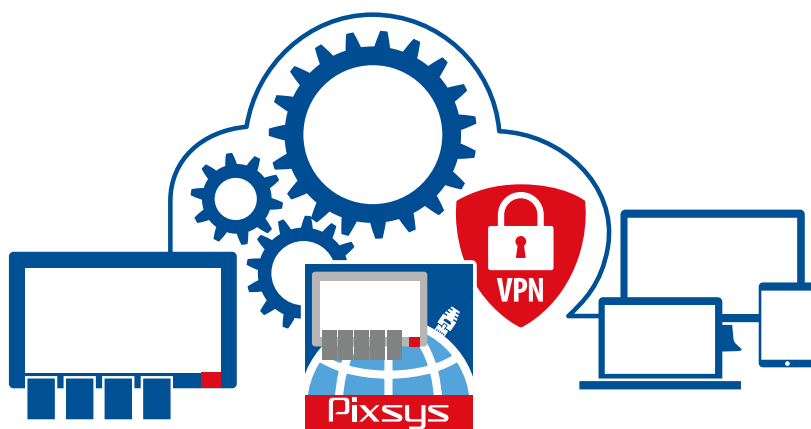




Pixsys Portal Service

VPN - Remote control - Remote assistance



User manual / Manuale d'uso

Table of contents

1	WHAT'S PIXSYS PORTAL	4
1.1	REQUIREMENTS	4
2	SERVICE CONFIGURATION IN DEVICES.....	5
2.1	Section "Details"	6
2.2	Section "Security"	7
2.3	Section "Network"	8
2.4	Section "Routing"	9
2.5	Section "VNC gateway"	11
2.6	Section "Web Bookmarks"	13
3	CREATING THE PIXSYS PORTAL ACCOUNT	13
4	USING THE PIXSYS PORTAL APPLICATION ON YOUR PC	14
4.1	Installing and using the PixsysPortal application	14
4.2	Associating a device to your PixsysPortal account	15
4.3	Make a remote connection to the device	16
4.3.1	Using the "Direct Control" function	17
4.3.2	Using the VPN function	17
4.4	Application details	18
4.5	PixsysPortal licence activation in devices.....	19
4.6	Sharing the device with other PixsysPortal accounts	19

Indice degli argomenti

1	COS'È PIXSYS PORTAL	22
1.1	PRE-REQUISITI DEL SERVIZIO	22
2	CONFIGURAZIONE DEL SERVIZIO NEI DISPOSITIVI	23
2.1	Sezione "Dettagli"	24
2.2	Sezione "Sicurezza"	25
2.3	Sezione "Network"	26
2.4	Sezione "Routing"	27
2.5	Sezione "VNC gateway"	29
2.6	Sezione "Segnalibri Web"	30
3	CREAZIONE DELL'ACCOUNT PIXSYS PORTAL	31
4	UTILIZZO DELL'APPLICAZIONE PIXSYS PORTAL SUL PROPRIO PC	32
4.1	Installazione dell'applicazione PixsysPortal e utilizzo	32
4.2	Associazione di un dispositivo al proprio account PixsysPortal	33
4.3	Effettuare la connessione remota al dispositivo.....	34
4.3.1	Utilizzo della funzione "Direct Control"	35
4.3.2	Utilizzo della funzione VPN	35
4.4	Dettagli dell'applicazione	36
4.5	Attivazione della licenza PixsysPortal nei dispositivi	37
4.6	Condivisione del dispositivo con altri account PixsysPortal	38

Introduction

Pixsys Portal is a software service enabling the transparent management of devices equipped with an Ethernet connection. The service is pre-installed on Pixsys HMIs, PLCs and Panel PCs and allows the creation of a VPN connection optimised for industrial communications, enabling remote control (Remote Desktop, Web Server, data exchange) and/or remote assistance (connection with development environments) of both Pixsys devices and third party devices connected to the same sub-network.

The service does not require firewall or static IP settings. A standard Internet connection via cable or via external devices such as 4G routers equipped with a data SIM card is required.

The Pixsys Portal PC application allows you to monitor all associated systems from a single point, facilitating the operation of users who need to perform remote control.

1 WHAT'S PIXSYS PORTAL

The PixsysPortal service enables the secure connection via VPN of Pixsys devices connected to the Internet and with enabled service, such as the PPH600 gateway, the PL600/PL700 PLCs, the "TC" series TouchController panels, the "WP" series WebPanels, the "PC" series PanelPCs, from any MS Windows computer through the PixsysPortal client application. The "DirectControl" functionality is accessible from any device equipped with a modern HTML5 Web Browser, such as Android/iOS smartphones and tablets.

1.1 REQUIREMENTS

The PixsysPortal client application, available in the "SOFTWARE" section of the relevant page of the Pixsys.net website, can be used on PCs running MS Windows 8.1 and later.

The PixsysPortal service installed in remote devices requires that they be connected, and suitably configured, to a LAN network with Internet connection. Eventually, Internet access is possible by means of a USB-Wifi key (Pixsys code 2400.10.021) or a 4G modem (Pixsys code 2200.20.008) that can be ordered as an accessory. For the "VPN" functionality, the ports used by the PixsysPortal service are 443 and 8005 in TCP/UDP, which must be open on the outgoing side. For the "DirectControl" functionality the technology used is WebRTC and only needs port 443 open at the output. Port 8080 in HTTPS is also used to access the service configuration Webserver in remote devices. Make sure with your IT manager that the requirements are met before using the PixsysPortal service.

The PixsysPortal service requires that the remote device must have a so-called RUNTIME licence in order to be able to make VPN and WebRTC connections without time limits. For more details please refer to the user licence.

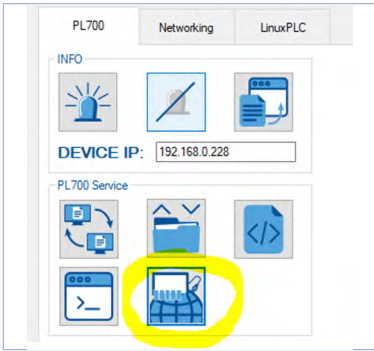
2 SERVICE CONFIGURATION IN DEVICES

On Linux-based devices with the service enabled, the PixsysPortal service runs automatically at start-up. The PL600/700, TC and WP devices integrate the PixsysPortal service, but this must be enabled in order for it to be started automatically when the devices are switched on, via the “cockpit” configuration interface.

For further information please refer to the user manuals of the respective products.

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

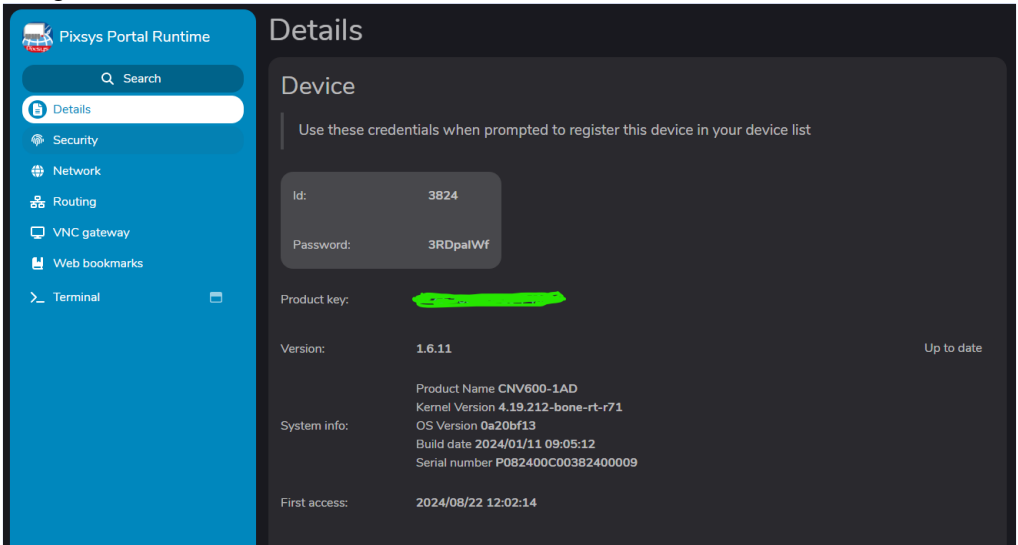
- Switch on the PLC and wait for the operating system services to load completely (RUN LED steady green).
- Connect the gateway to a local network with an Internet connection using the port indicated as WAN.
- Use the DeviceFinder utility to identify the IP address of the PLC:



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.

