



PPH600

Gateway VPN



Table of contents

1	Safety guidelines.....	5
1.1	Organization of safety notices.....	5
1.2	Safety Precautions.....	5
1.3	Precautions for safe use.....	6
1.4	Environmental policy / WEEE.....	7
2	Model Identification.....	7
3	Technical Data.....	7
3.1	General Features.....	7
3.2	Hardware Features.....	7
3.3	Software Features.....	7
4	Dimensions and installation.....	8
5	First steps.....	9
5.1	Default configuration.....	9
5.2	Procedure for the first connection to the gateway.....	9
5.3	VPN connection to devices in the LAN subnetwork.....	11
6	Pixsys Portal for PPH600 VPN Gateway.....	11
6.1	REQUIREMENTS.....	11
6.2	SERVICE CONFIGURATION.....	11
6.2.1	Section "Details".....	12
6.2.2	Section "Security".....	14
6.2.3	Section "Network".....	15
6.2.4	Section "Routing".....	16
6.2.5	Section "VNC gateway".....	18
6.2.6	Section "Web Bookmarks".....	19
6.3	INSTALLING THE APPLICATION ON YOUR COMPUTER AND CREATING THE PixsysPortal ACCOUNT.....	20
6.3.1	Using the PixsysPortal client.....	20
6.3.2	Associating the device with your PixsysPortal account.....	21
6.3.3	Make a remote connection to the device.....	23
6.3.4	Sharing the device with other PixsysPortal accounts.....	26

Indice degli argomenti

1	Norme di sicurezza.....	28
1.1	Organizzazione delle note di sicurezza.....	28
1.2	Note di sicurezza.....	28
1.3	Precauzioni per l'uso sicuro.....	29
1.4	Tutela ambientale e smaltimento dei rifiuti / Direttiva WEEE.....	30
2	Identificazione di modello.....	30
3	Dati tecnici.....	30
3.1	Caratteristiche generali.....	30
3.2	Caratteristiche Hardware.....	30
3.3	Caratteristiche software.....	30
4	Dimensioni e installazione.....	31
5	Primi passi.....	32
5.1	Configurazione predefinita.....	32
5.2	Procedura per la prima connessione al gateway.....	32
5.3	Collegamento VPN ai dispositivi presenti nella sottorete LAN.....	34
6	Pixsys Portal per i Gateway VPN PPH600.....	34
6.1	PRE-REQUISITI.....	34
6.2	CONFIGURAZIONE DEL SERVIZIO.....	34
6.2.1	Sezione "Dettagli".....	35
6.2.2	Sezione "Sicurezza".....	37
6.2.3	Sezione "Network".....	38
6.2.4	Sezione "Routing".....	39

6.2.5 Sezione "VNC gateway"	41
6.2.6 Sezione "Segnalibri Web"	42
6.3 INSTALLAZIONE DELL'APPLICAZIONE SUL PROPRIO COMPUTER E CREAZIONE DELL'ACCOUNT PixsysPortal	43
6.3.1 <i>Utilizzo del client PixsysPortal</i>	43
6.3.2 <i>Associazione del dispositivo al proprio account PixsysPortal</i>	44
6.3.3 <i>Effettuare la connessione remota al dispositivo</i>	46
6.3.4 <i>Condivisione del dispositivo con altri account PixsysPortal</i>	49

Introduction

PPH600 is a VPN gateway for remote control and/or remote assistance purposes, in a vertical configuration to optimise space on a DIN rail and 24Vdc power supply on terminal.

Two configurations are available, x0A and x1A. The x0A model consists of a pre-configured Ethernet switch with 3/6 LAN ports, 1 WAN port (for Internet access), 1 PLC port (tagged); this is the ideal solution to increase the number of Ethernet ports of the PL600 and PL700 series PLCs and operates as a VPN gateway if the PLCs are equipped with an active PixsysPortal service. The x1A model natively integrates the PixsysPortal service and is therefore a universal VPN gateway that allows access to any device equipped with an Ethernet connection.

1 Safety guidelines

Read carefully the safety guidelines and programming instructions contained in this manual before connecting/using the device.

Disconnect power supply before proceeding to hardware settings or electrical wirings to avoid risk of electric shock, fire, malfunction.

Do not install/operate the device in environments with flammable/explosive gases.

This device has been designed and conceived for industrial environments and applications that rely on proper safety conditions in accordance with national and international regulations on labour and personal safety. Any application that might lead to serious physical damage/ life risk or involve medical life support devices should be avoided.

Device is not conceived for applications related to nuclear power plants, weapon systems, flight control, mass transportation systems.

Only qualified personnel should be allowed to use device and/or service it and only in accordance to technical data listed in this manual.

Do not dismantle/modify/repair any internal component.

Device must be installed and can operate only within the allowed environmental conditions. Overheating may lead to risk of fire and can shorten the lifecycle of electronic components.

1.1 Organization of safety notices

Safety notices in this manual are organized as follows:

Safety notice	Description
Danger!	Disregarding these safety guidelines and notices can be life-threatening.
Warning!	Disregarding these safety guidelines and notices can result in severe injury or substantial damage to property.
Information!	This information is important for preventing errors.

1.2 Safety Precautions

This product is UL listed as open type process control equipment.	Danger!
If the output relays are used past their life expectancy, contact fusing or burning may occasionally occur. Always consider the application conditions and use the output relays within their rated load and electrical life expectancy. The life expectancy of output relays varies considerably with the output load and switching conditions.	Danger!
Loose screws may occasionally result in fire.	
For screw terminals of relays and of power supply, tighten screws to tightening torque of 0,51 Nm. For other terminals, tightening torque is 0,19 Nm	Warning!
A malfunction in the Digital Controller may occasionally make control operations impossible or prevent alarm outputs, resulting in property damage. To maintain safety in the event of malfunction of the Digital Controller, take appropriate safety measures, such as installing a monitoring device on a separate line.	Warning!

1.3 Precautions for safe use

Be sure to observe the following precautions to prevent operation failure, malfunction, or adverse effects on the performance and functions of the product. Not doing so may occasionally result in unexpected events. Do not handle the Digital Controller in ways that exceed the ratings.

- The product is designed for indoor use only. Do not use or store the product outdoors or in any of the following places.
 - Places directly subject to heat radiated from heating equipment.
 - Places subject to splashing liquid or oil atmosphere.
 - Places subject to direct sunlight.
 - Places subject to dust or corrosive gas (in particular, sulfide gas and ammonia gas).
 - Places subject to intense temperature change.
 - Places subject to icing and condensation.
 - Places subject to vibration and large shocks.
- Installing two or more controllers in close proximity might lead to increased internal temperature and this might shorten the life cycle of electronic components. It is strongly recommended to install cooling fans or other air-conditioning devices inside the control cabinet.
- Always check the terminal names and polarity and be sure to wire properly. Do not wire the terminals that are not used.
- To avoid inductive noise, keep the controller wiring away from power cables that carry high voltages or large currents. Also, do not wire power lines together with or parallel to Digital Controller wiring. Using shielded cables and using separate conduits or ducts is recommended. Attach a surge suppressor or noise filter to peripheral devices that generate noise (in particular motors, transformers, solenoids, magnetic coils or other equipment that have an inductance component). When a noise filter is used at the power supply, first check the voltage or current, and attach the noise filter as close as possible to the Digital Controller. Allow as much space as possible between the Digital Controller and devices that generate powerful high frequencies (high-frequency welders, high-frequency sewing machines, etc.) or surge.
- A switch or circuit breaker must be provided close to device. The switch or circuit breaker must be within easy reach of the operator, and must be marked as a disconnecting means for the controller.
- Wipe off any dirt from the Digital Controller with a soft dry cloth. Never use thinners, benzene, alcohol, or any cleaners that contain these or other organic solvents. Deformation or discoloration may occur.
- The number of non-volatile memory write operations is limited. Therefore, use EEprom write mode when frequently overwriting data, e.g.: through communications.
- Chemicals/solvents, cleaning agents and other liquids must not be used.
- Non-respect of these instructions may reduce performances and safety of the devices and cause danger for people and property.

For CT (Current Transformer) input:

- **Warning:** To reduce risk of electric shock, always open or disconnect circuit from power-distribution system (or service) of building before installing or servicing current transformers
- For use with Listed Energy-Monitoring Current Transformers
- The current transformers may not be installed in equipment where they exceed 75 percent of the wiring space of any cross-sectional area within the equipment
- Restrict installation of current transformer in an area where it would block ventilation openings
- Restrict installation of current transformer in an area of breaker arc venting
- Not suitable for Class 2 wiring methods
- Not intended for connection to Class 2 equipment
- Secure current transformer and route conductors so that the conductors do not directly contact live terminals or bus.

1.4 Environmental policy / WEEE

Do not dispose electric tools together with household waste material.

According to European Directive 2012/19/EU on waste electrical and electronic equipment and its implementation in accordance with national law, electric tools that have reached the end of their life must be collected separately and returned to an environmentally compatible recycling facility.

2 Model Identification

PPH600-30A	ETHERNET SWITCH 3LAN 1WAN 1PLC ports 24VDC
PPH600-60A	ETHERNET SWITCH 6LAN 1WAN 1PLC ports 24VDC
PPH600-31A	PIXSYS PORTAL GATEWAY 3LAN 1WAN 1USB ports 24VDC
PPH600-61A	PIXSYS PORTAL GATEWAY 6LAN 1WAN 1USB ports 24VDC

3 Technical Data

3.1 General Features

Operating temperature	Temperature: 0-45 °C -Humidity 35..95 uR%
Sealing	Box and terminals: IP20, terminals extractable
Material	Box and front panel PC UL94V2

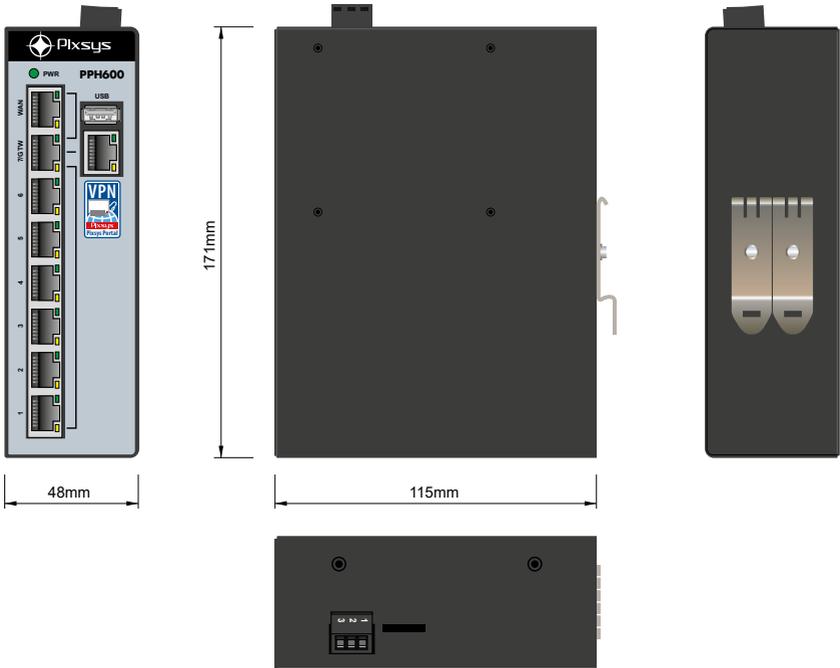
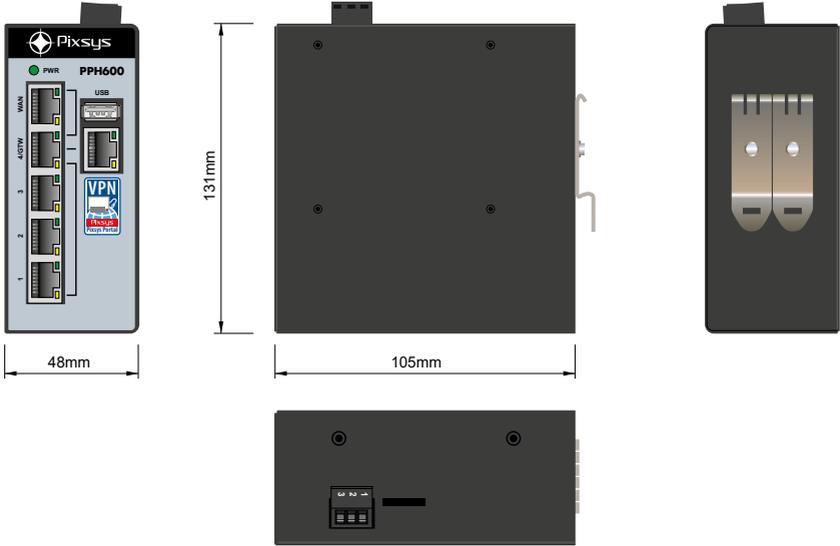
3.2 Hardware Features

	PPH600-30A	PPH600-60A	PPH600-31A	PPH600-61A
Power supply	24VDC ±10% 50/60 Hz			
Consumption	3 Watt/VA			
Dimensions	48 x 105 x 131mm	48 x 115 x 171mm	48 x 105 x 131mm	48 x 115 x 171mm
LAN ports	3	6	3	6
WAN ports	1	1	1	1
PLC ports	1	1	-	-
USB ports	-	-	1	1
Pixsys Portal	-	-	SI	SI

3.3 Software Features

VPN	Active Pixsys Portal service for remote desktop connection (VNC), Web Server, FTP Client, remote assistance
-----	---

4 Dimensions and installation



5 First steps

5.1 Default configuration

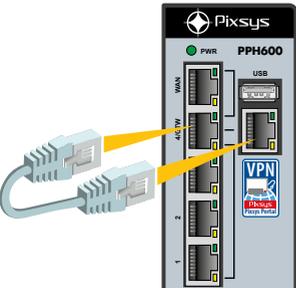
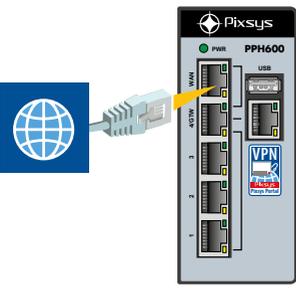
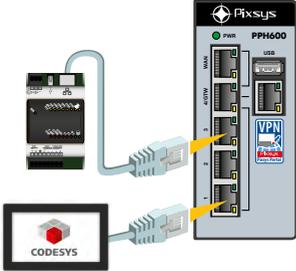
The PPH600 gateway has several Ethernet ports pre-configured with these values (visible in the label on the side of the gateway itself):

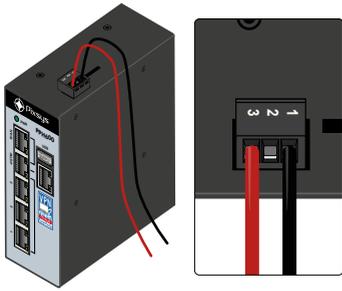
- WAN port (from which the PPH600 gateway accesses the Internet): automatic IP assignment (DHCP)
- GTW port (from which the PPH600 gateway reaches the devices connected to the switch): IPv4 address manually set to 192.168.10.1

The factory configuration therefore provides for internet access through the WAN port in DHCP and connection of local devices to one of the ports 1..3 (PPH600-31A) or 1..6 (PPH600-61A) with IP configuration compatible with the 192.168.10.xxx network.

The configuration WebServer of the PPH600 gateway is accessible from the IP address 192.168.10.1:8080 from any HTML5 browser.

