

MAIA Cloud system

MAIA Cloud system

User manual

Document revision: v. 2.0

Copyright © 2021, CARLO GAVAZZI Controls SpA

All rights reserved in all countries.

Any distribution, alteration, translation or reproduction, partial or total, of this document is strictly prohibited unless with prior authorization in writing from CARLO GAVAZZI Controls SpA with the exception of the following actions:

- Printing all or part of the document in its original format.
- Transferring the document on websites or other electronic systems.
- Copying contents without any modification and stating CARLO GAVAZZI Controls SpA as copyright owner.

CARLO GAVAZZI Controls SpA reserves the right to make modifications or improvements to the relative documentation without prior notice.

Requests for authorization, additional copies of this manual or technical information on the latter, must be addressed to:

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

MAIA Cloud system

MAIA Cloud system	4
Introduction to the MAIA Cloud system	5
Benefits of EDGE + PaaS solution value	5
MAIA system elements	5
Ports used	6
MAIA Cloud components	6
MAIA for energy monitoring and building automation	10
MAIA for car park guidance system	11
MAIA Cloud interface	12
Access types	12
MAIA Cloud licence types	12
MAIA Cloud browser	15
MAIA Cloud Connector desktop application	57
Legal notice	60
Download	61



Introduction to the MAIA Cloud system

Content

This chapter includes the following topics:

Benefits of EDGE + PaaS solution value	5
MAIA system elements	5
Ports used	6
MAIA Cloud components	6
MAIA for energy monitoring and building automation	10
MAIA for car park guidance system	11

Benefits of EDGE + PaaS solution value

- **EDGE reliability:** Carlo Gavazzi UWP 3.0 Edge is 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 UWP 3.0 or SBP2CPY24 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	<p>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.</p> <p><i>Supported browsers: latest versions of Chrome, Firefox and Safari.</i></p>
MAIA Cloud Connector Desktop Application	<p>A user-friendly application for supervising the installations controlled or monitored by the UWP 3.0 or SBP2CPY24 units. Thanks to this application, users and maintainers can connect to remote machines. The MAIA Cloud Connector desktop application has been designed for Windows® platforms.</p> <p><i>Operating system requirements: Windows 7 (updated version).</i></p> <p><i>Note: the MAIA Cloud Connector desktop application has been discontinued since the launch of the MAIA Cloud Connector plug-in (see below).</i></p>
MAIA Cloud Connector plug-in	<p>A plug-in which adds to MAIA Cloud the functions of the MAIA Cloud Connector desktop application. The MAIA Cloud Connector plug-in has been designed for Windows® platforms.</p> <p><i>Operating system requirements: Windows 7 (updated version).</i></p>



Ports used

Access	Port
MAIA Cloud (browser)	port 443/TCP and 1194/udp
MAIA Cloud Connector desktop application (desktop software)	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. <i>The Carlo Gavazzi UWP 3.0 and SBP2CPY24 are gateways.</i>
Endpoint	Any device with the following features: <ul style="list-style-type: none">• It can connect via a network.• It has its own IP address (unique). <p><i>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).</i></p> <ul style="list-style-type: none">• It may connect to local network and/or to the Internet by means of a gateway• It can be connected to one gateway only. <p><i>The Carlo Gavazzi Modbus/TCP Meters and UWP 3.0 TCP/IP services (such as the UWP 3.0 Web-App or the Web-API) are endpoints.</i></p>
User	Users can access and interact with MAIA Cloud, a gateway, or an endpoint according to their role. <i>Note: user who registers the root organization is called owner.</i> <i>The administrator defines the organization roles and assign roles to users (go to "IAM menu" on page 31 > Roles page for further details).</i>
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). <i>You can group different applications in an application profile. Each endpoint has an application profile that defines all the available and admitted connections.</i>



Element	Description
Organization (or domain)	<p>A collection of users, devices and applications arranged into groups. Every organization node is completely separated from, and invisible to, other organizations.</p> <p><i>Notice: a device can belong just to one organization, and user can be added to other suborganization of the same domain.</i></p> <p>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.</p> <p>MAIA Cloud organizations permit to perform the following tasks:</p> <ul style="list-style-type: none">• 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. <p><i>The organization structure is up to the owner of MAIA Cloud. For further details go to "What are organizations" below</i></p>
Resources	Users, devices, sub-organizations and month of VPN 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

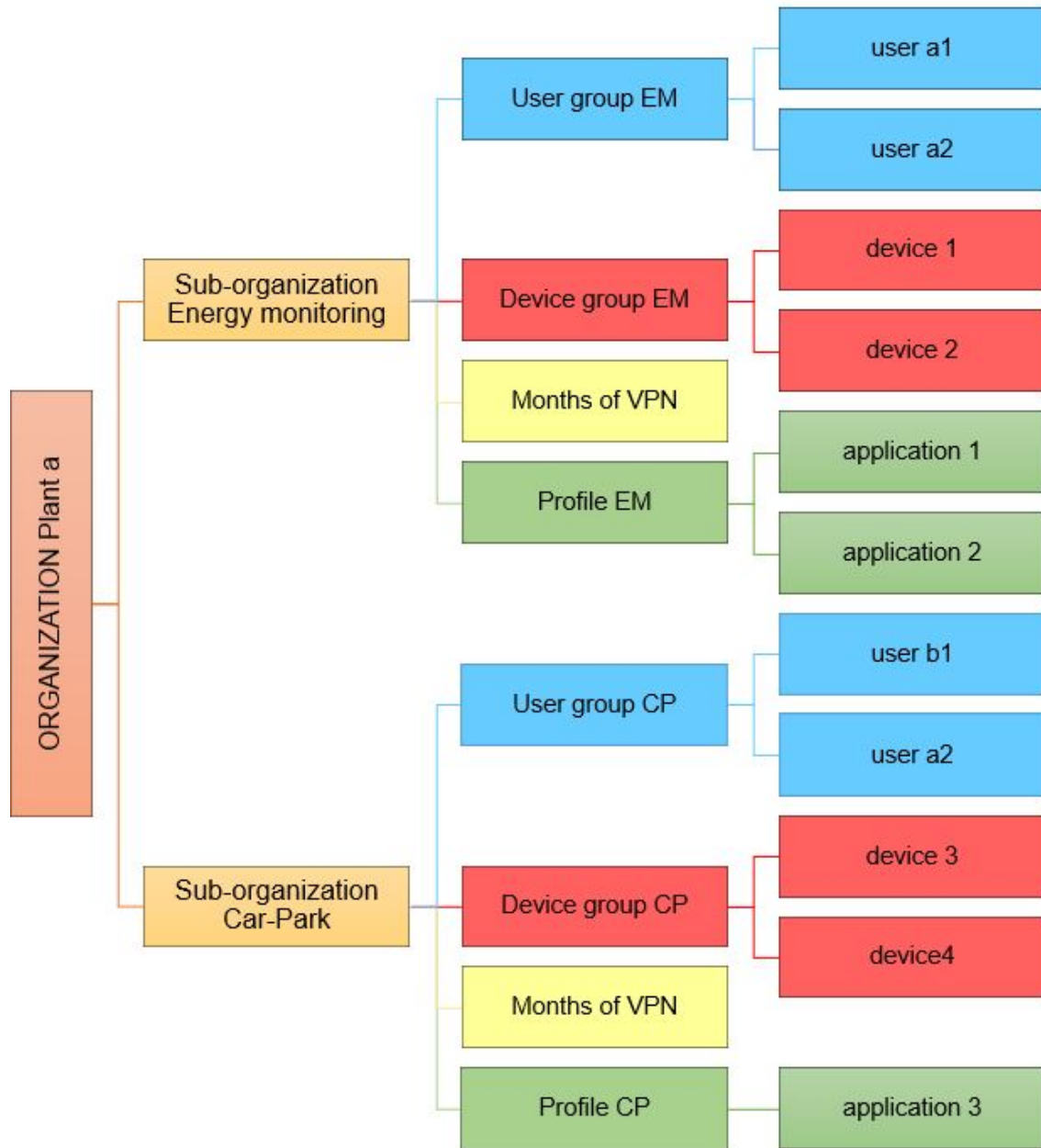
In case of complex organizations, you can split the main organization into sub-organizations.