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

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



Details

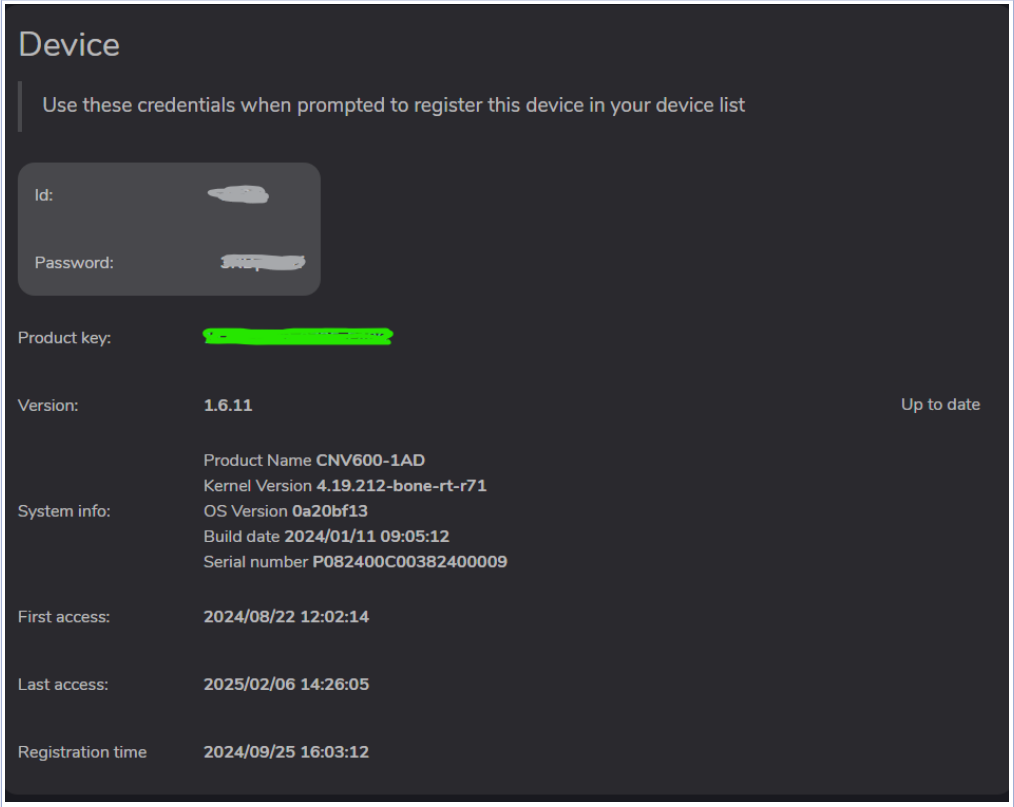
Device

Use these credentials when prompted to register this device in your device list

Id:	3824
Password:	3RDpalWf
Product key:	[REDACTED]
Version:	1.6.11 Up to date
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 P082400C00382400009
First access:	2024/08/22 12:02:14

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

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.

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)**

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.

Authentication

It is possible to set up a password authentication system to protect the Pixsys Runtime configuration from unauthorized access

Enabled: ☒

Password: 

Confirm password: 

Save

Logout all

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.

Connections

It is possible to enable or disable incoming connections to the device and set a shared secret key to increase connection security

Enabled: ☒

Vpn: ☒

Password:

Save

Disconnect all

2.3 Section “Network”

Network interfaces

During the VPN connection, the device is reachable via an IP selected by the client. It is possible to share one or more subnets of the device to make the nodes within them directly accessible to the client.

Remove all

☒	eth0	192.168.10.99 / 255.255.255.0	Manual
☒	wlan0	192.168.1.59 / 255.255.254.0	Automatic (DHCP)

Save

The devices, through the VPN connection, are accessible from a remote computer and can also make any other devices in their network accessible, with so-called passthrough. For example, any HMI, other PLC or inverter connected to the Pixsys device with an active PixsysPortal service can be accessed remotely.

It is only necessary to enable whether and which network card will use this functionality, without having to indicate the IPs of local devices or anything else.

The “Network Interfaces” tab allows you to enable which network cards (and the devices present in that

network) will be accessible once the VPN connection is established, i.e. you will have to put a tick 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, while the other network card will be the one used to allow Internet access to the PixsysPortal service running in the device).

In the example screenshot, the network ports 'eth0' and 'wlan0' have been enabled for the shared VPN "pass-through" connection, i.e. both will make any devices connected to them available. The screenshot shows a device configured with the wlan0 port (wifi USB card) as IP address 192.168.0.163 and the "eth0" port (physical RJ45 port) as 192.168.1.99 .

If a VPN connection is established via one of the two network interfaces, all requests from the remote PC to addresses in the 192.168.0.XXX or 192.168.1.XXX sub-network will automatically be directed to the local device in the sub-network of the correct address class.

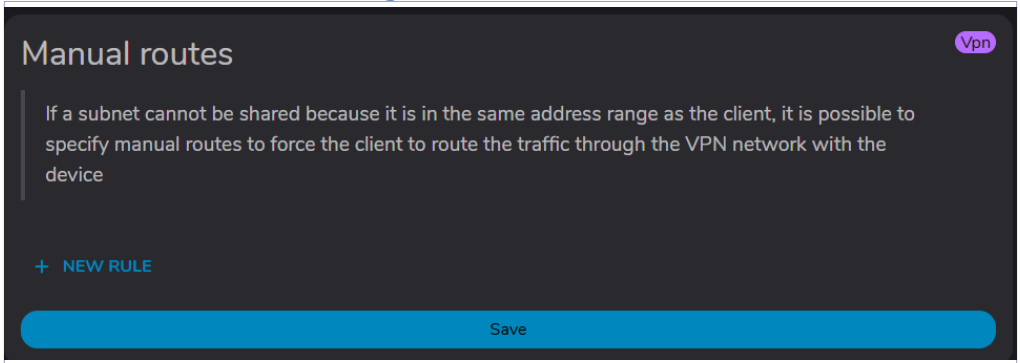
For example, if a local HMI is connected to the switch with IP address 192.168.1.25. to reach it from a PC via VPN, the user simply needs to use that '192.168.1.25' address on their development environment (or VNC client).

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.

2.4 Section "Routing"



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 to be able to access via VPN devices in the device subnetwork 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, as an example, is the rule that should 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 sub-network can access

the Internet via the WAN connection, i.e. the network interface that has access to the device's Internet (e.g. in the PPH600 the 'eth0.1' network, which is in DHCP by default).

NB: In order not to have internal network conflicts, only the interface that will have access to the Internet must have the Gateway IP address set, while the others must have this field empty.

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 Internet connection from the device’s “wlan0” network.

New gateway route

Source network (LAN)
eth0

Destination network (WAN)
wlan0

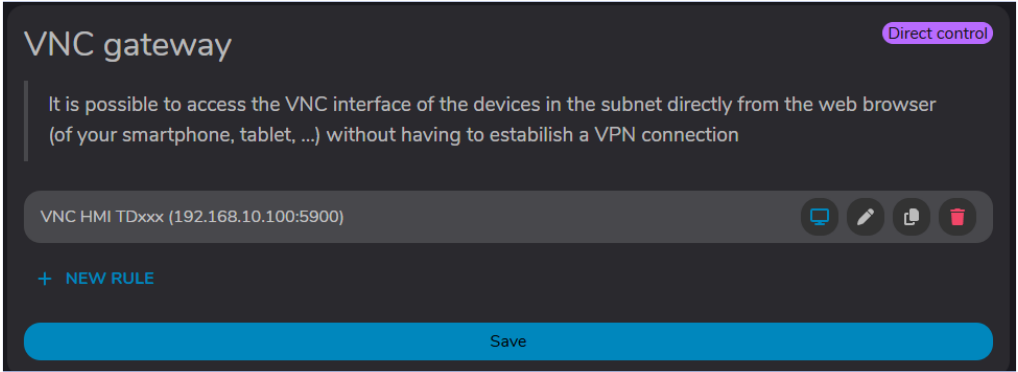
CANCEL CREATE

NB: In order for the devices in the sub-network to be able to access the internet, the IP address of the network interface of the Pixsys device they are connected to (e.g. in the PPH600 the network “eth0.2” which by default is 192.168.10.1) must be specified in their network configuration as the gateway address.

2.5 Section “VNC gateway”

The “VNC Gateway” function allows access to and interaction with the VNC interface of devices in the sub-network, without having to make a VPN connection, but by exploiting the WebRTC technology of the “Direct control” service on the device.

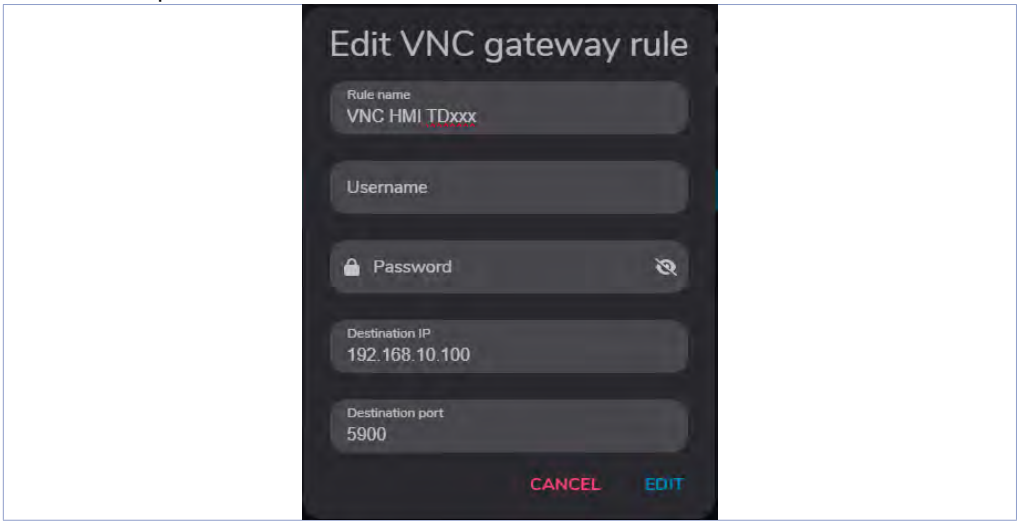
Multiple VNC rules can be entered, so that with access to the “Direct Control” function available in the PixsysPortal interface, users already have “hot buttons” to access the VNC interfaces of their devices, without having to remember their IP address and enter their credentials each time.



