USER MANUAL

VPN BOX2 Hardware

VPN BOX2 Virtual Machine

VIRTUAL PRIVATE NETWORK SERVER

SENECA s.r.l.

Via Austria, 26 - 35127 - PADOVA - ITALY

Tel. +39.049.8705355 - 8705359 Fax. +39.049.8706287

Website: www.seneca.it

Technical service: supporto@seneca.it (IT), support@seneca.it (Other)

Commercial information: commerciale@seneca.it (IT), sales@seneca.it (Other)

This document is the property of SENECA srl. Unauthorized duplication and reproduction (even partial) is prohibited. The content of this document refers to the described products and technologies. Despite the continuous effort to achieve perfection, all the technical data contained in this document can be modified or added for technical and commercial needs; it is impossible to completely eliminate discrepancies and inconsistencies. However, the content of this documentation is subject to periodic review. For any question, do not hesitate to contact our structure or write to the e-mail addresses indicated above.

CAUTION

SENECA does not guarantee that all specifications and/or aspects of the product and firmware, included in them, will meet the requirements of the actual final application even if the product referred to in this documentation is in compliance with the technological state of the art.
The user assumes full responsibility and/or risk with regard to the configuration of the product to achieve the intended results in relation to the specific installation and/or end application.
SENECA may, with prior agreement, provide consultancy services for the successful completion of the final application, but under no circumstances can it be held responsible for its proper functioning.
The SENECA product is an advanced product, the operation of which is specified in the technical documentation supplied with the product itself and/or can be downloaded, if desired prior to purchase, from the www.seneca.it website.
SENECA has a policy of continuous development and accordingly reserves the right to make and/or introduce - without prior notice - changes and/or improvements to any product described in this documentation.
The product described in this documentation may solely and exclusively be used by personnel qualified for the specific activity and in accordance with the relevant technical documentation, with particular attention being paid to the safety instructions.
Qualified personnel means personnel who, on the basis of their training, competence and experience, are able to identify risks and avoid potential hazards that could occur during the use of this product.
SENECA products may only be used for the applications and in the manner described in the technical documentation relating to the products themselves.
To ensure proper operation and prevent the occurrence of malfunctions, the transport, storage, installation, assembly, maintenance of SENECA products must comply with the safety instructions and environmental conditions specified in this documentation.
SENECA's liability in relation to its products is governed by the general conditions of sale, which can be downloaded from www.seneca.it.
Neither SENECA nor its employees, within the limits of applicable law, will in any case be liable for any lost profits and/or sales, loss of data and/or information, higher costs incurred for goods and/or replacement services, damage to property and/or persons, interruption of activities and/or provision of services, any direct, indirect, incidental, pecuniary and non-pecuniary, consequential damages in any way caused and/or caused, due to negligence, carelessness, incompetence and/or other liabilities arising from the installation, use and/or inability to use the product.

Date	Revision	Note	Author
02/05/2023	1	First edition	AS
12/05/2023	2	Translation	AZ
10/07/2023	3	Changed heading	AZ
16/02/2024	4	Various fixes, added the procedure for IOS/Android connection	FT/MM
25/06/2025	5	New instructions added for Client communicator 5	AV / MM

TABLE OF CONTENTS

1. SENECA VPN BOX2 6

2. SOFTWARE OPEN SOURCE 7

3. INTRODUCTION 7

3.1. HARDWARE SPECIFICATIONS 7

3.2. VIRTUAL MACHINE (VMWARE) SPECIFICATIONS 8

4. VPN BOX2 INSTALLATION 9

4.1. INSTALLATION OF THE HARDWARE VERSION 9

4.2. INSTALLATION OF THE VIRTUAL MACHINE VERSION 10

5. DEFAULT ETHERNET NETWORK CONFIGURATION 12

6. FIRST TIME CONFIGURATION OF THE VPN BOX2 13

6.1. LOGIN 14

6.2. WELCOME 15

6.1. MODE 16

6.1. NETWORK 17

6.1. SECURITY 20

6.1. LICENSE 21

7. SERVER ADMINISTRATION 22

7.1. HOME 22

7.2. DEVICES 24

7.3. USERS 26

7.4. GROUPS 29

7.5. NETWORKS (VPN) 32

7.6. CONFIG. GENERAL 35

7.7. CONFIG. NETWORK 36
7.8. CONFIG. SNMP 37
7.9. CONFIG. BACKUP (AUTOMATICI) 39
7.10. CONFIG. CERTBOT 41
7.11. CONFIG. ADVANCED 42
7.12. LOGS 43
7.13. BACKUP 44
8. FACTORY RESET AND UPDATE OF THE VPN BOX2 45
8.1. FACTORY RESET 45
8.1. VPN BOX2 UPDATE 46
9. CONFIGURATION OF THE ROUTER/FIREWALL ON THE VPN BOX2 SERVER ... 47
10. ROUTER/FIREWALL CONFIGURATION ON CLIENT PCS AND REMOTE DEVICES 49
11. SINGLE LAN VPN NETWORK OPERATING PRINCIPLE (SL) 50
11.1. VPN CONFIGURATION 51
12. POINT TO POINT VPN OPERATING PRINCIPLE (P2P) 52
12.1. VPN CONFIGURATION 53
13. CONNECTION VIA VPN CLIENT COMMUNICATOR 54
13.1. VPN CONNECTION 54
13.2. DIRECT CONNECTION FROM THE BROWSER 56
14. CONNECTION VIA ANDROID OR IOS CLIENT 58
14.1. PROCEDURE FOR CONNECTION WITH ANDROID CLIENT 58
14.2. PROCEDURE FOR CONNECTION WITH IOS CLIENT 61

1. SENECA VPN BOX2

ATTENTION!

IN NO EVENT, SHALL SENECA S.R.L. OR ITS SUPPLIERS BE LIABLE FOR LOSS OF REGISTRATION DATA/INCOME OR FOR* CONSEQUENTIAL OR ACCIDENTAL DAMAGES RESULTING FROM NEGLIGENCE OR THE IMPROPER OR IRRESPONSIBLE USE *OF THE PRODUCT, EVEN IF SENECA SRL IS AWARE OF SUCH POSSIBLE DAMAGES.

SENECA, ITS SUBSIDIARIES, AFFILIATES, GROUP COMPANIES, ITS SUPPLIERS AND ITS DEALERS DO NOT WARRANT THAT THE FUNCTIONS WILL FULLY MEET YOUR EXPECTATIONS OR THAT THE PRODUCT, FIRMWARE AND SOFTWARE ARE ERROR-FREE OR WORK IN A CONTINUOUS WAY.

2. SOFTWARE OPEN SOURCE

The Seneca VPN BOX2 product contains Open Source software distributed under the GPL license. In compliance with section 3b of said license, Seneca provides the sources of this software. It is possible to request the code by writing an email to support@seneca.it .

3. INTRODUCTION

VPN Box is a server device that allows you to create secure VPN (Virtual Private Network) connections between geographically distant Systems and Servers/PCs in a simplified way, maintaining centralized management of all SENECA devices enabled for the use of a VPN.

Remote connections based on VPN technology allow transparent communication using the most common TCP/IP protocols in the industrial world. Since these are connections based on IP (Internet Protocol), it is possible to convey multiple communication protocols simultaneously via VPN. For example, it will be possible to communicate in Modbus TCP/IP with a remote device while carrying out maintenance on the software of a PLC belonging to the same system.

The SENECA devices compatible with VPN BOX2 allow connections from the system both on the Ethernet and directly Mobile/Cellphone networks (only products equipped with modem).

The types of VPN that can be created with this product are of two types: VPN Single LAN and VPN Point to Point.

The Single LAN type solves the cases in which it is necessary to create a connection that allows communication between devices installed in different and distant sites, so as to form a single network which can also include the subnets of the devices, if desired; these cases are typical in SCADA and Telecontrol environments.

The Point to Point type allows a maintainer to reach a single device and, optionally, its subnet to intervene on it; the typical use is the remote assistance in the field of the machines and the reprogramming of a PLC/HMI, the verification of some functions and the solution of the problems.

VPN Box2 is a server device that needs to be configured via the web interface

The VPN Client Communicator software is provided to create the VPN tunnel between a remote PC and the network/device.

VPN BOX2 is only compatible with VPN Client Communicator versions > v4.0.0.0.

All the software needed to use the VPN BOX2 product can be downloaded from the official product page in the SOFTWARE & APP section.