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



Organization use cases

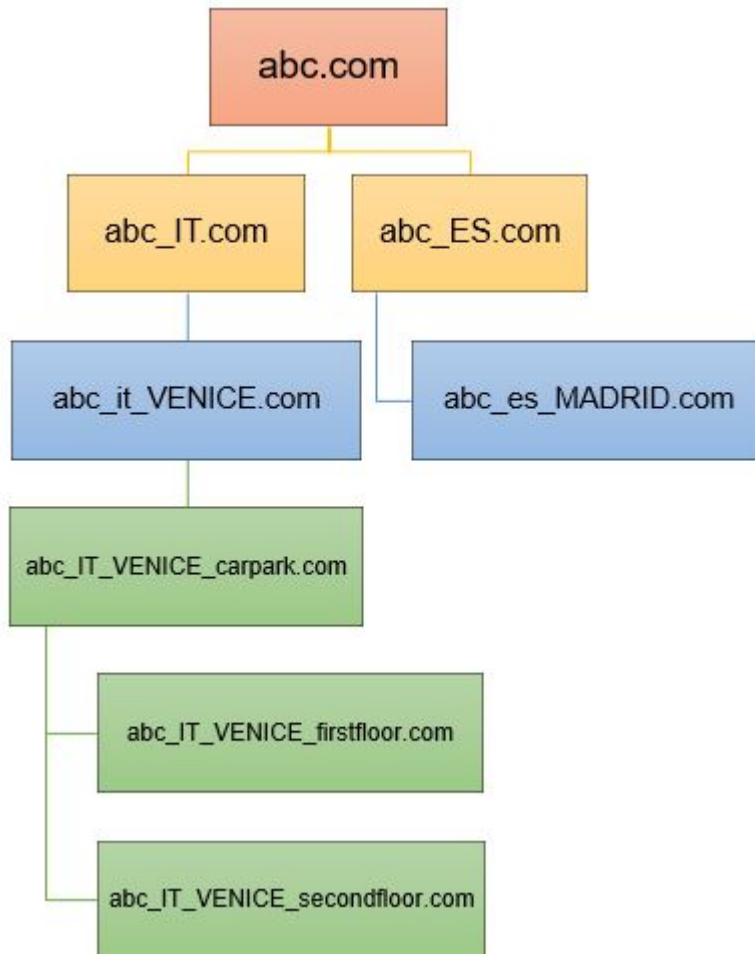
1. In an office building where several meters are installed for energy monitoring and there is a car park management system, you should split the root organization into two sub-organizations. In this case, one sub-organization is for the energy monitoring and the other is for the car park management.



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, building automation and car-park management.



2. Use case 2

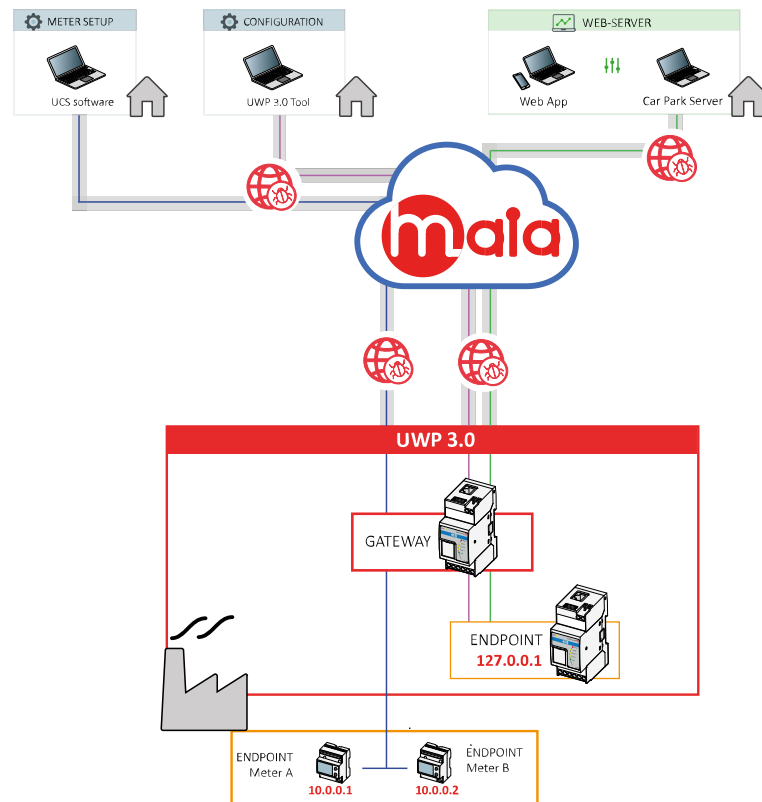
Within MAIA Cloud, every supermarket of the retail organization “hierarchy” represents a node.

*If you want to split some buildings into different nodes, you can add other levels and create sub-organizations (for example *abc_pt_porto_carpark.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



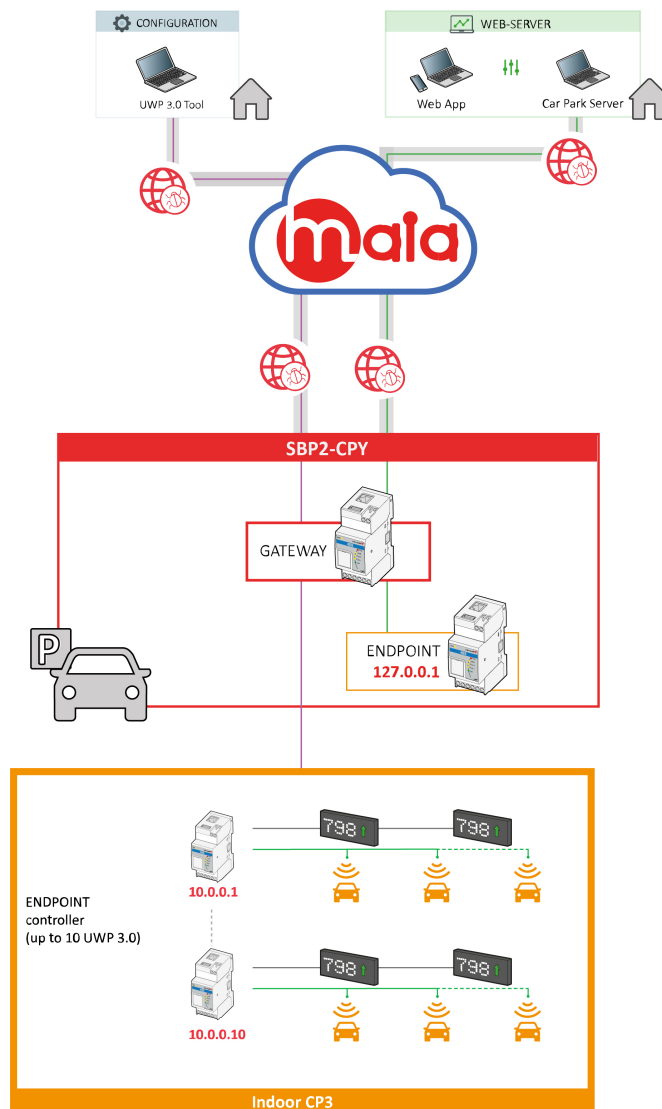
UWP 3.0 is a gateway that, in a remote connection, acts as an end-point providing the IP address of the local host. Following are the applications that permit a remote connection and that are compatible with UWP 3.0:

- UWP 3.0 Tool, configuration software.
- UWP 3.0 Web App, for viewing / exporting of data, controlling the automation functions and defining settings.
- UWP 3.0 Car Park Server, for setting up the system and monitoring the installation.

For the configuration of the endpoints and the monitoring of the Carlo Gavazzi meters, you can use our UCS software.



MAIA for car park guidance system



MAIA Cloud can be used to remotely manage a multi-site parking. In the cases of car park, SBP2CPY24 is a gateway that can be used as the unique access point to remotely operate both SBP2CPY24 and the UWP30 units on the same LAN. Following are the applications that permit a remote connection and that are compatible with devices:

- SBP2CPY24 Car Park server, for setting up the system and monitoring the installation.
- UWP 3.0 Tool, configuration software.
- UWP 3.0 Web App, for viewing / exporting of data, controlling the automation functions and defining settings.



MAIA Cloud interface

Content

This chapter includes the following sections:

Access types	12
MAIA Cloud licence types	12
MAIA Cloud browser	15

Access types

You can access our MAIA Cloud system through the [MAIA Cloud browser](#) or "[MAIA Cloud Connector desktop application](#)" on page 57.

