



# MAIA cloud system

---

## **USER MANUAL**

April 21

Document revision: 2.0

---

# Contents

---

<b>Introduction to MAIA Cloud system .....</b>	<b>3</b>
<i>Scope .....</i>	4
<i>Description.....</i>	4
MAIA system elements .....	4
Ports used by MAIA Cloud .....	4
MAIA Cloud components .....	5
MAIA Cloud architecture .....	7
Benefits.....	8
EDGE + PaaS solution value.....	8
<b>MAIA Cloud interface.....</b>	<b>9</b>
Introduction.....	9
What are organizations.....	10
Use case 1 .....	11
Use case 2 .....	12
MAIA Cloud licence types .....	13
Activation code .....	14
Licence code.....	16
How to check your organization’s resources .....	17
Browser vs desktop.....	18
How to log in via browser or desktop .....	19
How to manage the profile .....	20
MAIA Cloud interface tabs .....	21
<b>Legal notice.....</b>	<b>66</b>
<b>Download.....</b>	<b>67</b>

## Introduction to MAIA Cloud system

---

This manual describes the MAIA Cloud system, a service solution that allows to remotely manage different remote devices connected to a UWP 3.0 Edge unit. MAIA Cloud is a software platform designed for connecting users and machines through global networks like the Internet. MAIA Cloud includes all is needed for central supervision of energy monitoring and building automation installations, offering the best platform for teleservice and telecontrol.

## Scope

MAIA Cloud is a PaaS (*Platform as a Service*) solution that allows a seamless connection of different remote devices through UWP 3.0 gateways, so to develop the necessary energy management and building automation solutions by connecting and setting the relevant items. Users who have access to the MAIA Cloud can easily reach the gateways and the endpoints, provided they have the necessary access rights, using a PC application called **MAIA Cloud Connector**.

## Description

MAIA system elements	
Element	Description
<b>MAIA Cloud</b>	The heart of the whole infrastructure. It stores all the configuration data, the log files, the access policies, and keeps track of 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.
<b>MAIA Cloud Connector</b>	A user-friendly application for the supervision of installations controlled or monitored by UWP 3.0. Thanks to this application, users and maintainers can connect to remote machines. MAIA Cloud App has been designed for Windows® platforms. Operating system requirements: Windows 7 (updated version).

## Ports used by MAIA Cloud

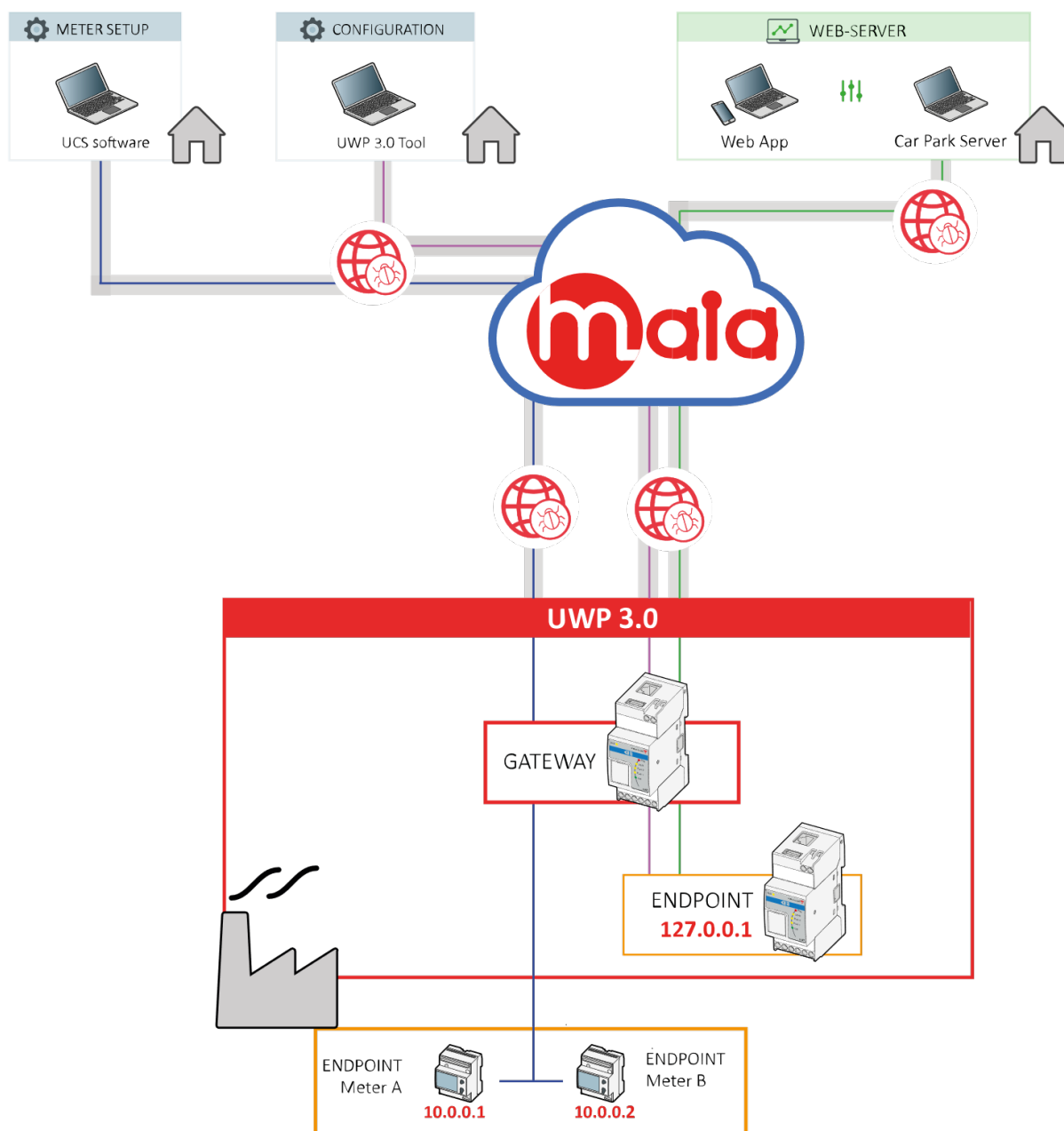
Access	Port
MAIA Cloud (browser)	port 443/TCP and 1194/udp
MAIA Cloud Connector (desktop software)	port 443/TCP and 1194/udp

## MAIA Cloud components

Element	Description
<b>Node</b>	Any object or user that is part of the <i>MAIA Cloud architecture</i> .
<b>Device</b>	Any gateway or endpoint managed by MAIA Cloud.
<b>Gateway</b>	<p>A door through which MAIA Cloud can reach endpoints. This virtual network can be expanded if necessary.</p> <p><i>The Carlo Gavazzi UWP 3.0 is a gateway.</i></p>
<b>Endpoint</b>	<p>Any device with the following features:</p> <ul style="list-style-type: none"> <li>• It can connect via a network.</li> <li>• It has its own IP address (unique).</li> </ul> <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"> <li>• It may connect to local network and/or to the Internet by means of a gateway</li> <li>• It can be connected to one gateway only.</li> </ul> <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>
<b>User</b>	<p>Users can access and interact with MAIA Cloud, a gateway, or an endpoint according to their role.</p> <p><i>Note: user who registers the root organization is called owner.</i></p> <p><i>The administrator defines the organization roles and assign roles to users (go to <b>Roles page</b> for further details).</i></p>
<b>Applications</b>	<p>Means to connect to an endpoint.</p> <p>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).</p> <p><i>You can group different applications in an application <b>profile</b>.</i></p> <p><i>Each endpoint has an application profile that defines all the available and admitted connections.</i></p>

Element	Description
<b>Organization (or domain)</b>	<p>A collection of users, devices and applications arranged into groups.</p> <p>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., <b>Root organization &gt; Children &gt; Descendants</b>). 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"> <li>• create and manage multiple domains within the same MAIA Cloud installation.</li> <li>• split a large enterprise into smaller departments independently managed within a single MAIA Cloud domain.</li> <li>• put a device or a user in the right group and give the device access to the right user.</li> <li>• create a suborganization invisible also to the root organization with full privacy option.</li> </ul> <p><i>The organization structure is up to the owner of MAIA Cloud.</i></p>
<b>Resources</b>	<p>Users, devices, suborganizations and month of VPN are resources which composed the organization.</p>

# MAIA Cloud architecture



UWP 3.0 is a gateway that, in a remote connection, acts as an end-point providing the IP address of the local host.

The applications permitting a remote connection and compatible to UWP 3.0 are the following:

- UWP 3.0 Tool (configuration software)
- UWP 3.0 Web App (web interface allowing the viewing / exporting of data, control of automation functions and definition of settings)
- UWP 3.0 Car Park Server (for setting up the system and for monitoring the installation).

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

# Benefits

## 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 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 Cloud interface

---

## Introduction

You can access our MAIA Cloud system through the **MAIA Connect web portal** (browser) or **MAIA Cloud Connector** (desktop).