The VPN BOX2 is available in two versions: Hardware and Virtual Machine (vmware) the following are the characteristics of each version.

3.1. HARDWARE SPECIFICATIONS

To obtain the technical specifications of the box pc with which the product is supplied in the "hardware" version, consult the installation manual of the VPN BOX2 product.

3.2. VIRTUAL MACHINE (VMWARE) SPECIFICATIONS

The Virtual Machine version is supplied in exported OVF format with a general indication of the hardware requirements of the Virtual application. These requirements must then be suitably modified by the user when creating the VPN BOX2 Virtual machine in order to take into account:

- *Number of Seneca devices to manage*
- *Number of users to manage*
- *Workload that the server will have to take care of*

For a minimal configuration it is recommended to meet the following requirements:

Requirement	**Minimum value admitted**
CPU	64 bit / 2 cores
RAM	8 GB
Disc	64 GB SSD
SO	compatible with LINUX distributions
Networking	1xETH (100/1000 Mbit)
Host/Hypervisor	Support host: Intel-VT or AMD-V / Hypervisor: VMware

The configurations can be changed after the creation of the server to ensure the application scalability.

For further instructions on using the OVF format to start a VPN BOX2 Virtual Machine see the VM Installation chapter.

4. VPN BOX2 INSTALLATION

4.1. INSTALLATION OF THE HARDWARE VERSION

To install the VPN BOX2 hardware, proceed as follows:

- *Place the server horizontally on a flat surface*
- *Connect the hardware box power terminals to a dedicated power source. Power requirements are listed in the user manual*
- *The VPN BOX2 hardware does not require a keyboard, mouse or monitor to operate. However, they may be required in case of technical service by Seneca personnel.*
- *Start the VPN BOX2 by pressing and releasing the ON/OFF button on the front panel of the box once only*
- *The POWER led will light up instantly but the server will not be immediately operational, it will take a few minutes to start up completely (start-up time max 5 min)*

ATTENTION!

the VPN BOX2 is a server device, needs to be switched on and off correctly, avoiding sudden power cuts. For this reason it is recommended to install a UPS to protect the server power supply.

To turn the server off:

- *Press and release the ON/OFF button once*
- *Wait for the POWER led to switch off completely*
- *In some cases the normal shutdown procedure may take 1 or 2 minutes.*

If the server is blocked from starting up or fails to shut down, proceed with a forced shutdown as follows:

- *Press and hold down the ON/OFF button once*
- *Keep the button pressed until the POWER led goes off.*
- *Repeat the start procedure*

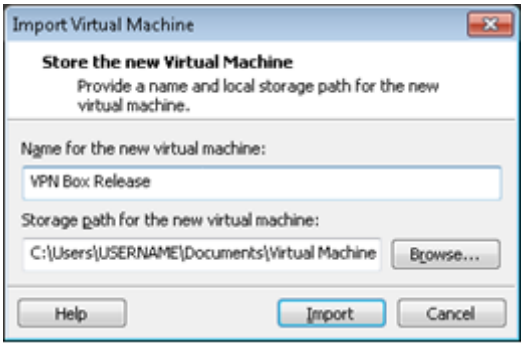
For further details on the installation of the VPN BOX2 hardware, consult the product installation manual.

4.2. INSTALLATION OF THE VIRTUAL MACHINE VERSION

In the case of virtual machine installation, the file with the ".ovf" extension must be imported into your virtualization software. All the supplied accessory files must be in the same folder as the OVF file to avoid errors during the import and creation of the virtual machine.

The OVF file is compatible with VMware Workstation Pro virtualization software, the instructions below show how to import the VPN BOX 2 virtual machine application into that software

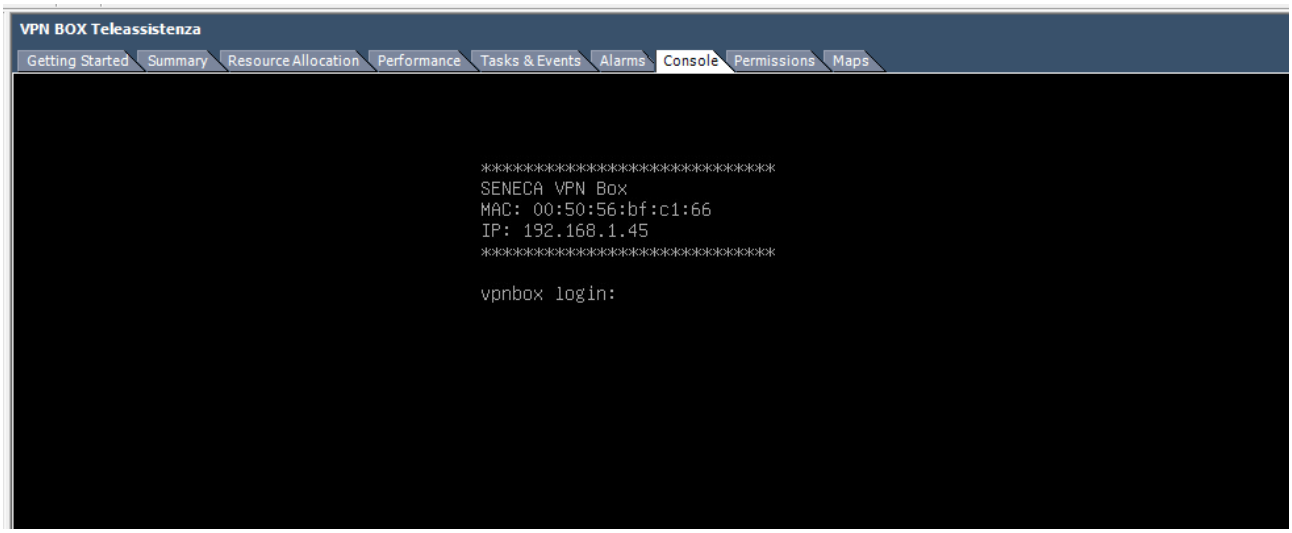
- *Double click on the file name with the .ovf extension to start the application import*
- *Follow the import virtual machine wizard*



- *Start the virtual application*
- *Once the start is complete, the login screen will be displayed on the console. As shown in the following screenshot*

ATTENTION!

No operator action is required on this screen. Simply minimize the console to an icon and use the VPN BOX2 server via web access with a compatible browser.



The VMware compatibility is set as follows:

- ESXi 7.0
- ESXi 6.7 U2*
- Fusion 12.2.x
- Fusion 12.x
- Fusion 11.x
- Workstation 16.2.x
- Workstation 16.x
- Workstation 15.x

ATTENTION!

The virtual machine and the Guest operating system is of the 64 bit type therefore the Server/PC Host must be compatible with the Intel-VT or AMD-V technologies which must be previously activated in the bios.

5. DEFAULT ETHERNET NETWORK CONFIGURATION

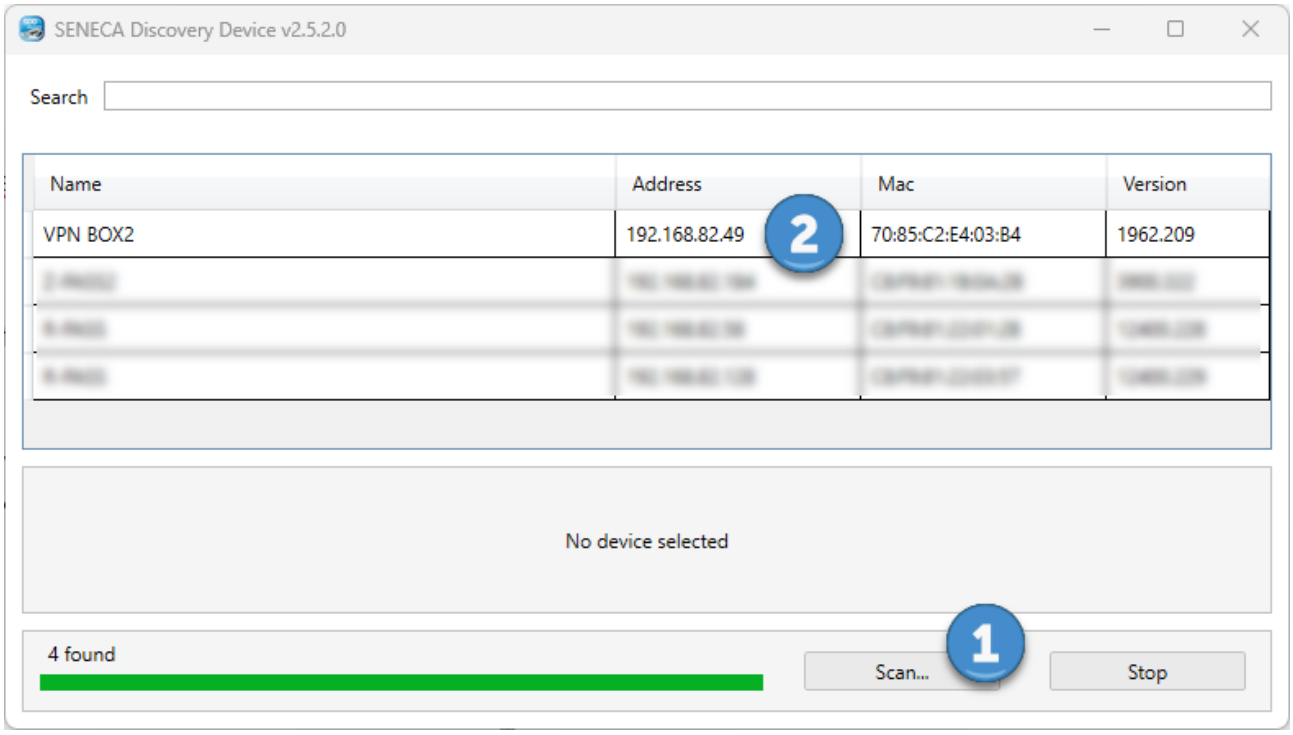
VPN BOX2 is supplied by default with the Network/Ethernet port set in DCHP (automatically obtain IP address from the network), if a DHCP server is not available the IP address 192.168.90.101 will be automatically set.