		Browser	Desktop application
Login requirements		Internet browser	Application installed
Perform the first login		V	X
Register into MAIA Cloud		V	X
Manage personal account		V	X
Activate devices		V	X
Manage organizations		V	X
VPN Remote access	built-in applications	V	V
	native applications	V <i>Note: install the MAIA Cloud Connector plug-in</i>	V

The MAIA Cloud system is based on two types of licence, the [Activation code](#) and the [Licence code](#). These [licences](#) allow user to add and activate resources composing the organization. The resources are the following:

- Devices
- Users
- Sub-organizations
- Months of VPN

From the **Login** page, you can register and create an organization.

For further information, go to "[MAIA Cloud licence types](#)" below > [How to register and create an organization](#) and "[MAIA Cloud components](#)" on page 6 > [What are organizations](#)

MAIA Cloud licence types

MAIA Cloud services are based on two types of licence: the activation (UWP-ACTIVATION-KEY kit) and the licence (UWP-LICENCE-Mxxx family) code. The UWP-ACTIVATION-KEY kit allows user to register on MAIA Cloud and activate a device of the organization.

For further details, go to [Activation code](#) below.

The UWP-LICENCE-Mxxx family allows user to add resources to the organization.



For further details, go to **Licence code** 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" on the previous page > How to register and create an organization.**

- activate only one supported device to a MAIA Cloud organization

For further information, go to [How to > Devices menu > Activate > How to activate a device](#)

The supported devices are UWP 3.0 and SBP2CPY24.

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.
- For further information about enabling the VPN service, go to [How to > Devices menu > Activate > How to enable the VPN service for an installed UWP 3.0/SBP2CPY24.](#)

Licence code

The licence code is included in our UWP-LICENCE-Mxxx family and allows user to add resources to an organization.

For further information, go to **"How to" on page 43 > IAM menu > Organizations > Resources > How to add resources to a root organization.**

After the registration (go to **"MAIA Cloud licence types" on the previous page > How to register and create an organization**), the organization is created with some trial resources that you can use for 30 days.

A licence is composed by resources that can be annual or for consumption. There are, in fact, two types of licence:

- Standard licence, with annual resources (i.e., users, devices, sub-organizations).
- Plus licence, with resources for consumption (i.e., months of VPN).

The following UWP-LICENCE-Mxxx family items are available:

Licence type	Carlo Gavazzi code	Licence composition			
		Annual resources			Resources for consumption
		Devices	Users	Sub-org.	VPN months
Standard	UWP-LICENCE-M02A	2	2	2	0
Standard	UWP-LICENCE-M10A	10	10	10	0
Standard	UWP-LICENCE-M50A	50	50	50	0
Plus	UWP-LICENCE-M01B	0	0	0	12
Plus	UWP-LICENCE-M02B	0	0	0	24
Plus	UWP-LICENCE-M04B	0	0	0	48
Plus	UWP-LICENCE-M05B	0	0	0	60
Plus	UWP-LICENCE-M25B	0	0	0	300

Standard licence

Standard licences are composed by annual resources, that are users, devices and sub-organizations.



When you activate a standard licence in a root organization, the relevant resources can be used for one year and the unused resources expire.

Notice: you cannot combine annual resources.

You can plan a renewal adding the licence you have already activated.

Example: you have activated a standard licence UWP-LICENCE-M10A that expires on 03/05/2021. You can buy and activate another UWP-LICENCE-M10A: doing so, your resources will expire on 03/05/2022.

When a standard licence expires:

- The resources activated the year before cannot be used.
- The unused resources expired.
- You have to buy and activate another licence code to avoid issues and disservices.

Plus licence

Plus licences are composed by resources for consumptions, that are months of VPN.

When you activate a Plus licence in a root organization, the relevant months of VPN are available for one year and unused months of VPN are added.

Note: you can combine resources for consumption.

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**).

When a Plus licence expires, unused months of VPN expire too.

How to register and create an organization

1. Open your browser
2. Go to MAIA Cloud login page: <https://app.maiacconnect.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.

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 31 > Organizations page.



MAIA Cloud browser

How to log in through a browser

1. Use a web browser to access MAIA Cloud (link [here](#))
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](#)), or if you log in to the "MAIA Cloud Connector desktop application" on [page 57](#), you can:

- access devices also through native application (e.g., UWP 3.0 Tool or UCS).
- use the remote devices through an IP address as if they were connected to the local network.

Home page

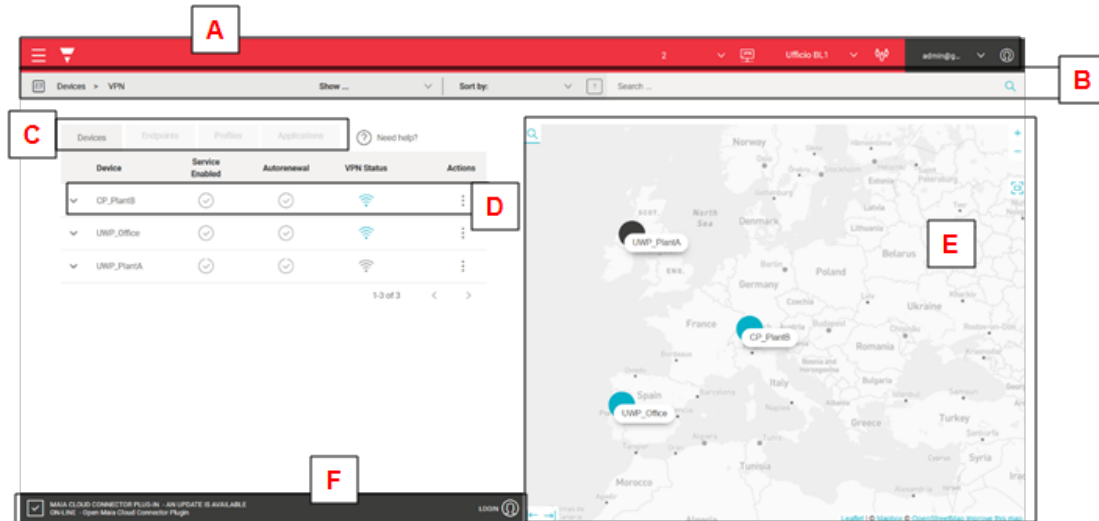
The home page is composed by the following elements:

- 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 43](#) > [IAM menu](#) > [Roles](#) > [Application roles](#) > [How to set up a direct access to favourite applications](#).





Element	Description
A	<p>Navigation bar, common to all the MAIA Cloud pages. It contains the following options:</p> <ul style="list-style-type: none">☰ opens the main menu <i>For further details, go to "Main menu" on the next page.</i>opens your organization resources details👤 represents your organization. If you click it, you can change the organization and the pages update according to the selection.👤 accesses your account details and options. <i>For further information, go to "Home page" on the previous page > How to manage the profile.</i>
B	<p>Secondary navigation bar. You can perform the following tasks:</p> <ul style="list-style-type: none">Filter the devices choosing the status (Show...)Sort by name the items in the listSearch an item.
C	<p>Devices, Endpoint, Profile and Applications tabs. <i>For further information, go to "Devices menu" on page 19.</i></p>
D	<p>The connection drop-down menu allows you to manage the devices VPN connection. <i>For further information, go to "Devices menu" on page 19 > VPN page > Devices > The Connection drop-down menu and side panel.</i></p>



Element	Description
E	<p>The connection map showing the location of your devices. You can perform the following tasks:</p> <ul style="list-style-type: none"> • Open the device action menu clicking on the relevant device. <i>For further information, go to "Devices menu" on page 19 > VPN page > Devices.</i> • Enter a connection address () • Zoom in or out with  or  • Zoom all with  to see all the devices in the map <p><i>When you type an address, the map enlarges on the selected connection place.</i></p>
F	<p>MAIA Cloud Connector Plug-in status bar allows you to manage the plug-in connection. <i>For further information, go to "Devices menu" on page 19 > VPN page > Devices > The Connection drop-down menu and side panel.</i></p>

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.
- **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.**