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 nor any app installation. All you have to do is access the portal.pixsys.net web page, enter your credentials and, once you have selected the desired gateway, press the “Direct Control” button:



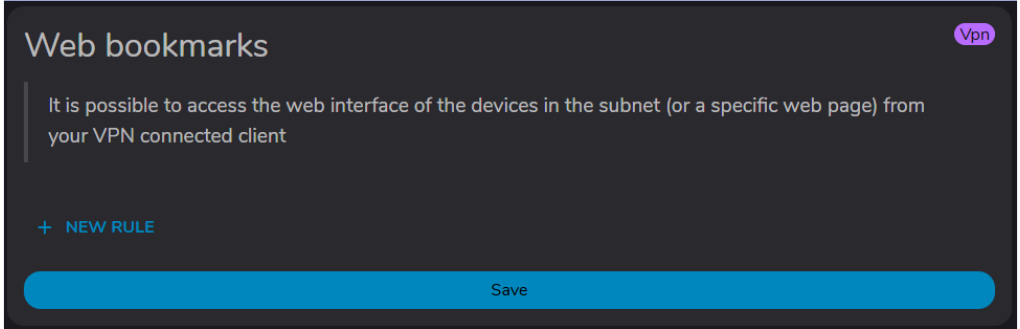
The following rule, for example, allows access to the VNC server of a TD710 panel with IP address 192.168.10.100 (port 5900 is the default for VNC):



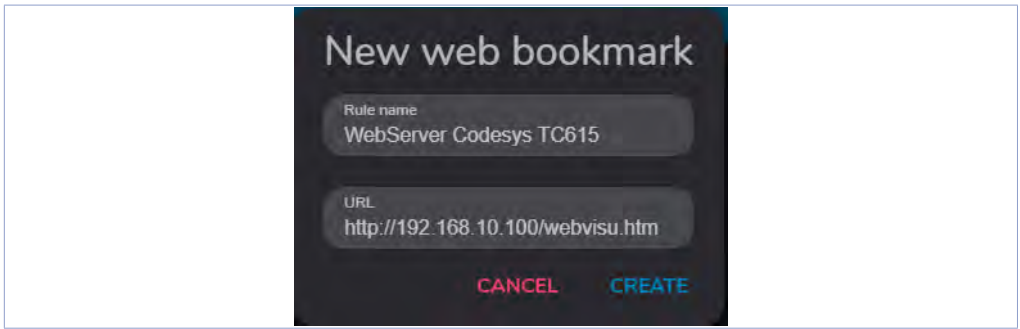
2.6 Section “Web Bookmarks”

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:



3 CREATING THE PIXSYS PORTAL ACCOUNT

The service requires the user to have a personal PixsysPortal account, with specific credentials (an email and a secure password), to which the various Pixsys devices you wish to access remotely can be associated.

- Using a web browser, from a PC or smartphone, access portal.pixsys.net, then click SIGN IN / LOG IN to create your account and follow the instructions provided (you will have to confirm account activation by clicking on the link that will be provided to the e-mail you entered during registration).

- At this point, from a smartphone you can also install the webapp via the appropriate icon, so as to have a quick link to the portal, otherwise it will be accessed via portal.pixsys.net.
 From a Windows PC, on the other hand, you can install the appropriate application, following the instructions in the next chapter.

NB: With the webapp alone (or from portal.pixsys.net), it is possible to associate and check the list of one's own devices, as well as share them with other accounts and make a *"Direct Control"* connection (access to the devices' VNC server), but not make a VPN connection.

With the application installed on your Windows PC, you will be able to make both *"Direct Control"* and VPN connections for full access to your remote devices.

4 USING THE PIXSYS PORTAL APPLICATION ON YOUR PC

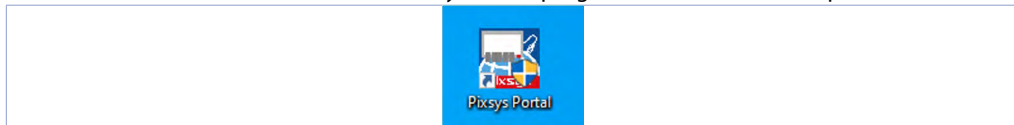
The VPN connection from your Windows PC to Pixsys remote devices requires the installation of the PixsysPortal application, available at the url:

[https://releases.portal.pixsys.net/o20010/01/win/PixsysPortal installer.zip](https://releases.portal.pixsys.net/o20010/01/win/PixsysPortal%20installer.zip).

4.1 Installing and using the PixsysPortal application

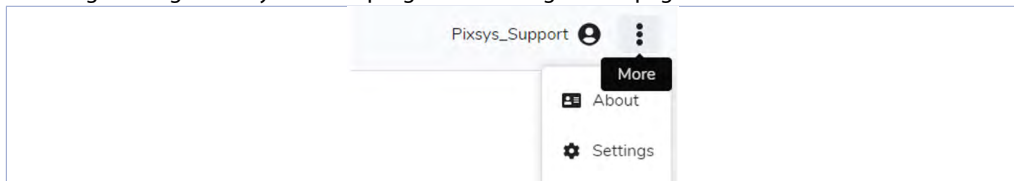
- After downloading the application setup, proceed to install it by following the simple on-screen instructions

- Once the client is installed, launch the *"Pixsys Portal"* programme from the desktop icon

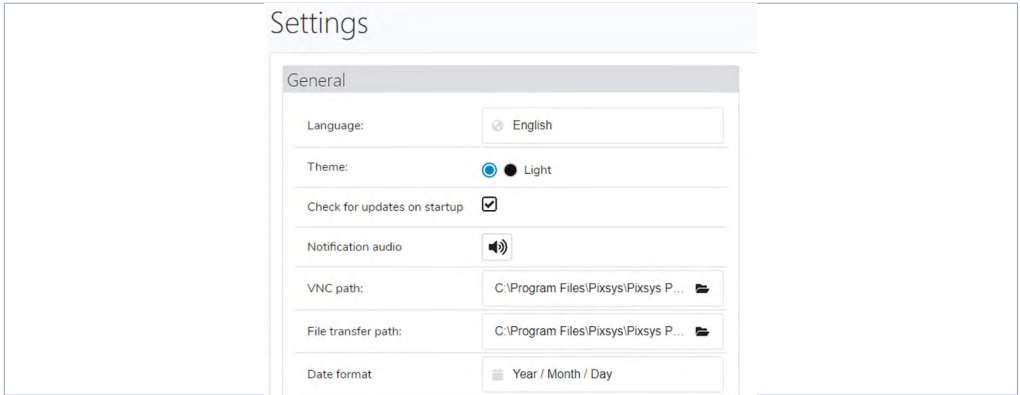


- Then log in with the credentials chosen during account activation

- The name of the connected account is displayed at the top right, 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 automatically set during installation (it is not necessary to change them except in specific cases)

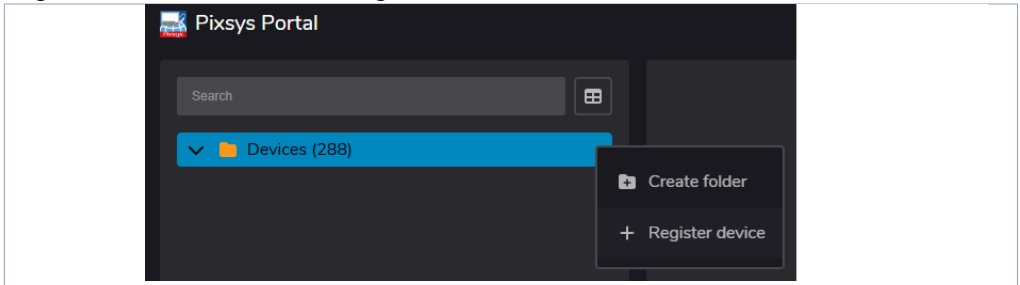


NB: it is important to press the “Save” button in each section, to ensure that the configuration just made is saved.

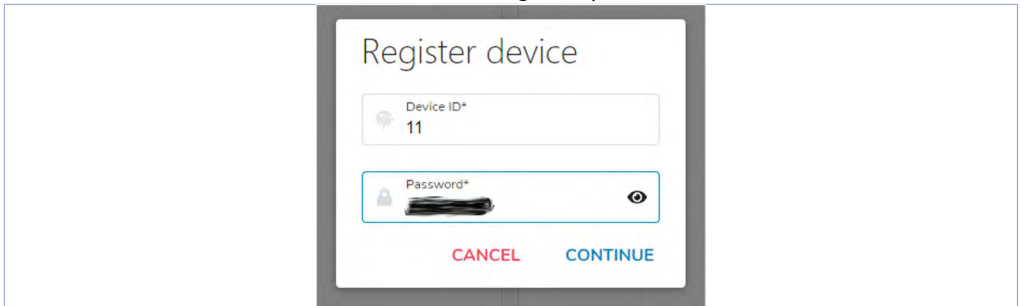
- To return to the main screen, press the Pixsys Portal logo in the top left-hand corner.

