
3. Open the **main menu** (☰)
4. Go to ***Devices > Activate***
5. Complete the Activation page with the device in:
   - Device Label (the device name)
   - Latitude and longitude of the location

     Note: you can navigate the map or use the search box.
   - UWP-ACTIVATION-KEY: write a valid Carlo Gavazzi activation key included in your UWP-ACTIVATION-KEY item.

   *For further information, go to **"MAIA Cloud licence types" on page 12 > Activation code**.*
6. Click ✔ to activate the device.
7. Go to your MAIA Cloud home page
8. Click ⋮ ***> Assign credit*** to enable the VPN service for your device

   *Note: to assign credits, you need at least one unused VPN month. To add resources to your organization, you need a UWP-LICENCE code. For further information, go to **"MAIA Cloud licence types" on page 12**.*
9. If you want to use UWP 4.0 in few seconds the device will be online

If you want to use the UWP 3.0 version…	Then…
8.4.0.3 onwards	In few seconds the device will be online
8.4.0.3 backwards	go to "How to enable the VPN service for an installed UWP 3.0" below

If you want to use the XAP or a BTM with BSP version…	Then…
3.1.110 onwards	Access the machine config Go to System Settings> Service Settings> MAIA Cloud / VPN Service Enabled the service clicking on the icon ✔ Write the Activation code in the relevant window Save In few seconds the device will be online
3.1.xxx backwards	Update your device BSP to 3.1.110 or later. For more info click here

How to enable the VPN service for an installed UWP 3.0

1. Go to your MAIA Cloud organization and activate your UWP 3.0

*For further information, go to **"How to activate a Device" on the previous page**.*

2. Log in to the UWP 3.0 web app
3. Open the main menu (☰)
4. Go to ***Service > Remote VPN Services***
5. Enable the service
6. Click 💾 to save

   Note: the green icon informs you that the procedure is successfully finished.

Devices menu > Manage > Device groups

How to add a device group

1. Click ☰ to open the main menu
2. Go to ***Devices > Manage***
3. Go to the **Device Group** tab
4. Choose the type of group

If you want to…	Then…
Add a group	Click +
Create a group within an existing group	Click from the **Actions** column of an existing group

5. Enter your device group name.
6. Click **Enter** to save.

Devices menu > VPN > Devices

How to connect to gateway/endpoints (VPN tunnel)

1. Go to your MAIA Cloud home page
2. If the device you need to connect is online, you can perform different actions:

If you want to…	Then…
Use the Virtual IP as if it were a Local IP	Open the action menu Click Connect Copy the VPN IP address that you find in the left part of the connection drop down-menu or in the top part of the connection side-panel, anduse this IP as if you were using a local IP the VPN IP address that you find in the bottom part of the pop-up, in your browser.
Use a predefined application to create a VPN tunnel to the gateway	Click one of the available applications you find in the connection drop-down menu or in the connection side-panel *For further information, go to "The connection drop-down menu and side-panel".*
Disconnect from the endpoints/gateway	Open the action manu Click **Disconnect**

Notes:

i. *more than one user can access the device at the same time. We recommend connecting remotely only to one user at time, in order to avoid interferences while user's working.*

ii. *you can set up users with a direct access to the favourite application permissions. These users will not access the standard MAIA Cloud portal, but they can directly access the favourite applications after the login in MAIA Cloud.*

iii. *For further information, go to* ***"How to set a direct access to favourite applications " on page 51****.*

How to connect remotely to UWP 4.0 IDE application

1. Go to your MAIA Cloud home page
2. Choose the device you need to connect
3. You can follow one of the following procedure

If you want to…	Then…
Use the Virtual IP as if it were a Local IP	Open the action menu Click Connect Open the UWP 4.0 IDE sw Go to step 4
Launch automatically UWP 4.0 IDE sw	Click UWP IDE application you find in the connection drop-down menu or in the connection side-panel *For further information, go to "The connection drop-down menu and side-panel".* Go to step 4

4. Copy the VPN IP address that you find in the left part of the connection drop down-menu or in the top part of the connection side-panel
5. In the IDE connection profile area, click @ to open the Controller Connection Management window
6. Click + to add a connection profile
7. Paste the Virtual IP copied at step 4 in the IP address column
8. Save
9. Click ► to set up the remote connection

Devices menu > VPN > Endpoints

How to add an endpoint

1. Click ☰ to open the main menu
2. Go to ***Devices > VPN***
3. Go to the **Endpoints** tab
4. Click + from the **Actions** column of the desired device
5. From the **Endpoint options** menu, enter the following information:
   - Name
   - Description

   Note: it is not mandatory but it is useful to find an endpoint faster.

   - IP address
   - Application profile. Click ⌄ and choose one of the available profiles

   *For further information, go to **"Devices menu" on page 19 > VPN page > Profiles**.*
6. Check the **Enabled** box to activate the endpoint

   *Note: **Source NAT** is optional, it allows you to use a real IP instead of a virtual IP. When an endpoint is connected to the MAIA Cloud server, by default it gets a virtual IP address. It may be necessary for the endpoints to maintain the real IP used in the local network even if reached through the VPN. In these use cases you can select the Source NAT option.*

7. Click ✔ to save the configuration.

Devices menu > VPN > Profiles

How to create a profile

1. Click ☰ to open the main menu
2. Go to ***Devices > VPN***
3. Go to the **Profiles** tab
4. Click + **Add profile**
5. Complete the profile **Options** with the following information:
   - Name
   - Description

     Note: it is not mandatory but it is useful to find an endpoint faster.