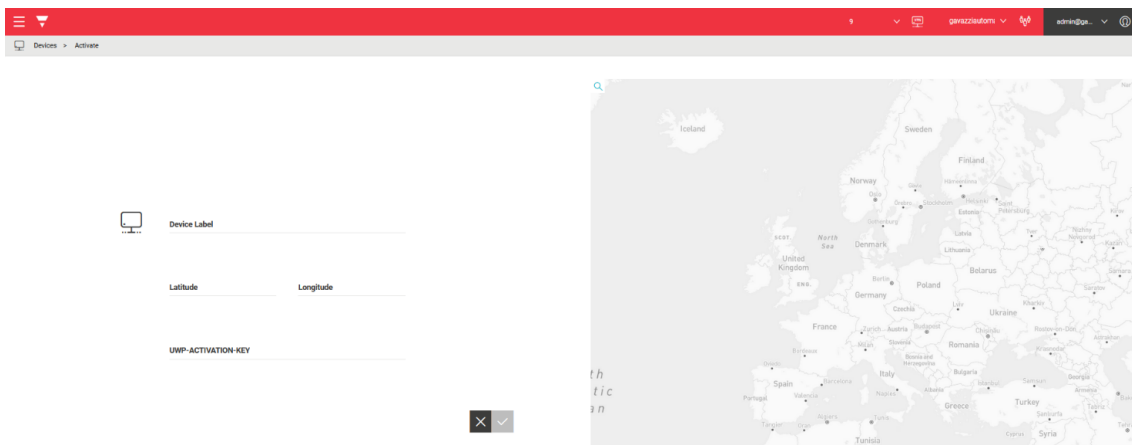
Activation page

 *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

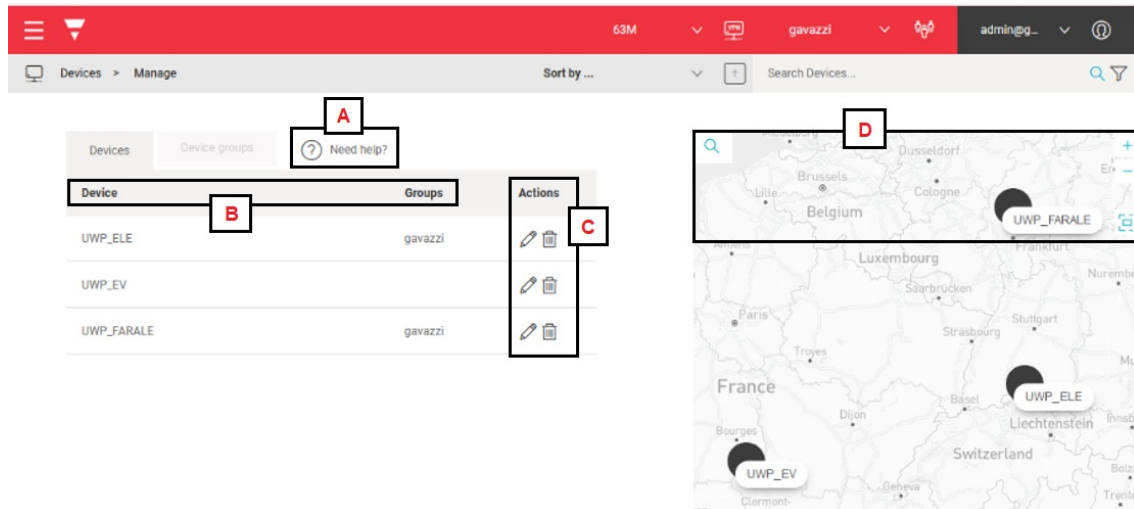
Devices > Manage page

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

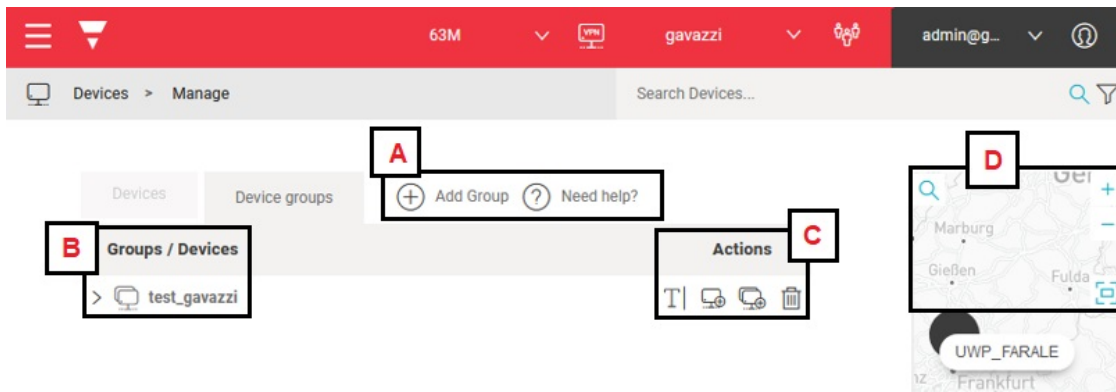


Element	Description
A	? Need help: opens the context help.
B	Devices information: device label and device Group. <i>For further information, go to "How to" on page 43> Devices menu > Manage > Device groups > How to add a device group</i>
C	Actions. You can edit () the device information or delete () a device. The edit button allows you to perform the following tasks: <ul style="list-style-type: none"> • See the device information, such as: <ul style="list-style-type: none"> ◦ Label of the device, set during the activation procedure. <i>Note: from this menu you can change the device label. The changes will be automatically saved after the VPN service reset.</i> ◦ ID, useful for the technical support team ◦ Activation code • Add the device in an existing Device Group (Add) • Change the location ()








Element	Description
D	<p>The connection map showing the location of your devices. You can perform the following tasks:</p> <ul style="list-style-type: none"> • Enter a connection address (🔍) • Zoom in or out (+ or -) • Zoom all (⌘ ↵) to see all the devices in the map <p><i>When you choose an address, the map enlarges on the selected area.</i></p>

Devices menu > Manage page > Device groups



Element	Description
A	<p>+ Add Group. <i>For further information. go to "How to" on page 43 > Devices menu > Manage > Device groups > How to add a device group.</i></p> <p>? Need help: opens the context help.</p>
B	Groups / Devices name. If you click > you can see the group members.
C	<p>Actions. You can perform the following tasks:.</p> <ul style="list-style-type: none"> • 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 <p><i>For further information. go to "How to" on page 43 > Devices menu > Manage > Device groups > How to add a device group.</i></p>



Element	Description
D	<p>The connection map showing the location of your devices. You can perform the following tasks:</p> <ul style="list-style-type: none">• Enter a connection address ()• Zoom in or out ( or )• Zoom all ( ) to see all the devices in the map <p><i>When you choose an address, the map enlarges on the selected area.</i></p>



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 Logs

The screenshot displays the VPN page interface. At the top, there are tabs for 'Devices', 'Endpoints', 'Profiles', and 'Applications', along with a 'Need help?' link. Below the tabs is a table with the following columns: 'Device', 'Service Enabled', 'Autorenewal', 'VPN Status', and 'Actions'. The table contains three rows of data:








Device	Service Enabled	Autorenewal	VPN Status	Actions
CP_PlantB	✓	✓	📶	⋮
UWP_Office2	✓	✓	📶 <small>RESET required</small>	⋮
UWP_PlantA	✓	✓	📶	⋮

Below the table, there is a pagination indicator '1-3 of 3'. To the right of the table is a map showing the locations of the devices. A context menu is open over the 'UWP_Office2' device on the map, listing the following actions: 'Applications', 'Connect', 'Disconnect', 'Reset the device VPN connection', 'Autorenewal' (with a toggle switch), and 'Logs'. At the bottom of the page, there is a status bar with a 'MAIA CLOUD CONNECTOR PLUG-IN ON-LINE - Open Maia Cloud Connector Plugin' indicator and a 'LOGIN' button.



Element	Description
---------	-------------

Device 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  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.

A

• **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 and endpoint 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.

Notes:


- *only administrator users in device roles can manage autorenewal and assign credits.*









Element	Description
B	Click  you open the Connection drop down-menu which allows you to manage the VPN connection. <i>For further information, go to "The Connection drop-down menu and side-panel" below</i>
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. <i>For further information, go to "The Connection drop-down menu and side-panel" below</i>
D	MAIA Cloud Connector plug-in status bar: allows you to check and manage the plug-in connection status. <i>For further information, go to "The MAIA Cloud Connector plug-in" below</i>

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**.

Endpoint	Application	Status
gateway connected - Disconnect Gateway Real IP: 127.0.0.1 Virtual IP: 192.18.0.84	CP3_WebApp_HTTP	
	CP3_WebApp_HTTPS	
UWP_OfficePlantB not connected - Connect Real IP: 10.1.5.120 Virtual IP: 100.64.0.161	UCS_7_HOME_PATH	Native App 
	UWP_Tool	Native App 
	WebApp_HTTP	
	WebApp_HTTPS	

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
- 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



[Here](#) you can download the MAIA Cloud Connector plug-in or directly from the status bar of the MAIA Cloud browser homepage.

Note: uninstall the MAIA Cloud Connector desktop application before installing the plug-in.