4.2 Associating a device to your PixsysPortal account

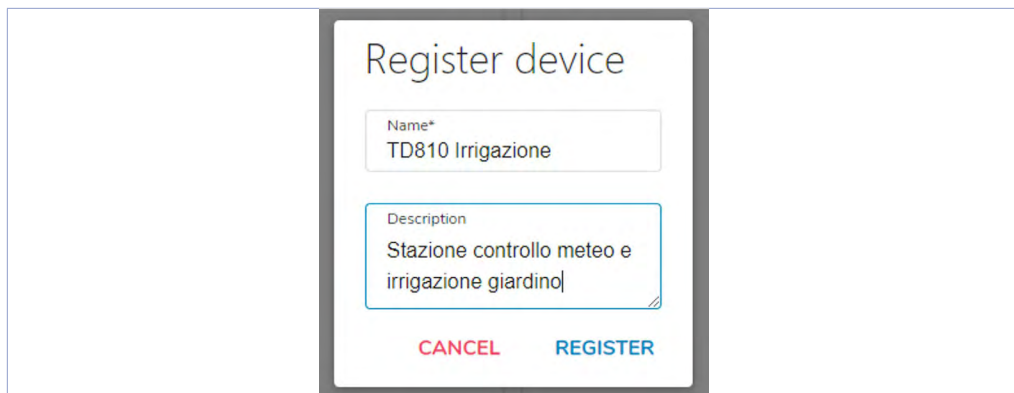
- Right-click on Devices and select Register Device



- In the window that appears, enter the credentials (ID and Password) indicated in the device’s WebServer (label on the side in the case of PPH600 gateways) and click on “CONTINUE”.

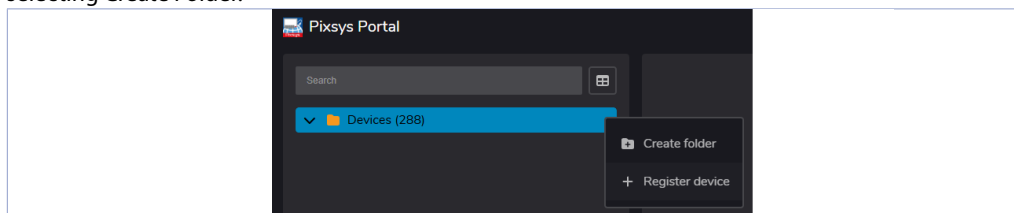


- Give the device a name of your choice and possibly a description and confirm



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

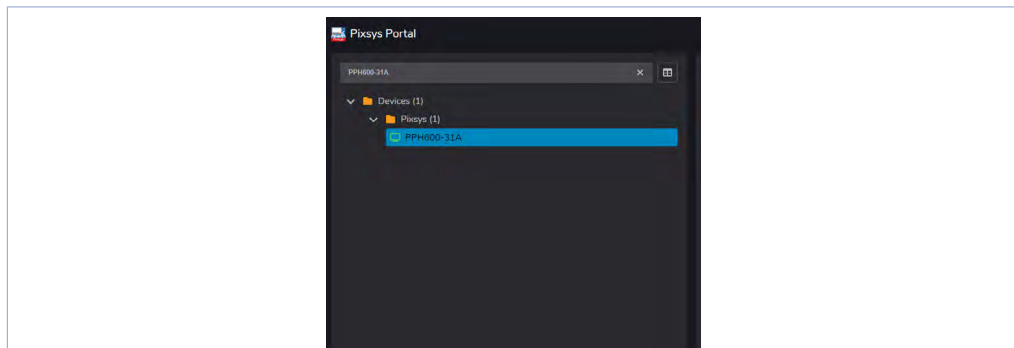
- You can also group the different devices into folders by right-clicking on the Devices item and selecting Create Folder.



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

4.3 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 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

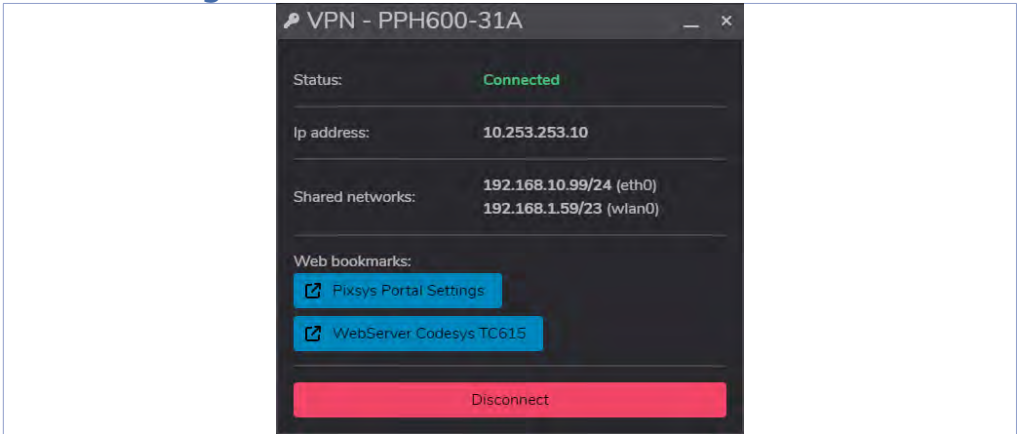
“Direct Control” function to access the VNC of the devices in the sub-network, or the “VPN” function to establish the VPN tunnel.

4.3.1 Using the “Direct Control” function



After selecting a device from those online (green icon), clicking 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 2.5 “VNC gateway” section for more information). “Disconnect” terminates the WebRTC connection from the device.

4.3.2 Using the VPN function



After selecting a device from those online (green icon), clicking on the “VPN” button and then on “Connect” displays the window showing the buttons giving access to the various configured WebServers (see section 2.6 “Web Bookmarks” for more information). It will also display the virtual IP address assigned to that device and the information of the accessible networks (see Section 2.3 “Network” for more information). In this case, the device has virtual IP address 10.253.253.10 and has shared the two networks “eth0” and “wlan0”. This means that from your PC by pointing to IP address 10.253.253.10 you will directly access the remote device (connection to the development environments, etc.) while to connect to one of the devices in the sub-network, you will have to point directly 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 sub-network of ‘eth0’, you only need to use this IP address to connect from the PLC development environment. The quick button “Pixsys Portal Settings” allows access to the configuration WebServer of the device’s PixsysPortal service, without having to know its local IP address (a web page at address 10.253.253.10:8080 will be opened).

“Disconnect” terminates the VPN connection from the device.

4.4 Application details

The PixsysPortal application installed on your PC allows you to see certain properties of the selected device.

Details’ tab

The “Details” tab shows the device’s main information, licence status, usage counters and the currently installed firmware version, as well as checking for updates.

Details

Id	[REDACTED]		
Name	PPH600-31A		
Description	2		
Public IP	93.39.118.6		[Location Icon]
Network interfaces	192.168.0.110/24 (eth0.1) 192.168.10.1/24 (eth0.2)		
Product key	[REDACTED]		
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)		

The licence management for remote connection to devices is described in section 2 “Activating the PixsysPortal licence in devices”.

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 sectio 2.2 “Security”).

Local options

Password			
VPN subnet	10.253.253.0		/ 24
VPN auto reconnect	☐		
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 (default 10.253.253.10).

The “Automatic VPN reconnection” flag allows the PC client 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 paragraph 4.6 *"Sharing the device with other PixsysPortal accounts"* for more information.

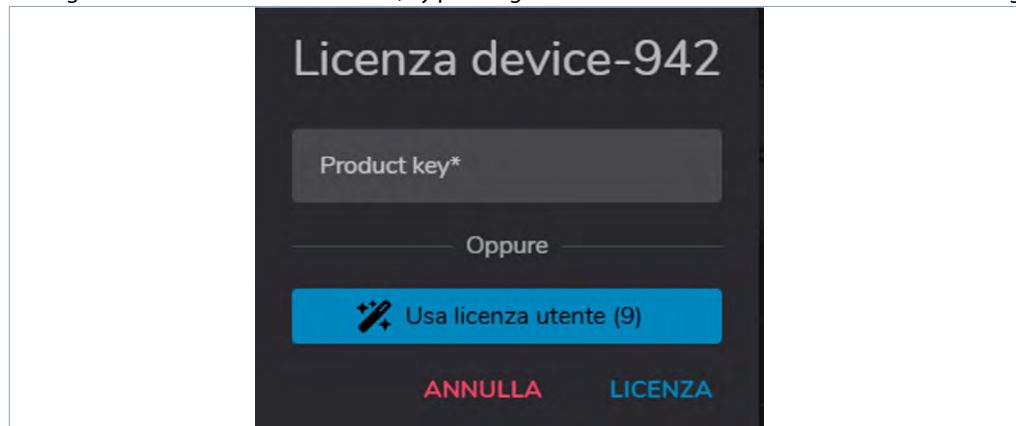
4.5 PixsysPortal licence activation in devices

The PixsysPortal service requires that the remote device must have a so-called RUNTIME licence in order to be able to make VPN and WebRTC connections without time limits. For more details please refer to the PixsysPortal service terms of use document, available on the relevant page of the pixsys.net website.

If your device is unlicensed, the WebRTC and/or VPN connection will last for a maximum of 15 minutes, after which you will have to wait for 2 hours to connect again).