To detect the current IP address of the VPN BOX2 it is recommended to use the SDD (Seneca Discovery Device) software installed on a PC connected to the same network as the box or running directly on the same Host server on which the Virtual Machine is running.

The SDD software can be easily installed by running the installation program available at the following link:

http://www.seneca.it/products/sdd

once the network has been scanned with the "Scan..." button, the IP address will be visible in the "Address" column corresponding to the row of the "VPN BOX2" device:



6. FIRST TIME CONFIGURATION OF THE VPN BOX2

To configure the VPN BOX2 it is necessary to use a browser of the same type used for Internet browsing.

Once you have obtained the current IP of the server via SDD, start the web browser and enter the following URL in the address bar:

Errore. Riferimento a collegamento ipertestuale non valido.

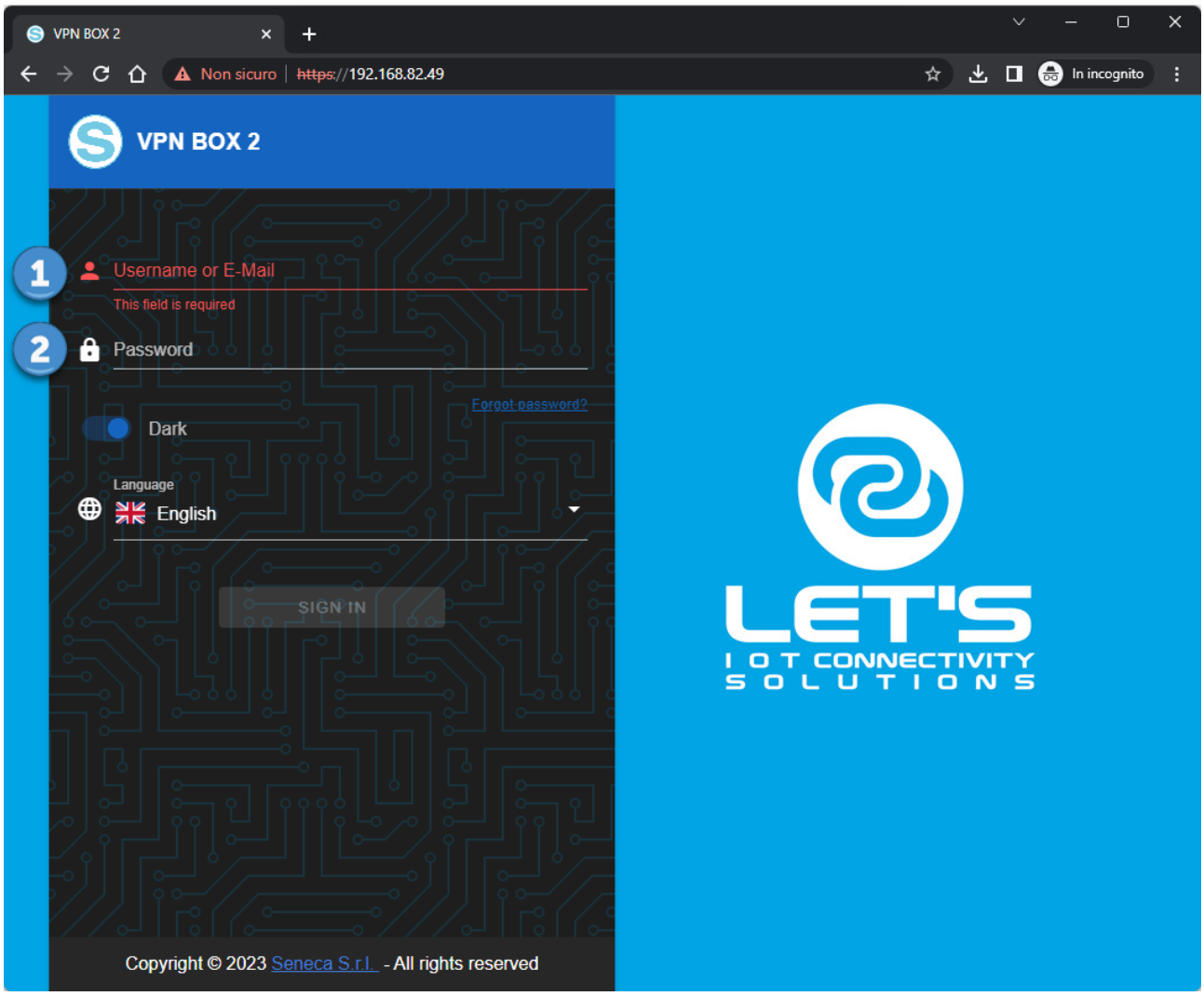
NOTE: replace the value with <actual-ip-address> with the IP address found via SDD e.g. 192.168.90.101, an example of a valid URL is as follows:

https://192.168.90.101/

at this point the browser will show the login screen.

6.1. LOGIN

At each access, including the first configuration, the server asks the user to identify himself:



The default login credentials are as follows:

Username: supervisor

Password: seneca

ATTENTION!

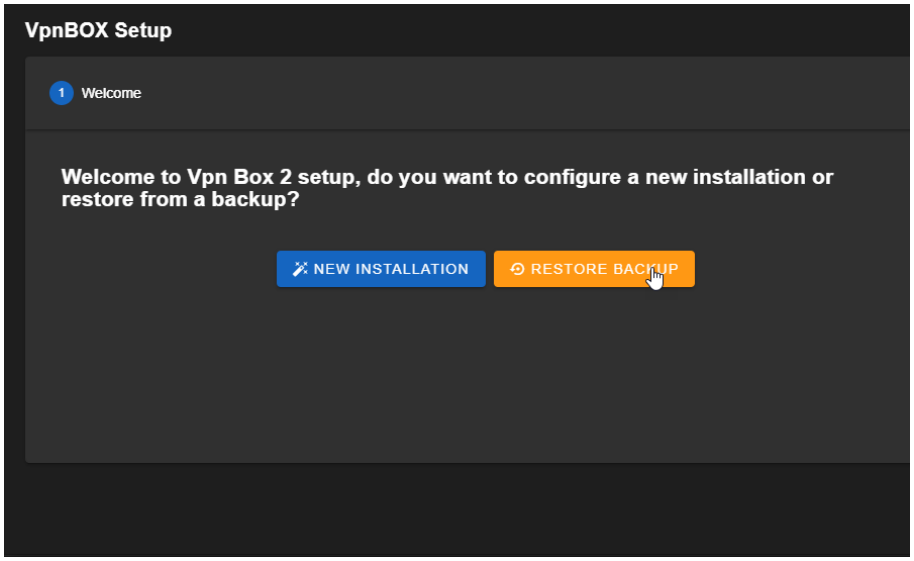
For security reasons it is recommended to change the default credentials of the user with maximum "supervisor" privileges and it is recommended to create a user for each individual who needs to access the system.