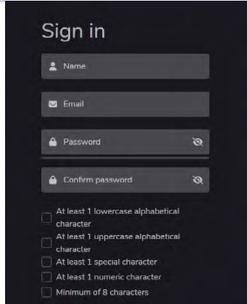
5.2 Procedure for the first connection to the gateway

 <p>The diagram shows the front panel of the Pixsys PPH600 gateway. A blue Ethernet cable is plugged into the WAN port (labeled 'WAN' and '40/100'). Another blue Ethernet cable is plugged into the port labeled 'VPN Pixsys Portal' (labeled '1..3'). The gateway has a power button (PWR) and a USB port.</p>	<p>1- Connect the supplied Ethernet cable between the switch's "GTW" port and the port identified by the "VPN Pixsys Portal" logo.</p>
 <p>The diagram shows the front panel of the Pixsys PPH600 gateway. A blue Ethernet cable is plugged into the WAN port (labeled 'WAN' and '40/100'). A blue globe icon is shown next to the WAN port, indicating Internet access. The gateway has a power button (PWR) and a USB port.</p>	<p>2- Connect the switch's "WAN" port to a network with Internet access and DHCP function enabled (typically the corporate network).</p>
 <p>The diagram shows the front panel of the Pixsys PPH600 gateway. A CODESYS device is connected to port 1 (labeled '1..3'). A switch is connected to port 2 (labeled '1..6'). The gateway has a power button (PWR) and a USB port.</p>	<p>3- Connect your devices to one of the available ports 1..3 (PPH600-31A) or 1..6 (PPH600-61A).</p>

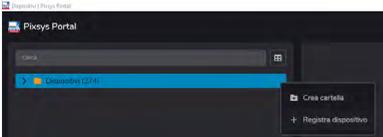


4- Supply power to the PPH600 gateway via the removable terminal on the top of the device

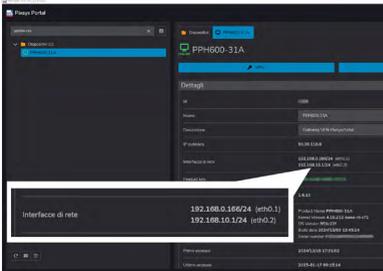
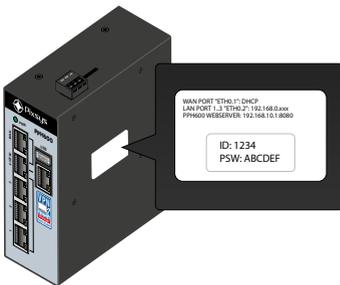
- 1= 0V
- 2= earth
- 3= 24V



5- Switch to your PC: download the latest version of the PixsysPortal client from portal.pixsys.net, install it on your Windows PC and create your own account by following the on-screen instructions.



6- Once logged in, register the PPH600 gateway in your PixsysPortal account by right-clicking above the "Devices" item and choosing "Register Device". In the fields "ID" and "Password" enter the data from the label attached to the side of the PPH600 gateway, then give the gateway a name and possibly a description to recognise it in the device list.



7- At this point, the name of the newly registered PPH600 gateway will appear in the device list, flanked by a green icon if it is already available online, or a red icon if it is offline. If online, selecting the gateway will allow you to read its characteristics, such as firmware version or current network port configuration: Eth0.1 identifies the WAN network (from which the PPH600 gateway accesses the Internet). Eth0.2 identifies the LAN network (from which the PP600 gateway reaches devices connected to the switch)

5.3 VPN connection to devices in the LAN subnetwork

1- Start the PixsysPortal client on your PC

2- Select, from the list on the left, the PPH600 gateway you wish to access

3- Press the “VPN” button and then “Connect”.

4- Once connected, the devices connected to the switch of the PPH600 gateway are available with their “native” IP address, so you only need to use this IP address to reach them in the development/ BrowserWeb environments.

N.B. To configure the LAN sub-network of the PPH600 gateway differently (from the default 192.168.10.xxx) or to take advantage of the quick links to the VNC / WebServer HTML5 interfaces of the devices or to enable advanced port-forwarding functions, once the VPN connection has been made, access the configuration WebServer of the PPH600 gateway by pressing the “PixsysPortal Settings” button or access the IP address 10.253.253.10:8080 from any HTML5 browser.

6 Pixsys Portal for PPH600 VPN Gateway

The PixsysPortal service allows the secure connection, via VPN, of devices connected to the PPH600 gateways from any computer running Windows 8.1, 10, 11 (if you use Windows 7, you must first install the MS PowerShell 5.1 available from the “PowerShell Win7.zip” file in the download area of the Pixsys website).

6.1 REQUIREMENTS

The PixsysPortal service requires PPH600 devices to be connected, and suitably configured, to a LAN network with Internet connection. Internet access is possible via a USB-Wifi key (Pixsys code 2400.10.021) or 4G modem (Pixsys code 2200.20.008) that can be ordered as an accessory. The ports used by the PixsysPortal service are: 443 and 8005 in TCP/UDP (outgoing). For the Webserver of the service, port 8080 is also used.

6.2 SERVICE CONFIGURATION

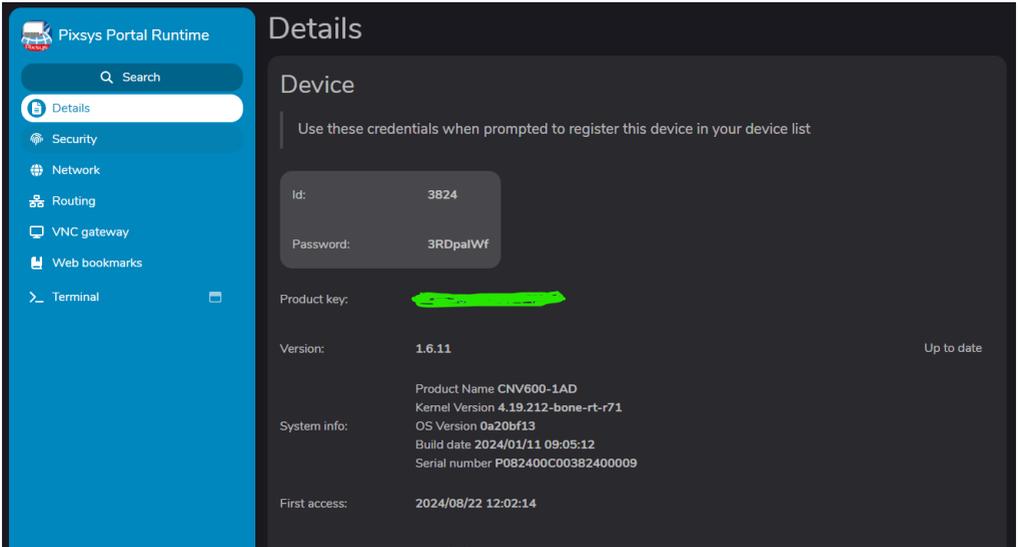
The PPH600 VPN Gateways are devices based on the Linux Debian 11 operating system and the PixsysPortal service runs automatically when they are started.

To configure PixsysPortal’s options, access its WebServer from any device residing in the same address class:

- Switch on the PLC and wait for the operating system services to load completely (RUN LED steady green).
- Connect the gateway to a local network with an Internet connection using the port indicated as WAN.
- Use the DeviceFinder utility to identify the IP address of the PLC:

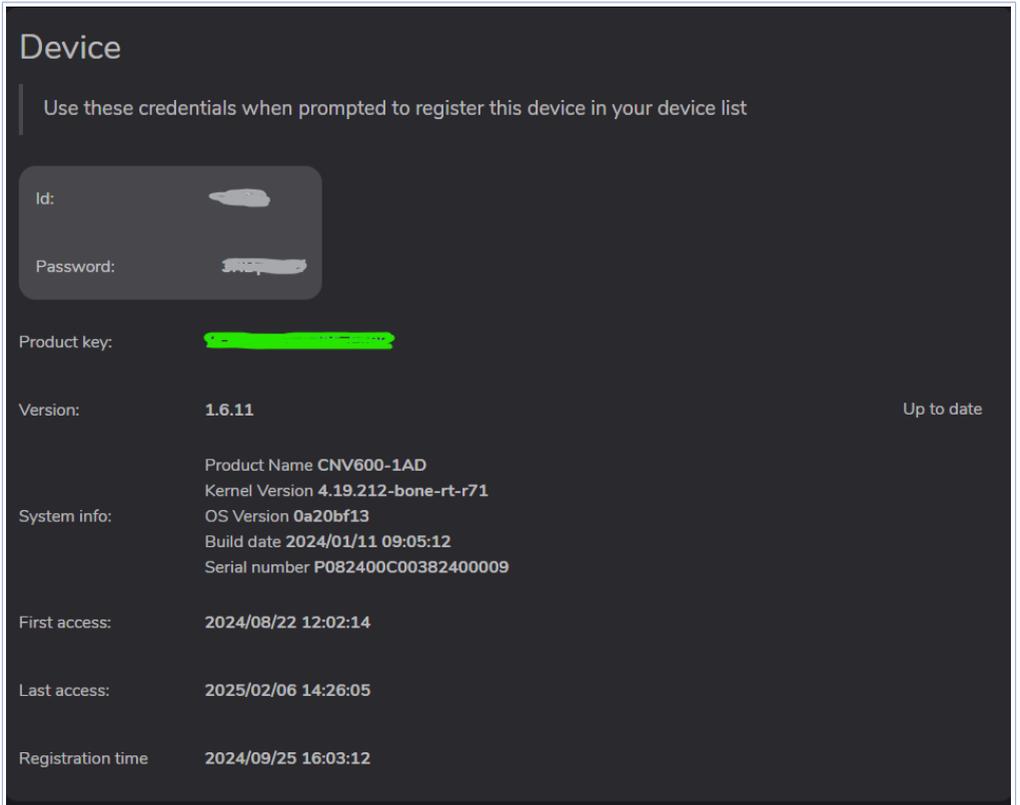
	<p>When using the DeviceFinder utility, select the gateway from the list on the left and press the icon highlighted in the image to connect to its integrated WebServer.</p> <p>In other cases, open a Web browser and enter the gateway address in the address bar, specifying port 8080, e.g. 192.168.0.99:8080</p>
--	---

- This opens the WebServer of the PixsysPortal service, from which you can proceed with the configuration.



The menu on the left allows you to view the different sections containing the relevant settings.

6.2.1 Section “Details”



The “*Device*” tab displays basic device information, the current PixsysPortal firmware version and other operating system info.

The credentials “*ID*” and “*Password*” are the data required to associate the gateway with your PixsysPortal account (please refer to the next section for details).

The “*Product key*” field shows the service activation key.

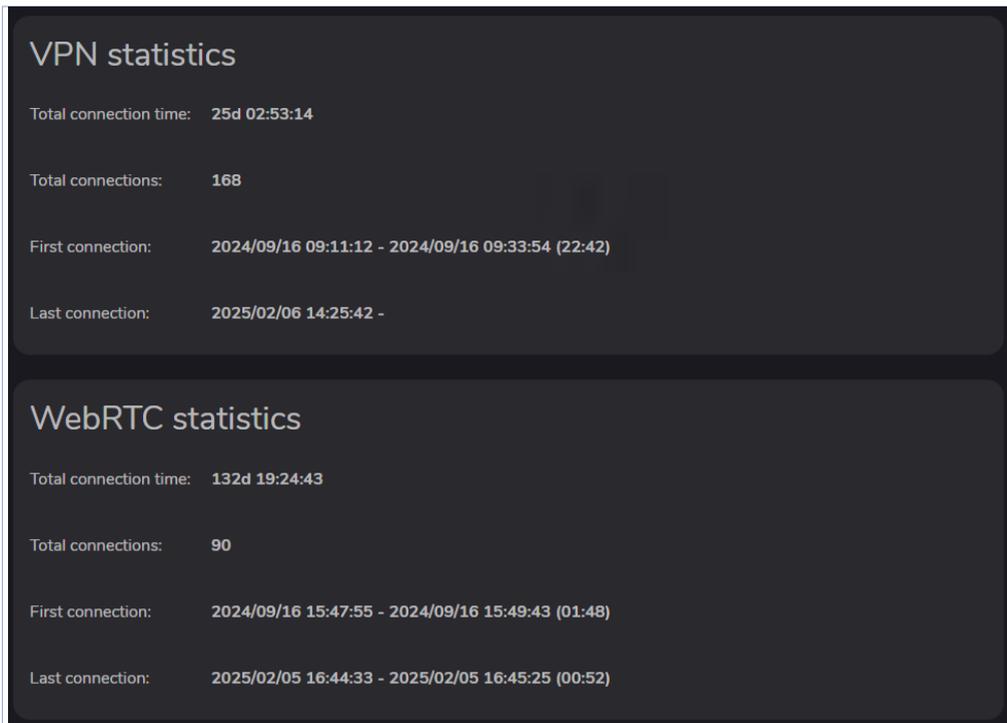
The “*Version*” field shows the version of the PixsysPortal firmware currently installed in the gateway.

The “*Search for updates*” button allows you to check for new updates and if necessary to install them.

The field “*System info*” shows information about the gateway, such as its name, serial number and other info concerning the operating system.

The fields “*First Access*”, “*Last Access*” and “*Registration Date*” show respectively the date and time of the gateway’s first connection to the Pixsys server, the last one and when the gateway registered for the first time (i.e. when it connected to the Internet and received a unique ID and password from the Pixsys server).

The tabs “*VPN statistics*” and “*WebRTC statistics*” display several counters referring to the gateway’s VPN and WebRTC connections. The “*Reset*” button resets this data to zero.

The image shows two dark-themed panels with white text. The top panel is titled "VPN statistics" and contains four rows of data: "Total connection time: 25d 02:53:14", "Total connections: 168", "First connection: 2024/09/16 09:11:12 - 2024/09/16 09:33:54 (22:42)", and "Last connection: 2025/02/06 14:25:42 -". The bottom panel is titled "WebRTC statistics" and contains four rows of data: "Total connection time: 132d 19:24:43", "Total connections: 90", "First connection: 2024/09/16 15:47:55 - 2024/09/16 15:49:43 (01:48)", and "Last connection: 2025/02/05 16:44:33 - 2025/02/05 16:45:25 (00:52)".

VPN statistics

Total connection time: 25d 02:53:14

Total connections: 168

First connection: 2024/09/16 09:11:12 - 2024/09/16 09:33:54 (22:42)

Last connection: 2025/02/06 14:25:42 -

WebRTC statistics

Total connection time: 132d 19:24:43

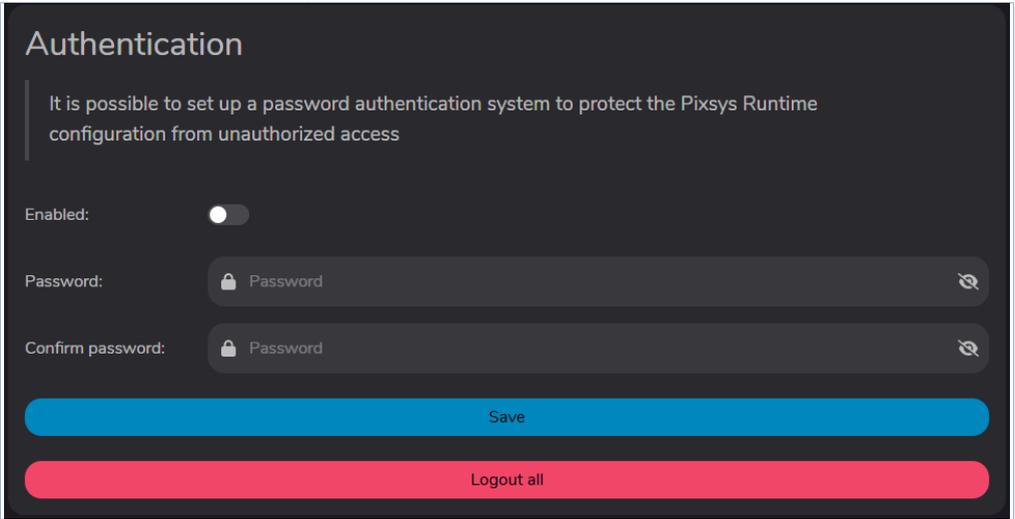
Total connections: 90

First connection: 2024/09/16 15:47:55 - 2024/09/16 15:49:43 (01:48)

Last connection: 2025/02/05 16:44:33 - 2025/02/05 16:45:25 (00:52)

6.2.2 Section “Security”

Under “Authentication” a password can be enabled and managed to protect access to the PixsysPortal configuration WebServer. At first access, you will be asked to choose whether or not to enable this protection, in order to protect your configuration from unwanted access.