*For further information, go to **Browser vs desktop**.*

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
- Suborganizations
- Months of VPN

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

*For further information, go to **How to register and create an organization** and **What are organizations**.*

# What are organizations

MAIA Cloud organizations are composed by:

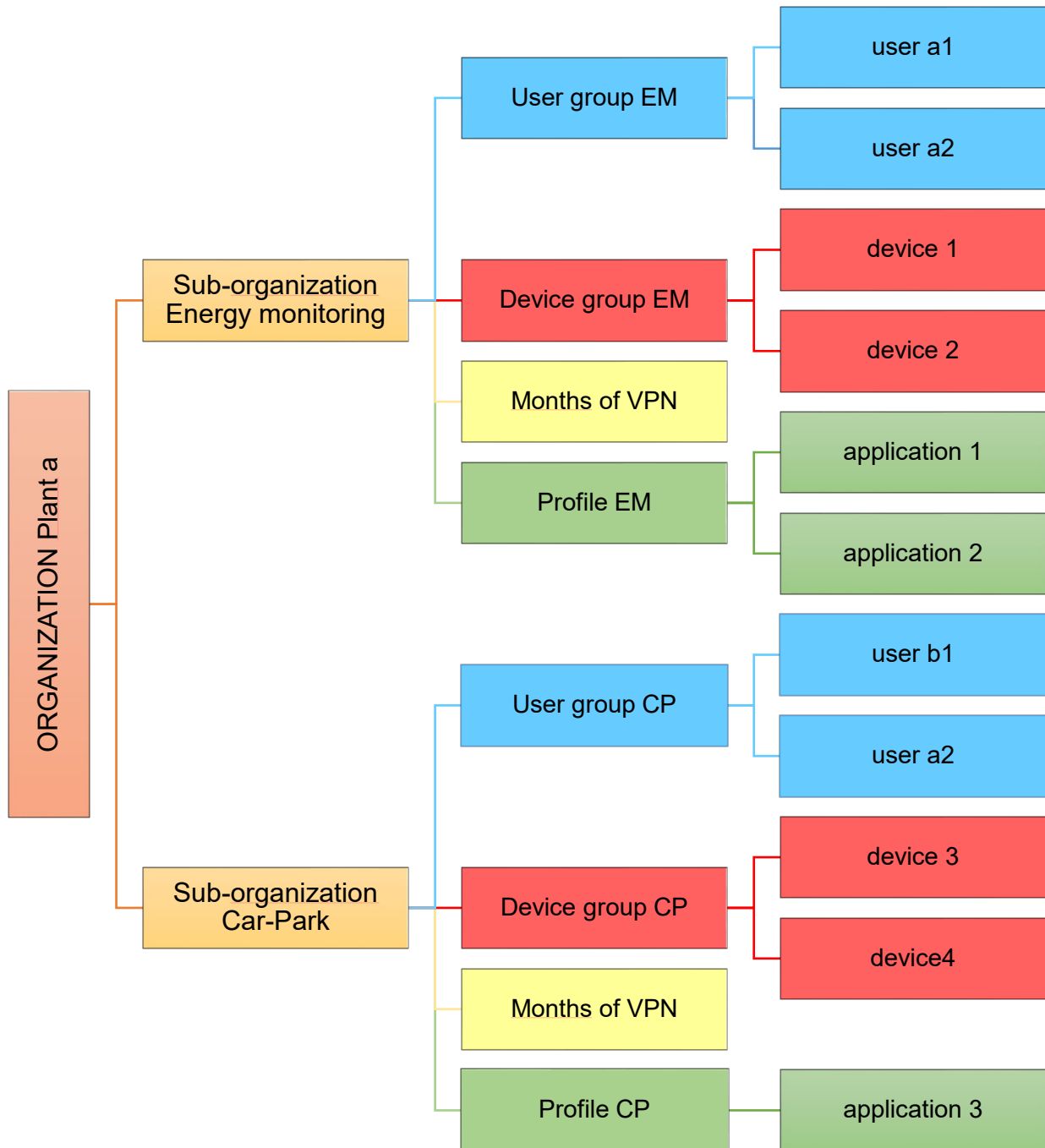
- **Users** that can be aggregated into user groups and connect remotely to a device through applications.
- **Devices** that can be aggregated into device groups.
- **Applications** grouped into profiles.
- **Months of VPN** consumed by devices

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

*For further information, go to **Use case 1** and **Use case 2**.*

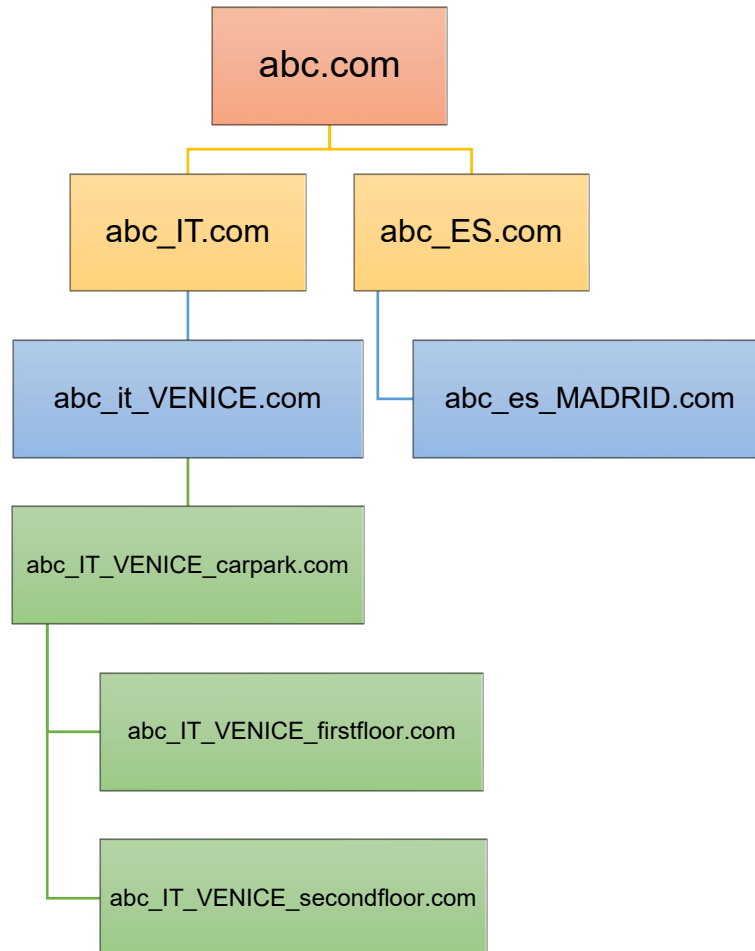
# Use case 1

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 suborganizations. In this case, one sub-organization is for the energy monitoring and the other is for the car park management.



## Use case 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.



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 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**.*

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

*For further details, go to **Licence code**.*

## Activation code

The activation code is included in our **UWP-ACTIVATION-KEY** kit.

Users have to use this code to register on MAIA Cloud.

*For further information, go to **How to register and create an organization**.*

Moreover, the activation code allows user to activate a UWP 3.0 device in MAIA Cloud.

*For further information, go to **How to activate a Device**.*

### 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 UWP 3.0.*

## 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 ID for Registration** (the Carlo Gavazzi activation key included in your UWP-ACTIVATION-KEY kit)
  - **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

You can now access the MAIA Cloud portal with your credentials.

### Notes:

- *After the first login, you can access your organization also through the desktop application MAIA Cloud Connector (for further details, go to **Browser vs desktop**).*
- *Your user is automatically register as Admin of the organization named after your company.*
- *The **Activation key** can be used once to register on MAIA Cloud. Use the same key to add the device to your organization. For further details, go to **How to activate a Device**.*

## 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 add resources to root organization**.*

After the registration (go to **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 suborganizations.

When you activate a standard license 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 (VPN page)**), 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 details, go to **VPN page**).

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

## How to check your organization's resources

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

*For further details, go to **Organizations page**.*

# Browser vs desktop

You can access your gateways and endpoints through the **MAIA Cloud (browser)** or the **MAIA Cloud Connector (desktop)**.

*Note: for MAIA Cloud you only need an Internet browser. You don't need to install any additional applications.*

Through the **browser** access, you can configure the entire environment (**Organizations, Users, Devices and Applications**), monitor the endpoints through the **Dashboard** page (go to **MAIA Cloud** interface tabs) and manage organization's resources.

*Note: If you use the browser, you can access UWP 3.0 only through the built-in applications (such as SSH, HTTP, HTTPS).*

*For further information, go to **Applications**.*

Through the **desktop** access, you can create a VPN network and use the remote devices through an IP address as if they were connected to the local network. Moreover, you can use both built-in and local applications (e.g., UWP 3.0 Tool or UCS Software). With the desktop version, you can see only the devices activated from the MAIA Cloud portal.

*The MAIA Cloud and MAIA Cloud Connector have the same function and the same **VPN portal** page. For further details, go to **VPN portal**.*

		Browser	Desktop
<b>Login requirements</b>		Internet browser	MAIA Cloud Connector installed
<b>Perform the first login</b>		V	X
<b>Register into Maia Cloud</b>		V	X
<b>Manage personal account</b>		V	X
<b>Activate devices</b>		V	X
<b>Manage organizations</b>		V	X
<b>VPN Remote access</b>	<b>built-in applications</b>	V	V
	<b>local applications</b>	X	V

## How to log in via browser or desktop

If you have been added to a MAIA organization by an administrator user, follow this procedure to log in:

If you access through...	Then....
<b>Browser</b>	<ol style="list-style-type: none"> <li>1. Use a web browser to access MAIA Cloud (link <a href="#">here</a>)</li> <li>2. Enter the credentials <i>You can click  to modify your credentials.</i></li> <li>3. Sign in.</li> </ol>
<b>Desktop</b>	<ol style="list-style-type: none"> <li>1. Download (link <a href="#">here</a>) and install the MAIA Cloud Connector</li> <li>2. Enter your credentials</li> <li>3. Click <b>Ok</b> <i>Your credentials are saved for the next login.</i></li> <li>4. Click <b>Sign in</b>. <i>If you want to log in with another account, click  from the <b>Login</b> page and enter your credentials.</i></li> </ol>


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.*

## How to manage the profile

1. Go to the MAIA Connect **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** menu and click*



## MAIA Cloud interface tabs

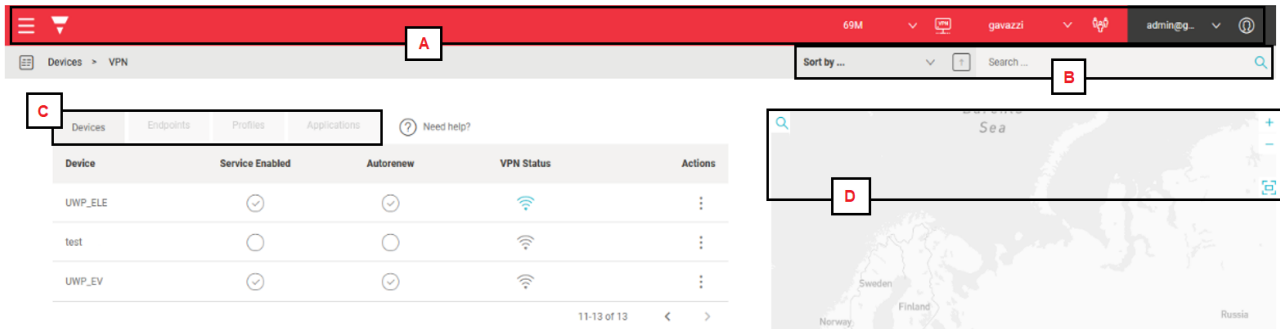
### Home page: dashboard tab




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 set up a direct access to favourite applications***.