Once login is verified, if the server has never been configured, the first configuration wizard will appear, otherwise the Home panel will be displayed.

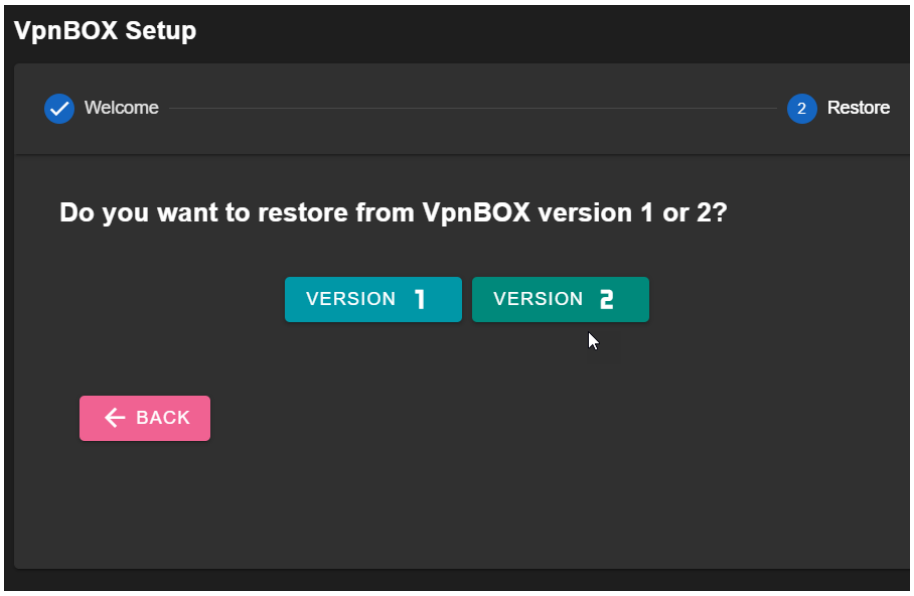
6.2. WELCOME

When first started, a first configuration wizard will appear which will allow the operator to choose between

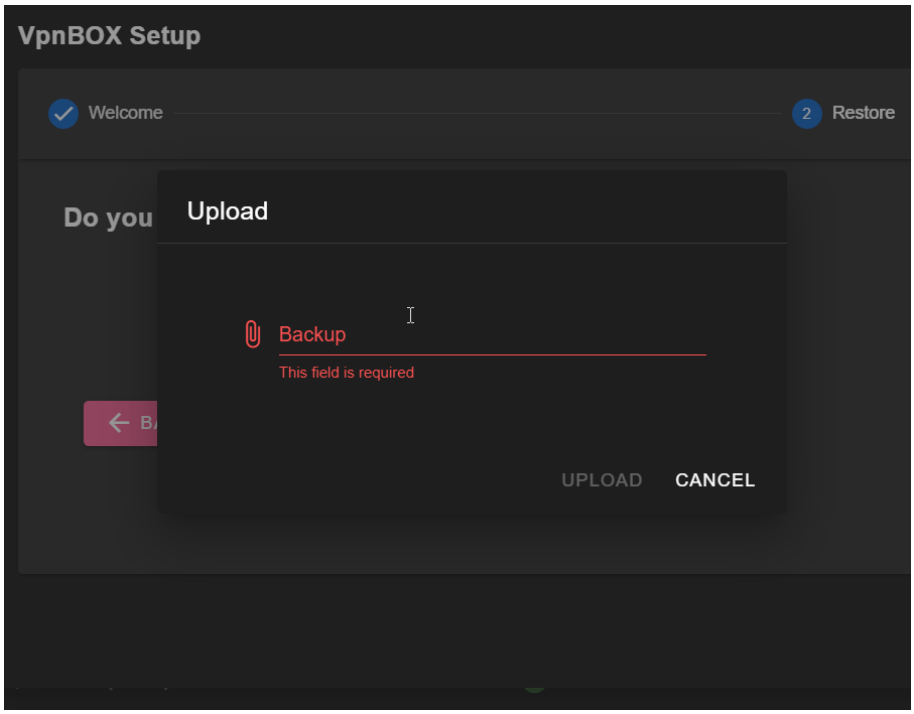
- *Creating a new configuration*
- *Restoring a VPN BOX2 from backup file*



In the case of restoring the backup file, you can choose whether to import a file from a previous VPN BOX v1 installation or a file from a VPN BOX2



Click on the "Backup" text, select the backup file you wish to restore and confirm by clicking on "upload":



At the end of the file upload, the VPN BOX2 server will restart, wait for the procedure to complete.

6.1. MODE

In the case of a new installation, the basic network mode selection popup will appear where it will be possible to choose between the options:

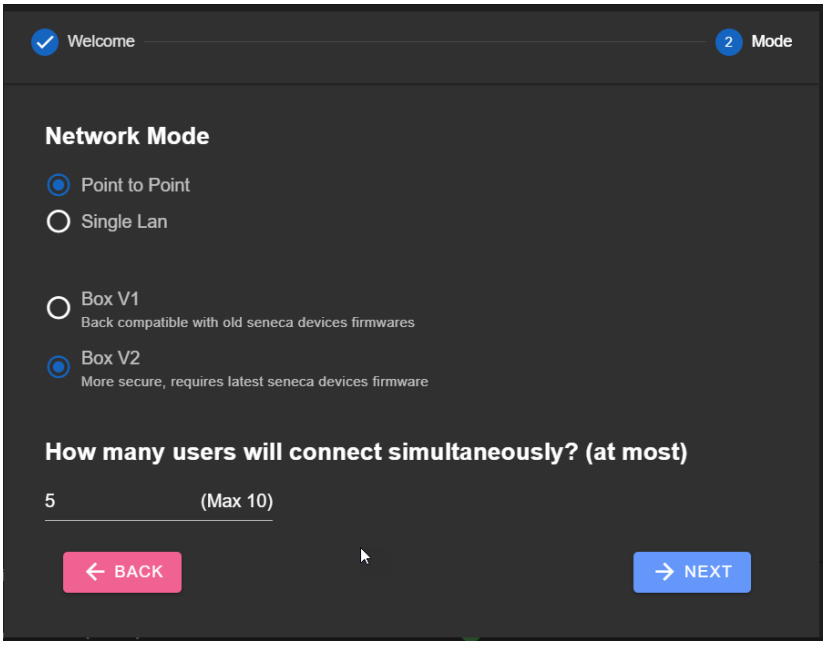
- *Point to Point*
- *Single LAN*

And among the compatibility modes with Seneca devices:

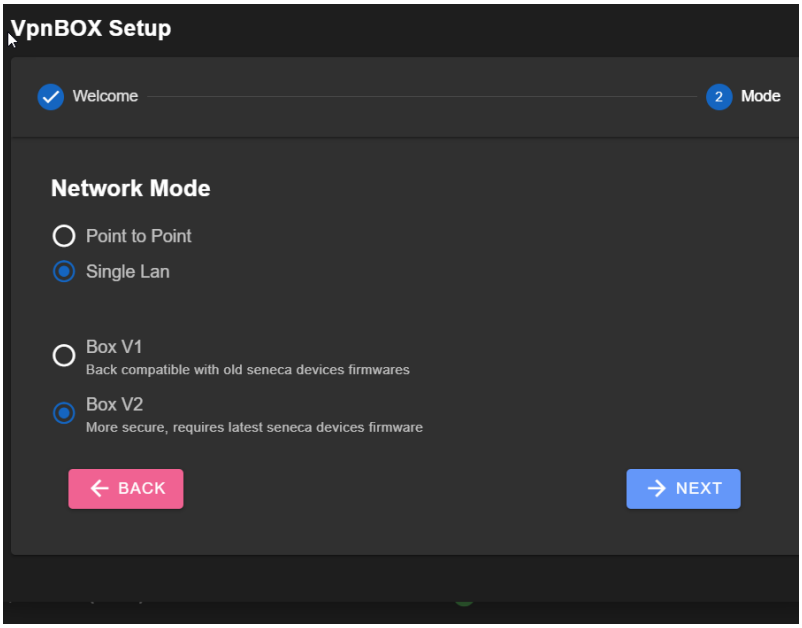
- *Box V1: all the devices will connect to the VPN BOX2 believing they are accessing a previous version VPN BOX (v1). Activation of the VPN connection is slower as the protocol used is not realtime. It is the only possibility if you only have Seneca devices and firmwares not compatible with VPN BOX2.*
- *Box V2: VPN BOX2 compatible devices will use all the features available on the server such as: minimization of waiting times in activating the VPN connection.*

it will always be possible to change these settings at a later date through the appropriate Networks menu.