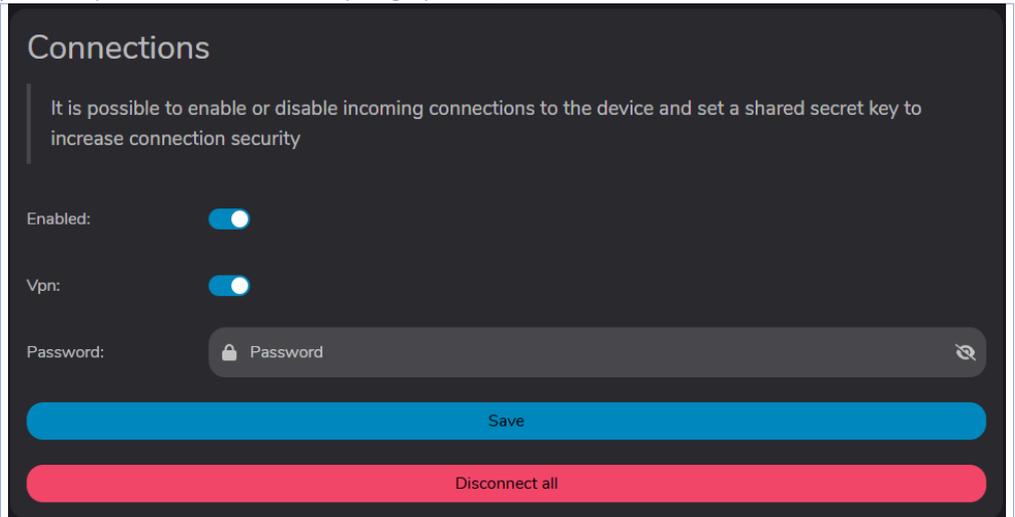
The screenshot shows the 'Authentication' configuration page. At the top, the title 'Authentication' is displayed. Below it, a descriptive text states: 'It is possible to set up a password authentication system to protect the Pixsys Runtime configuration from unauthorized access'. The main configuration area includes an 'Enabled:' toggle switch, which is currently turned off. Below this are two password input fields: 'Password:' and 'Confirm password:', both containing the placeholder text 'Password'. Each password field has a lock icon on the left and a clear icon on the right. At the bottom of the form, there are two prominent buttons: a blue 'Save' button and a red 'Logout all' button.

The “Connections” tab enables and manages the connection to the Pixsys server and the VPN connection:

Enable the “Enabled” flag to allow the gateway to connect to the Pixsys server.

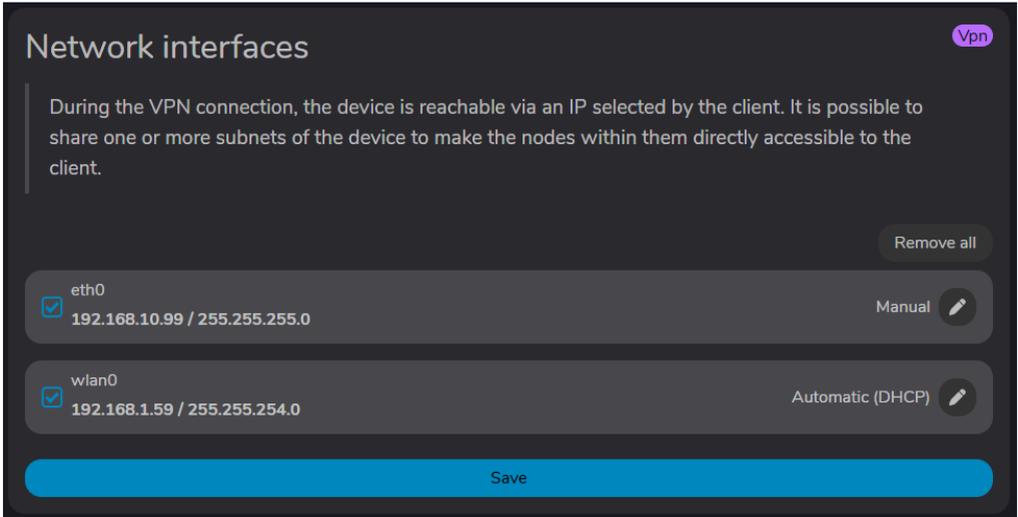
Enable the “VPN” flag to allow the gateway to connect VPN to your PC.

You can enter a security password that you must enter when establishing the VPN connection from your computer (for details refer to paragraph XXX).



The screenshot shows the 'Connections' configuration page. At the top, the title 'Connections' is displayed. Below it, a descriptive text states: 'It is possible to enable or disable incoming connections to the device and set a shared secret key to increase connection security'. The main configuration area includes an 'Enabled:' toggle switch, which is currently turned on. Below this is a 'Vpn:' toggle switch, also turned on. At the bottom of the configuration area is a 'Password:' input field containing the placeholder text 'Password', with a lock icon on the left and a clear icon on the right. At the bottom of the form, there are two prominent buttons: a blue 'Save' button and a red 'Disconnect all' button.

6.2.3 Section “Network”



The “*Network Interfaces*” tab allows you to enable which network cards (and their devices in that network) will be accessible once the VPN connection is established. The check mark next to the network card that will be part of the LAN sub-network where the devices to be reached when the VPN connection is established will be located, so that the gateway can perform the pass-through function (e.g. you will be able to remotely reach a possible HMI, other PLC or inverter connected to that gateway network card, while the other will be the one used to allow Internet access to the PixsysPortal service). In this example screen, the network ports eth0 and wlan0 have been enabled for the shared VPN pass-through connection:

In the configuration showed in the picture, the PPH600 gateway is configured with port wlan0 (wifi) as 192.168.1.59 (IP address form DHCP server) and with port eth0 as 192.168.10.99 (manual IP).

If a VPN connection is established on port wlan0, all requests/connections from the user PC to addresses in the sub-network 192.168.10.xxx will automatically be routed via VPN to the local device in the sub-network where eth0 is connected.

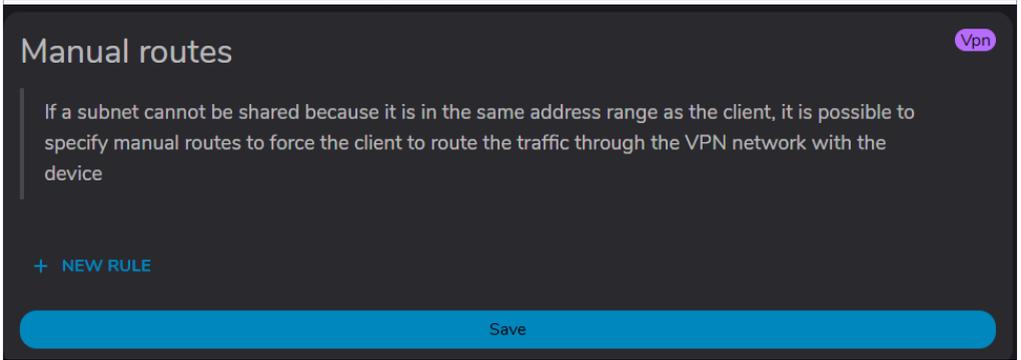
For example, if a local HMI is connect to the switch with IP address 192.168.10.25, to reach it from a PC via VPN the user will only need to use that IP address 192.168.10.25.

NB: It is important to press the “*Save*” button in each section to ensure that the configuration you have just made is saved.

If the network configuration is changed by accessing the webserver remotely (i.e. via VPN connection), please note that:

- the currently established connection may be lost;
- network interfaces configured as accessible will become valid on the next VPN connection.

6.2.4 Section “Routing”



Manual routes Vpn

If a subnet cannot be shared because it is in the same address range as the client, it is possible to specify manual routes to force the client to route the traffic through the VPN network with the device

+ NEW RULE

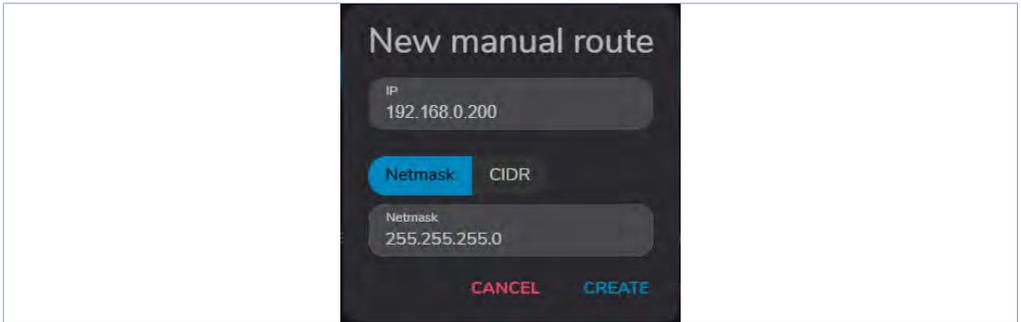
Save

The routing section allows options for configuring manual routing, port-forwarding and gateway routes, as well as filtering access to devices in the sub-network through white-list ranges.

- The “Manual Routing” tab allows you to create one or more rules for VPN access to devices in the gateway sub-network that have the same address class as your PC.

If, for example, your PC has IP address 192.168.0.100 and you want to reach a remote device with IP 192.168.0.200, you must create a rule in this section, otherwise all requests sent from your PC would remain “local” and would not go through the VPN to reach the remote device.

Below is the rule that should therefore be created:



New manual route

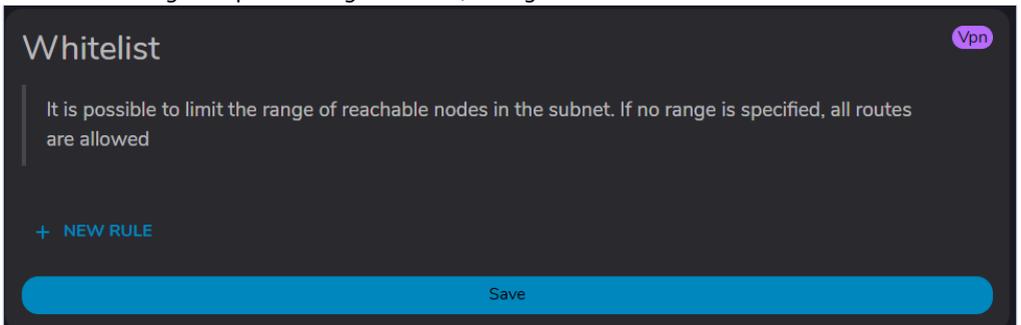
IP
192.168.0.200

Netmask CIDR

Netmask
255.255.255.0

CANCEL CREATE

- The “Whitelist” tab allows you to enable a range of IP addresses (or just one IP address) that will be accessible through the pass-through function, hiding all others.



Whitelist Vpn

It is possible to limit the range of reachable nodes in the subnet. If no range is specified, all routes are allowed

+ NEW RULE

Save

If no rule is present (default), all device IPs in the subnetwork will be reachable.

- The "Port forwarding" tab allows the creation of rules to forward requests received on a specific port to a specific IP address in the sub-network.

Port forwarding

Port forwarding allows all requests received on a certain port to be forwarded to another device on an internal network, without the latter needing to be exposed to the public network

Ex. to reach thru VNC(5900) a subnet PC 192.168.0.1 using port 1234:
1234 [tcp,udp] → 192.168.0.1:5900

Ex. to reach thru SSH(22) a subnet PC 192.168.0.2 using port 5678:
5678 [tcp] → 192.168.0.2:22

+ NEW RULE

Save

- The "Gateway Routes" tab allows you to create a rule whereby devices in the subnetwork can access the Internet via the gateway's WAN connection.

In order for the devices in the sub-network to be able to access the Internet, the IP address of the PPH600's eth0.2 network (default 192.168.10.1) must be specified as the gateway address in their network configuration.

Gateway routes

It is possible to provide internet access to devices in your local subnet by choosing which is the internet access connection (WAN) and which is the local connection (LAN)

N.B. In order for devices in the subnet to access the internet, you need to configure their gateway with the IP address of the device's LAN network

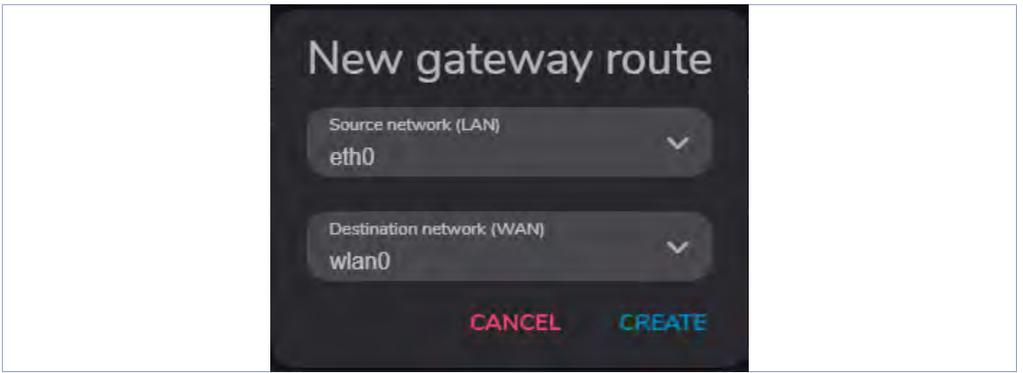
Ex. to allow devices connected on local network (eth0) to reach internet thru network connected to the router (eth1):
eth0 → eth1

eth0 → wlan0

+ NEW RULE

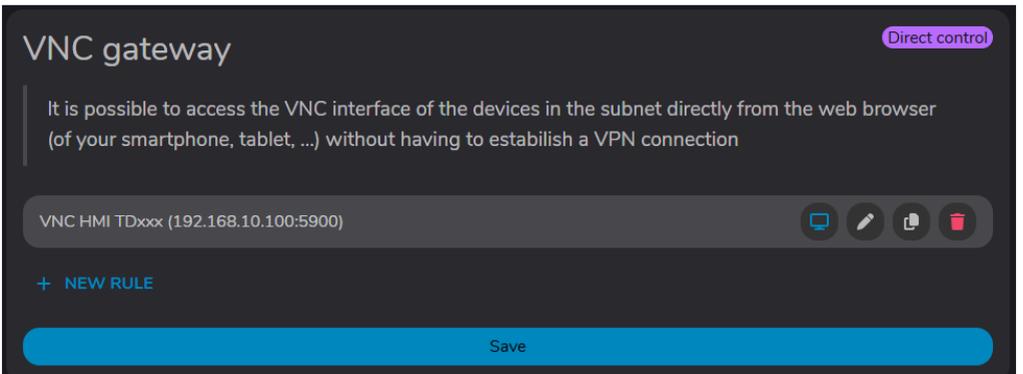
Save

For example, by creating a rule as in the image below, devices in the eth0 sub-network will be able to access the Internet via the WAN wlan0 connection of the PPH600 gateway.