Element	Description
A	<p><b>Navigation bar</b>, common to all the MAIA Cloud pages. It contains the following options:</p> <ul style="list-style-type: none"> <li>☰ opens the <b>main menu</b></li> </ul> <p><i>For further details, go to <b>Main menu</b>.</i></p> <ul style="list-style-type: none"> <li> opens your organization resources details</li> <li> represents your organization. If you click it, you can change the organization and the pages update according the selection.</li> <li> accesses your account details and options.</li> </ul> <p><i>For further information, go to <b>How to manage the profile</b>.</i></p>
B	<p><b>Secondary navigation bar</b>. You can <b>Sort</b> the items in the list and <b>Search</b> an item.</p>
C	<p>Information about <b>Devices</b>, <b>Endpoint</b>, <b>Profile</b> and <b>Applications</b> tabs.</p> <p><i>For further information, go to <b>Devices (VPN page)</b>.</i></p>
D	<p>The connection <b>map</b> showing the location of your devices. You can perform the following tasks:</p> <ul style="list-style-type: none"> <li>Enter a connection address (🔍)</li> <li>Zoom in or out with <b>+</b> or <b>-</b></li> <li><b>Zoom all</b> with <b>[📄]</b> to see all the devices in the map</li> </ul> <p><i>When you type an address, the map enlarges on the selected connection place.</i></p>

## Main menu

1. From the **Main menu** you can manage your organization.

The main menu is composed by the following elements:

- **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 submenus:
  - **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 submenus:
  - **Organizations.** It permits you to manage your organization and add suborganizations, 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 web help.

2. *Note: if you select a submenu, you open the relevant **Options** page.*

## Devices menu

### Introduction

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


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

Each submenu has its **Options** page.

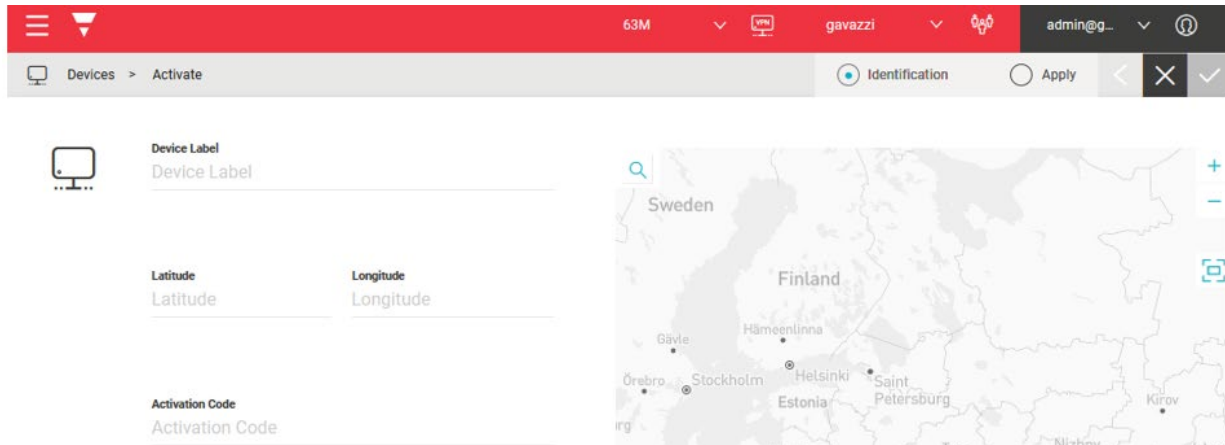


## Activation page

### Description

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.*






### How to activate a Device

1. Open the **main menu**
2. Go to **Devices > Activate**
3. Enter the following device information in the **Activation** page:
  - **Device Label:** the device name
  - **Latitude** and **longitude** for the geolocation

*Note: you can navigate the map or search a specific geolocation.*

- **Activation Code:** enter a valid UWP activation code

*For further information, go to **Activation code**.*

4. Click 
5. From the **Apply** page, you can check the device information.
6. Click  to activate the device.
7. Open the **main menu**
8. Go to **Devices > VPN**
9. Click  > **Assign credit** to enable the VPN service for your UWP 3.0

*Notice: for the installed UWP 3.0 device, after the activation you have to enable the service into the UWP 3.0 web app.*

*For further information, go to **How to enable VPN service for UWP 3.0**.*


## How to enable VPN service for 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**.*

2. Update your UWP 3.0.

*Note: the VPN service is available in the UWP 3.0 Tool 8.4.0.3 onwards.*

3. Log into the UWP 3.0 web app
4. Click  to open the **main menu**
5. Go to **Service > Remote VPN Services**
6. Enable the service
7. Enter the **activation code** included in your UWP-ACTIVATION-KEY kit

*Note: please be sure to set **Standard Maia Cloud Server**.*

8. Click  to save.


*Note: when the status icon is green, the procedure is successfully finished.*

## Manage page

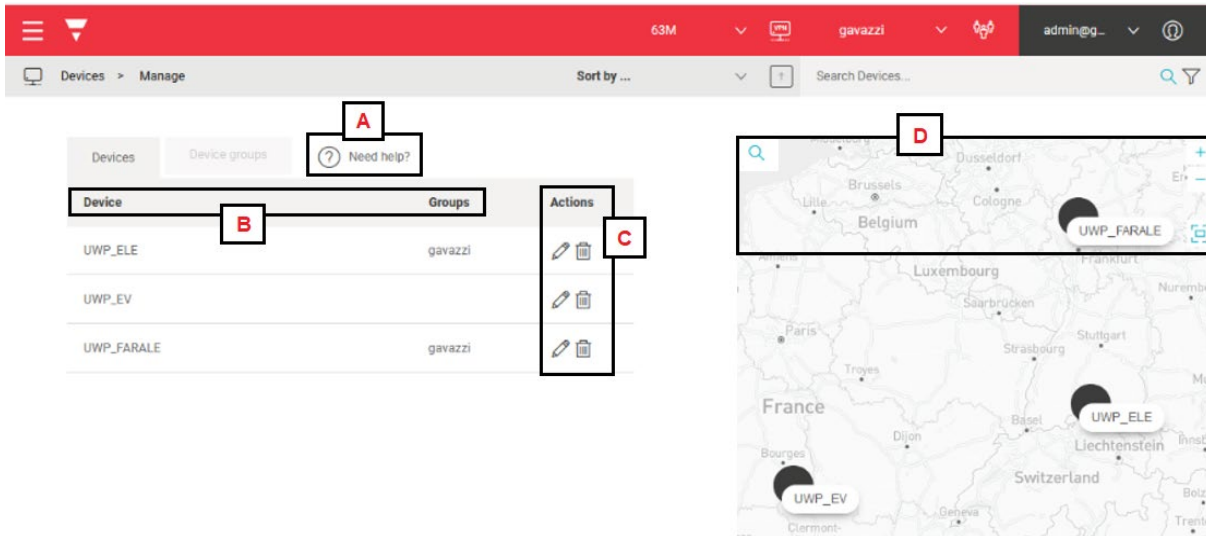
### Description

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

Two tabs compose it: **Devices** and **Device Groups**.

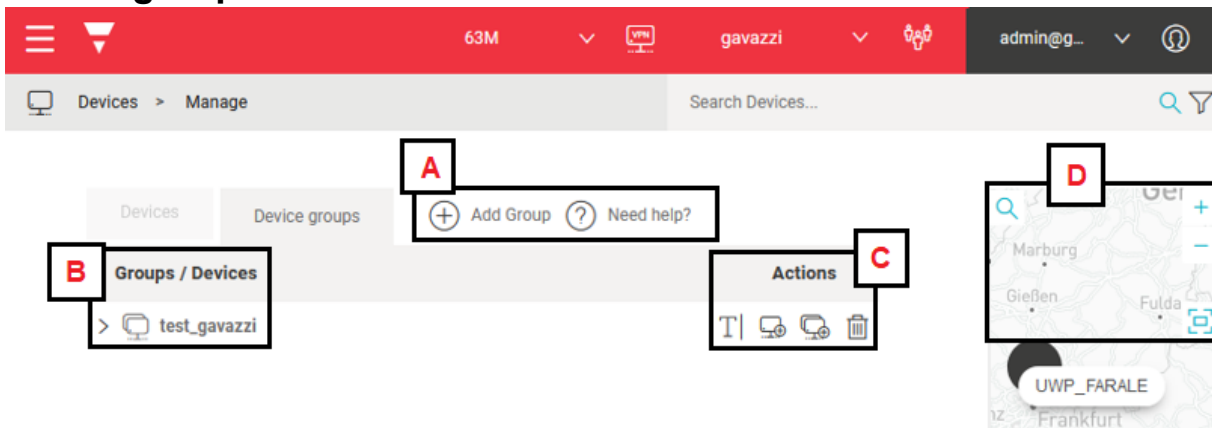
*You can change your reference organization clicking  from the navigation bar. The **Manage** page is updated according to the selected organization.*