In Point to Point mode it is necessary to choose the maximum number of simultaneous connections that the VPN BOX2 server in P2P mode will have to manage. From this count, the SL connections must be excluded, which will be counted separately and better defined in the Networks (VPN) setup in the Server Administration section:



In Single LAN mode it is not necessary to choose between the number of simultaneous users as all users belonging to that network will have simultaneous access to all the devices of the Single LAN network:

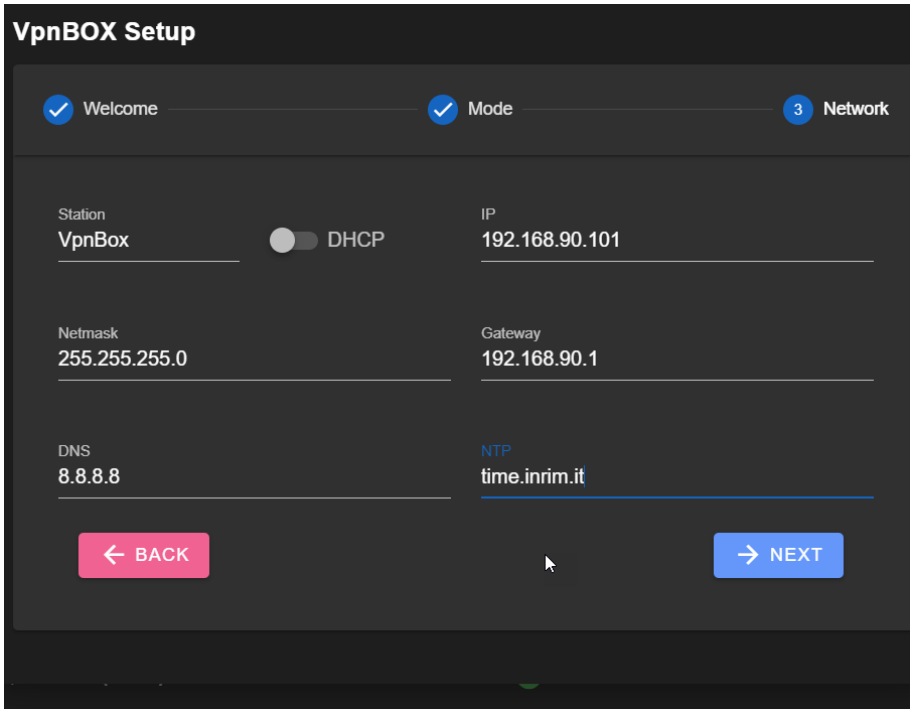


To learn more about the differences between the two operating modes Single Lan and Point to Point, see the respective chapters on the operating principles: "vpn network single lan operating principle" and "vpn network point to point operating principle".

6.1. NETWORK

The "network" popup of the first configuration wizard allows you to set the communication parameters of the VPN BOX2.

The following window shows the classic network settings of an Ethernet-based device which can be static or dynamic with the help of DHCP:



The meaning of each parameter is shown in the following table:

Parameter	**Meaning**
Station	Name of the vpn box which will be shown in the title bar for easier identification of the server function. Default: VpnBox
DHCP	Indicates whether the IP address for the vpn box should be obtained automatically from the network. If enabled, the IP, Netmask, Gateway, DNS parameters can no longer be set by the user. Default: ON
IP	IP address for the vpn box Default: 192.168.90.101
Netmask	Netmask for vpn box Default: 255.255.255.0
Gateway	IP address of the Host Gateway that allows the vpn box to surf the Internet

	Default: 192.168.90.1
DNS	Address of the server for name resolution, it can be an IP belonging to the LAN of the VPN BOX2 or even external. Default: 8.8.8.8
NTP	IP address or hostname of the NTP server to be used for time synchronization of the VPN BOX2 server Default: time.inrim.it

ATTENTION!

The ***vpn box must be able to browse the Internet in order to carry out the following essential operations for correct operation:***

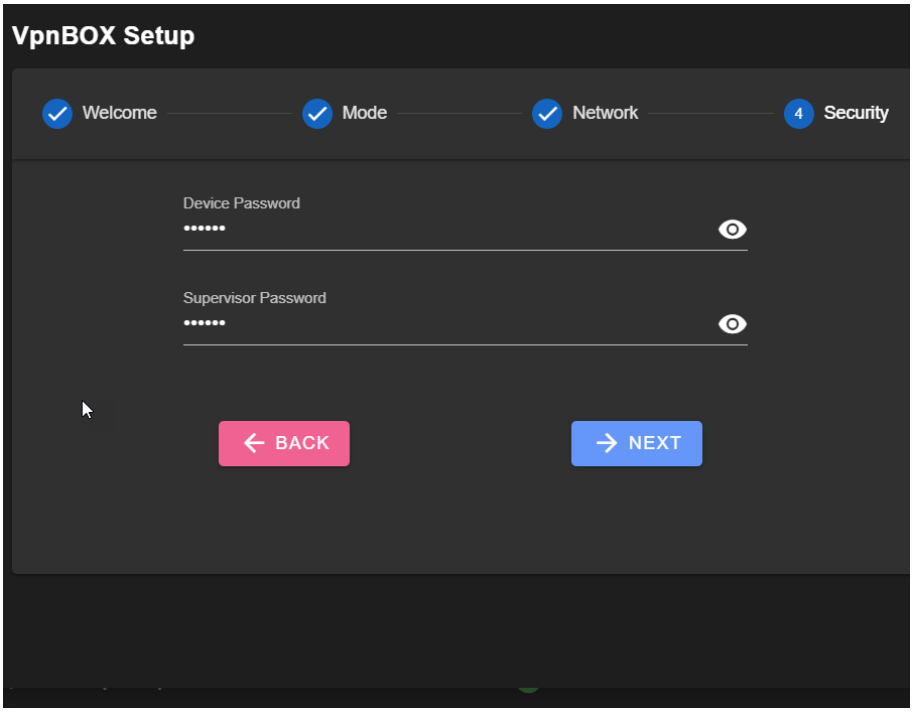
- ***to synchronize the system clock (NTP) without which the vpn could not be created***
- ***security updates***
- ***application updates***

6.1. SECURITY

The "security" popup of the first configuration wizard allows you to set/change the default passwords

- *of the user with maximum "supervisor" access privileges*
- *of devices for preliminary authentication (to be entered in the configuration menu of the device itself)*

For comparison, see the user manual of the device used in the "VPN configuration" paragraph:



6.1. LICENSE

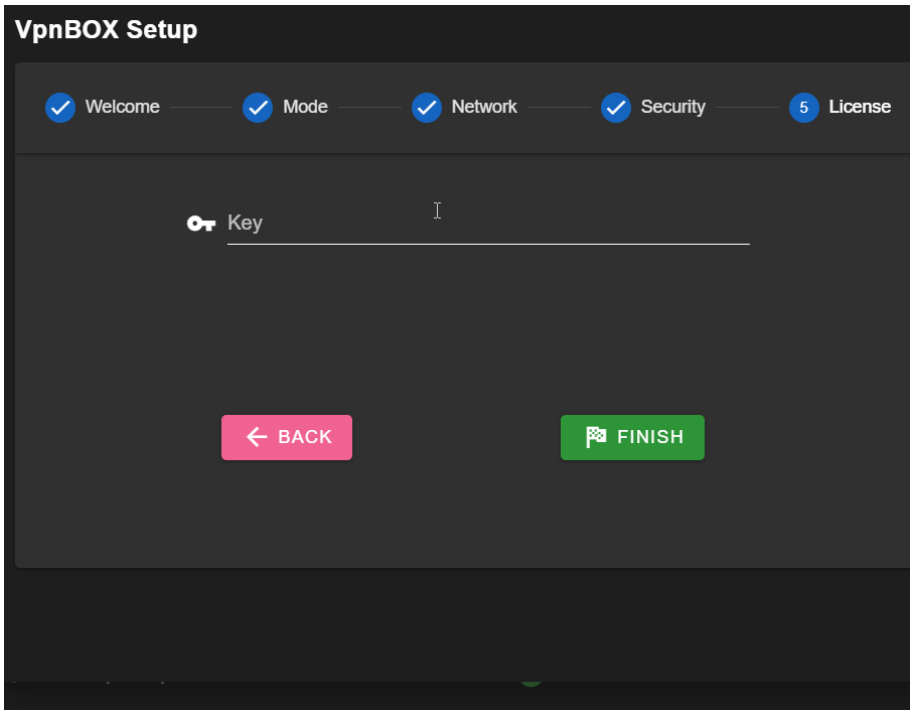
The "security" popup of the first configuration wizard allows you to load the VPN BOX2 software user license

The license code is present in the coupon provided with the product.