6.2.5 Section “VNC gateway”

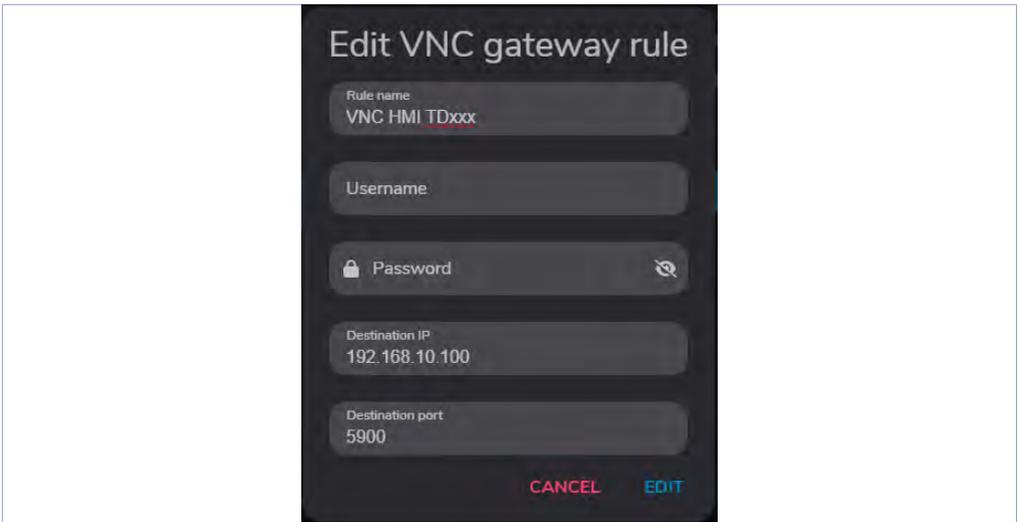
The “VNC Gateway” function allows access to and interaction with the VNC interface of the devices present in the sub-network, **without having to make a VPN connection**, by exploiting the gateway’s “direct control” service. Several VNC rules can be entered, so that with access to the “Direct Control” function, the user already has predefined buttons to access the interfaces of their devices, without having to know their IP address and credentials.



This functionality can therefore be exploited from any device with a web browser (i.e. smartphone, tablet, etc.) and therefore does not require a Windows PC. All you have to do is access the www.portal.pixsys.net web page, enter your credentials and, once you have selected the desired gateway, press the “Direct Control” button:



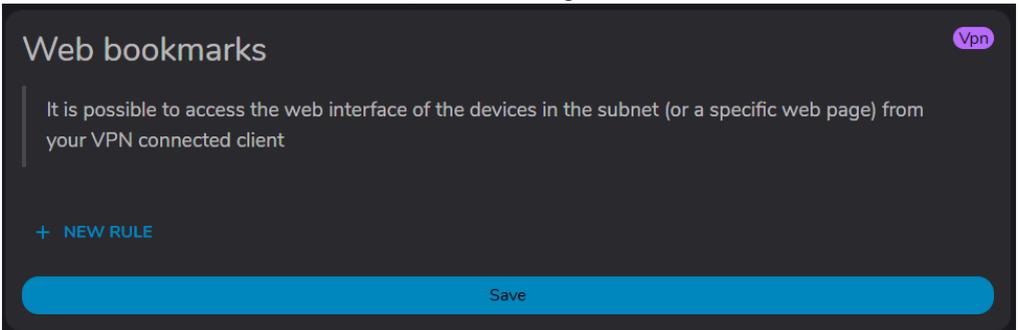
The following rule, for example, allows access to the VNC server of a TD710 panel with IP address 192.168.10.100:



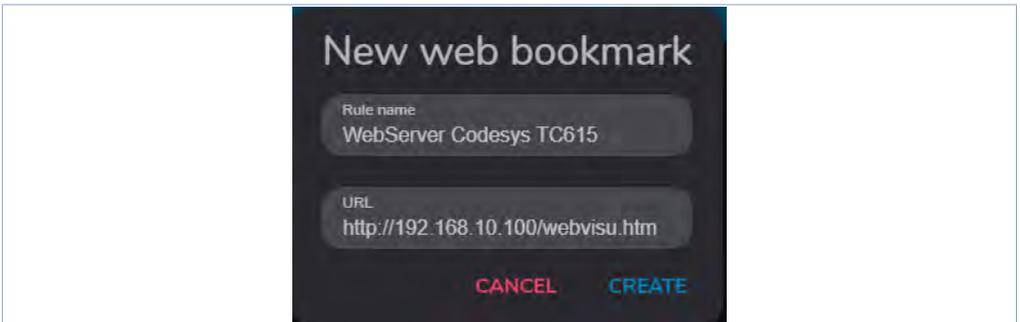
6.2.6 Section “Web Bookmarks”

The “*Web Bookmarks*” function allows access and interaction with the WebServers of the devices in the sub-network, via VPN connection.

Multiple Web Bookmarks can be inserted, so that the user already has predefined buttons to access the WebServer interfaces of their devices, without having to know their IP address and credentials.



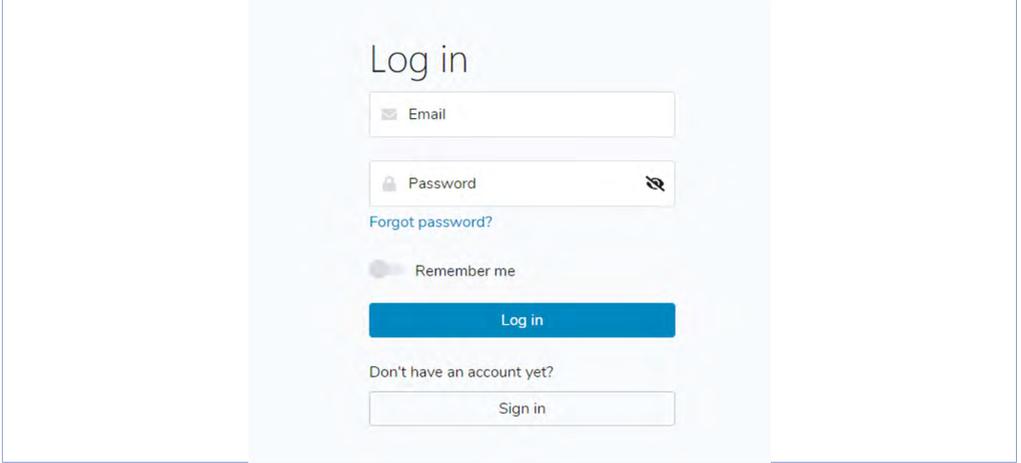
The following rule, for example, allows access to the Codesys WebServer (WebVisu) of a TC615 panel with IP address 192.168.10.100:



6.3 INSTALLING THE APPLICATION ON YOUR COMPUTER AND CREATING THE PixsysPortal ACCOUNT

The VPN connection between a PC and the PPH600 gateways is made via a special “client” software that must be installed on your Windows PC.

- Go to the PixsysPortal service page (Pixsys Portal | VPN Software) and from the “software” menu download PixsysPortal Installer.zip, extract it and install PixsysPortal Installer.exe
- Once started, click on SIGN IN to create your account and follow the instructions provided (you will have to confirm account activation by clicking on the link provided in the e-mail received).

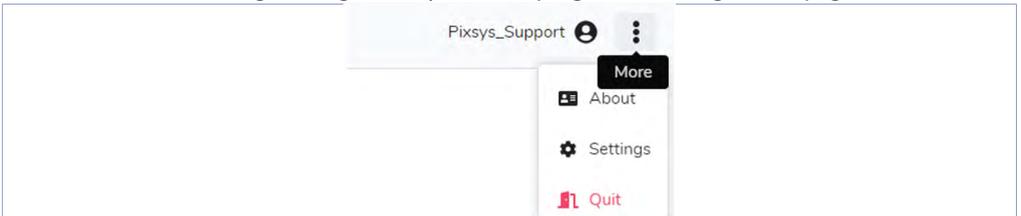


6.3.1 Using the PixsysPortal client

- Once the client is installed, start the “Pixsys Portal” programme from the desktop icon



- Then log in with the credentials chosen during account activation
- The name of the connected account is displayed in the top right-hand corner, and pressing the three vertical dots and choosing ‘Settings’ takes you to the programme configuration page



From this screen you can choose the system language, light/dark theme and other operating details that are automatically set during installation (it is not necessary to change them except in specific cases)

Settings

The screenshot shows the 'General' settings page in the Pixsys Portal. It includes the following options:

- Language: English
- Theme: Light (selected)
- Check for updates on startup:
- Notification audio:
- VNC path: C:\Program Files\Pixsys\Pixsys P...
- File transfer path: C:\Program Files\Pixsys\Pixsys P...
- Date format: Year / Month / Day

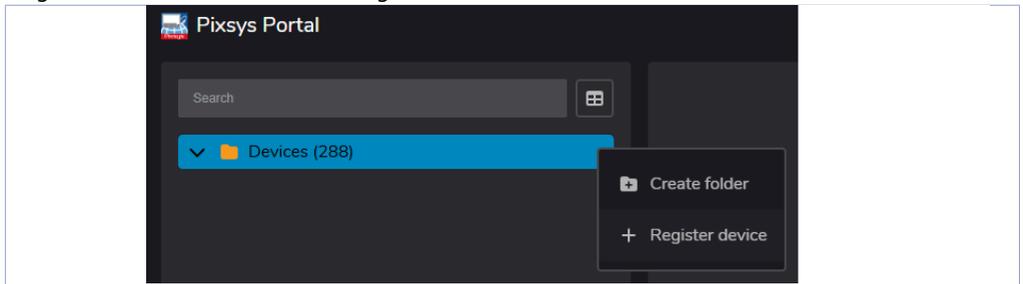
A blue 'Save' button is located at the bottom of the settings panel.

NB: it is important to press the 'Save' button in each section, to ensure that the configuration just made is saved.

- To return to the main screen, press the Pixsys Portal logo in the top left-hand corner.

6.3.2 Associating the device with your PixsysPortal account

- Right-click on Devices and select Register Device



- Enter the credentials (ID and Password) indicated in the PLC WebServer in the window that appears on your computer and click CONTINUE

The screenshot shows the 'Register device' dialog box. It contains the following fields and buttons:

- Device ID*: 11
- Password*:
- CANCEL button
- CONTINUE button

- Give the device a name of your choice and possibly a description and confirm

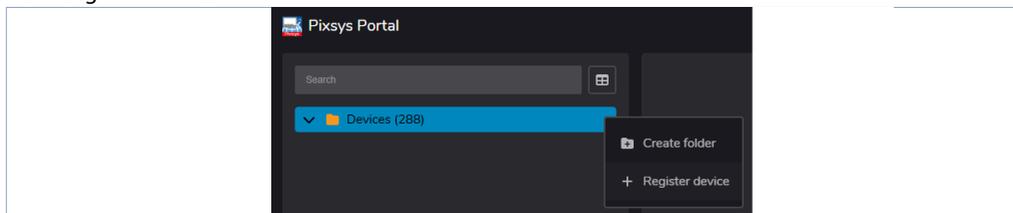


The screenshot shows a 'Register device' dialog box with the following fields and buttons:

- Name***: TD810 Irrigazione
- Description**: Stazione controllo meteo e irrigazione giardino
- CANCEL** button (red text)
- REGISTER** button (blue text)

At this point, the PLC just registered to your account will appear in the list of your devices.

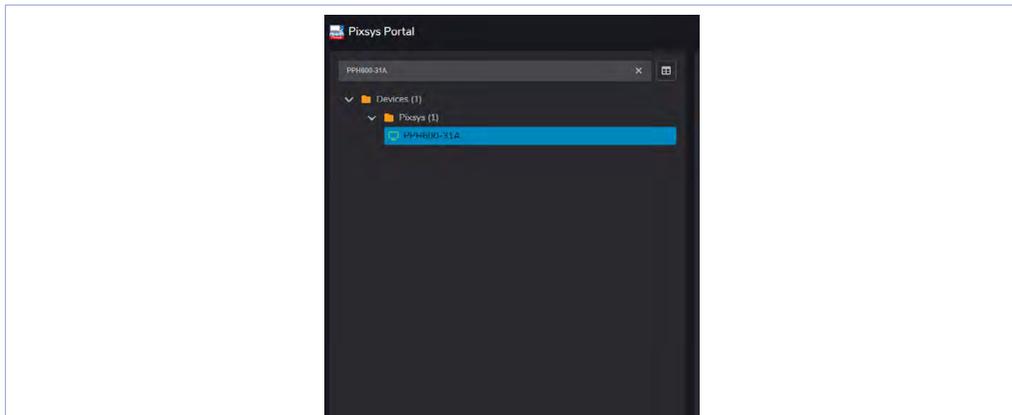
- You can also group the different devices into folders by right-clicking on the Devices item and selecting Create Folder.



Next, simply drag the desired device into the newly created folder.

6.3.3 Make a remote connection to the device

- Once you have started the PixsysPortal application and logged into your account, you will see the list of associated devices.



It is also possible to view one's device list in tabular mode, for quick reference of the statistical data of each device.

NB: the green icon indicates that the device is reachable from PixsysPortal's servers and therefore it will be possible to make the VPN connection to it; the red icon, on the other hand, indicates that the device is offline and therefore not reachable from PixsysPortal's servers. In this case, check the device's internet connection and its network configurations, possibly switching it off and on again if these change.

Proceed by selecting a device from those online (green icon), at which point you can either use the "Direct Control" function to access the VNC of the devices in the sub-network, or the 'VPN' function to establish the VPN tunnel.



Pressing on the "Direct Control" button and then on Connect displays the window showing the buttons giving access to the various configured VNC servers (see section "VNC gateway" for more information).



Clicking on “Disconnect” terminates the WebRTC connection from the gateway. Instead, clicking on the “VPN” button and then on “Connect” displays the window showing the buttons giving access to the various configured WebServers (see section 6 “Web Bookmarks” in the first paragraph for more information). You will also see the IP address assigned to that device and the information of the accessible networks (see section 3 “Network” of the first paragraph for more information).

In this case the gateway has IP address 10.253.253.10 and has the two networks eth0 and wlan0 and their connected devices remotely accessible.

It is then possible to connect to one of the devices in the PLC sub-network with the development software by directly pointing to the ‘local’ IP address of the device itself.

If, for example, you have a PLC with address 192.168.1.50 connected in the eth0 sub-network, it will be sufficient to use this IP address to connect from the development environment. The “Pixsys Portal Settings” button allows access to the WebServer for configuring the gateway’s PixsysPortal service, without having to know the local IP address (a web page at address 10.253.253.10:8080 will be opened). With “Disconnect” you terminate the VPN connection from the gateway.

Details’ tab

The Details tab shows the gateway’s main information, licence status, usage counters and the currently installed firmware version, as well as whether there are any updates (for more information see section 1- “Details” in the first paragraph).