## Devices (manage page tab)




Element	Description
A	<b>? Need help:</b> opens the context help.
B	<b>Devices information: device label and device Group.</b> <i>For further information, go to <b>How to add a device group</b>.</i>
C	<b>Actions.</b> You can edit (✎) the device information or delete (🗑️) a device. The edit button allows you to: <ul style="list-style-type: none"> <li>• See the following device information <ul style="list-style-type: none"> <li>○ Label of the device, set during the activation procedure. <i>Note: if you want to change the device label, you have to disable the VPN service from the UWP 3.0 Web App.</i></li> <li>○ ID, useful for the technical support team</li> <li>○ Activation code</li> </ul> </li> <li>• Add the device in an existing Device Group (<b>Add</b>)</li> <li>• Change the geolocation (📍)</li> </ul>
D	The connection <b>map</b> showing the location of your devices. You can perform the following tasks: <ul style="list-style-type: none"> <li>• Enter a connection address (🔍)</li> <li>• Zoom in or out (+ or -)</li> <li>• Zoom all (📏) to see all the devices in the map</li> </ul> <i>When you choose an address, the map enlarges on the selected area.</i>



## Device groups



Element	Description
A	<p><b>+ Add Group.</b></p> <p><i>For further information, go to <b>How to add a device group.</b></i></p> <p><b>? Need help:</b> opens the context help.</p>
B	<p><b>Groups / Devices name.</b> If you click &gt; you can see the group members.</p>
C	<p><b>Actions.</b> You can perform the following tasks:</p> <ul style="list-style-type: none"> <li>• Rename</li> <li>• Add device: allows you to add device into an existing group</li> <li>• Add group: this tab allows you to create a group into an existing group.</li> <li>• Delete</li> </ul> <p><i>For further information, go to <b>How to add a device group.</b></i></p>
D	<p>The connection <b>map</b> shows the location of your devices.</p> <p>You can perform the following tasks:</p> <ul style="list-style-type: none"> <li>• Enter a connection address (🔍)</li> <li>• Zoom in or out (+ / -)</li> <li>• Zoom all (📏) to see all the devices in the map</li> </ul> <p><b>i</b> <i>When you choose an address, the map enlarges on the selected area.</i></p>

## How to add a device group

1. Click  to open the **main menu**.
2. Go to **Devices > Manage**.
3. Go to the **Devices 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 <b>Actions</b> column of an existing group

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

## VPN page


### Description

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:

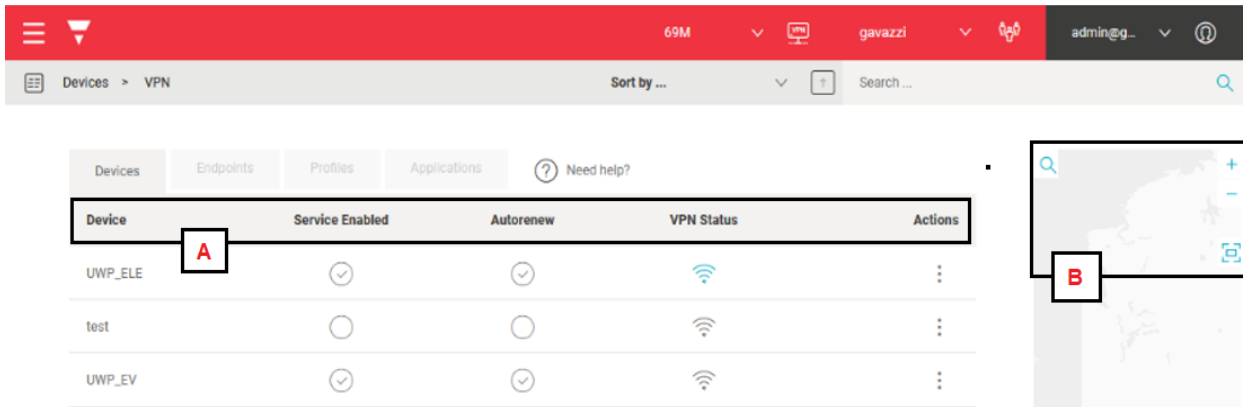
- Devices
- Endpoints
- Profiles
- Applications.





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

## Devices (VPN page)

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
<b>A</b>	<p>Device's information in the grid:</p> <ul style="list-style-type: none"> <li>• <b>Device</b> name.</li> <li>• <b>Service enabled.</b> Check it to enable the VPN service. If you leave it unchecked, you have to assign credits to enable the service.</li> <li>• <b>Autorenewal.</b> Check it to enable the <b>VPN Autorenewal</b></li> <li>• <b>VPN status.</b> The coloured icon means that the device is available and that you can connect to it through VPN.</li> <li>• <b>Actions.</b> This column allows you to perform the following tasks: <ul style="list-style-type: none"> <li>○ connect to the VPN service</li> <li>○ enable/disable the VPN service autorenewal</li> <li>○ assign credits</li> <li>○ access the device's logs</li> <li>○ get support data. If you click this button, you can download a .json file useful for technical support.</li> </ul> </li> </ul> <p><i>Notes:</i></p> <ul style="list-style-type: none"> <li>• <i>this function is available only for the administrator users in device roles.</i></li> <li>• <i>only administrator users in device roles can manage autorenewal and assign credits.</i></li> <li>• <i>only user with "iam.audit.read" permission in application role can access to device's logs.</i></li> </ul> <p><i>If you click <b>Connect to VPN</b>, you are redirected to the <b>VPN portal</b>.</i></p>
<b>B</b>	<p>The connection <b>map</b> shows the location of your devices. You can perform the following tasks:</p> <ul style="list-style-type: none"> <li>• Enter a connection address (.</li> </ul> <p><i>When you enter an address, the map enlarges on the selected connection place.</i></p> <ul style="list-style-type: none"> <li>• Zoom in or out ( or .</li> <li>• Zoom all () to see all the devices in the map.</li> </ul>

## How to connect to gateway/endpoints (VPN tunnel)

If you use...	Then...
<b>Browser</b>	<ol style="list-style-type: none"> <li>1. Go to your MAIA Cloud home page or open the <b>main menu</b> and go to <b>Devices &gt; VPN</b></li> <li>2. Click <b>☰</b> to select the available device you need to connect</li> <li>3. Click <b>Connect to VPN</b>.</li> </ol> <p><i>Note: A pop up informs you that you will be redirected to the VPN portal (see <b>VPN portal</b>).</i></p> <ol style="list-style-type: none"> <li>4. Click <b>Continue</b></li> </ol>
<b>Desktop</b>	Open your MAIA Cloud Connector

5. Select the device you need to connect

6. From the gateway pop-up, you can perform different actions:

If you want to...	Then...
create a VPN tunnel to endpoints/gateway  <i>Note: it is valid only if you use Maia Cloud Connector.</i>	<ol style="list-style-type: none"> <li>7. Click <b>Connect to all endpoints</b> or <b>Connect to gateway</b> button</li> </ol> <p><i>If the connection is correctly established, the button colour changes.</i></p> <ol style="list-style-type: none"> <li>8. Enter the VPN IP address that you find in the bottom part of the pop-up, in your browser.</li> </ol>
Use a predefined application to create a VPN tunnel to the gateway	Click one of the available applications  <i>For further information go to <b>How to associate a profile to an endpoint</b>.</i>
Disconnect from the endpoints/gateway	Click <b>Disconnect from endpoints/gateway</b>

### Notes:

- *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 more information, go to **How to set up a direct access to favourite applications**.*



## Endpoints

This tab of the VPN page allows you to manage and add endpoints to your devices.

Device	Endpoint	Description	IP Address	Application profile	Enabled	Source NAT	Actions
UWP_Alessio							
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><b>Endpoints tab information:</b></p> <ul style="list-style-type: none"> <li>•  the coloured icon means that the device is available and that you can connect to it through VPN</li> <li>• <b>Device</b> name</li> <li>• <b>▼</b> if you click it, you see the endpoints and the relevant information: <ul style="list-style-type: none"> <li>○ <b>Endpoint</b> name</li> <li>○ <b>Endpoint</b> description</li> <li>○ <b>Endpoint IP address</b></li> </ul> <p><i>Note: each UWP3.0 is considered an endpoint called gateway and its IP address is the local host. This endpoint is automatically created when you activate the UWP3.0.</i></p> <li>○ <b>Application profile</b> assigned to the endpoint.</li> <li><i>For further information, go to <b>How to associate a profile to an endpoint.</b></i></li> <li>○ <b>Enabled.</b> If the endpoint has been correctly added and activated, it appears checked.</li> <li>○ <b>Source NAT.</b> It allows you to use a real IP instead of a virtual IP (optional). <i>When an endpoint is connected to the MAIA Cloud server, by default it gets a virtual IP address.</i> <i>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 <b>Source NAT</b> option.</i></li> </li></ul>

Element	Description
B	<p><b>Actions.</b> It permits you to perform the following tasks:</p> <ul style="list-style-type: none"> <li>• Edit gateway (✎). You can: <ul style="list-style-type: none"> <li>○ Check the <b>Do not translate real IPs into virtual IPs</b> option to maintain the real IP used in the local network even if reached through the VPN.</li> </ul> <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 <b>Do not translate real IPs into virtual IPs</b> option.</i></p> <li>○ Set the <b>Maximum number of endpoints</b> available for the relevant gateway.</li> </li></ul> <p><i>Note: 2 is the default value.</i></p> <ul style="list-style-type: none"> <li>• Create an endpoint (+). Click it to open the <b>Endpoint Options</b> menu. <i>For further information, go to <b>How to add an endpoint</b>.</i></li> </ul> <p>Click (▼) to see the <b>Endpoints Actions</b> which allow you to edit (✎) or delete (🗑) an endpoint.</p>

## How to add an endpoint

1. 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 **Profiles**.*
6. Check the **Enabled** box to activate the endpoint
7. **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.*
8. Click **✓** to save the configuration.