The license consists of an alphanumeric code with 4 groups of 4 digits of the type:

AAAA-BBBB-CCCC-DDDD

to enter in the “Key” field:



When the "Finish" button is pressed, all the settings entered in the previous wizard pop-ups will be applied to the server and the license associated with the code just entered will be activated.

If the user does not have a license code, he can continue leaving the "Key" field empty, the VPN BOX2 will still be operational in “Demo” mode, with the following limitations:

Number of enabled users: 2

Number of connectable devices: 2

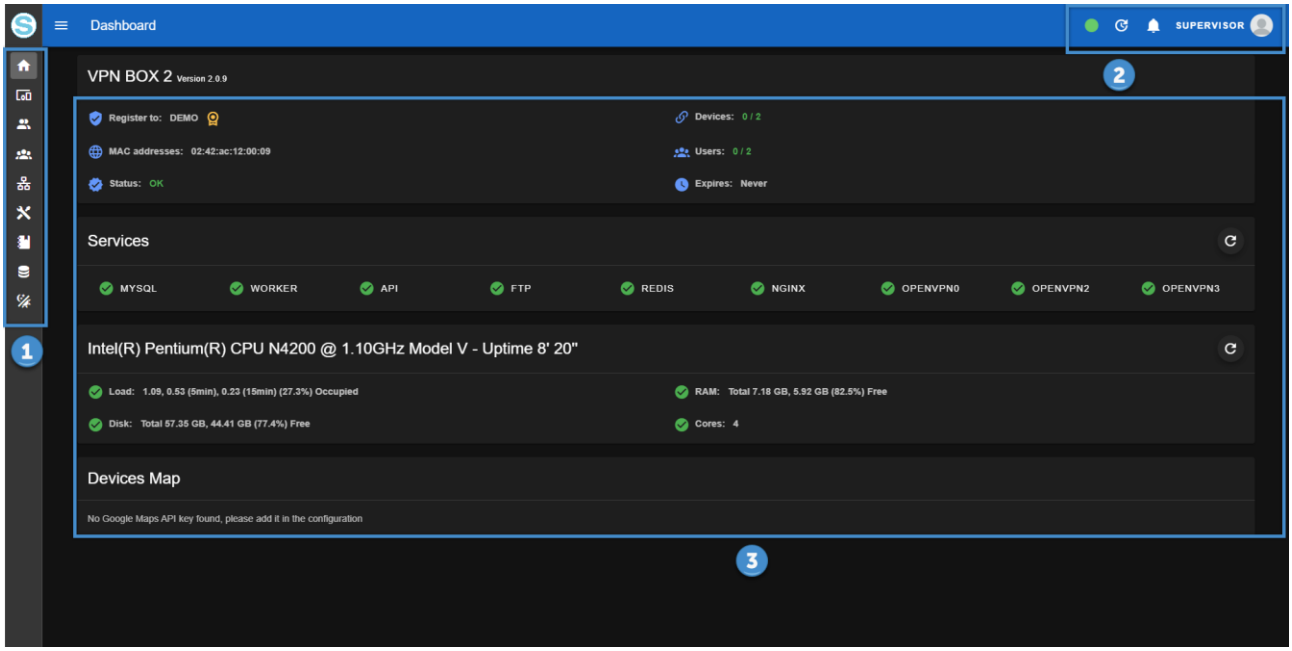
It will be possible to introduce the license at a later time.

7. SERVER ADMINISTRATION

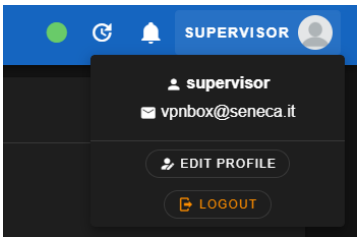
In this chapter the functions of each item of the navigation menu of the VPN BOX2 server will be studied in depth.

7.1. HOME

The home page will be visible immediately after the user login. It is divided into 3 main sections: the navigation menu (1), the user management bar with attached notification area (2) and the central panel (3) divided in turn into several status panels:



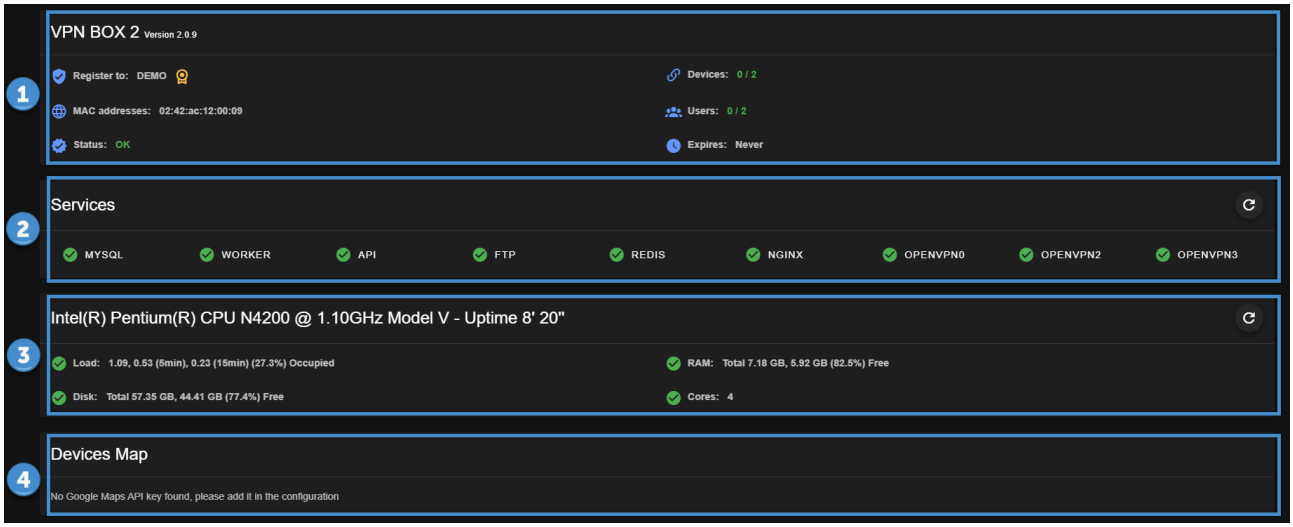
The currently logged in user management bar allows logout and management of user preferences:



by pressing the "Edit profile" button in this section it will be possible to:

- *Modify your email*
- *Change your credentials (password)*
- *Activate 2-factor authentication (2FA)*
- *Change your web interface language preference*

The home page status panels consist of the following:



The upper part showing the version of the VPN BOX2 application, the license and the related characteristics of the supported devices and users (1)

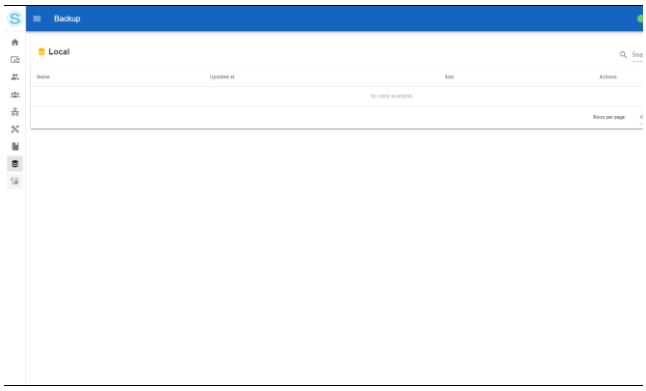
Panel of active services (2) which reflects the server's operation at that precise moment. In the event of a service not working properly, the icon placed alongside would be a red X to indicate an error status.

It is advisable to consult the Logs menu to detect the anomaly that caused the service to stop. For correct server operation, all services must be active.