If your account has PixsysPortal Runtime licences, you can associate one to your unlicensed device, scaling it down from the available ones, by pressing the barcode icon next to the *"Unlicensed"* wording



From the window that appears, you will be able to manually enter a licence code that may have been provided by Pixsys via email or use the "Use user licence (xxx)" button to deduct one from your total available licences.

4.6 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 for the PixsysPortal service).

The device can be shared as a simple user or owner:

- Simple user: the account that *"gets"* the device can check its connection status and details, and make VPN/WebRTC connections to it. However, he may NOT share the device with other users or see the list of owners.

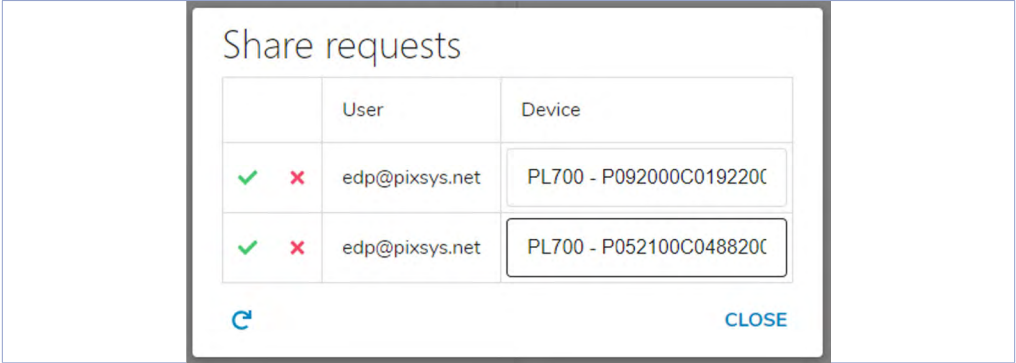
- Owner user: the account that *'gets'* the device can perform the operations possible as a simple user and also share the device with other PixsysPortal users as well as delete a specific user from the device's owners/users.

In any case, the PixsysPortal account receiving a sharing request will see a red dot notification appear

next to its 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.

For details of the liability of Pixsys srl and the user of the service, please refer to the document of the terms of use of the PixsysPortal service, available on the relevant page of the pixsys.net website, and to the user licence.

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

Introduzione

Pixsys Portal è un servizio software che permette di gestire in modo trasparente i dispositivi dotati di connessione Ethernet. Il servizio è pre-installato su HMI, PLC e Panel PC Pixsys e consente la creazione di una connessione VPN ottimizzata per le comunicazioni industriali, abilitando il controllo da remoto (Desktop remoto, Web Server, scambio dati) e/o la teleassistenza (connessione con gli ambienti disviluppo) sia dei dispositivi Pixsys, sia dei dispositivi di terze parti collegati alla medesima sotto rete. Il servizio non richiede impostazioni di firewall o IP statici. E' necessaria una connessione ad internet standard tramite cavo o tramite dispositivi esterni quali router 4G dotati di SIM dati. L'applicazione Pixsys Portal PC permette di monitorare da un unico punto tutti gli impianti associati facilitando l'operatività degli utenti che necessitano di eseguire il controllo a distanza.

1 COS'È PIXSYS PORTAL

Il servizio PixsysPortal permette la connessione sicura via VPN dei dispositivi Pixsys connessi ad internet e con servizio abilitato, quali il gateway PPH600, i PLC PL600/PL700, i pannelli TouchController serie "TC", i WebPanel serie "WP", i PanelPC serie "PC", da un qualsiasi computer MS Windows attraverso l'apposita applicazione client PixsysPortal. La funzionalità "DirectControl" è accessibile da un qualsiasi dispositivo dotato di browser web HTML5 moderno, come smartphone e tablet Android/iOS.

1.1 PRE-REQUISITI DEL SERVIZIO

L'applicazione client PixsysPortal, reperibile nella sezione "SOFTWARE" della relativa pagina del sito Pixsys.net è utilizzabile su PC con sistema operativo MS Windows 8.1 e successivi.

Il servizio PixsysPortal installato nei dispositivi remoti prevede che questi 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. Per la funzionalità "VPN" le porte utilizzate dal servizio PixsysPortal sono la 443 e la 8005 in TCP/UDP che devono essere aperte in uscita. Per la funzionalità "DirectControl" la tecnologia utilizzata è di tipo WebRTC e necessita solo della porta 443 aperta in uscita. Per accedere al Webserver di configurazione del servizio nei dispositivi remoti, viene inoltre utilizzata la porta 8080 in HTTPS. Assicurarsi col proprio responsabile IT che i requisiti richiesti siano soddisfatti prima di utilizzare il servizio PixsysPortal.

Il servizio PixsysPortal prevede che per poter effettuare connessioni VPN e WebRTC senza limiti di tempo il dispositivo remoto debba avere una licenza cosiddetta di RUNTIME. Per maggiori dettagli fare riferimento alla licenza d'utilizzo.

2 CONFIGURAZIONE DEL SERVIZIO NEI DISPOSITIVI

Sui dispositivi basati su sistema operativo Linux con il servizio abilitato, il servizio PixsysPortal viene eseguito automaticamente all'avvio.

I dispositivi PL600/700, TC e WP integrano il servizio PixsysPortal ma questo deve essere abilitato affinché venga avviato automaticamente all'accensione dei dispositivi stessi, tramite l'apposita interfaccia di configurazione "cockpit".

Per maggiori informazioni fare riferimento ai manuali utente dei relativi prodotti.

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

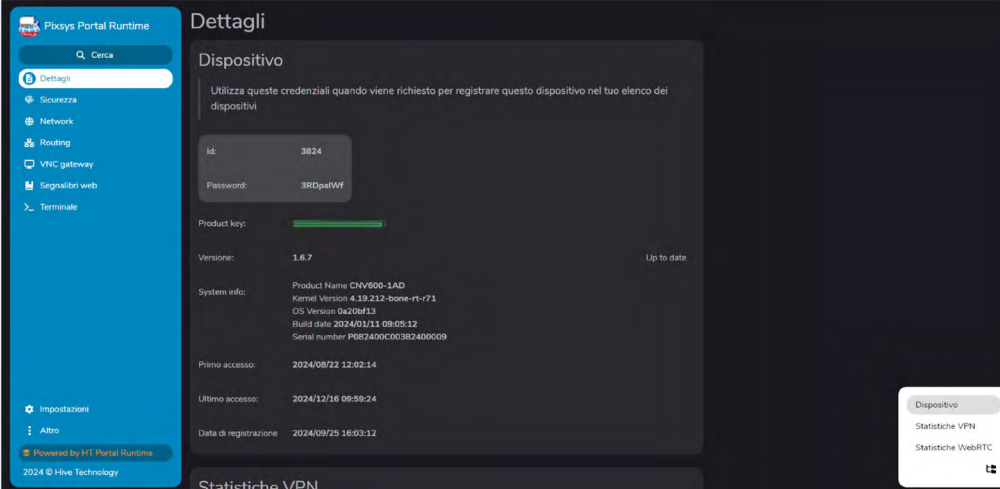
- Accendere il PLC e attendere il completo caricamento dei servizi del sistema operativo.
- Collegare il gateway ad una rete locale dotata di connessione ad internet.
- Utilizzare l'utility DeviceFinder (reperibile da devicefinder.pixsys.net) per identificare l'indirizzo IP del dispositivo:



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.

2.1 Sezione “Dettagli”

Dispositivo

Utilizza queste credenziali quando viene richiesto per registrare questo dispositivo nel tuo elenco dei dispositivi

Id:

Password:

3RDpaIWf

Product key:

Versione:

1.6.7

Up to date

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 09:59:24

Data di registrazione

2024/09/25 16:03:12

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” azzerà 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)**

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.

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

2.3 Sezione “Network”

Interfacce di rete

VPN

Durante la connessione VPN il dispositivo è raggiungibile tramite un IP selezionato dal client. È possibile condividere una o più sotto-reti del dispositivo per rendere accessibili anche i nodi al loro interno direttamente al client

Rimuovi tutte

☒	eth0	192.168.1.99 / 255.255.255.0	 
☒	wlan0	192.168.0.163 / 255.255.255.0	 

Salva

I dispositivi, attraverso la connessione VPN, sono accessibili da un computer remoto e possono anche rendere accessibili eventuali altri dispositivi presenti nella loro rete, con il cosiddetto passthrough. Ad esempio si potrà raggiungere da remoto un eventuale HMI, altro PLC o inverter connessi col dispositivo Pixsys dotato di servizio PixsysPortal attivo.

È necessario solamente abilitare se e quale scheda di rete userà tale funzionalità, senza dover indicare gli IP dei dispositivi locali o altro.

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, cioè, messa 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, mentre l'altra scheda di rete sarà quella usata per consentire l'accesso ad internet al servizio PixsysPortal in esecuzione nel dispositivo).

Nella schermata di esempio sono state abilitate le porte di rete "eth0" e "wlan0" per la connessione VPN condivisa "pass-through" cioè entrambe renderanno disponibili eventuali dispositivi connessi a tali schede. La schermata mostra in particolare un dispositivo configurato con la porta wlan0 (scheda USB wifi) con indirizzo IP 192.168.0.163 e la porta "eth0" (porta RJ45 fisica) come 192.168.1.99 .

Se una connessione VPN viene instaurata attraverso una delle due interfacce di rete, tutte le richieste del PC remoto agli indirizzi presenti nella sotto-rete 192.168.0.XXX o 192.168.1.XXX saranno automaticamente direzionate al dispositivo locale presente nella sotto-rete della classe di indirizzi corretta.