## Profiles

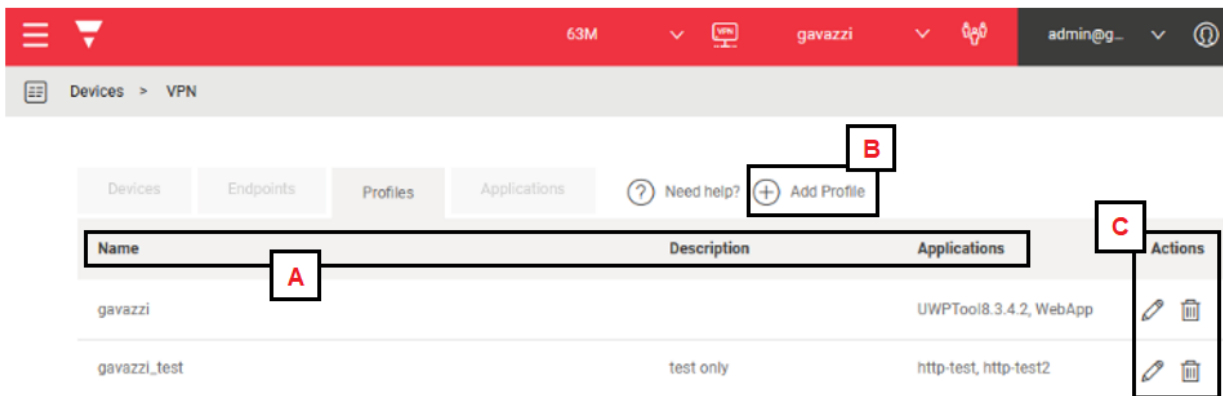
This tab of the **VPN page** allows you to manage and add profiles.

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 UWP 3.0 default profile is ready to use, just add this profile to your devices.

See **How to associate a profile to an endpoint** for further details.



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

## How to create a profile

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

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

- Application. Click **▼** and choose the available applications you want to include in the relevant profile.

*For further information, go to **Applications**.*

6. Click **✓** to save

## How to associate a profile to an endpoint

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

*Note: each UWP3.0 is an endpoint called gateway and its IP address is the local host. This endpoint is automatically created when you activate the UWP3.0.*

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.

## 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:

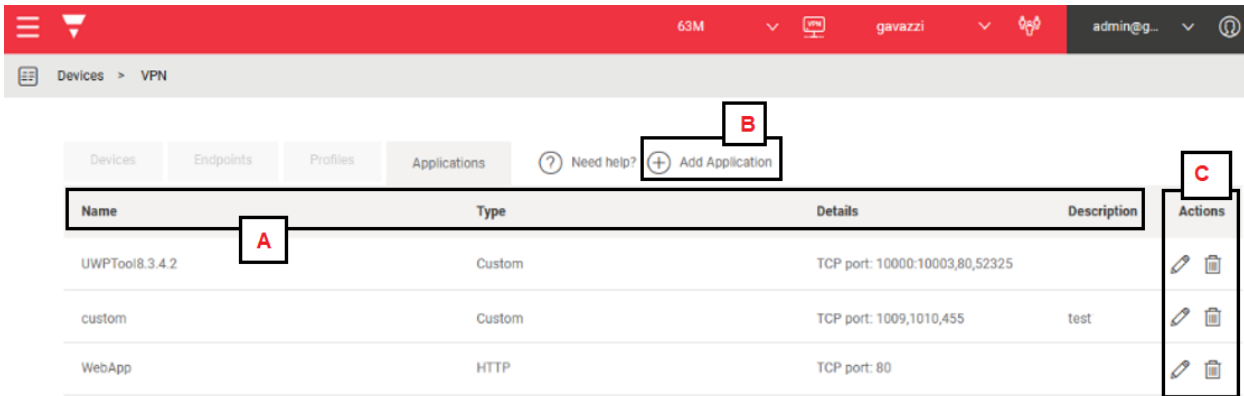
- UCS 7 Software
- UWP 3.0 Tool
- UWP 3.0 Web App
- SSH remote support (only for Carlo Gavazzi Support Team)

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
<b><i>Built-In Application</i></b>	<ul style="list-style-type: none"> <li>• SSH</li> <li>• HTTP</li> <li>• HTTPS</li> </ul>	<ul style="list-style-type: none"> <li>• Browser</li> <li>• Desktop</li> </ul>
<b><i>Local Application</i></b>	<ul style="list-style-type: none"> <li>• Custom</li> </ul>	<ul style="list-style-type: none"> <li>• Desktop</li> </ul>

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 add an application.***



Element	Description
A	<p><b>Applications information:</b></p> <ul style="list-style-type: none"> <li>• <b>Name</b></li> <li>• <b>Type</b> (SSH, RDP, VNC, Telnet, HTTP, HTTPS, Custom)</li> <li>• <b>Details</b> (protocol and port used)</li> <li>• <b>Description</b> additional information</li> </ul>
B	<p><b>+ Add Application.</b> Click <b>+</b> to open the application <b>Options</b> menu.  <i>For further information, go to <b>How to add an application</b>.</i></p>
C	<p><b>Actions.</b> You can edit () or delete () an application.</p>

## The 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	TCP	443
	WebApp_HTTP	HTTP	TCP	80
	CP3_WebApp_HTTPS	HTTPS	TCP	443
	CP3_WebApp_HTTP	HTTP	TCP	80
Local application	UWP_Tool	Custom	TCP	10000:10002 80 443 52326
	UCS_7_PROGRAM_PATH	Custom (Bridge Modbus)	TCP	443, 41214 <i>Note: it can be changed by the user</i>
	UCS_7_HOME_PATH	Custom (Bridge Modbus)	TCP	443, 41214 <i>Note: it can be changed by the user</i>



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

1. Open the MAIA Cloud Connector application and sign in

See *How to log in via browser or desktop* for further details

2. Select the device you need to connect to
- 3.

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

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

## How to add an application

1. Open the **main menu**
2. Go to **Devices > VPN**
3. Open 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**.*

If you want to set up...	Then...
an <b>SSH</b> ( <i>Secure Shell Connection</i> ) application	<ol style="list-style-type: none"> <li>7. Select the <b>Protocol</b> type and the <b>Port</b> number from the <b>Application</b> tab</li> <li>8. Choose the options from the <b>Advanced parameters</b> tab (not mandatory)</li> </ol>
<b>HTTP</b> <i>Web interface in a browser</i> <b>HTTPS</b> <i>Web interface over a secured connection in a browser</i>	<ol style="list-style-type: none"> <li>9. Select the <b>Protocol</b> type and the <b>Port</b> number</li> <li>10. Fill in the <b>URL to open</b>.</li> </ol> <p><i>For further information, go to <b>Placeholders</b>.</i></p>
a <b>CUSTOM</b> application	<p>From the <b>Application</b> tab select:</p> <ul style="list-style-type: none"> <li>• <b>Protocol</b> type</li> <li>• <b>Port</b> number</li> <li>• <b>Command path</b> and <b>arguments</b></li> </ul> <p><i>For more information see <b>Placeholders</b> and <b>How to use Command path and argument for local applications</b>.</i></p> <p><i>From the <b>Advance parameters</b> tab, you can set other custom parameters (not required).</i></p>
<ol style="list-style-type: none"> <li>11. Enable the application</li> <li>12. Click <b>✓</b> to save</li> </ol>	


## 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 <b>URL to open</b> field	Define the rules to connect to the relevant application
Custom applications	Fill in the <b>Command Path</b> and, if necessary, the <b>Command Arguments</b> fields	Define the rules to connect to the relevant application. <i>For more information see <a href="#">How to use Command path and argument for local applications</a>.</i>

## How to use Command path and argument for local applications

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

1. Open the **main menu**
2. Go to **Devices > VPN**
3. Open the **Applications** tab
4. Click  edit from the action 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.

## VPN portal

### Description

This page 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
- See the device on a map

Two tabs compose it: **Dashboard** (as the **Connections** tab) and **Map**.

The **Remote access** page opens if you click **Connect on VPN** from the **Actions** column (browser home page or browser VPN page).