Details

Id	[REDACTED]
Name	PPH600-31A
Description	2
Public IP	93.39.118.6
Network interfaces	192.168.0.110/24 (eth0.1) 192.168.10.1/24 (eth0.2)
Product key	1123-8802-0722E-F109
Runtime version	1.6.11 Check for updates
System info	Product Name CNV600-1AD Kernel Version 4.19.212-bone-rt-r71 OS Version 0a20bf13 Build date 2024/01/11 09:05:12 Serial number [REDACTED]
First access	2024/08/22 12:02:14
Last access	2025-02-06 14:47:08
Registration time	2024/09/25 16:03:12
VPN connections	First connection 2024/09/16 09:11:12 - 2024/09/16 09:33:54 (22:42) Last connection 2025/02/06 14:42:29 - 2025/02/06 14:46:45 (04:16)
WebRTC connections	First connection 2024/09/16 15:47:55 - 2024/09/16 15:49:43 (01:48) Last connection 2025/02/05 16:44:33 - 2025/02/05 16:45:25 (00:52)

Local Options' Tab

On the local options tab, the password, which may have been enabled, must be entered in order to be able to make the VPN connection to the gateway (for more information see section 2- "Security" in the first paragraph).

Local options

Password	[REDACTED]
VPN subnet	10.253.253.0 / 24
VPN auto reconnect	<input type="checkbox"/>
Save	

The "VPN Network" item shows and allows the change of the IP address that the gateway will obtain when the VPN connection is established.

The "Automatic VPN reconnection" flag allows the client on the PC to re-establish the VPN connection automatically if it is interrupted for external reasons (unstable network, loss of Internet connection, etc.).

Users' tab

The users tab shows and allows you to manage the users (PixsysPortal accounts) who have access to the gateway. See the following section for more information.

6.3.4 Sharing the device with other PixsysPortal accounts

Via the Users menu, the device can be shared with other PixsysPortal users (i.e. accounts already registered to the PixsysPortal service). The device can be shared as simple user or owner:

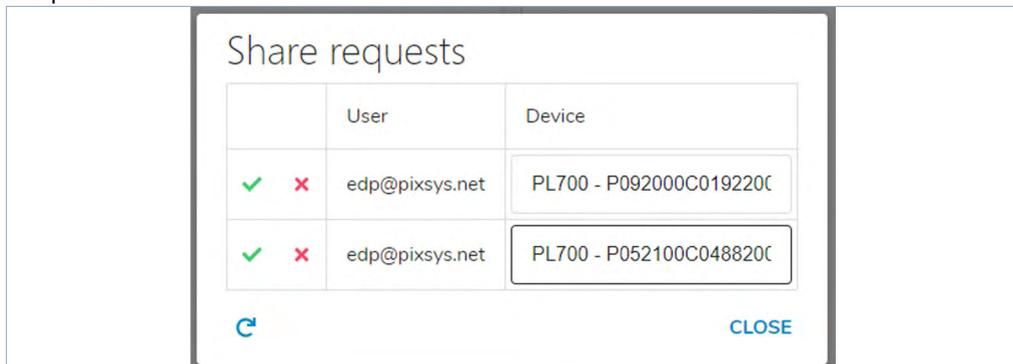
Simple user: the account that "gets" the device can check its connection status and details as well as make the VPN connection to it. He/she may NOT share the device with other users.

Owner: The account that "gets" the device can perform the operations possible as a simple user but also share the device with other PixsysPortal users as well as delete a specific user from the device's owners.

The PixsysPortal user who "gets" the device will receive on his PixsysPortal application a notification in the form of a red dot next to his username



If you click on your name, the drop-down menu will show the same red dot also on the item Sharing Requests, clicking on that item will open a window showing any sharing requests received but not yet accepted



At this point, through the icons ✓ ✗ it is possible to decide whether to accept or reject the sharing request of the specific device.

Introduzione

PPH600 è un gateway VPN con finalità di telecontrollo e/o teleassistenza, in configurazione verticale per ottimizzare gli spazi su barra DIN e alimentazione 24Vdc su morsetto.

Due le configurazioni disponibili, x0A ed x1A. Il modello x0A si compone di uno switch ethernet pre-configurato con 3/6 porte LAN, 1 porta WAN (per l'accesso ad internet), 1 porta PLC (tagged); questa è la soluzione ideale per aumentare il numero di porte ethernet dei PLC serie PL600 e PL700 e opera come gateway VPN qualora i PLC siano dotati di servizio PixsysPortal attivo. Il modello x1A integra nativamente il servizio PixsysPortal ed è quindi un Gateway VPN universale che consente l'accesso a qualsiasi dispositivo dotato di connessione ethernet.

1 Norme di sicurezza

Prima di utilizzare il dispositivo leggere con attenzione le istruzioni e le misure di sicurezza contenute in questo manuale. Disconnettere l'alimentazione prima di qualsiasi intervento su connessioni elettriche o settaggi hardware al fine di prevenire il rischio di scosse elettriche, incendio o malfunzionamenti.

Non installare e non mettere in funzione lo strumento in ambienti con sostanze infiammabili, gas o esplosivi. Questo strumento è stato progettato e realizzato per l'utilizzo convenzionale in ambienti industriali e per applicazioni che prevedano condizioni di sicurezza in accordo con la normativa nazionale e internazionale sulla tutela della delle persone e la sicurezza dei luoghi di lavoro. Deve essere evitata qualsiasi applicazione che comporti gravi rischi per l'incolumità delle persone o sia correlata a dispositivi medici salvavita. Lo strumento non è progettato e realizzato per installazione in centrali nucleari, armamenti, sistemi di controllo del traffico aereo o della sicurezza in volo, sistemi di trasporto di massa.

L'utilizzo/manutenzione è riservato a personale qualificato ed è da intendersi unicamente nel rispetto delle specifiche tecniche dichiarate in questo manuale.

Non smontare, modificare o riparare il prodotto né toccare nessuna delle parti interne.

Lo strumento va installato e utilizzato esclusivamente nei limiti delle condizioni ambientali dichiarate. Un eventuale surriscaldamento può comportare rischi di incendio e abbreviare il ciclo di vita dei componenti elettronici.

1.1 Organizzazione delle note di sicurezza

Le note sulla sicurezza in questo manuale sono organizzate come segue:

Note di sicurezza	Descrizione
Danger!	La mancata osservanza di queste linee guida e avvisi di sicurezza può essere potenzialmente mortale.
Warning!	La mancata osservanza di queste linee guida e avvisi di sicurezza può comportare lesioni gravi o danni sostanziali alla proprietà.
Information!	Tali informazioni sono importanti per prevenire errori.

1.2 Note di sicurezza

Questo prodotto è classificato come apparecchiatura di controllo del processo di tipo a fronte quadro.	Danger!
Se i relè di uscita vengono utilizzati oltre la loro aspettativa di vita, possono verificarsi occasionalmente fusioni o bruciature dei contatti.	
Considerare sempre le condizioni di applicazione e utilizzare i relè di uscita entro il loro carico nominale e l'aspettativa di vita elettrica. L'aspettativa di vita dei relè di uscita varia notevolmente con il carico in uscita e le condizioni di commutazione.	Danger!
Per i morsetti a vite dei relè e dell'alimentazione stringere le viti ad una coppia di serraggio pari a 0,51 Nm. Per gli altri morsetti la coppia è di 0,19 Nm.	Warning!
Un malfunzionamento nel controllore digitale può occasionalmente rendere impossibili le operazioni di controllo o bloccare le uscite di allarme, con conseguenti danni materiali. Per mantenere la sicurezza, in caso di malfunzionamento, adottare misure di sicurezza appropriate; ad esempio con l'installazione di un dispositivo di monitoraggio indipendente e su una linea separata.	Warning!

1.3 Precauzioni per l'uso sicuro

Assicurarsi di osservare le seguenti precauzioni per evitare errori, malfunzionamenti o effetti negativi sulle prestazioni e le funzioni del prodotto. In caso contrario, occasionalmente potrebbero verificarsi eventi imprevedibili. Non utilizzare il controller digitale oltre i valori nominali.

- Il prodotto è progettato solo per uso interno. Non utilizzare o conservare il prodotto all'aperto o in nessuno dei seguenti posti:
 - Luoghi direttamente soggetti a calore irradiato da apparecchiature di riscaldamento.
 - Luoghi soggetti a spruzzi di liquido o atmosfera di petrolio.
 - Luoghi soggetti alla luce solare diretta.
 - Luoghi soggetti a polvere o gas corrosivi (in particolare gas di solfuro e gas di ammoniaca).
 - Luoghi soggetti a forti sbalzi di temperatura.
 - Luoghi soggetti a formazione di ghiaccio e condensa.
 - Luoghi soggetti a vibrazioni e forti urti.
- L'utilizzo di due o più controller affiancati o uno sopra l'altro possono causare un incremento di calore interno che ne riduce il ciclo di vita. In questo caso si raccomanda l'uso di ventole per il raffreddamento forzato o altri dispositivi di condizionamento della temperatura interno quadro.
- Controllare sempre i nomi dei terminali e la polarità e assicurarsi di effettuare una cablatrice corretta. Non collegare i terminali non utilizzati.
- Per evitare disturbi induttivi, mantenere il cablaggio dello strumento lontano da cavi di potenza con tensioni o correnti elevate. Inoltre, non collegare linee di potenza insieme o in parallelo al cablaggio del controller digitale. Si consiglia l'uso di cavi schermati e condotti separati. Collegare un limitatore di sovratensione o un filtro antirumore ai dispositivi che generano rumore (in particolare motori, trasformatori, solenoidi, bobine o altre apparecchiature con componenti induttivi). Quando si utilizzano filtri antidisturbo sull'alimentazione, controllare tensione e corrente e collegare il filtro il più vicino possibile allo strumento. Lasciare più spazio possibile tra il controller e dispositivi di potenza che generano alte frequenze (saldatrici ad alta frequenza, macchine per cucire ad alta frequenza, ecc.) o sovratensioni.
- Un interruttore o un sezionatore deve essere posizionato vicino al regolatore. L'interruttore o il sezionatore deve essere facilmente raggiungibile dall'operatore e deve essere contrassegnato come mezzo di disconnessione per il controller.
- Rimuovere lo sporco dallo strumento con un panno morbido e asciutto. Non usare mai diluenti, benzina, alcool o detersivi che contengano questi o altri solventi organici. Possono verificarsi deformazioni o scolorimento.
- Il numero di operazioni di scrittura della memoria non volatile è limitato. Tenere conto di questo quando si utilizza la modalità di scrittura in EEPROM ad esempio nella variazione dei dati durante le comunicazioni seriali.
- Non utilizzare prodotti chimici/solventi, detersivi e altri liquidi.
- Il mancato rispetto di queste istruzioni può ridurre le prestazioni e la sicurezza dei dispositivi e causare pericolo per persone e cose.

Per ingressi CT (Current Transformer):

- **Warning:** Per ridurre il rischio di scosse elettriche, scollegare sempre il circuito dal sistema di distribuzione dell'energia dell'edificio prima di installare/riparare i trasformatori di corrente.
- Per il monitoraggio dell'energia utilizzare trasformatori di corrente certificati.
- I trasformatori di corrente non possono essere installati in apparecchiature dove superano il 75% dello spazio di cablaggio in qualsiasi area della sezione trasversale all'interno dell'apparecchiatura.
- Evitare l'installazione del trasformatore di corrente in un'area in cui possa bloccare le aperture di ventilazione.
- Evitare l'installazione del trasformatore di corrente in un'area di sfianto dell'arco di rottura.
- Non adatto a metodi di cablaggio di classe 2.
- Non destinato al collegamento con apparecchiature di classe 2.
- Fissare il trasformatore di corrente e indirizzare i conduttori in modo che questi non entrino in contatto con terminali sotto tensione o bus.

1.4 Tutela ambientale e smaltimento dei rifiuti / Direttiva WEEE

Non smaltire le apparecchiature elettriche ed elettroniche tra i rifiuti domestici. Secondo la Direttiva Europea 2012/19/EU le apparecchiature esauste devono essere raccolte separatamente al fine di essere reimpiegate o riciclate in modo eco-compatibile.

2 Identificazione di modello

PPH600-30A	ETHERNET SWITCH 3LAN 1WAN 1PLC ports 24VDC
PPH600-60A	ETHERNET SWITCH 6LAN 1WAN 1PLC ports 24VDC
PPH600-31A	PIXSYS PORTAL GATEWAY 3LAN 1WAN 1USB ports 24VDC
PPH600-61A	PIXSYS PORTAL GATEWAY 6LAN 1WAN 1USB ports 24VDC

3 Dati tecnici

3.1 Caratteristiche generali

Condizioni operative	Temperatura: 0-45 °C - Umidità 35..95 uR% senza condensa
Protezione	Contenitore e morsettiere: IP20, terminali estraibili
Materiali	Contenitore metallo, frontale PC UL94V2

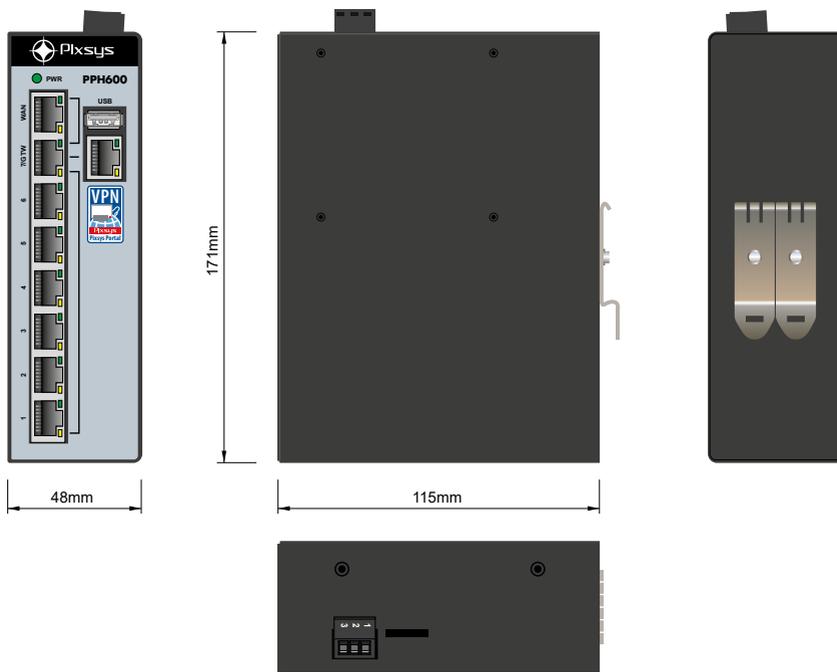
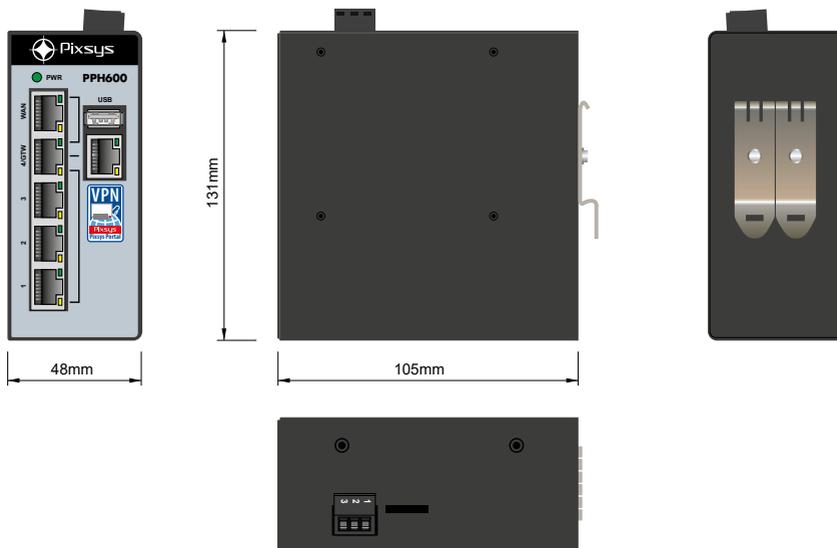
3.2 Caratteristiche Hardware