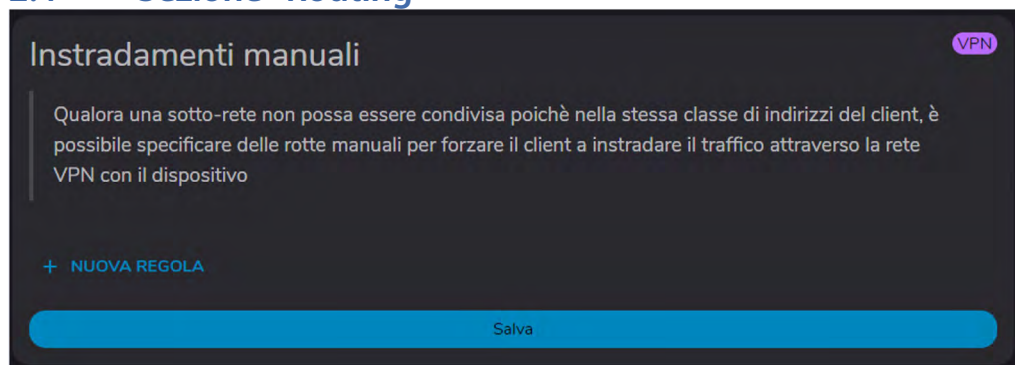
Per esempio, se un HMI locale è connesso allo switch con indirizzo IP 192.168.1.25. per raggiungerlo da un PC via VPN l'utente dovrà semplicemente usare quell'indirizzo "192.168.1.25" sul proprio ambiente di sviluppo (o VNC client).

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

Se la configurazione delle reti viene effettuata accedendo al WebServer da remoto (attraverso quindi una connessione VPN già stabilita), tenere presente che:

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

2.4 Sezione "Routing"



La sezione routing permette di gestire le opzioni per la configurazione degli instradamenti manuali, il port-forwarding e le rotte dispositivo, 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 dispositivo 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, come esempio, la regola che andrebbe 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 i dispositivi presenti nella sotto-rete saranno raggiungibili.

- La scheda "Port forwarding" permette di 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, cioè l'interfaccia di rete che ha accesso ad internet del dispositivo (ad esempio nel PPH600 la rete "eth0.1" che di default è in DHCP).

NB: Per non avere conflitti di rete interni, solo l'interfaccia che avrà l'accesso ad internet dovrà avere impostato l'indirizzo IP di Gateway mentre le altre dovranno avere questo campo vuoto.

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 "wlan0" del dispositivo.

Nuova rotta gateway

Rete di ingresso (LAN)
eth0

Rete di destinazione (WAN)
wlan0

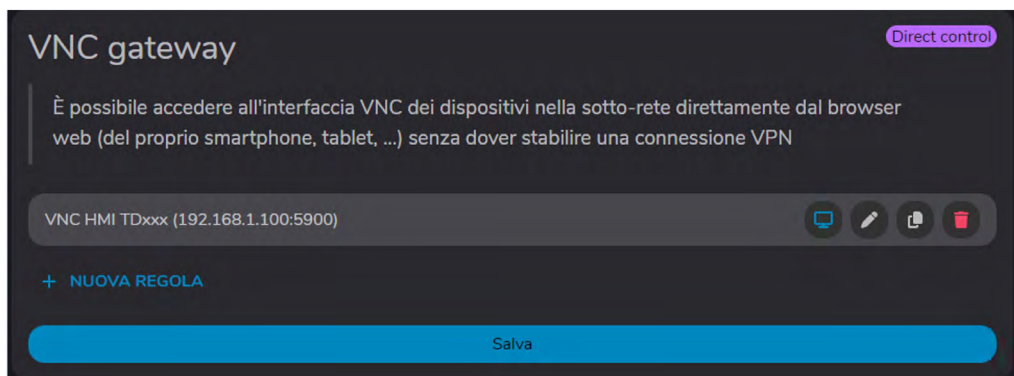
ANNULLA CREA

NB: Affinché i dispositivi nella sotto-rete possano accedere ad internet, è necessario che nella loro configurazione di rete come indirizzo di Gateway sia indicato l'indirizzo IP dell'interfaccia di rete del dispositivo Pixsys a cui sono collegati (ad esempio nel PPH600 la rete "eth0.2" che di default è 192.168.10.1).

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**, ma sfruttando la tecnologia WebRTC del servizio "Direct control" sul dispositivo.

È possibile inserire più regole VNC, in modo che con l'accesso alla funzione "Direct Control" disponibile nell'interfaccia PixsysPortal, l'utente abbia già dei "pulsanti rapidi" per poter accedere alle interfacce VNC dei propri dispositivi, senza doverne ricordare l'indirizzo IP ed inserire ogni volta le relative credenziali.



Questa funzionalità può essere sfruttata quindi da qualsiasi dispositivo dotato di un browser web (smartphone, tablet ecc) e non richiede perciò l'utilizzo di un PC Windows né dell'installazione di app. Sarà sufficiente, infatti, accedere alla pagina web portal.pixsys.net, inserire le credenziali del proprio account PixsysPortal e, una volta loggato, selezionare il dispositivo desiderato e premere sul pulsante "Direct Control".

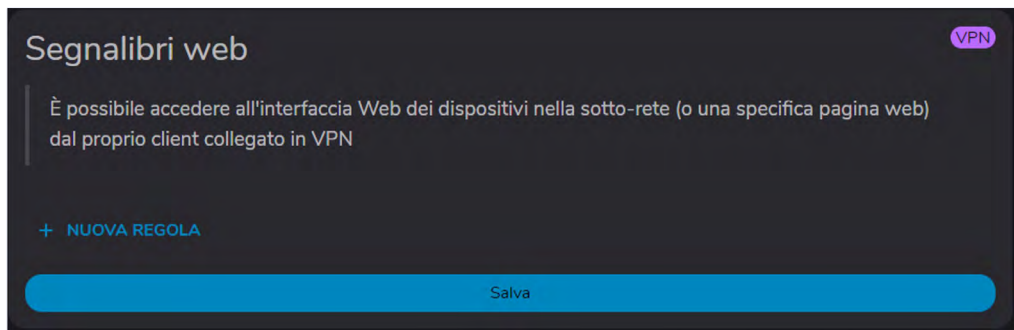


Come esempio, la regola seguente permette di accedere al server VNC di un pannello TD710 con indirizzo IP 192.168.0.100 (la porta 5900 è la default per VNC):

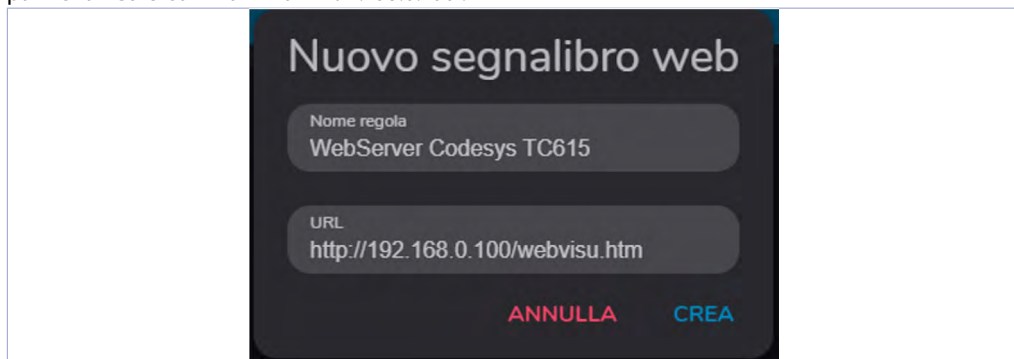
2.6 Sezione "Segnalibri Web"

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 rapidi" per poter accedere alle interfacce WebServer dei propri dispositivi, senza doverne ricordare l'indirizzo IP ed inserire ogni volta le relative credenziali.



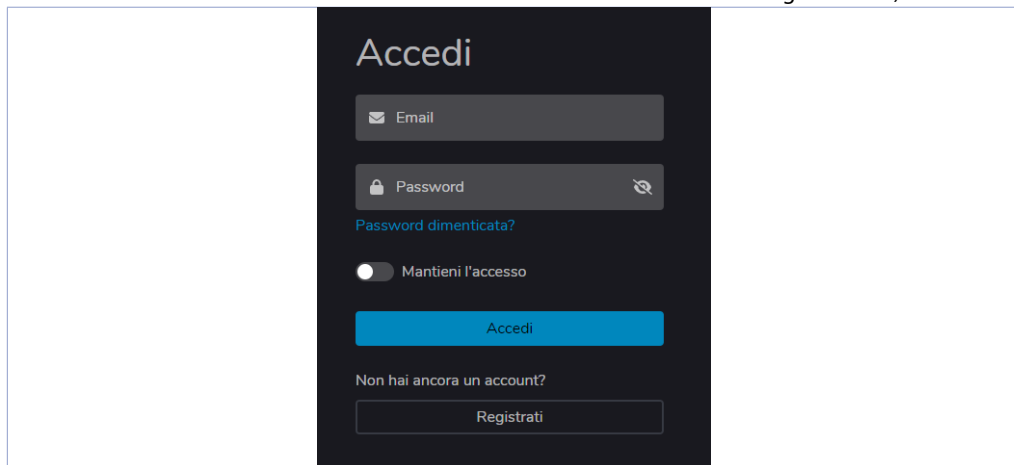
Come esempio, la regola seguente permette di accedere al WebServer Codesys (WebVisu) di un pannello TC615 con indirizzo IP 192.168.0.100 :



3 CREAZIONE DELL'ACCOUNT PIXSYS PORTAL

Il servizio prevede che l'utente disponga di un account PixsysPortal personale, con credenziali specifiche (una email ed una password sicura), a cui si potranno associare i vari dispositivi Pixsys a cui si vorrà accedere da remoto:

- Con un browser web, da PC o smartphone, accedere a portal.pixsys.net, poi premere su SIGN IN / ACCEDI per creare un proprio account e seguire le istruzioni fornite (si dovrà confermare l'attivazione dell'account cliccando sul link che verrà fornito alla e-mail inserita in fase di registrazione).