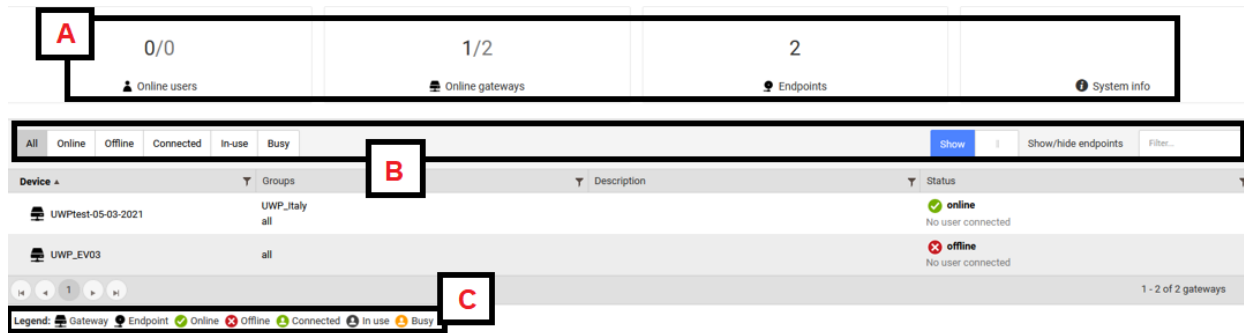
*Note: The **VPN portal** and MAIA Cloud Connector have the same interface and functions.*

## Dashboard – Connections tab

This tab allows users 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

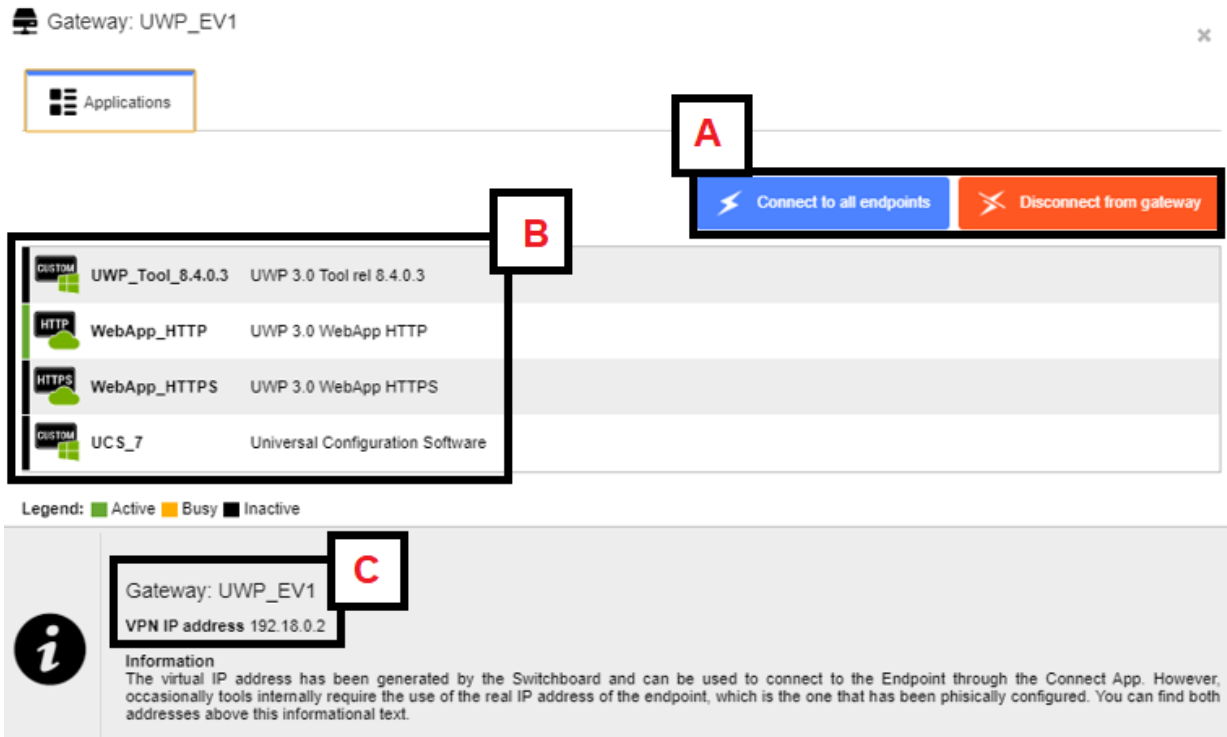
For further information about how to set up the tunnelling, go to **How to connect to gateway/endpoints (VPN tunnel)**.





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

## Gateway details pop-up

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

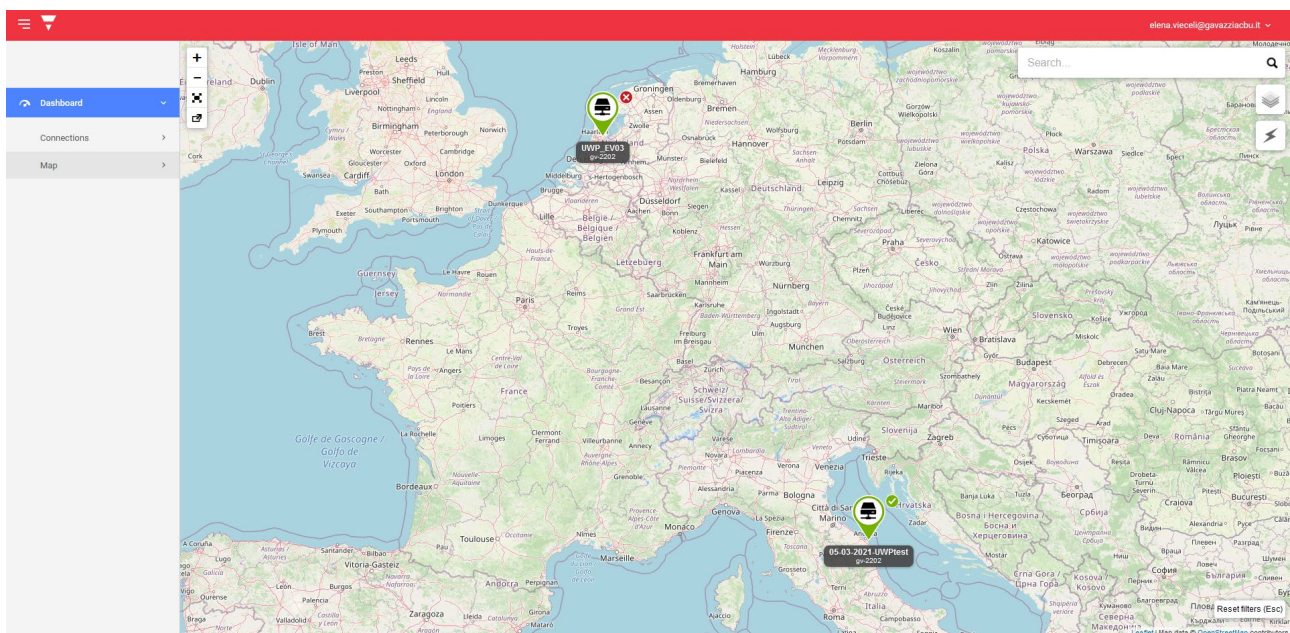


Element	Description
A	You can <b>Connect/disconnect to all endpoints</b> or <b>Connect/disconnect from gateway</b> <i>Note: when you click <b>Connect</b>, the colours change and become <b>Disconnected</b>.</i>
B	The applications that you can use to set a remote connection up. The applications classes are  <b>Built-In Application</b> , that can be used also through the web portal, and  <b>Local Application</b> , that can be used only through the MAIA Cloud Connector. <i>For further information, go to <b>Applications</b>.</i>
C	Additional gateway information: <ul style="list-style-type: none"> <li>• Label</li> <li>• Organization</li> <li>• Virtual Private Network IP address</li> </ul>

## Map tab

The **Map** tab shows the location of your devices. You can perform the following tasks:

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



## IAM menu

### Introduction

This menu permits you to manage your organization through three submenus:

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


Each submenu has its own page.

## Organizations page

This page permits you to perform the following tasks:

- manage your organization
- add suborganizations
- arrange your resources
- monitor the consumptions.

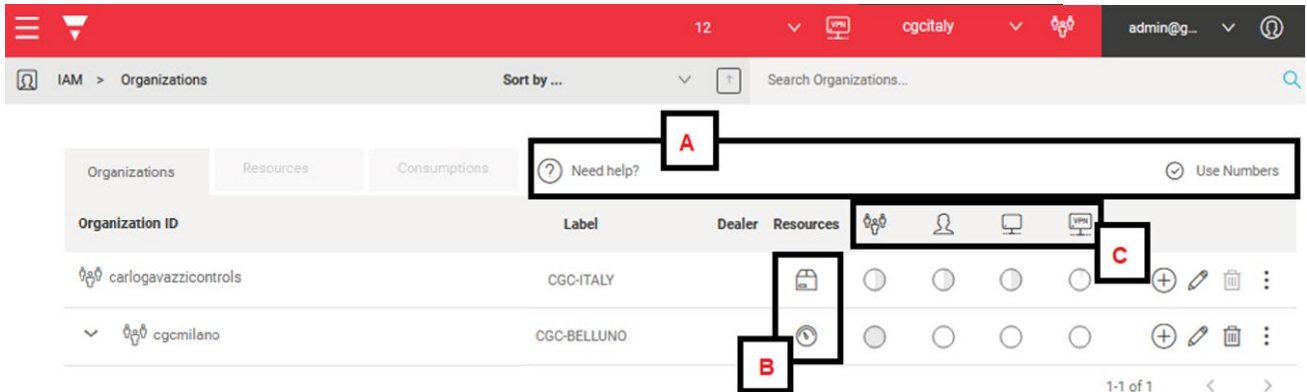
It is composed by three tabs: **Organizations**, **Resources** and **Consumptions**.







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





## Organizations (Organization page tab)

This section allows you to manage / add suborganizations and monitor / add suborganization resources.