	PPH600-30A	PPH600-60A	PPH600-31A	PPH600-61A
Alimentazione	24VDC \pm 10% 50/60 Hz			
Consumo	3 Watt/VA			
Dimensioni	48 x 105 x 131mm	48 x 115 x 171mm	48 x 105 x 131mm	48 x 115 x 171mm
Porte LAN	3	6	3	6
Porte WAN	1	1	1	1
Porte PLC	1	1	-	-
Porte USB	-	-	1	1
Pixsys Portal	-	-	SI	SI

3.3 Caratteristiche software

VPN	Servizio Pixsys Portal attivo per connessione desktop remoto (VNC), Web Server, Client FTP, teleassistenza.
-----	---

4 Dimensioni e installazione



5 Primi passi

5.1 Configurazione predefinita

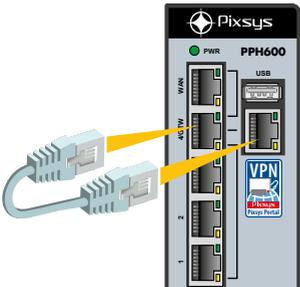
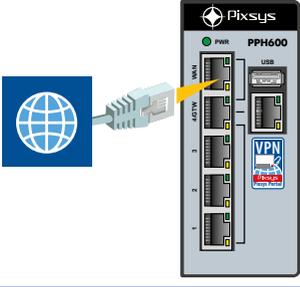
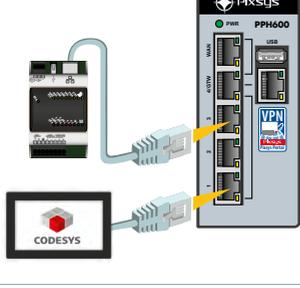
Il gateway PPH600 è dotato di diverse porte Ethernet preconfigurate con questi valori (visibili nell'etichetta posta a lato del gateway stesso):

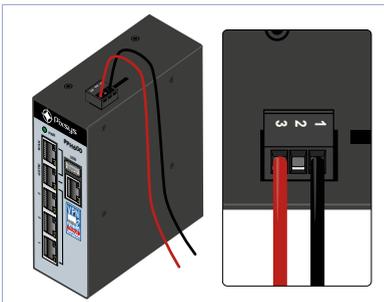
- Porta WAN (da cui il gateway PPH600 accede ad internet): assegnazione IP automatico (DHCP)
- Porta GTW (da cui il gateway PPH600 raggiunge i dispositivi collegati allo switch): Indirizzo IPv4 impostato manualmente a 192.168.10.1

Nella configurazione di fabbrica si prevede quindi l'accesso ad internet attraverso la porta WAN in DHCP ed il collegamento dei dispositivi locali ad una delle porte 1..3 (PPH600-31A) o 1..6 (PPH600-61A) con configurazione IP compatibile con la rete 192.168.10.xxx .

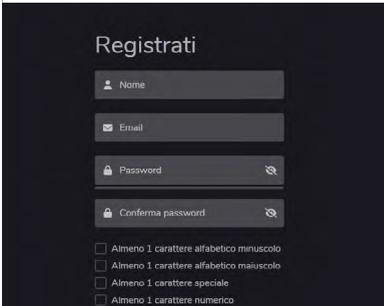
Il WebServer di configurazione del gateway PPH600 è accessibile dall'indirizzo IP 192.168.10.1:8080 da un qualsiasi browser HTML5.

5.2 Procedura per la prima connessione al gateway

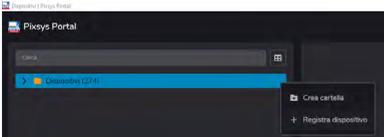
	<p>1- Collegare il cavo ethernet fornito in dotazione tra la porta "GTW" dello switch e quella identificata dal logo "VPN PixsysPortal".</p>
	<p>2- Collegare la porta "WAN" dello switch ad una rete dotata di accesso ad Internet e funzione DHCP abilitata (tipicamente la rete aziendale).</p>
	<p>3- Collegare i propri dispositivi ad una delle porte 1..3 (PPH600-31A) o 1..6 (PPH600-61A) disponibili.</p>



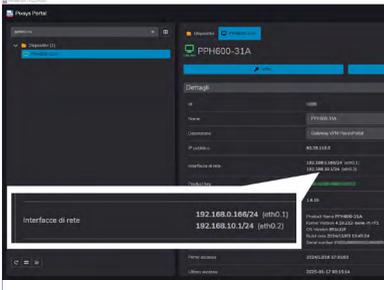
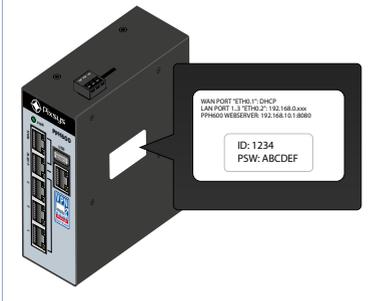
- 4- Alimentare il gateway PPH600 attraverso il morsetto estraibile presente sulla parte superiore del dispositivo
- 1= 0V
 - 2= terra
 - 3= 24V



- 5- Passare al proprio PC: Scaricare da portal.pixsys.net l'ultima versione del client PixsysPortal, installarla sul proprio PC Windows e creare un proprio account seguendo le istruzioni a video.



- 6- Una volta eseguito l'accesso, registrare il gateway PPH600 nel proprio account PixsysPortal facendo click destro sopra la voce "Dispositivi" e scegliendo "Registra dispositivo". Nei campi "ID" e "Password" inserire i dati presenti nell'etichetta applicata lateralmente al gateway PPH600, fornire poi un nome ed eventualmente una descrizione al gateway stesso per riconoscerlo nell'elenco dispositivi.



- 7- A questo punto, nell'elenco dei dispositivi apparirà il nome del gateway PPH600 appena registrato, affiancato da una icona verde nel caso sia già disponibile online oppure rossa nel caso risulti offline. Se online, selezionando il gateway sarà possibile leggerne le caratteristiche, come la versione firmware o la configurazione attuale delle porte di rete:
- Eth0.1 identifica la rete WAN (da cui il gateway PPH600 accede ad internet).
 - Eth0.2 identifica la rete LAN (da cui il gateway PP600 raggiunge i dispositivi collegati allo switch)

5.3 Collegamento VPN ai dispositivi presenti nella sottorete LAN

1- Avviare sul proprio PC il client PixsysPortal

2- Selezionare, dall'elenco a sinistra, il gateway PPH600 a cui si vuole accedere

3- Premere il pulsante "VPN" e successivamente su "Connetti"

4- A connessione avvenuta, i dispositivi collegati allo switch del gateway PPH600 sono disponibili con il proprio indirizzo IP "nativo", quindi per raggiungerli sarà sufficiente utilizzare negli ambienti di sviluppo/BrowserWeb tale indirizzo IP.

N.B. Per configurare diversamente (dalla configurazione di default 192.168.10.xxx) la sottorete LAN del gateway PPH600 o poter sfruttare i collegamenti rapidi alle interfacce VNC / WebServer HTML5 dei dispositivi o abilitare funzioni avanzate di port-forwarding, una volta effettuata la connessione VPN, accedere al WebServer di configurazione del gateway PPH600 premendo il pulsante "Impostazioni PixsysPortal" oppure accedere all'indirizzo IP 10.253.253.10:8080 da un qualsiasi browser HTML5.

6 Pixsys Portal per i Gateway VPN PPH600

Il servizio PixsysPortal permette la connessione sicura, via VPN, di dispositivi connessi ai gateway PPH600 da un qualsiasi computer con Windows 8.1, 10, 11 (se si usa Windows 7, è necessario prima installare la MS PowerShell 5.1 reperibile dal file "PowerShell Win7.zip" presente nell'area download del sito Pixsys).

6.1 PRE-REQUISITI:

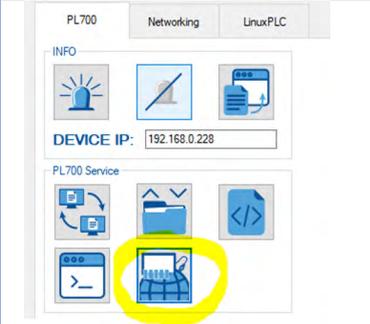
Il servizio PixsysPortal prevede che i dispositivi PPH600 siano connessi, ed opportunamente configurati, ad una rete LAN con connessione ad Internet. Eventualmente è possibile l'accesso ad internet tramite chiavetta USB-Wifi (codice Pixsys 2400.10.021) o modem 4G (codice Pixsys 2200.20.008) ordinabili come accessorio. Le porte utilizzate dal servizio PixsysPortal sono: 443 e la 8005 in TCP/UDP (in uscita). Per il Webserver del servizio, viene inoltre utilizzata la porta 8080.

6.2 CONFIGURAZIONE DEL SERVIZIO

I Gateway VPN PPH600 sono dispositivi basati su sistema operativo Linux Debian 11 ed il servizio PixsysPortal viene eseguito automaticamente all'avvio di questi.

Per configurare le opzioni di PixsysPortal, si accede al suo WebServer da un qualsiasi dispositivo che risiede nella stessa classe di indirizzi:

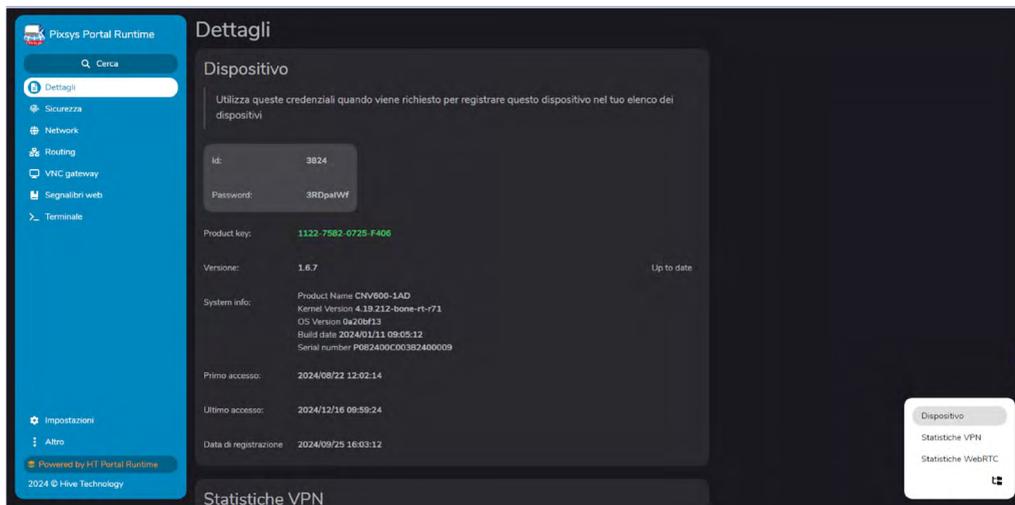
- Accendere il PLC e attendere il completo caricamento dei servizi del sistema operativo (led RUN verde acceso fisso).
- Collegare il gateway ad una rete locale dotata di connessione ad internet usando la porta indicata come WAN.
- Utilizzare l'utility DeviceFinder per identificare l'indirizzo IP del PLC:



In caso di uso dell'utility DeviceFinder, selezionare il gateway dall'elenco di sinistra e premere l'icona evidenziata nell'immagine per connettersi al suo WebServer integrato.

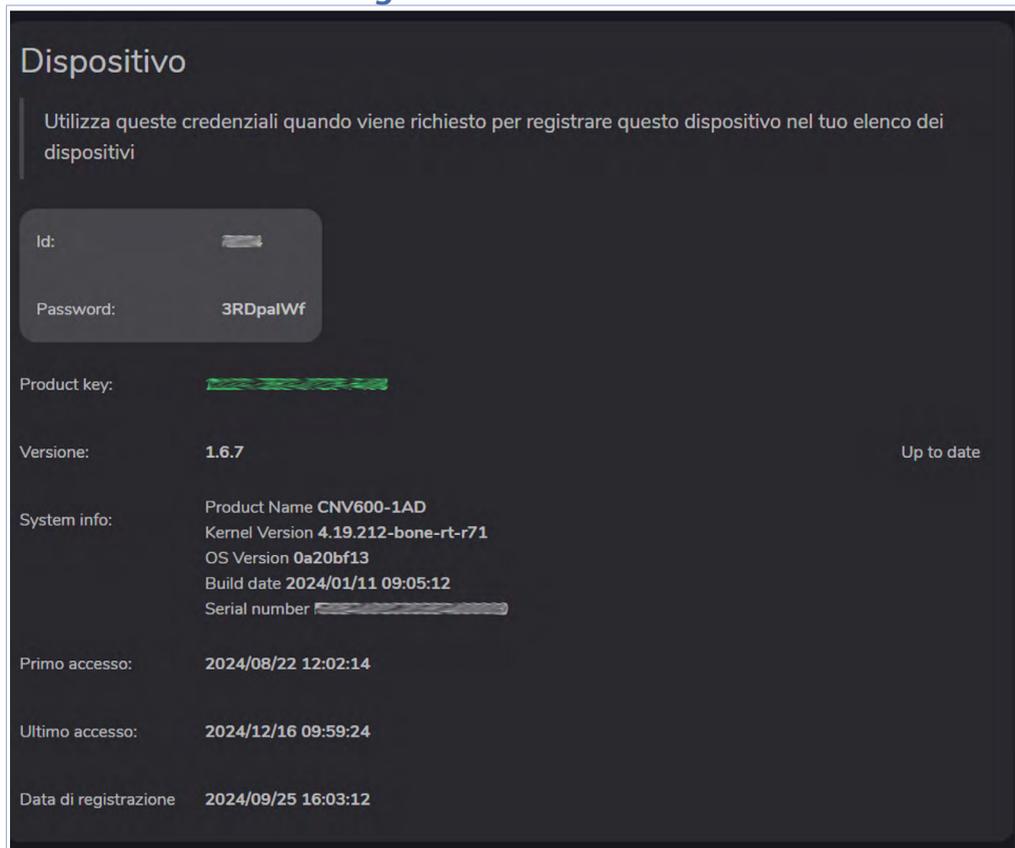
Negli altri casi, aprire un Web browser ed inserire nella barra degli indirizzi, l'indirizzo del gateway specificando la porta 8080, ad esempio 192.168.0.99:8080

- A questo punto si apre il WebServer del servizio PixsysPortal, da cui è possibile procedere alla configurazione.



Il menu a sinistra permette di visualizzare le diverse sezioni che contengono le relative impostazioni.

6.2.1 Sezione “Dettagli”



Nella scheda "Dispositivo" sono visualizzate le informazioni di base del dispositivo, la versione del firmware PixsysPortal corrente e altre info del sistema operativo.

Le credenziali "ID" e "Password" sono i dati necessari per poter associare il gateway al proprio account PixsysPortal (per i dettagli fare riferimento al prossimo paragrafo).

Il campo "Product key" mostra la chiave di attivazione del servizio.

Il campo "Versione" mostra la versione del firmware PixsysPortal attualmente installata nel gateway.