- A questo punto, da smartphone è possibile inoltre installare la webapp tramite l'apposita icona, in modo da avere un collegamento rapido al portale, altrimenti si accederà a questo tramite l'indirizzo portal.pixsys.net.

Da PC Windows invece è possibile installare l'applicazione apposita, seguendo le istruzioni del paragrafo successivo.

NB: con la sola webapp (o dal sito portal.pixsys.net) è possibile associare e verificare la lista dei propri dispositivi, nonché condividerli con altri account ed effettuare la connessione "Direct Control" (accesso al server VNC dei dispositivi) ma non effettuare una connessione VPN.

Con l'applicazione installata sul proprio PC Windows sarà possibile effettuare sia connessioni "Direct Control" che VPN, per un accesso totale ai propri dispositivi remoti.

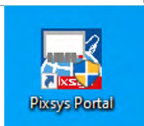
4 UTILIZZO DELL'APPLICAZIONE PIXSYSportal SUL PROPRIO PC

La connessione VPN dal proprio PC Windows verso i dispositivi remoti Pixsys prevede l'installazione dell'applicazione PixsysPortal, reperibile all'url:

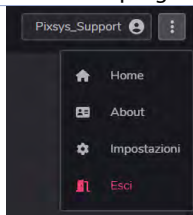
[https://releases.portal.pixsys.net/o20010/01/win/PixsysPortal installer.zip](https://releases.portal.pixsys.net/o20010/01/win/PixsysPortal%20installer.zip).

4.1 Installazione dell'applicazione PixsysPortal e utilizzo

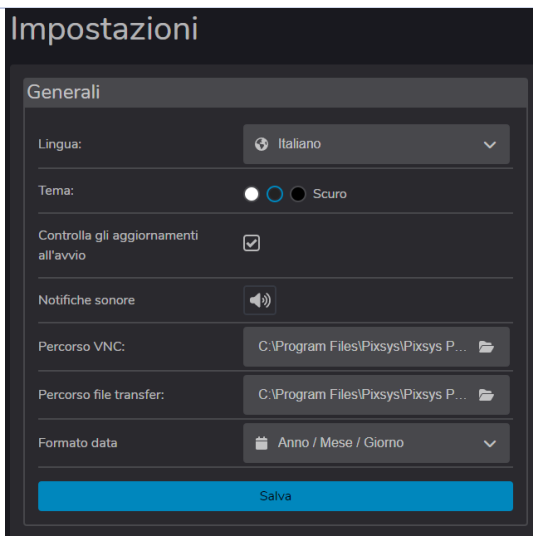
- Scaricato il setup dell'applicazione, procedere ad installarla seguendo le semplici istruzioni a video
- Una volta installato il client, avviare dall'icona sul desktop il programma "Pixsys Portal"



- 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)

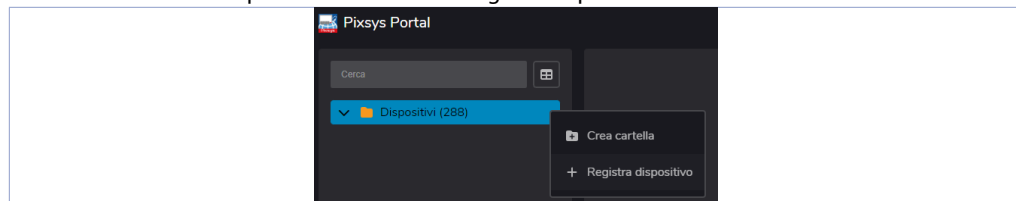


NB: è importante premere il pulsante “Save/Salva” in ogni sezione, per garantire il salvataggio della configurazione appena effettuata.

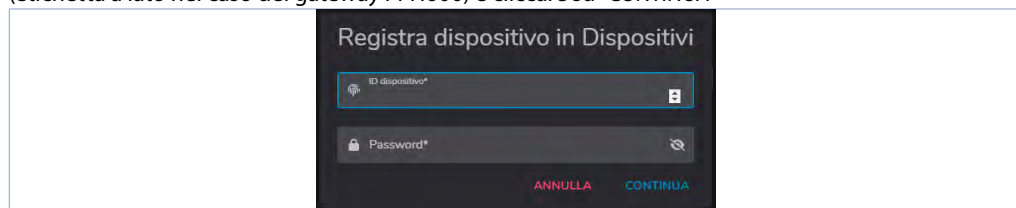
- Per tornare alla schermata principale, premere il logo Pixsys Portal in alto a sinistra nella schermata.

4.2 Associazione di un dispositivo al proprio account PixsysPortal

- Fare click destro su Dispositivi e selezionare Registra dispositivo



- Nella finestra che appare, inserire le credenziali (ID e Password) indicate nel WebServer del dispositivo (etichetta a lato nel caso dei gateway PPH600) e cliccare su “CONTINUA”



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

Registra dispositivo in Dispositivi

Nome*

TC615

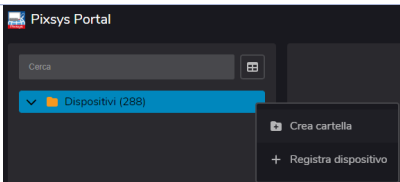
Descrizione

Stazione controllo melao n.1

ANNULLA

REGISTRA

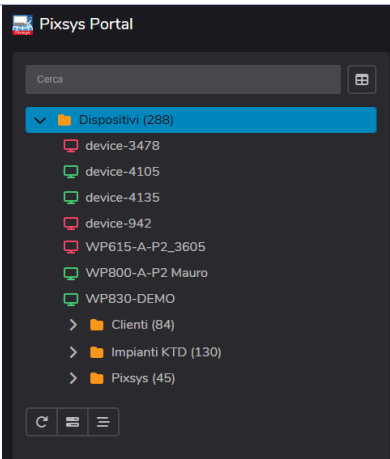
A questo punto il PLC appena registrato al proprio account apparirà nell'elenco dei propri dispositivi.
- È anche possibile raggruppare i diversi dispositivi in cartelle, facendo click destro sulla voce Dispositivi e selezionando Crea Cartella.



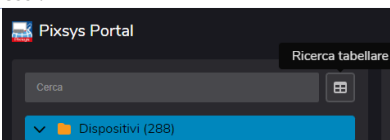
Successivamente, è sufficiente trascinare il dispositivo desiderato nella cartella appena creata.

4.3 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.

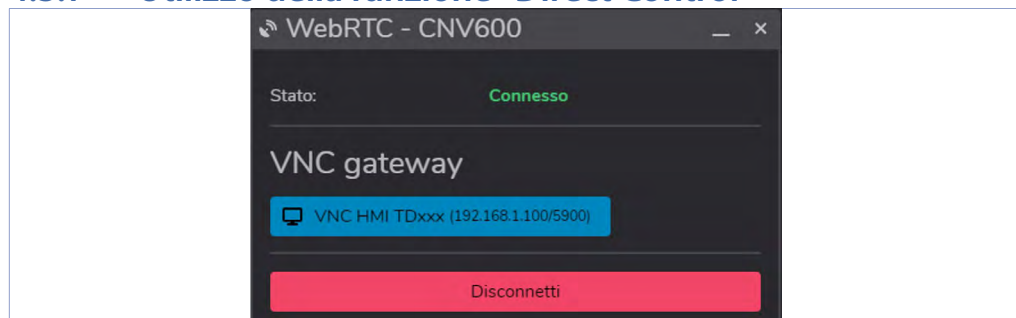


NB: l'icona verde indica che il dispositivo è raggiungibile dai server di PixsysPortal e quindi sarà

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.

Dopo aver selezionato un dispositivo tra quelli online (icona verde), è possibile sfruttare la funzione *“Direct Control”* per accedere al VNC del dispositivo stesso o degli eventuali dispositivi presenti nella sotto-rete, oppure la funzione *“VPN”* per stabilire il tunnel VPN.

4.3.1 Utilizzo della funzione *“Direct Control”*



Dopo aver selezionato un dispositivo tra quelli online (icona verde), 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 il paragrafo 2.5 Sezione *“VNC gateway”* per maggior informazioni). Con *“Disconnetti”* si termina la connessione WebRTC dal dispositivo.

4.3.2 Utilizzo della funzione VPN



Dopo aver selezionato un dispositivo tra quelli online (icona verde), premendo sul pulsante *“VPN”* e poi su *“Connetti”* si visualizza la finestra che mostra i pulsanti che danno l'accesso ai vari WebServer configurati (vedere il paragrafo 2.6 Sezione *“Segnalibri Web”* per maggior informazioni).