Element	Description
A	<p><b>? Need help:</b> opens the context help.</p> <p><b>✓ Use numbers.</b> If you check it, you see the organization resources as number (used/total).</p>
B	<p><b>Resources.</b> This column shows the following suborganization type:</p> <p> if the <b>lives on own resources</b> option is disabled, it means that this organization receives the resources from the root organization.</p> <p> if the <b>lives on own resources</b> option is enabled, it means that in this organization the resources are added with UWP Licences.</p> <p><i>See <b>How to activate a licence and add resources to an organization</b> for further details.</i></p>
C	<p>The pie charts show the following available resources for each licence:</p> <ul style="list-style-type: none"> <li> suborganization</li> <li> user</li> <li> device</li> <li> VPN service</li> </ul> <p><i>For further information, see <b>Licence code</b>.</i></p>

Element	Description
D	<p><b>Actions.</b> You can perform the following tasks:</p> <ul style="list-style-type: none"> <li>• Click <b>+</b> to add a suborganization Go to <b>How to add a suborganization</b> for further details</li> <li>• Click <b></b> to perform the following tasks: <ul style="list-style-type: none"> <li>○ Change the organization label</li> <li>○ Set a hostname if it is not already set <i>Note: once set the hostname, you cannot change it or disable it.</i></li> <li>○ Enable or disabled full privacy <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></li> <li>○ Add resources to the relevant suborganization. <i>For further information, go to <b>How to activate a licence and add resources to an organization.</b></i></li> </ul> </li> <li>• Click <b></b> to delete an organization.</li> <li>• Click <b>Get support data</b> to download a file useful for technical support.</li> </ul>

## How to add a suborganization

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

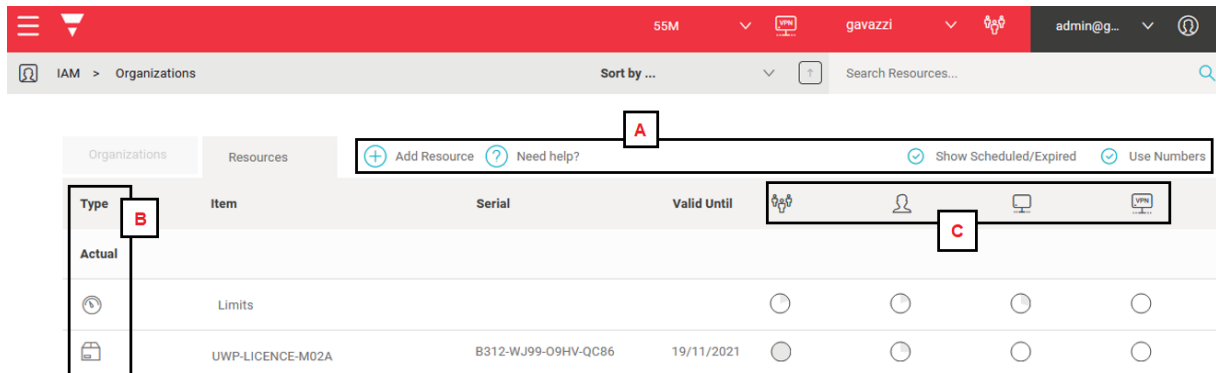
<b>If you want to...</b>	<b>Then enable...</b>
set a hostname to the suborganization	<b>“Has hostname”</b>
create a suborganization and allow user to set up full privacy preventing all other users (also administrators) to see them	<b>“Allow full privacy”</b>
create an organization which lives on own resources	<b>“Lives on own resources”</b> <i>For further details, go to <b>How to activate a licence and add resources to an organization.</b></i>







6. Click **✓** to save and add suborganization

*When you set a suborganization’s hostname, it cannot be changed.*

## Resources

This tab allows you to check the available resources, the expired and scheduled licences and to add resources.



Element	Description
A	<p><b>+ Add resource.</b> For further information, go to <b>How to activate a licence and add resources to an organization.</b></p> <p><b>? Need help:</b> opens the context help.</p> <p><b>✓ Show Scheduled/Expired.</b> If you check it, you see the scheduled and/or expired licences.</p> <p><b>✓ Use numbers.</b> If you check it, you see the organization resources as numbers (used/total).</p>
B	<p><b>Type.</b> This column shows the following suborganization types:</p> <p> if the <b>lives on own resources</b> option is disabled, it means that this organization receives resources from the root organization.</p> <p> if the <b>lives on own resources</b> option is enabled, it means that in this organization the resources are added with UWP licences.</p> <p>For further information, go to <b>How to activate a licence and add resources to an organization.</b></p>
C	<p>The pie charts show the following available resources for each licence:</p> <ul style="list-style-type: none"> <li> suborganization</li> <li> user</li> <li> device</li> <li> VPN service</li> </ul> <p>For further information, go to <b>Licence code.</b></p>

## 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 **Licence code**.

## How to activate a licence and add resources to an organization

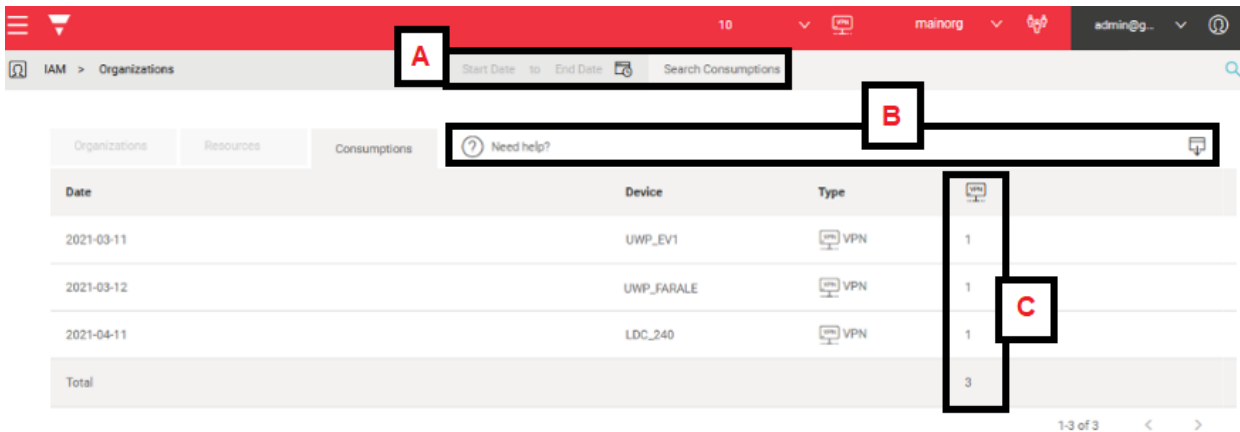
The procedure depends on the **lives on own resources** option.

If “lives on own resources” is...	Then...
Disabled	<ol style="list-style-type: none"> <li>1. Open the <b>main menu</b></li> <li>2. Go to <b>IAM &gt; Organization</b></li> <li>3. Open the <b>Organization</b> tab</li> <li>4. Click  <b>Edit</b> from the <b>Actions</b> column of the suborganization you want to manage</li> <li>5. From the settings menu, you can add Users, Devices, Suborganization and Month of VPN</li> <li>6. Click ✓ to save</li> </ol> <p>This way, the root organization’s resources go to the suborganization.</p>
Enabled	<ol style="list-style-type: none"> <li>1. From the top bar, select the suborganization where you want to add resources</li> <li>2. Open the <b>main menu</b></li> <li>3. Go to <b>IAM &gt; Organization</b></li> <li>4. Open the <b>Resources</b> tab</li> <li>5. Click <b>+ Add Resources</b></li> <li>6. Write the UWP licence code</li> </ol> <p><i>Note: if your code is valid, you see automatically the licence type (<b>standard</b> or <b>plus</b>), the licence expiration date, and the resources composing the licence.</i></p> <ol style="list-style-type: none"> <li>7. Click ✓ to save.</li> </ol>

For more information about organizations and organization type, go to **Organizations page**.

## Consumptions


This tab shows the consumption of your organization's devices and allows you to download this information as a csv file.



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

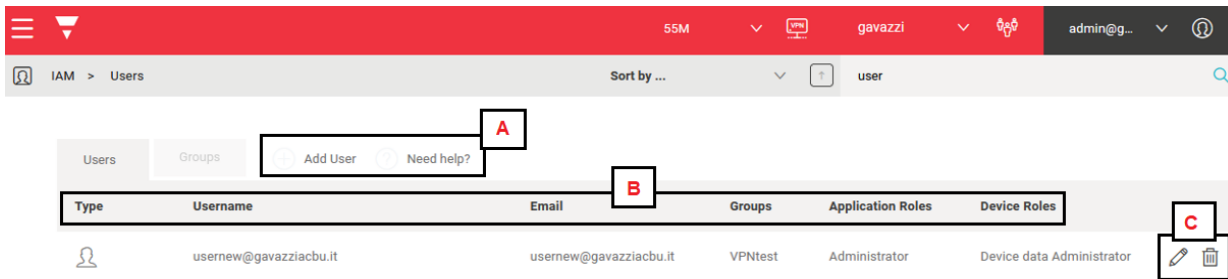
## Users page




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

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

## Users (users page tab)

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



Element	Description
A	<p><b>+ Add user.</b> If you click it, you are redirected to the <b>Options</b> page.</p> <p><i>For further information, go to <b>How to add a user</b>.</i></p> <p><b>? Need help:</b> opens the context help.</p>
B	<p>Information about users:</p> <ul style="list-style-type: none"> <li>• <b>Type</b></li> <li>• <b>Username</b></li> <li>• <b>Email</b></li> <li>• <b>Organization</b></li> <li>• <b>Group</b> (see user groups for further details)</li> <li>• <b>User roles for specific fields (Application, VPN)</b></li> </ul>
C	<p><b>Actions.</b>  (edit) and  (delete).</p> <p> permits you to perform the following tasks:</p> <ul style="list-style-type: none"> <li>• See user information (username, E-mail)</li> <li>• Add user to a group or change them (<b>Group membership</b>) <i>Go to <b>User groups</b> for further details</i></li> <li>• Set or change user permissions (<b>Application roles</b> and <b>Device roles</b>) <i>Go to <b>Roles page</b> for further details</i> <i>Note: you can add more than one permission to the same user.</i></li> <li>• Create, import or export favourite applications for user with direct access to favourite applications (<b>Favourite Apps</b>). <i>For more information go to <b>How to set up a direct access to favourite applications</b>.</i></li> </ul> <p><i>Note: to allow user to log into MAIA Cloud, you need to set at least one <b>Application role</b> and one <b>Device role</b>. Otherwise, you can add a user to a group: this way, user inherits the users' group roles.</i></p>