The **MAIA Cloud Connector plug-in** is a desktop application that allows you to access devices through native application (e.g., UWP 3.0 Tool 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.








If the bar is...	Then it means that...
Red	<p>the application is not working or you need to launch the MAIA Cloud plug-in.</p> <p>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.</p>
Black	<p>you are not connected ()</p> <p><i>Clicking Open MAIA Cloud Connector plug-in, you open the app. This way, you can access the app logs and change the path of the native applications.</i></p>
Blue	<p>you are connected and you can see the connected users.</p> <p><i>Clicking Open MAIA Cloud Connector plug-in, you open the app. This way, you can access the app logs and change the path of the native applications.</i></p>

Devices menu > VPN page > Endpoints

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

Device	Endpoint	Description	IP Address	Application profile	Enabled	Source NAT	Actions
UWP_Alessio	A						 
UWP_EV1							 
UWP_LUCSCO							 
	gateway		127.0.0.1	UWP3.0_Default_Profile	<input checked="" type="checkbox"/>	<input type="checkbox"/>	 
	mc		192.168.1.100	UWP3.0_Default_Profile	<input checked="" type="checkbox"/>	<input type="checkbox"/>	 
	XAP_ETH0		192.168.1.73	UWP3.0_Default_Profile	<input checked="" type="checkbox"/>	<input type="checkbox"/>	 
	XAP_ETH1		192.168.1.72	UWP3.0_Default_Profile	<input checked="" type="checkbox"/>	<input type="checkbox"/>	 



Element	Description
A	<p>Endpoints tab information:</p> <ul style="list-style-type: none"> •  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: <ul style="list-style-type: none"> ◦ Endpoint name ◦ Endpoint description ◦ Endpoint IP address <p><i>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</i></p> <ul style="list-style-type: none"> ◦ Application profile assigned to the endpoint. <p><i>For further information, go to "How to" on page 43 > Devices menu > VPN > Profiles > How to associate a profile to an endpoint.</i></p> <ul style="list-style-type: none"> ◦ Enabled. If the endpoint has been correctly added and activated, it appears checked. ◦ Source NAT. It allows you to use a real IP instead of a virtual IP (optional). <p><i>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.</i></p>
B	<p>Actions. It permits you to perform the following tasks:</p> <ul style="list-style-type: none"> • Edit gateway (). You can: <ul style="list-style-type: none"> ◦ 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. <p><i>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.</i></p> <ul style="list-style-type: none"> ◦ Set the Maximum number of endpoints available for the relevant gateway. <p><i>Note: 2 is the default value.</i></p> <ul style="list-style-type: none"> • Create an endpoint (). Click it to open the Endpoint Options menu. <p><i>For further information, go to How to add an endpoint.</i></p> <p>Click () to see the Endpoints Actions which allow you to edit () or delete () an endpoint.</p>

Devices menu > VPN page > Profiles

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



UWP 3.0 default profile is available and the following applications compose it:

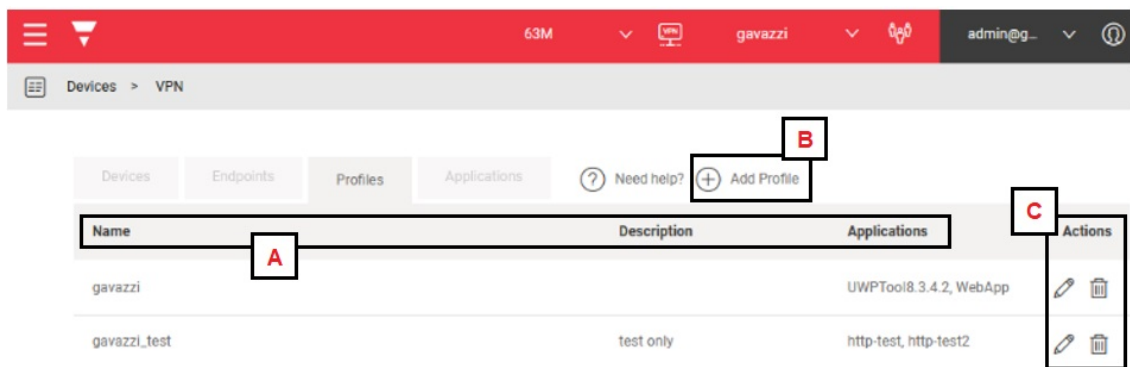
- UCS 7 Software
- UWP 3.0 Tool
- UWP 3.0 Web App
- SSH remote support (only for Carlo Gavazzi Support Team).




The CPY default profile is available and the following applications compose it:

- CP3 Web App
- SSH remote support (only for Carlo Gavazzi Support Team).

The UWP 3.0 and CPY default profiles are ready to be used: just add one of those profiles to your devices.

For further information, go to [Devices menu > VPN > Profiles > How to associate a profile to an endpoint for further details](#).



Element	Description
A	<p>Profiles information:</p> <ul style="list-style-type: none"> • Profile name • Profile description • Applications composing the profile. <p>For further information, go to "Devices menu > VPN page > Applications" below.</p>
B	<p>Profiles actions. Click  Add Profile to open the profile Options menu.</p> <p>For further information, go to Devices menu > VPN > Profiles > How to create a profile.</p>
C	<p>Actions. You can change the profile name and/or description and add/delete the applications composing the profile () or delete the profile (). <i>Note: if you delete a profile, the relevant applications are not removed.</i></p>

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
- UWP 3.0 Web App
- CP3 Web App
- 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	<ul style="list-style-type: none"> SSH HTTP HTTPS 	<ul style="list-style-type: none"> 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 "How to" on page 43 > 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 *UWP_Default_Profile* 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
Native application	UWP_Tool	Custom		10000:10002 80 443 52326
	UCS_7_PROGRAM_PATH	Custom (Bridge Modbus)		443, 41214 <i>Note: it can be changed by the user</i>
	UCS_7_HOME_PATH	Custom (Bridge Modbus)		443, 41214 <i>Note: it can be changed by the user</i>

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. <i>For more information, go to "How to" on page 43 > Devices menu > VPN > Applications > Placeholders > How to use Command path and argument for native applications.</i>



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:

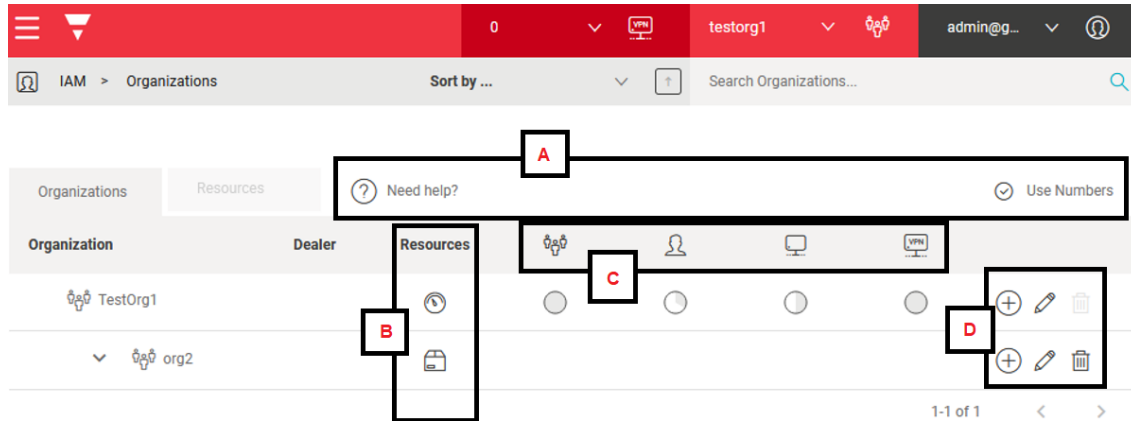
- **Organizations**. This section allows you to manage / add suborganizations and monitor / add suborganization resources.
- **Resources**. This tab allows you to check the available resources, the expired and scheduled licences and to add resources.
- **Consumptions**. This tab shows the consumption 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