Il pulsante "Cerca aggiornamenti" permette di verificare la presenza di nuovi aggiornamenti ed in caso di installarli.

Il campo "System info" mostra le informazioni del gateway, come il suo nome, la matricola e altre info riguardanti il sistema operativo.

I campi "Primo accesso", "Ultimo accesso" e "Data di registrazione" mostrano rispettivamente la data e l'ora del primo collegamento del gateway al server Pixsys, l'ultimo e quando il gateway si è registrato per la prima volta (cioè quando si è connesso in internet e ha ricevuto ID e password univoci dal server Pixsys).

Nelle schede "Statistiche VPN" e "Statistiche WebRTC" sono visualizzati diversi contatori che fanno riferimento alle connessioni VPN e WebRTC del gateway. Il pulsante "Reset" azzerava questi dati.

Statistiche VPN

Tempo connessione totale: **22d 02:16:05**

Connessioni totali: **88**

Prima connessione: **2024/09/16 09:11:12 - 2024/09/16 09:33:54 (22:42)**

Ultima connessione: **2024/12/16 09:51:42 - 2024/12/16 09:57:46 (06:04)**

Statistiche WebRTC

Tempo connessione totale: **118d 14:30:32**

Connessioni totali: **57**

Prima connessione: **2024/09/16 15:47:55 - 2024/09/16 15:49:43 (01:48)**

Ultima connessione: **2024/12/12 21:13:08 - 2024/12/12 21:13:55 (00:47)**

6.2.2 Sezione “Sicurezza”

Nella “Autenticazione” è possibile abilitare e gestire una password che protegga l’accesso al WebServer di configurazione di PixsysPortal. Al primo accesso, sarà infatti richiesto di scegliere se abilitare oppure no questa protezione, per proteggere la configurazione da accessi indesiderati.

Autenticazione

È possibile impostare un sistema di autenticazione con password per proteggere la configurazione di Pixsys Runtime da accessi indesiderati

Abilitato:

Password:

Conferma password:

Salva

Scollega tutti

La scheda “Connessioni” permette di abilitare e gestire la connessione al server Pixsys e quella VPN:

- Abilitare il flag “*Abilitato*” per consentire al gateway la connessione al server Pixsys.
- Abilitare il flag “*VPN*” per consentire al gateway la connessione VPN al proprio PC.

È possibile inserire una password di sicurezza che l’utente dovrà inserire al momento di stabilire la connessione VPN dal proprio computer (per i dettagli fare riferimento al paragrafo XXX).

Connessioni

È possibile abilitare o disabilitare le connessioni in entrata al dispositivo ed impostare una chiave segreta condivisa per aumentare la sicurezza di connessione

Abilitato:

VPN:

Password:

Salva

Disconnetti tutti

6.2.3 Sezione “Network”



La scheda “Interfacce di rete” permette di abilitare quali schede di rete (e relativi dispositivi presenti in tale rete) saranno accessibili una volta stabilita la connessione VPN. Andrà quindi abilitata la spunta a fianco della scheda di rete che farà parte della sotto-rete LAN dove saranno presenti i dispositivi da raggiungere quando la connessione VPN è stabilita, affinché il gateway possa svolgere la funzione di pass-through (ad esempio si potrà raggiungere da remoto un eventuale HMI, altro PLC o inverter connessi a tale scheda di rete del gateway, mentre l'altra sarà quella usata per consentire l'accesso ad internet al servizio PixsysPortal).

Nella schermata di esempio sono state abilitate le porte di rete eth0 ed wlan0 per la connessione VPN condivisa “pass-through”.

Nell'immagine mostrata il gateway PPH600 è configurato con la porta wlan0 (wifi) come 192.168.0.163 (indirizzo IP dal server DHCP) e la porta eth0 come 192.168.1.99 (IP manuale).

Se una connessione VPN viene istaurata attraverso la porta wlan0, tutte le richieste del PC dell'utente agli indirizzi presenti nella sotto-rete 192.168.1.XXX saranno automaticamente direzionate al dispositivo locale presente nella sotto-rete dove la porta eth0 è connessa.

Per esempio, se un HMI locale è connesso allo switch con indirizzo IP 192.168.1.25. per raggiungerlo da un PC via VPN l'utente dovrà usare direttamente quel indirizzo 192.168.1.25

NB: è importante premere il pulsante “Salva” in ogni sezione, per garantire il salvataggio della configurazione appena effettuata.

Se la configurazione di rete viene modificata accedendo al webserver da remoto (attraverso quindi la connessione VPN), tenere presente che:

- si potrebbe perdere la connessione corrente;
- le interfacce di rete configurate come accessibili diverranno valide alla successiva connessione VPN.

6.2.4 Sezione “Routing”

Instradamenti manuali VPN

Qualora una sotto-rete non possa essere condivisa poichè nella stessa classe di indirizzi del client, è possibile specificare delle rotte manuali per forzare il client a instradare il traffico attraverso la rete VPN con il dispositivo

+ NUOVA REGOLA

Salva

La sezione routing permette di gestire le opzioni per la configurazione degli instradamenti manuali, il port-forwarding e le rotte gateway, nonché filtrare l'accesso a dispositivi presenti nella sotto-rete attraverso range di white-list.

- La scheda “Instradamenti manuali” permette di creare una o più regole per poter accedere via VPN a dispositivi nella sotto-rete del gateway che hanno la stessa classe di indirizzi del proprio PC.

Se ad esempio il proprio PC ha indirizzo IP 192.168.0.100 e si vuole raggiungere un dispositivo remoto con IP 192.168.0.200, è necessario creare una regola in questa sezione, altrimenti tutte le richieste inviate dal proprio PC resterebbero “locali” e non passerebbero attraverso la VPN per raggiungere il dispositivo remoto. Qui sotto la regola che andrebbe quindi creata:

Nuovo instradamento manuale

IP
192.168.0.200

Netmask CIDR

Netmask
255.255.255.0

ANNULLA CREA

- La scheda “Whitelist” permette di abilitare un range di indirizzi IP (o solo un indirizzo IP) che saranno accessibili attraverso la funzione di “pass-through”, nascondendo tutti gli altri.

Whitelist VPN

È possibile limitare il range dei nodi della sotto-rete raggiungibili. Se nessun intervallo viene specificato, tutte le rotte sono consentite

+ NUOVA REGOLA

Salva

Se nessuna regola è presente (default), tutti gli IP dei dispositivi nella sotto-rete saranno raggiungibili.

- La scheda "Port forwarding" permette creare regole per inoltrare le richieste ricevute su una determinata porta ad un preciso indirizzo IP della sotto-rete.

Port forwarding

Il port forwarding consente di inoltrare tutte le richieste ricevute su una determinata porta ad un altro dispositivo su una rete interna, senza che quest'ultimo debba essere esposto alla rete pubblica

Es. per raggiungere tramite VNC(5900) un PC nella sotto-rete 192.168.0.1 attraverso la porta 1234:
1234 [tcp,udp] → 192.168.0.1:5900

Es. per raggiungere tramite SSH(22) un PC nella sotto-rete 192.168.0.2 attraverso la porta 5678:
5678 [tcp] → 192.168.0.2:22

+ NUOVA REGOLA

Salva

- La scheda "Rotte gateway" permette di creare una regola per cui i dispositivi presenti nella sotto-rete potranno accedere ad internet attraverso la connessione WAN del gateway.

Affinché i dispositivi nella sotto-rete possano accedere ad internet, è necessario che, nella loro configurazione di rete, come indirizzo Gateway sia indicato l'indirizzo IP della rete eth0.2 del PPH600 (default 192.168.10.1)

Rotte gateway

È possibile fornire l'accesso ad internet ai dispositivi presenti nella sotto-rete locale scegliendo quale è la connessione con accesso a internet (WAN) e quale è la connessione locale (LAN)

N.B. Affinché i dispositivi della sotto-rete possano accedere ad internet, è necessario configurare il loro gateway con l'indirizzo IP della rete WAN del dispositivo

Es. per consentire ad un dispositivo collegato alla rete locale (eth0) di raggiungere internet tramite la rete collegata al router (eth1):
eth0 → eth1

+ NUOVA REGOLA

Salva

Ad esempio, creando una regola come nell'immagine seguente, i dispositivi nella sotto-rete eth0 saranno in grado di accedere ad internet attraverso la connessione internet proveniente dalla rete WAN wlan0 del gateway PPH600.

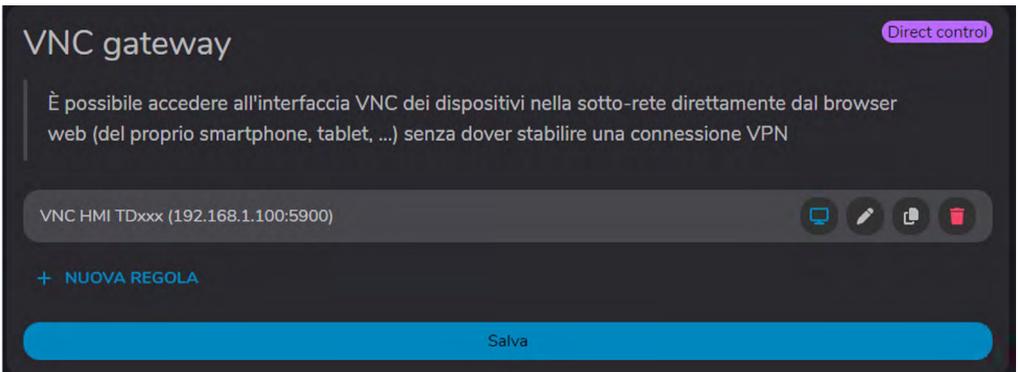


NB: affinché i dispositivi nella sotto-rete possa accedere ad internet attraverso la porta eth0 del PPH600, questi dovranno avere impostato come gateway l'indirizzo della porta eth0 del PPH600 stesso.

6.2.5 Sezione "VNC gateway"

La funzione "VNC Gateway" permette di accedere ed interagire con l'interfaccia VNC dei dispositivi presenti nella sotto-rete, **senza dover effettuare una connessione VPN**, sfruttando il servizio "Direct control" del gateway.

È possibile inserire più regole VNC, in modo che con l'accesso alla funzione "Direct Control", l'utente abbia già dei pulsanti predefiniti per poter accedere alle interfacce dei propri dispositivi, senza doverne conoscere l'indirizzo IP e le relative credenziali.



Questa funzionalità può essere sfruttata quindi da qualsiasi dispositivo dotato di una browser web (quindi smartphone, tablet ecc) e non richiede perciò l'utilizzo di un PC Windows. Sarà sufficiente infatti accedere alla pagina web www.portal.pixsys.net inserire le proprie credenziali e, una volta selezionato il gateway desiderato, premere sul pulsante "Direct Control":



La regola seguente, ad esempio, permette di accedere al server VNC di un pannello TD710 con indirizzo IP 192.168.0.100 :

The screenshot shows a dark-themed form titled "Modifica regola VNC gateway". It contains five input fields: "Nome regola" with the value "VNC HMI TD710", "Username", "Password" (with a lock icon and a visibility toggle), "IP di destinazione" with the value "192.168.0.100", and "Porta di destinazione" with the value "5900". At the bottom right, there are two buttons: "ANNULLA" in red and "MODIFICA" in blue.

6.2.6 Sezione "Segnalibri Web"

La funzione "Segnalibri Web" permette di accedere ed interagire con i WebServer dei dispositivi presenti nella sotto-rete, attraverso la connessione VPN.

È possibile inserire più segnalibri Web, in modo che l'utente abbia già dei pulsanti predefiniti per poter accedere alle interfacce WebServer dei propri dispositivi, senza doverne conoscere l'indirizzo IP e le relative credenziali.

The screenshot shows a dark-themed section titled "Segnalibri web" with a purple "VPN" badge in the top right corner. Below the title is a text block: "È possibile accedere all'interfaccia Web dei dispositivi nella sotto-rete (o una specifica pagina web) dal proprio client collegato in VPN". Below this is a blue button with a plus sign and the text "NUOVA REGOLA". At the bottom, there is a large blue button labeled "Salva".

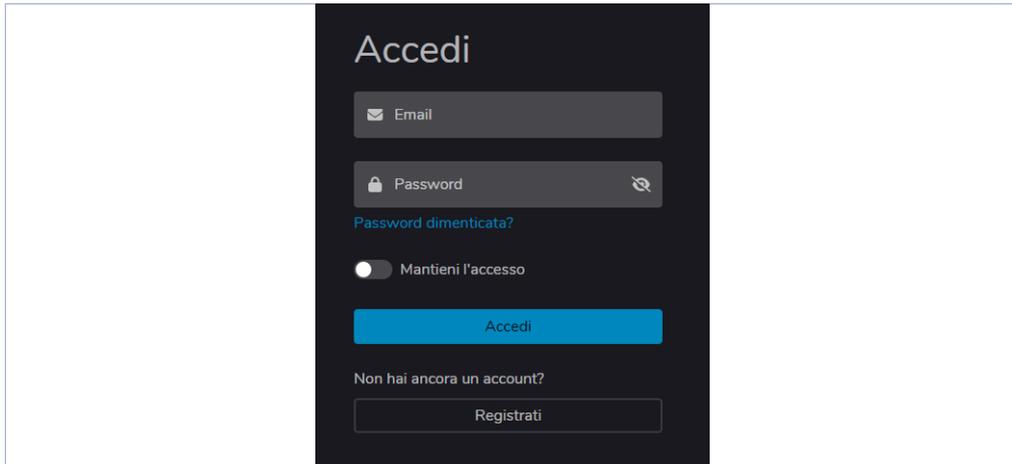
La regola seguente, ad esempio, permette di accedere al WebServer Codesys (WebVisu) di un pannello TC615 con indirizzo IP 192.168.0.100 :

The screenshot shows a dark-themed form titled "Nuovo segnalibro web". It contains two input fields: "Nome regola" with the value "WebServer Codesys TC615" and "URL" with the value "http://192.168.0.100/webvisu.htm". At the bottom right, there are two buttons: "ANNULLA" in red and "CREA" in blue.

6.3 INSTALLAZIONE DELL'APPLICAZIONE SUL PROPRIO COMPUTER E CREAZIONE DELL'ACCOUNT PixsysPortal

La connessione VPN tra un PC e i gateway PPH600 avviene tramite un apposito software "client" che va installato nel proprio PC Windows.

- Accedere alla pagina del servizio PixsysPortal (Pixsys Portal | Software VPN) e dal menu "software" scaricare PixsysPortal Installer.zip, estrarlo ed installare PixsysPortal Installer.exe
- Una volta avviato, premere su SIGN IN per creare un proprio account e seguire le istruzioni fornite (si dovrà confermare l'attivazione dell'account cliccando sul link che verrà fornito dalla e-mail ricevuta).