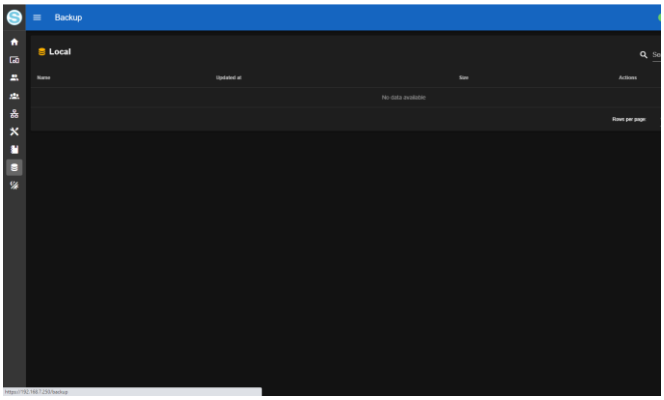
The server statistics panel (3) shows the operating status of the physical or virtual machine hosting the VPN BOX application. The statistics are: CPU load, RAM usage percentage, disk and number of processor cores.

On each page it is possible to adjust the background of the application according to your visual comfort by clicking on the last button of the menu to obtain the following:

Light background

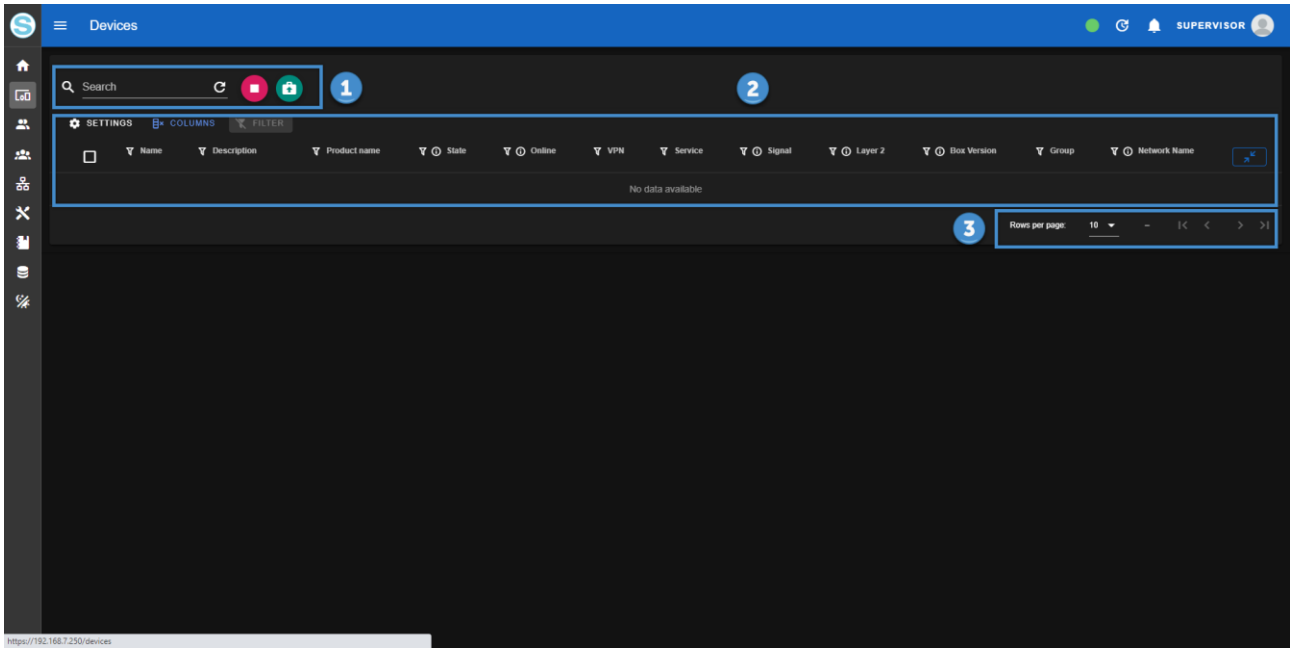


Dark background (default)



7.2. DEVICES

The Device section contains the list of all Seneca devices connected to the VPN BOX2. There is no add device button as it is the device itself which, properly configured, will appear in the list.



Once configured locally via your Web Server, Seneca devices will register on the VPN BOX2 and will appear in this section: this operation could take up to 2 minutes in case of poor quality of the server-device communication channel.

During this time, each device will communicate any changes in status and will receive new configurations from the server for the first "initialization".

The Devices page is equipped with a "full text" type search filter (1) where each typed text will be searched for in all the device attributes, a table/list (2) constitutes the central view while the lower part contains the table pagination control (3). By default, 10 devices are shown per page.

The status of the device determines the colour of the text with which it is displayed on the page as shown in the following table:

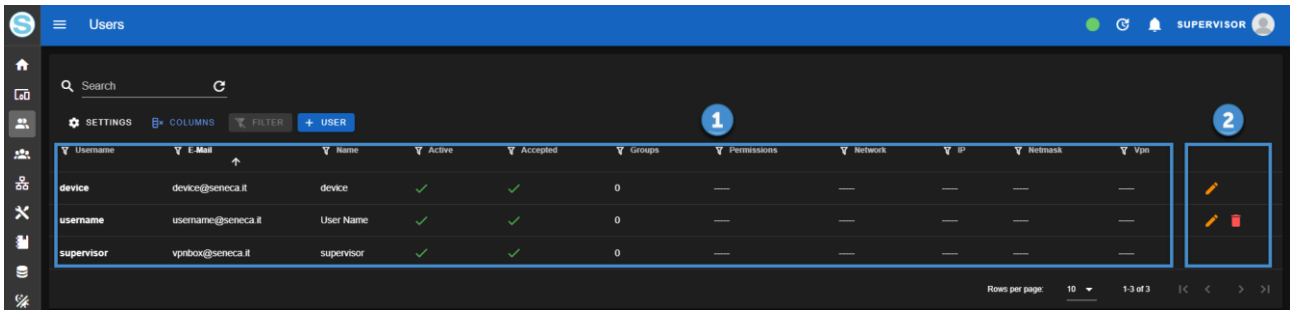
Status	Colour
New (to be assigned to a Group)	Gray
Configured and connected	Green
Not connected	Red

Immediately after registration, the device status is "New" and the device itself is waiting to be configured; in this state the device will not perform any operation and will not connect in VPN. During registration, the device provides its identification data:

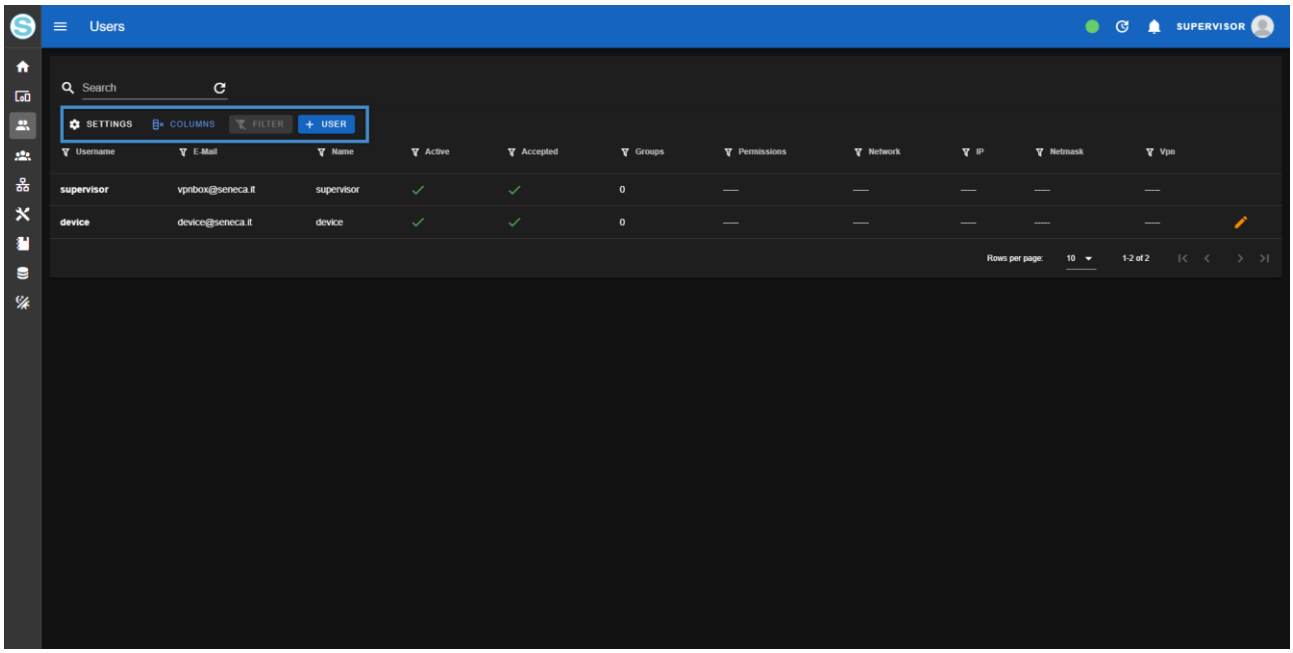
- *its MAC address,*
- *the IMEI (if equipped with a modem),*
- *the name of the TAG (identifier chosen by the user and entered in the device configuration via its web page)*
- *the configuration of the local LAN network of the device.*