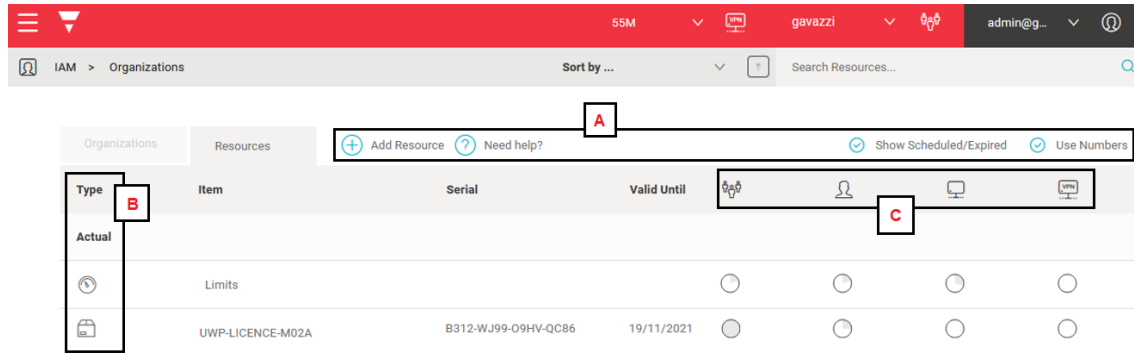
Element	Description
A	 Need help: opens the context help.  Use numbers. If you check it, you see the organization resources as number (used/total).
B	Resources. This column shows the following sub-organization type:  if the lives on own resources option is disabled, it means that this organization receives 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. <i>For further information, go to "How to" on page 43 > IAM menu > How to activate a licence and add resources to an organization.</i>



Element	Description
C	<p>The pie charts show the following resources (according to each licence availability):</p> <ul style="list-style-type: none">•  sub-organization•  user•  device•  VPN service <p><i>For further information, go to "MAIA Cloud licence types" on page 12 > Licence code.</i></p>
D	<p>Actions. You can perform the following tasks:</p> <ul style="list-style-type: none">• Click  to add a sub-organization <i>For further information, go to "How to" on page 43 > IAM menu > How to add a sub-organization.</i>• Click  to perform the following tasks:<ul style="list-style-type: none">• Change the organization label• Set a host name if it is not already set<p><i>Note: once set the host name, you cannot change it or disable it.</i></p><ul style="list-style-type: none">• Enable or disabled full privacy<p><i>Note: if full privacy is enabled, you allow user to set up full privacy preventing all other users (also administrators) to see them.</i></p><ul style="list-style-type: none">• Add resources to the relevant sub-organization.<p><i>For further information, go to "How to" on page 43 > IAM menu > How to activate a licence and add resources to an organization.</i></p>• 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	<p> Add resource. <i>For further information, go to "How to" on page 43 > IAM menu > How to activate a licence and add resources to an organization.</i></p> <p> Need help: opens the context help.</p> <p> Show Scheduled/Expired. If you check it, you see the scheduled and/or expired licences.</p> <p> Use numbers. If you check it, you see the organization resources as number (used/total).</p>
B	<p>Type. This column shows the following sub-organization types:</p> <p> if the lives on own resources option is disabled, it means that this organization receives the resources from the root organization.</p> <p> if the lives on own resources option is enabled, it means that in this organization the resources are added with UWP Licences. <i>For further information, go to "How to" on page 43 > IAM menu > How to activate a licence and add resources to an organization.</i></p>
C	<p>The pie charts show the following available resources for each licence:</p> <ul style="list-style-type: none"> sub-organization user device VPN service <p><i>For further information, go to "MAIA Cloud licence types" on page 12 > Licence code.</i></p>



IAM > Organizations > Consumptions

Date	Device	Type	
2021-03-11	UWP_EV1	VPN	1
2021-03-12	UWP_FARALE	VPN	1
2021-04-11	LDC_240	VPN	1
Total			3

Element	Description
A	From the secondary tab you can choose the time period to consider () or search a specific device name.
B	 Need help: opens the context help  Exports a csv file
C	The pie charts show the VPN months consumed by each device of your organization. <i>Note: this tab allows you to also check the consumption of devices which has been deleted.</i>



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.

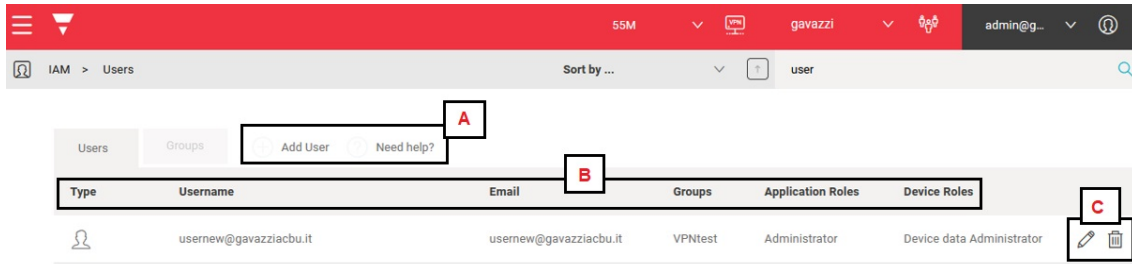
Note: you can change your reference organization clicking






from the navigation bar. The Users page is updated according to the selected organization.



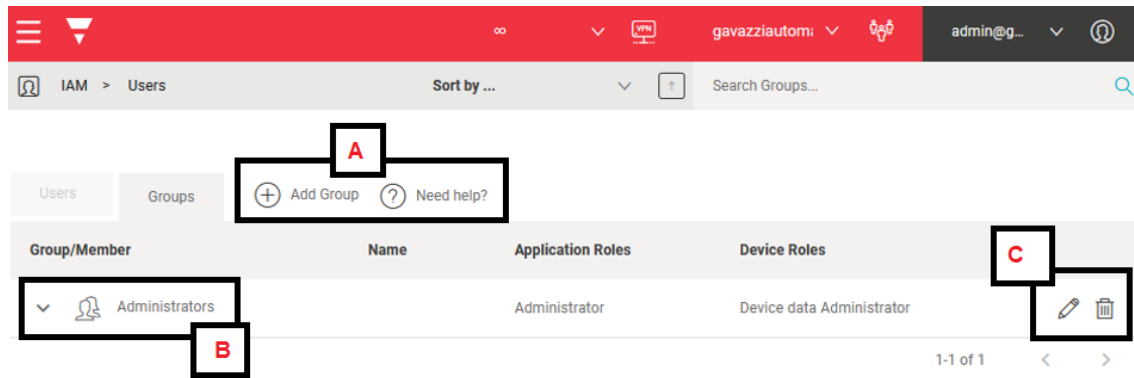
IAM > Users > Users








Element	Description
<p>A</p>	<p>+ Add user. If you click it, you are redirected to the Options page. <i>For further information, go to "How to" on page 43> IAM menu > How to add a user</i></p> <p>? Need help: opens the context help.</p>
<p>B</p>	<p>Information about users:</p> <ul style="list-style-type: none"> • Type • Username • Email • Organization • Group (see user groups for further details) • User roles for specific fields (Application, VPN)
<p>C</p>	<p>Actions.  (edit) and  (delete).</p> <p> permits you to perform the following tasks:</p> <ul style="list-style-type: none"> • See user information (username, E-mail) • Add user to a group or change them (Group membership) <i>Go to User groups for further details</i> • Set or change user permissions (Application roles and Device roles) <i>Go to Roles page for further details</i> <i>Note: you can add more than one permission to the same user.</i> • 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. <i>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.</i>



IAM > Users > User groups



Element	Description
A	<p> Add Group. For further information, go to "How to" on page 43> IAM menu > How to add a user group</p> <p> Need help: opens the context help.</p>
B	<p>User groups information:</p> <ul style="list-style-type: none">• User group name• Application roles• Devices roles <p>If you click  , you can see the group members.</p>
C	<p>Actions. You can change and/or add roles and add/delete user members () or delete ()</p>



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.
 - lam.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.