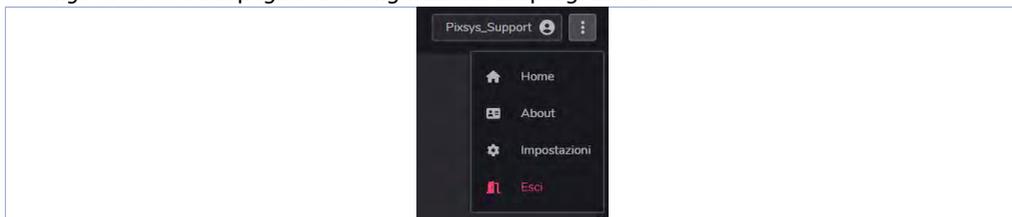


6.3.1 Utilizzo del client PixsysPortal

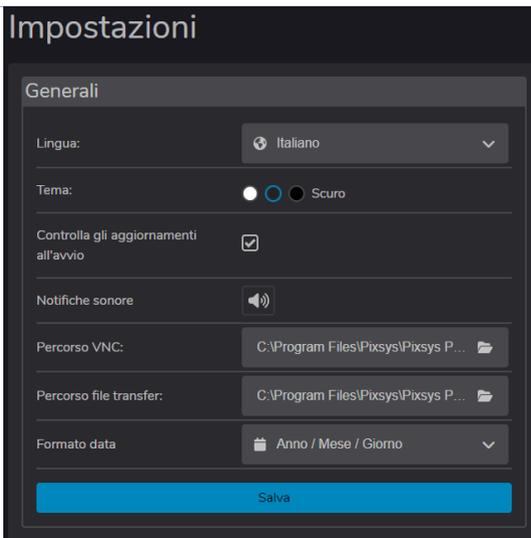
- Una volta installato il client, avviare dall'icona sul desktop il programma "Pixsys Portal"



- Accedere quindi con le credenziali scelte in fase di attivazione account
- In alto a destra si visualizza il nome dell'account collegato, premendo i tre punti verticali e scegliendo "Settings" si accede alla pagina di configurazione del programma



Da questa schermata è possibile scegliere la lingua di sistema, il tema chiaro/scuro ed altri dettagli di funzionamento che sono automaticamente impostati durante l'installazione (non è necessario variarli se non in casi specifici)

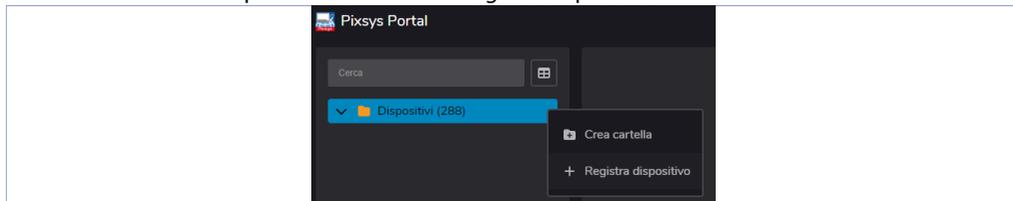


NB: è importante premere il pulsante "Save" in ogni sezione, per garantire il salvataggio della configurazione appena effettuata.

- Per tornare alla schermata principale, premere il logo Pixsys Portal in alto a sinistra.

6.3.2 Associazione del dispositivo al proprio account PixsysPortal

- Fare click destro su Dispositivi e selezionare Registra dispositivo



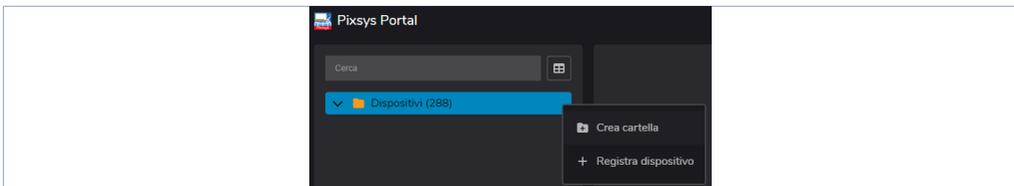
- Inserire le credenziali (ID e Password) indicate nel WebServer del PLC nella finestra che appare sul proprio computer e cliccare su CONTINUA



- Dare un nome a piacere al dispositivo ed eventualmente una sua descrizione e confermare



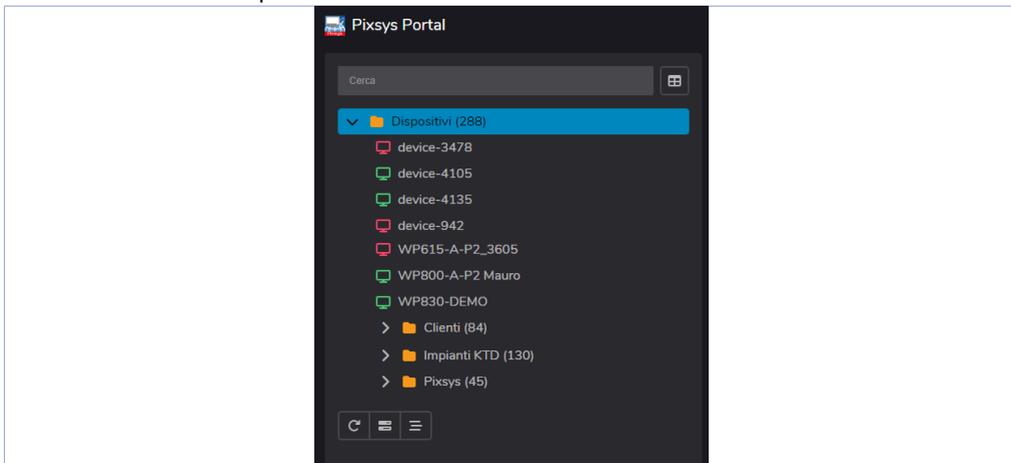
A questo punto il PLC appena registrato al proprio account apparirà nell'elenco dei propri dispositivi.
- È anche possibile raggruppare i diversi dispositivi in cartelle, facendo click destro sulla voce Dispositivi e selezionando Crea Cartella.



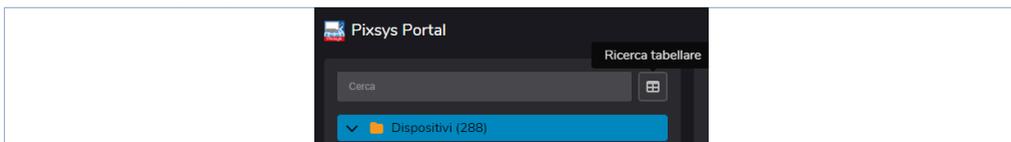
Successivamente, è sufficiente trascinare il dispositivo desiderato nella cartella appena creata.

6.3.3 Effettuare la connessione remota al dispositivo

- Una volta avviata l'applicazione PixsysPortal ed effettuato l'accesso al proprio account, viene visualizzata la lista dei dispositivi associati.



E' anche possibile vedere la propria lista dispositivi in modalità tabellare, per una rapida consultazione dei dati statistici di ciascuno di essi.



NB: l'icona verde indica che il dispositivo è raggiungibile dai server di PixsysPortal e quindi sarà possibile effettuare la connessione VPN a questo; l'icona rossa invece indica che il dispositivo è offline e quindi non raggiungibile dai server di PixsysPortal. In questo caso, verificare la connessione ad internet del dispositivo e le sue configurazioni di rete, eventualmente spegnendo e riaccendendolo in caso di modifica di queste.

Procedere selezionando un dispositivo tra quelli online (icona verde), a questo punto è possibile sfruttare la funzione "Direct Control" per accedere al VNC dei dispositivi presenti nella sotto-rete, oppure la funzione "VPN" per stabilire il tunnel VPN.



Premendo sul pulsante "Direct Control" e poi su Connetti si visualizza la finestra che mostra i pulsanti che danno l'accesso ai vari server VNC configurati (vedere la sezione 5 "VNC gateway" per maggior informazioni).



Con *"Disconnetti"* si termina la connessione WebRTC dal gateway.

Prendo invece sul pulsante *"VPN"* e poi su *Connetti* si visualizza la finestra che mostra i pulsanti che danno l'accesso ai vari WebServer configurati (vedere la sezione 6 *"Segnalibri Web"* del primo paragrafo per maggior informazioni). Si visualizzerà inoltre l'indirizzo IP assegnato a quel dispositivo e le informazioni delle reti accessibili (vedere la sezione 3 *"Network"* del primo paragrafo per maggior informazioni).

In questo caso il gateway ha indirizzo IP 10.253.253.10 e ha le due reti eth0 e wlan0 e i relativi dispositivi connessi accessibili da remoto.

A questo punto è quindi possibile collegarsi ad uno dei dispositivi presenti nella sotto-rete PLC con i software di sviluppo, puntando direttamente l'indirizzo IP *"locale"* del dispositivo stesso.

Se ad esempio si dispone di un PLC con indirizzo 192.168.1.50 collegato nella sotto-rete di eth0 sarà sufficiente utilizzare tale indirizzo IP per collegarsi dall'ambiente di sviluppo.

Il pulsante *"Impostazioni Pixsys Portal"* permette di accedere al WebServer di configurazione del servizio PixsysPortal del gateway, senza doverne conoscere l'indirizzo IP locale (verrà infatti aperta una pagina web all'indirizzo 10.253.253.10:8080).

Con *"Disconnetti"* si termina la connessione VPN dal gateway.

Scheda *"Dettagli"*

La scheda *Dettagli* mostra le informazioni principali del gateway, lo stato della licenza, i contatori di utilizzo e la versione del firmware correntemente installato, nonché l'eventuale presenza di aggiornamenti (per maggiori informazioni vedere la sezione 1- *"Dettagli"* del primo paragrafo).

Dettagli

Id	4
Nome	CNV600-Lab.
Descrizione	
IP pubblico	93.39.118.6
Interfacce di rete	192.168.1.99/24 (eth0) 192.168.0.145/24 (eth1)
Product key	
Versione runtime	1.6.7 Controlla aggiornamenti
System info	Product Name CNV600-1AD Kernel Version 4.19.212-bone-rt-r71 OS Version 0a20bf13 Build date 2024/01/11 09:05:12 Serial number
Primo accesso	2024/08/22 12:02:14
Ultimo accesso	2024-12-16 12:50:59
Data di registrazione	2024/09/25 16:03:12
Connessioni VPN	Prima connessione 2024/09/16 09:11:12 - 2024/09/16 09:33:54 (22:42) Ultima connessione 2024/12/16 12:33:46 - 2024/12/16 12:48:32 (14:46)
Connessioni WebRTC	Prima connessione 2024/09/16 15:47:55 - 2024/09/16 15:49:43 (01:48) Ultima connessione 2024/12/16 12:31:20 - 2024/12/16 12:33:44 (02:24)

Scheda "Opzioni locali"

Nella scheda opzioni locali andrà inserita la password, eventualmente abilitata, per poter effettuare la connessione VPN al gateway ((per maggiori informazioni vedere la sezione 2- "Sicurezza" del primo paragrafo).

Opzioni locali

Password	
Rete VPN	10.253.253.0 / 24
Riconnessione automatica VPN	<input type="checkbox"/>
Salva	

La voce "Rete VPN" mostra e permette la modifica dell'indirizzo IP che il gateway otterrà nel momento che la connessione VPN viene stabilita.

Il flag "Riconnessione automatica VPN" permette al client su PC di riefettuare la connessione VPN automaticamente in caso questa si interrompa per motivi esterni (rete instabile, perdita di connessione internet ecc).

Scheda "Utenti"

La scheda utenti mostra e permette di gestire gli utenti (account PixsysPortal) che hanno accesso al gateway. Per maggiori info vedere il paragrafo seguente.

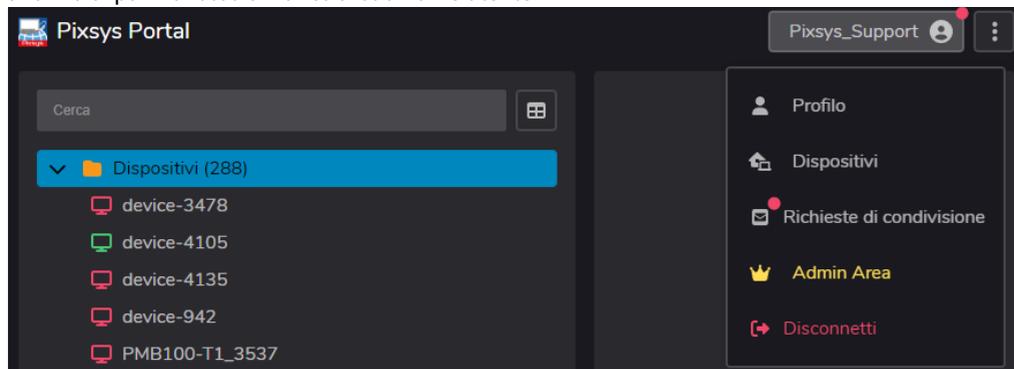
6.3.4 Condivisione del dispositivo con altri account PixsysPortal

Tramite il menu Utenti è possibile condividere il dispositivo ad altri utenti PixsysPortal (cioè account già registrati al servizio PixsysPortal). Il dispositivo può essere condiviso come utente semplice o proprietario:

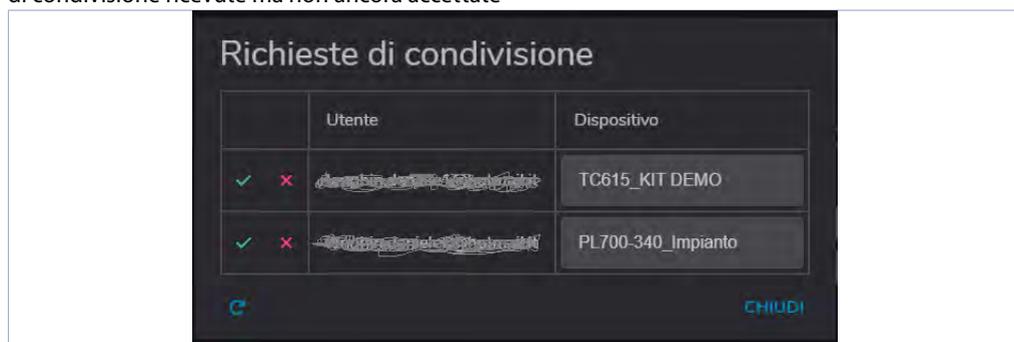
Utente semplice: l'account che "ottiene" il dispositivo può verificarne lo stato di connessione e i dettagli, nonché effettuare la connessione VPN ad esso. NON può condividere il dispositivo con altri utenti.

Proprietario: l'account che "ottiene" il dispositivo può effettuare le operazioni possibili come utente semplice ma anche condividere il dispositivo con altri utenti PixsysPortal nonché eliminare uno specifico utente dai proprietari del dispositivo stesso.

L'utente PixsysPortal che "ottiene" il dispositivo riceverà sulla sua applicazione PixsysPortal una notifica a forma di pallino rosso di fianco al suo nome utente



Cliccando sul proprio nome, il menu a tendina mostrerà lo stesso pallino rosso anche sulla voce Richieste di condivisione, cliccando su tale voce, si aprirà una finestra che mostra le eventuali richieste di condivisione ricevute ma non ancora accettate



A questo punto, attraverso le icone ✓ ✗ è possibile decidere se accettare o scartare la richiesta di condivisione dello specifico dispositivo.

Read carefully the safety guidelines and programming instructions contained in this manual before using/connecting the device.

Prima di utilizzare il dispositivo leggere con attenzione le informazioni di sicurezza e settaggio contenute in questo manuale.

Vor Verwendung des Gerätes sind die hier enthaltenen Informationen bezüglich Sicherheit und Einstellung aufmerksam zu lesen.

Avant d'utiliser le dispositif lire avec attention les renseignements de sûreté et installation contenus dans ce manuel.



PIXSYS s.r.l.

www.pixsys.net

sales@pixsys.net - support@pixsys.net

online assistance: <https://forum.pixsys.net>

via Po, 16 I-30030

Mellaredo di Pianiga, VENEZIA (IT)

Tel +39 041 5190518



2300.10.392-RevA

200125