Si visualizzerà inoltre l'indirizzo IP virtuale assegnato a quel dispositivo e le informazioni delle reti accessibili (vedere il paragrafo 2.3 Sezione *“Network”* per maggior informazioni).

In questo caso il dispositivo ha indirizzo IP virtuale 10.253.253.10 e ha condiviso le due reti *“eth0”* e *“wlan0”*. Questo significa che dal proprio PC puntando l'indirizzo IP 10.253.253.10 si accederà direttamente al dispositivo remoto (collegamento agli ambienti di sviluppo ecc) mentre per collegarsi ad uno dei dispositivi presenti nella sotto-rete, si dovrà puntare 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 del PLC stesso.

Il pulsante rapido “*Impostazioni Pixsys Portal*” permette di accedere al WebServer di configurazione del servizio PixsysPortal del dispositivo, 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 dispositivo.

4.4 Dettagli dell'applicazione

L'applicazione PixsysPortal installata sul proprio PC permette di vedere alcune proprietà del dispositivo selezionato.

Scheda “Dettagli”

La scheda “*Dettagli*” mostra le informazioni principali del dispositivo, lo stato della licenza, i contatori di utilizzo e la versione del firmware correntemente installato, nonché di controllare l’eventuale presenza di aggiornamenti.

Dettagli

Id

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)

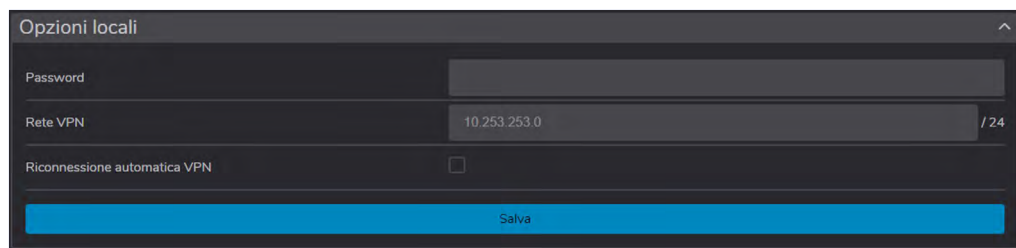
Connessioni WebRTC

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)

La gestione della licenza per il collegamento da remoto ai dispositivi è descritta nel paragrafo 2 “*Attivazione della licenza PixsysPortal nei dispositivi*”.

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 il paragrafo 2.2 “*Sezione Sicurezza*”).



La voce “Rete VPN” mostra e permette la modifica dell’indirizzo IP che il dispositivo otterrà nel momento che la connessione VPN viene stabilita (default 10.253.253.10).

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 dispositivo. Per maggiori info vedere il paragrafo 4.6 “Condivisione del dispositivo con altri account PixsysPortal”.

4.5 Attivazione della licenza PixsysPortal nei dispositivi

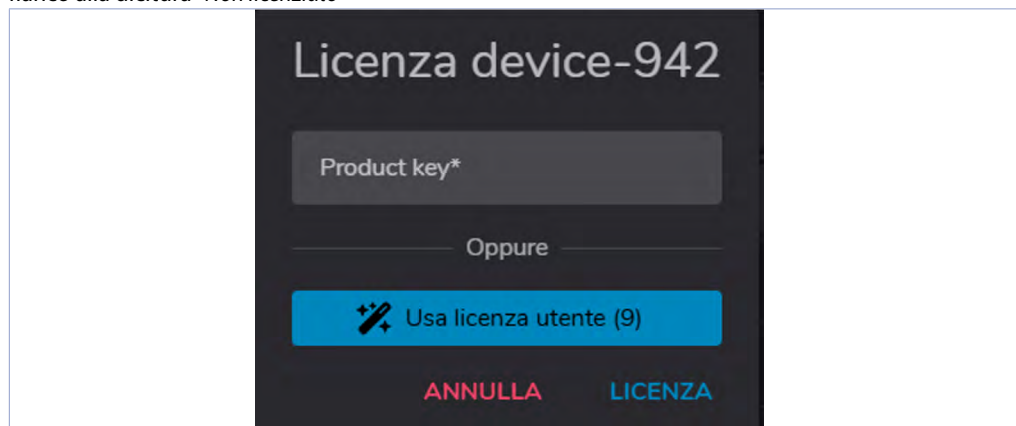
Il servizio PixsysPortal prevede che per poter effettuare connessioni VPN e WebRTC senza limiti di tempo il dispositivo remoto debba avere una licenza cosiddetta di RUNTIME.

Per maggiori dettagli fare riferimento al documento dei termini di utilizzo del servizio PixsysPortal, disponibile nella relativa pagina del sito pixsys.net .

Se il proprio dispositivo non risulta licenziato, la connessione WebRTC e/o VPN avrà una durata massima di 15 minuti, dopodichè sarà necessario attendere un tempo di 2 ore per poter effettuare nuovamente una nuova connessione).



Se il proprio account dispone di licenze Runtime PixsysPortal, è possibile associarne una al proprio dispositivo non licenziato, scalandola da quelle disponibili, premendo l’icona del codice a barre a fianco alla dicitura “Non licenziato”



Dalla finestra che appare sarà possibile inserire manualmente un codice licenza eventualmente fornito

da Pixsys via email oppure utilizzare il pulsante “Usa licenza utente (xxx)” per scararne una dal proprio totale di licenze disponibili.

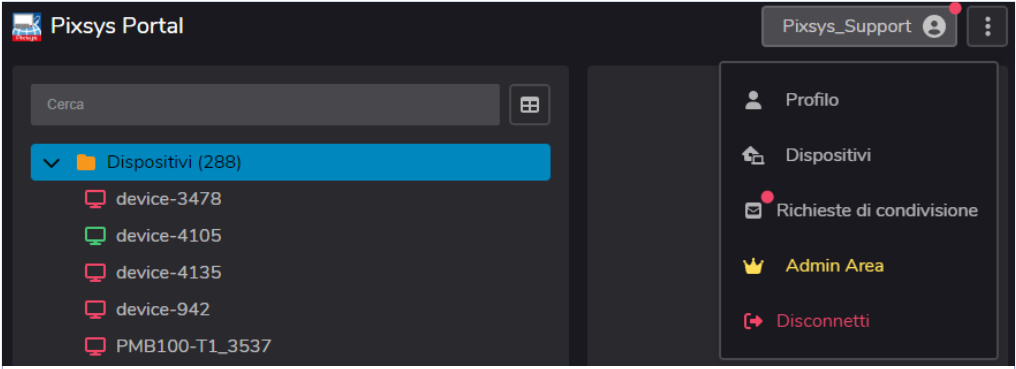
4.6 Condivisione del dispositivo con altri account PixsysPortal

Tramite il menu “Utenti” è possibile condividere il dispositivo con altri utenti PixsysPortal (cioè account già registrati al servizio PixsysPortal).

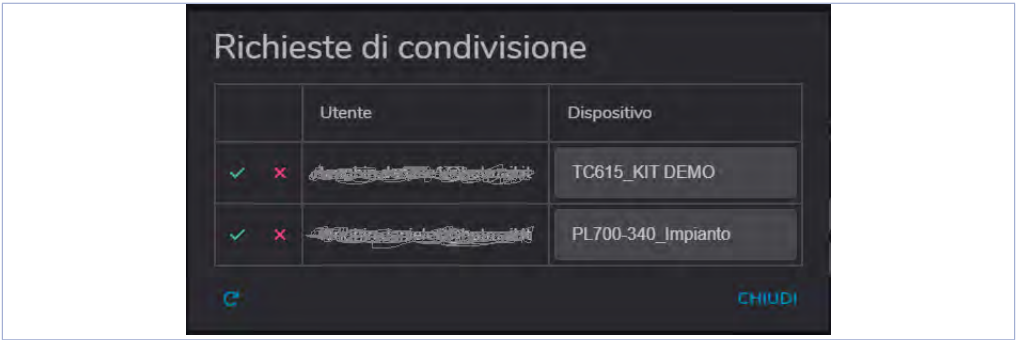
Il dispositivo può essere condiviso come utente semplice o proprietario:

- Utente semplice: l’account che “ottiene” il dispositivo può verificarne lo stato di connessione e i dettagli, nonché effettuare le connessioni VPN/WebRTC ad esso. NON può però condividere il dispositivo con altri utenti né vederne la lista dei proprietari.
- Utente proprietario: l’account che “ottiene” il dispositivo può effettuare le operazioni possibili come utente semplice ed inoltre condividere il dispositivo con altri utenti PixsysPortal nonché eliminare uno specifico utente dai proprietari/utenti del dispositivo stesso.

In ogni caso, l’account PixsysPortal che riceve una richiesta di condivisione vedrà apparire, a fianco del suo nome utente, una notifica a forma di pallino rosso



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.

Responsabilità limitata

Per i dettagli di responsabilità di Pixsys srl e dell'utente utilizzatore del servizio, si prega di fare riferimento al documento dei termini di utilizzo del servizio PixsysPortal, disponibile nella relativa pagina del sito pixsys.net, ed alla licenza d'uso.

Note / Aggiornamenti

This image shows a single sheet of white paper with horizontal blue or grey ruling lines, typical of notebook paper. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

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



2300.10.403-RevA

100525