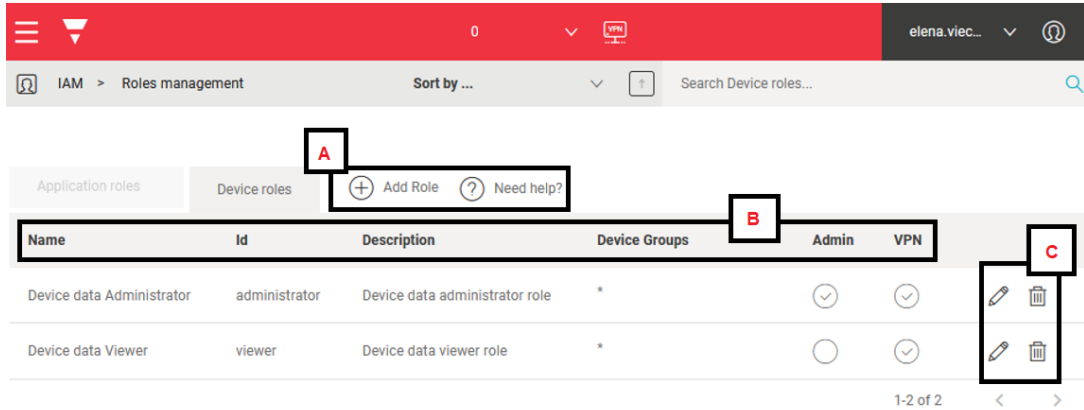
IAM > Roles > Application roles



Name	Id	Description	
Administrator	administrator	Administrator role	
Viewer	viewer	Viewer role	
Editor	editor	Editor role	

Element	Description
A	<p>+ Add roles. If you click it, you are redirected to the relevant Options page. <i>For further details, go to "How to" on page 43 > IAM menu > How to add an application role.</i></p> <p>? Need help: opens the context help.</p>
B	<p>Role information:</p> <ul style="list-style-type: none">• Role Name (administrator, viewer and editor are the standard roles)• Role ID• Description
C	<p>Actions. You can change the role name, description and permission () or delete ()</p>



IAM > Roles > Device roles



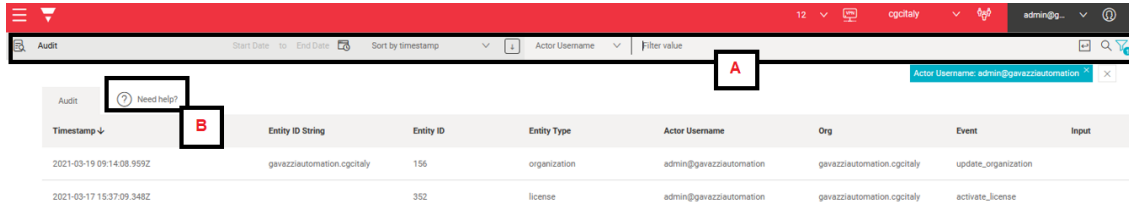
Element	Description
A	<p>+ Add roles. If you click Add roles you are redirected to the relevant Options page. For further details, go to "How to" on page 43 > IAM menu > How to add a device role.</p> <p>? Need help: opens the context help.</p>
B	<p>Role information:</p> <ul style="list-style-type: none"> • Role Name <i>Note: administrator is the default role.</i> • 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. <i>Note: a regular user in "Devices menu" on page 19 > VPN page cannot assign credits to devices or enable/disable the auto renewal.</i> • VPN: if you check it, you enable the VPN access.
C	<p>Actions. You can change the role name, description and the role permission () or delete ().</p>





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	<p>From the secondary tab you can:</p> <ul style="list-style-type: none"> 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	<p>? Need help: opens the context help.</p>




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


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 <i>For further information, go to "How to activate a licence and add resources to an organization" on the facing page</i>

 **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	<ol style="list-style-type: none"> 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 <p><i>This way, the root organization resources go to the sub-organization.</i></p>
Enabled	<ol style="list-style-type: none"> 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 <p><i>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.</i></p> <ol style="list-style-type: none"> 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 page 46




9. Click  to add user to your organization



For more information about user roles, go to **"IAM menu" on page 31 > 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	<ol style="list-style-type: none"> 8. Disable the Access only favourite applications option 9. Choose the permissions from the list
Only the favourite applications	<ol style="list-style-type: none"> 8. Enable the Access only favourite applications option 9. Check the <i>iam.device.read</i> 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.maiacconnect.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 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 VPN service for an installed UWP 3.0
If you want to use the SBP2CPY24 version...	Then...
2.6.3 onwards	In few seconds the device will be online
2.6.3 backwards	go to How to enable VPN service for an installed SBP2CPY24


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" above.
2. Update your UWP 3.0
Note: the VPN service is available for the UWP 3.0 Tool 8.4.0.3 onwards.
3. Log in to the UWP 3.0 web app
4. Open the main menu ()
5. Go to **Service > Remote VPN Services**



6. Enable the service
7. Write the activation code of your UWP-ACTIVATION-KEY kit
Note: check that the Standard MAIA Cloud Server has been set.
8. Click  to save
Note: the green icon informs you that the procedure is successfully finished.


How to enable the VPN service for an installed SBP2CPY24



1. Go to your MAIA Cloud organization and activate your SBP2CPY24
*For further information, go to "**How to activate a Device**" on the previous page.*
 2. Update your SBP2CPY24
Note: the VPN service is available for the SBP2CPY24 2.6.3 onwards.
 3. Log in to the CPY server
 4. Go to **System settings > VPN settings**
 5. Enable the service
 6. Write the activation code of your UWP-ACTIVATION-KEY kit
Note: check that the Standard MAIA Cloud Server has been set.
 7. Click  to save
Note: the green icon informs you that the operation completed successfully.
-



 **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. Log in to your MAIA Cloud ([click here](#))
2. Open the home page or open the **main menu** and go to **Devices > VPN**



3. If you want to...	Then...
<p>Use a predefined application to create a VPN tunnel to the gateway</p>	<p>You can</p> <p></p> <p>a. Click  to open the Connection drop-down menu of the device</p> <p>or</p> <p>b. Click on the device you want to connect in the map and click Applications to open the Connection side panel</p> <p>After that, click one of the available applications.</p> <p>If the connection is correctly established, the status icon becomes green</p>
<p>open all the ports of the application which composed the device and endpoint profile</p>	<p>You can</p> <p>a. Click  of the device > Connect from the action menu</p> <p>Or</p> <p>b. Click  to open the Connection drop-down menu of the device and click Connect</p> <p>Or</p> <p>c. Click on the device you want to connect in the map and click Connect</p> <p>After that, you can enter the Virtual IP address that you find in the Connection drop-down menu or side panel, in your browser or in your application.</p>
<p>Disconnect from the endpoints/gateway</p>	<p>You can</p> <p>a. Click  > Disconnect from the Action menu of the device</p> <p>Or</p> <p>b. Click  to open the Connection drop-down menu of the device and click Disconnect</p> <p>Or</p> <p>c. Click on the device you want to connect in the map and click Disconnect</p>

Notes:



- *to set up a VPN tunnel using a native application you need to be logged in with the MAIA Cloud Connector plug-in*
- *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. You can check if someone else is connected to the device from the **VPN portal (Status column)**.*



- 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.
- For further information, go to "**How to set a direct access to favourite applications** " on page 46.


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.

Note: after this procedure, you have to reset the VPN service.


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.**

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 drop-down 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 (<i>Secure Shell Connection</i>) application	<ol style="list-style-type: none"> 8. Select the Protocol type and the Port number from the Applications tab 9. Choose the options from the Advanced parameters tab (not mandatory)
<ul style="list-style-type: none"> • HTTP <i>Web interface in a browser</i> • HTTPS <i>Web interface over a secured connection in a browser</i> 	<ol style="list-style-type: none"> 8. Select the Protocol type and the Port number 9. Fill in the URL to open. <p><i>For further information, go to Devices menu > VPN page > Applications > Place holders</i></p>
a CUSTOM application	<p>From the Application tab select:</p> <ul style="list-style-type: none"> • Protocol type • Port number • Command path and arguments <p><i>For further information, go to Devices menu > VPN page > Applications > Place holders and "How to use Command path and argument for native applications" on the next page.</i></p> <p><i>Note: from the Advance parameters tab, you can set other custom parameters (not required).</i></p>

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.

If you are using...	Description
MAIA Cloud Connector plug-in	<ol style="list-style-type: none"> 1. Use a web browser to access MAIA Cloud (click here) 2. Log in to MAIA Cloud Connector Plug-in <i>For further information, go to "Devices menu" on page 19 > VPN page > Devices > MAIA Cloud Connector plug-in</i> 3. Open the Apps tab <p><i>Go to step 5</i></p>
MAIA Cloud Connector desktop application <i>Note: the desktop application has been discontinued since the launch of MAIA Cloud Connector plug-in.</i>	<ol style="list-style-type: none"> 1. Log in to MAIA Cloud Connector desktop application <i>For further information, go to "MAIA Cloud Connector desktop application" on page 57</i> 2. Open your PC system tray <i>Note: the system tray, called the Notification area, is generally on the right side of the task bar.</i> 3. Right click on MAIA status icon  4. Go to Server settings > Applications tab

5.