     - IP address
     - Application profile. Click ⌄ and choose the available applications you want to include in the relevant profile

     For further information, go to ***"Devices menu" on page 19*** *> VPN page > Applications*.
6. Click ✔ to save.

How to associate a profile to an endpoint

1. Click ☰ to open the main menu
2. Go to ***Devices > VPN***
3. Go to the **Endpoints** tab
4. Click ⌄ of the device your endpoint belongs to

   Note: each device activated with a UWP-ACTIVATION-KEY is considered an endpoint called gateway and its IP address is the local host. This endpoint is automatically created when you activate the device.
5. Click ✎ from the **Actions** column of your endpoint to open the endpoint **Options** menu
6. Click the **Application profile**
7. Choose one of the available profiles
8. Click ✔ to save.

Devices menu > VPN > Applications

How to use UCS 7 application to set up a VPN tunnel

1. Log in to your MAIA Cloud (click here)
2. Open the home page or open the **main menu** and go to ***Devices > VPN***
3. Select the device you need to connect to and open the connection drop-down menu or the side panel

*For further information, go to **Devices menu > VPN page > Devices > The connection dropdown menu and side panel**.*

4.

If you have installed UCS…	Then from the gateway pop-up click…
for all users	UCS_7_PROGRAM_PATH
for current user	UCS_7_HOME_PATH

5. Use **Connection via UWP Secure Bridge**
6. Click **Connect**
7. Choose the **Manual connection**
8. Write the virtual IP address you find in your gateway pop-up (VPN page)
9. Click **Connect**
10. Write your UWP Secure Bridge credentials and write the connection parameters
11. Click **Connect**

How to add an application

1. Click ☰ to open the main menu
2. Go to ***Devices > VPN***
3. Go to the **Applications** tab
4. Click **+ Add application**
5. Complete the application **Options** menu with the following information:
   - Enter a Name and a Description.
   - Choose the Application Type and the protocol from the drop-down menu.
   - Write the Port number

   Note: if the application uses more than one port for example 80, 10010, 10011, 10012 you can write 80, 10010:10012
6. Check the **Advance parameter** field to enter the advanced information.

   *The **Application Options** menu and the **Advanced parameters** change according to the **Application** type.*
7.

If you want to set up…	Then…
an **SSH** (*Secure Shell Connection*) application	8. Select the **Protocol** type and the **Port** number from the **Applications** tab 9. Choose the options from the **Advanced parameters** tab (not mandatory)
• **HTTP** *Web interface in a browser* • **HTTPS** *Web interface over a secured connection in a browser*	8. Select the Protocol type and the Port number 9. Fill in the URL to open. *For further information, go to **Devices menu > VPN page > Applications> Placeholders.***

If you want to set up…	Then…
a **CUSTOM** application	From the **Application** tab select: • Protocol type • Port number • Command path and arguments *For further information, go to Devices menu > VPN page > Applications> **Placeholdersand "How to use Command path and argument for native applications" below.*** *Note: from the **Advance parameters** tab, you can set other custom parameters (not required).*

10. Enable the application
11. Click ✔ to save.

Devices menu > VPN > Applications > Placeholders

How to use Command path and argument for native applications

For native applications, you can customize the **Command path** adding your directory address. This way, when you use for example the UWP 3.0 Tool to set up the VPN connection, you directly open the software.

1. Click ☰ to open the main menu
2. Go to ***Devices > VPN***
3. Go to the **Applications** tab
4. Click ✎ from the **Actions** column
5. Change the **Command path**

   Example with UWP 3.0 Tool: if your workstation is equipped with Windows and the program UWP 3.0 Tool 8.4.0.3 is installed in Programs (x86) folder, write C:\Programmi (x86)\UWP3 Tool 8.4.0.3\Sx TOOL.exe

6. Click ✔ to save.

How to change a native application path

For default native applications and other native applications where **Command path** has not been defined (*for further information, go to **"How to use Command path and argument for native applications" above***), the path can be manually set at the first use. Then this path is automatically saved, and MAIA Cloud directly opens the software when user wants to set up VPN connection through the relevant native application.

1. Use a web browser to access MAIA Cloud (click here)
2. Log in to MAIA Cloud Connector Plug-in

   *For further information, go to Devices menu > VPN page > Devices> **MAIA Cloud connector plug-in***

3. Open your PC system tray

   Note: the system tray, called the Notification area, is generally located on the right side of the taskbar

4. Right click the MAIA status icon 
5. Click **Show MAIA Cloud Connector Plug-in**
6. Open **APPS** tab
   Go to step 7

7.

If want to…	Then…
Change only one application path	8. Choose one of the available native applications from the list 9. Click **reset selected**
Change all the application paths	8. Click **reset all**

9. Click **OK** to reset the path of the chosen application and close the window
10. Go back to MAIA Cloud and set up a VPN connection through the native application you need to upload
11. Set the new path which is automatically saved

Legal notice

- *MAIA Cloud - Terms and conditions (multilingual)*
- *MAIA Cloud - Privacy Policy (multilingual)*