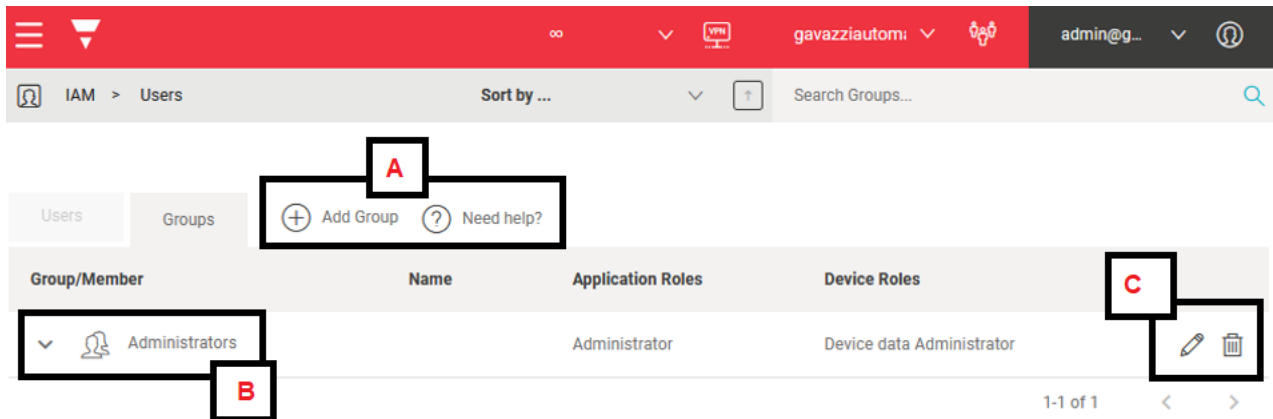
## How to add a user

1. Open the **main menu**
2. Go to **IAM > Users**
3. Open 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 up a user with the direct access to favourite applications, you need to define at least one application clicking **+**.  
*For more information go to **How to set up a direct access to favourite applications.***
9. Click **✓** to add user to your organization

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

## 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.




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

### **How to add a user group**


1. Open the **main menu**
2. Go to **IAM > Users**
3. Go to the **User Group** 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 into a user group**

1. Open the **main menu**
2. Go to **IAM > Users**
3. Go to the **User Group** tab
4. Click  to edit the group
5. Select the users to add from the list
6. Click **Enter** to save

## Roles page

This page allows you to manage and modify users' roles. It is composed by the **Application Roles** and **Devices roles** tabs.

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

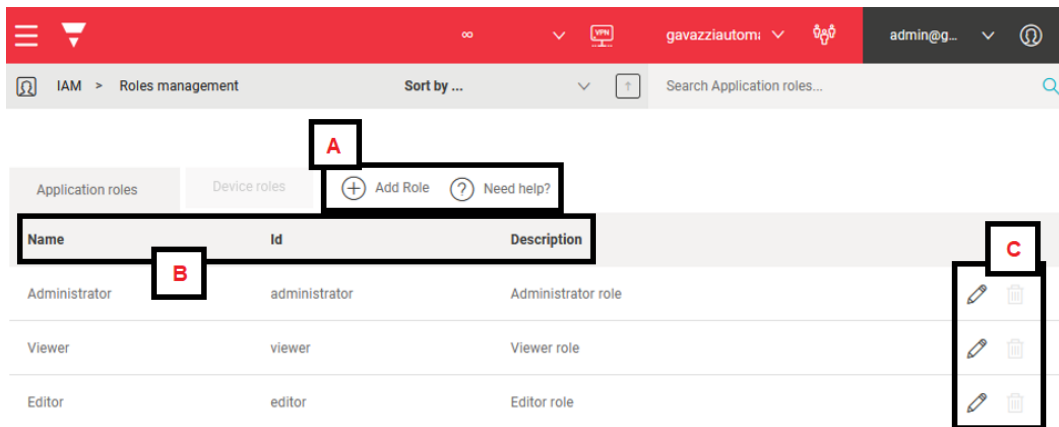
### Application roles

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.



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

## How to add an application role

1. Open the **main menu**
2. Go to **IAM > Roles**
3. Go to **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"> <li>8. Disable the <b>Access only favourite applications</b> option</li> <li>9. Choose the permissions from the list</li> </ol>
Only the favourite applications	<ol style="list-style-type: none"> <li>8. Enable the <b>Access only favourite applications</b> option</li> <li>9. Check the permission <i>iam.device.read</i></li> </ol>

10. Click **✓** to save

## How to set up a direct access to favourite applications

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

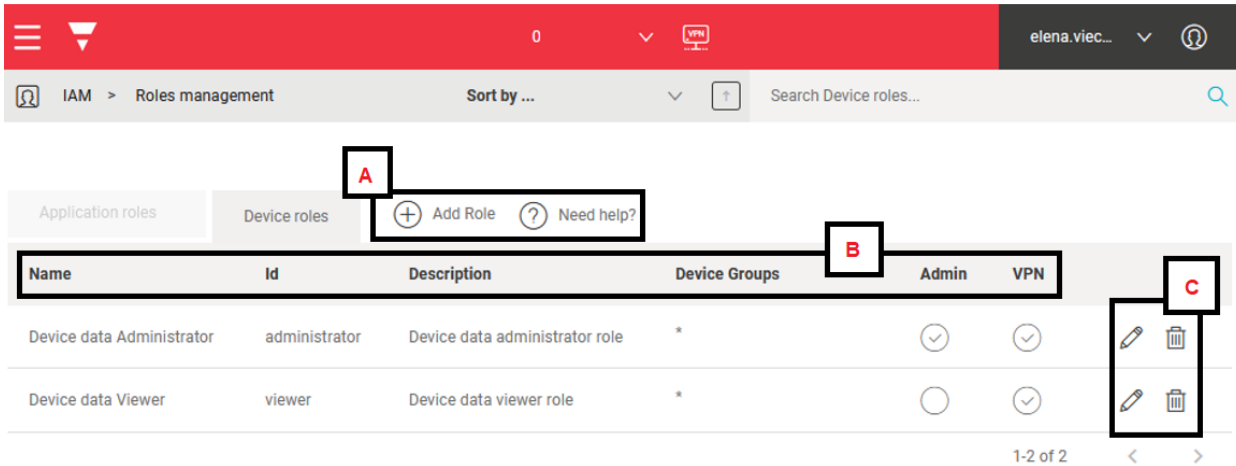
*See **How to add an application role** for more information*





2. Go to **IAM > Users > Edit user** or **Add user**
3. Set the application role of point 1 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 clicking *
11. Click **✓** to save

## Device 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.



Name	Id	Description	Device Groups	Admin	VPN	
Device data Administrator	administrator	Device data administrator role	*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	 
Device data Viewer	viewer	Device data viewer role	*	<input type="checkbox"/>	<input checked="" type="checkbox"/>	 

Element	Description
A	<p><b>+ Add roles.</b> If you click <b>Add roles</b> you are redirected to the relevant <b>Options</b> page. <i>For further details, go to <b>How to add a device role</b>.</i></p> <p><b>? Need help?</b> Opens the web help</p>
B	<p><b>Roles information:</b></p> <ul style="list-style-type: none"> <li>• <b>Role Name</b> <i>Note: <b>Administrator</b> is the default role.</i></li> <li>• <b>Role ID</b></li> <li>• <b>Description</b></li> <li>• <b>Device groups.</b> The devices which this role is related to</li> <li>• <b>Admin:</b> if you check it, you enable the administrator permission. Otherwise, you set the regular user. <i>Note: a regular user in <b>Devices &gt; VPN page</b> cannot assign credits to devices or enable/disable the autorenewal.</i></li> <li>• <b>VPN:</b> if you check it, you enable the VPN access.</li> </ul>
C	<p><b>Actions.</b> You can change the <b>Role Name</b>, description and the role permission () or delete ()</p>

## How to add a device role

1. Open the **main menu**
2. Go to **IAM > Roles**
3. Go to **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 up 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.*

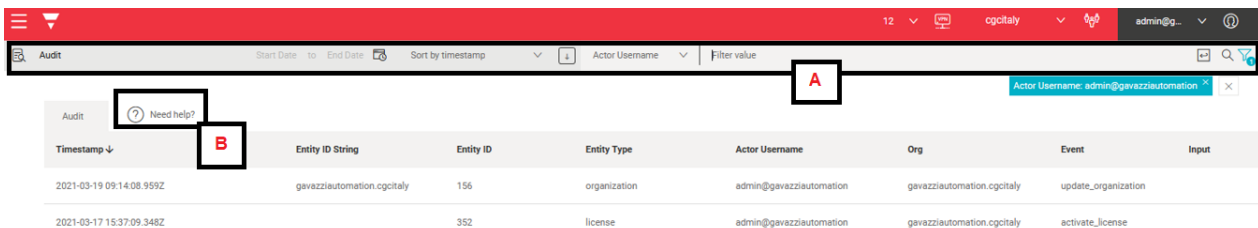
9. Check VPN access to allow users to use VPN
10. Click **✓** to save.





## Audit menu

This menu shows you the organization's 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"> <li>choose the time period to consider ()</li> <li>sort by allows you to sort the log list by a specific category</li> <li>filter by a specific category ()</li> </ul>
B	<b>? Need help:</b> opens the context help.

## Legal notice

---

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

## Download

---

Download the **MAIA Cloud application** from these links:

[MAIA Cloud Connector App Download](#)

[www.productselection.net/Download/UK/MAIACloud\\_download.pdf](http://www.productselection.net/Download/UK/MAIACloud_download.pdf)

# Intellectual property

---

**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](mailto:info@gavazzi-automation.com)

[www.gavazziautomation.com](http://www.gavazziautomation.com)

+39 0437 355811