If want to...	Then...
Change only one application path	<ol style="list-style-type: none"><li data-bbox="821 212 1469 280">6. Choose one of the available native applications from the list<li data-bbox="821 297 1469 380">7. Click Reset selected <i>Go to step 8</i>
Change all the application paths	<ol style="list-style-type: none"><li data-bbox="821 398 1469 432">6. Click Reset all<li data-bbox="188 479 1469 512">8. Click OK to reset the path of the chosen application and close the window<li data-bbox="188 528 1469 562">9. Go back to MAIA Cloud and set up a VPN connection through the native application you need to upload<li data-bbox="188 577 1469 611">10. Set the new path which is automatically saved




MAIA Cloud Connector desktop application

 The **MAIA Cloud Connector desktop application** has been discontinued since the launch of **MAIA Cloud Connector plug-in**.

How to log in to the MAIA Cloud Connector desktop app

 You can log in to the **MAIA Cloud Connector desktop application** if you have been added to a MAIA organization by an administrator and if you register your user as the administrator of a MAIA organization.

1. **Download** and install the **MAIA Cloud Connector desktop application**
2. Enter your credentials

Click  to modify your credentials.

1. Click **Ok**

Your credentials are saved for the next login.

2. Click **Sign in**.
3. Create a new password and click submit

Only for the first login.

4. 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.

If you want to log in with another account, click  from the **Login** page, click  and enter your credentials.

Desktop application tabs

 You can download the **MAIA Cloud Connector desktop application** clicking [here](#)

Note: as an alternative to the **MAIA Cloud Connector desktop application**, you can decide to install the **MAIA Cloud Connector plug-in**, which allows you to perform the same functions using just a browser.

The **MAIA Cloud Connector desktop application** allows you to perform the following tasks:

- Log in with different users belonging to different organizations
- Show / Hide the connections
- Filter the connection viewing
- Open the gateway details pop up and set up the VPN remote connection both through built-in and native applications
- See the device on a map
- Set and/or delete a path which automatically opens a native application

For further information, go to "**Gateway details pop-up**" on the facing page.

Two tabs compose it: **Dashboard** and **Map**.

Dashboard (connections) tab

This tab allows you to perform the following tasks:



- Show / Hide the connections
- Filter the connection viewing
- Open the gateway details pop up and set up the VPN remote connection

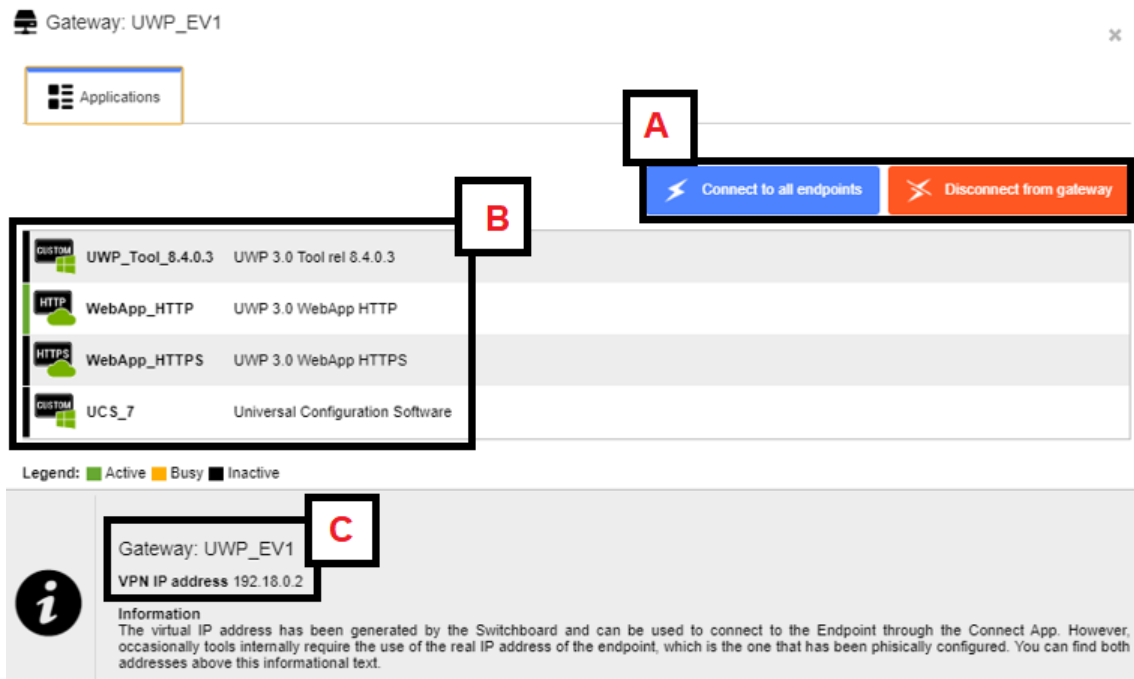
For further information about how to set up the tunnelling, go to **MAIA Cloud browser > "How to" on page 43 > Devices menu > How to connect to gateway/endpoints (VPN tunnel).**



Element	Description
A	General information about the users' gateways and endpoints available in the organization.
B	<p>Connection list of all your available devices. You can perform the following tasks:</p> <ul style="list-style-type: none"> • View the desired connections (All, Online, Offline, Connected, In-use, Busy). • Show / hide endpoints. • Filter. • See connection information (device, organization, groups, description, status). <p><i>Click one of the available devices to open the gateway details pop-up and set the VPN connection up.</i></p> <p><i>For further information, go to "Gateway details pop-up" below.</i></p>
C	Legend

Gateway details pop-up

If you click one of the available gateways in the dashboard, the following pop-up opens.



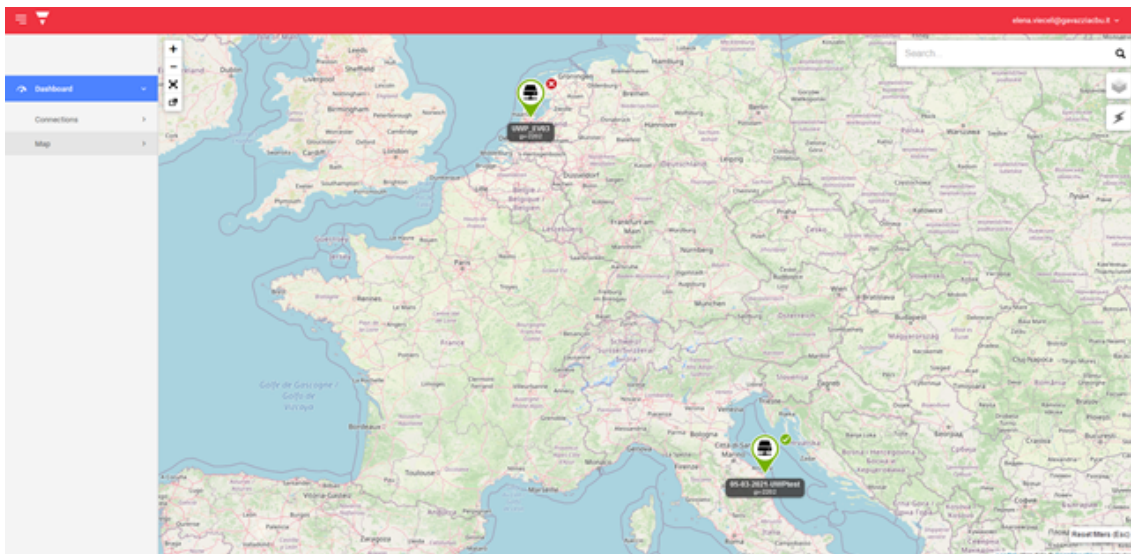


Element	Description
A	You can Connect/disconnect to all endpoints or Connect/disconnect from gateway <i>Note: when you click Connect, the colours change and become Disconnected.</i>
B	The applications that you can use to set a remote connection up. <i>For further information, go to MAIA Cloud browser > "Devices menu" on page 19 > VPN page > Applications.</i> The applications classes are Built-In Application and Native Application . <i>Note: when you use a native application for the first time you need to define the path to automatically launch the relevant program. This path is automatically saved; if you need to change a Native application path, go to MAIA Cloud browser > "How to" on page 43 > Devices menu > How to change a native applications path</i>
C	Additional gateway information: <ul style="list-style-type: none">• Label• Organization• Virtual Private Network IP address

Map tab

The **Map** tab shows the location of your devices and allows you to perform the following tasks:

- See devices information (name, organization, status, location).
- Search devices.
- Filter devices by to their organization/group.
- Filter devices by their status (online/offline).
- Connect/disconnect to devices.





Legal notice

 [MAIA Cloud - Terms and conditions \(multilingual\)](#)

 [MAIA Cloud - Privacy Policy \(multilingual\)](#)



Download

 [MAIA Cloud Connector Plug-in](#)