7.3. USERS

The Users section contains the list of all users authorized to log in to the VPN BOX2 server. The content of the page is divided into two parts: the user list in tabular form (1) and the commands/actions area (2). An edit and delete button will appear for each user line except for the two system accounts "device" and "supervisor":

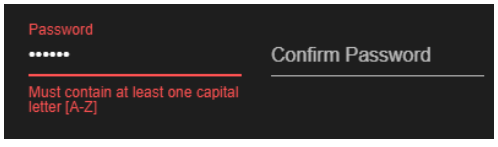


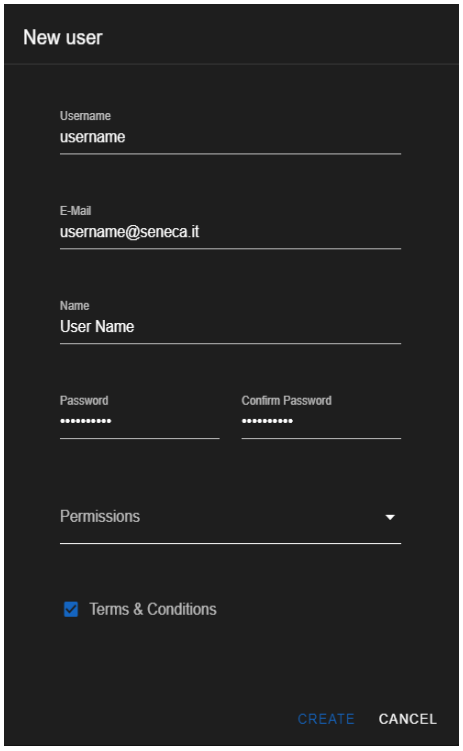
The upper part of the page allows you to filter users with full text search:

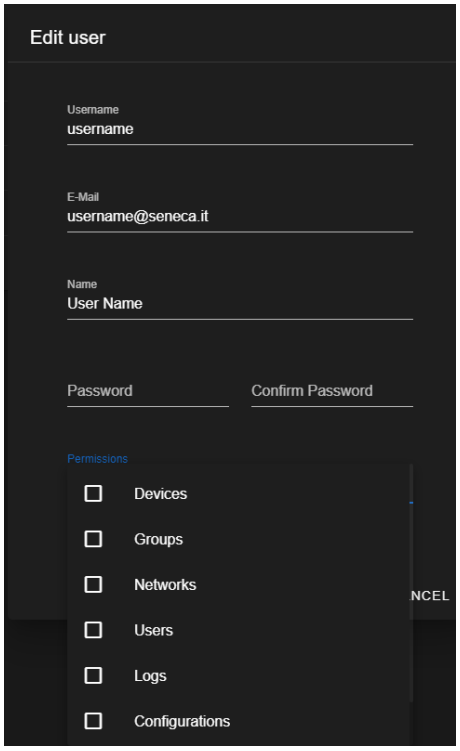


By clicking on the "+ User" button, the new user insertion pop-up will appear through which it will be possible to enter his/her data and credentials. Confirm your entry with the "Create" button.

In the event of an entry error or constraints not complied with in the field (e.g. Password that does not comply with the minimum security requirements) the value will be highlighted in a red text colour and immediately below the editable field a suggestion will appear to guide the user in the correction.





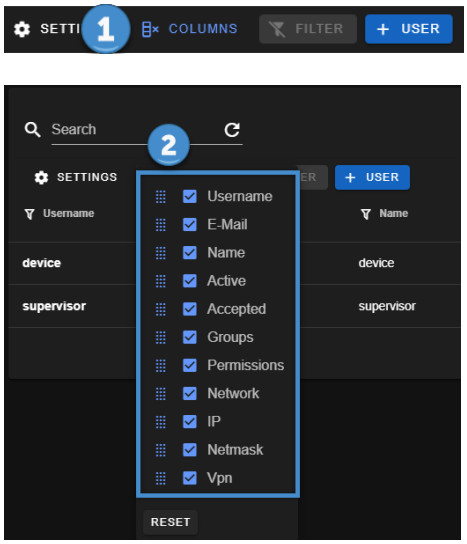


The meaning of each parameter is shown in the following table:

Parameter	**Meaning**
Username	Short username
Email	User email address Can be valid or invalid. A valid address is required in case of activation of the 2FA authentication service with relative enabling of the mail sending service: Server administration > Config. Snmp
Name	Extended user name
Password/Confirm Password	User password to be entered twice to verify correct entry from the keyboard
Permissions	Checklist to select all privileges to assign to the user. The available privileges and their functions are listed below **Devices**: allows you to manage the devices and view the relative menu page **Groups**: allows you to manage groups and view the relative menu page **Metworks**: allows you to manage the VPN networks and view the relative menu page **Users**: allows you to manage users and view the relative menu page **Logs**: allows you to view the system log page of the VPN BOX2 application **Configurations**: allows you to manage the configurations of the VPN BOX2 server. See Server administration > Config. chapters

	System: creates a replica of the "supervisor" user by assigning the user being created maximum privileges on the system.
Term & Conditions	Tick to accept the terms of service of the VPN BOX2 software

By clicking on the "Columns" button (1) it is possible to control the table display settings such as the sorting of the columns and which ones to display/hide (2):



Each created user will have the possibility to access the VPN BOX2 through the Login via browser but does not yet have the possibility to connect with the VPN to the devices. To do this, it is necessary to create an access group which will put a certain number of users in relation with the devices they can access and above all with the relative access method to be used, SL or P2P.

To proceed with the configuration, see the Server administration > Groups paragraph.

Users can be added, edited and deleted as desired; clearly, if an account is cancelled while in use, it will only be effectively closed when you disconnect from the VPN.

ATTENTION!

Username and password are case sensitive.

7.4. GROUPS

This section represents the connection element between users, devices and VPN access modes (SL or P2P). Each group can contain a subset of devices and users. In particular, the following rules apply:

- *A user can belong to multiple groups*
- *A device can belong to one and only one group, however it can be moved to another group if necessary*
- *The group to which it belongs defines the VPN access mode to the device*

Example:

Suppose we have two users called X and Y and 4 Seneca devices Z, X, Q, K. We want to configure the VPN BOX2 server so that user X can see all the devices while user Y only Q and K.

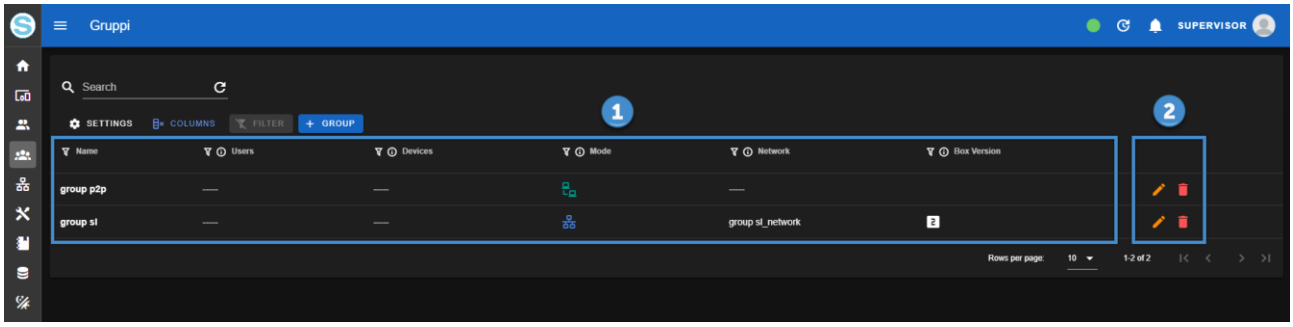
To do this we will have to create two groups:

- *A group 1 containing devices Z, X*
- *A group 2 with only Q and K.*

the user-group assignment must be carried out as follows:

- *User X belonging to both groups 1 and 2*
- *User Y belonging to group 2 only*

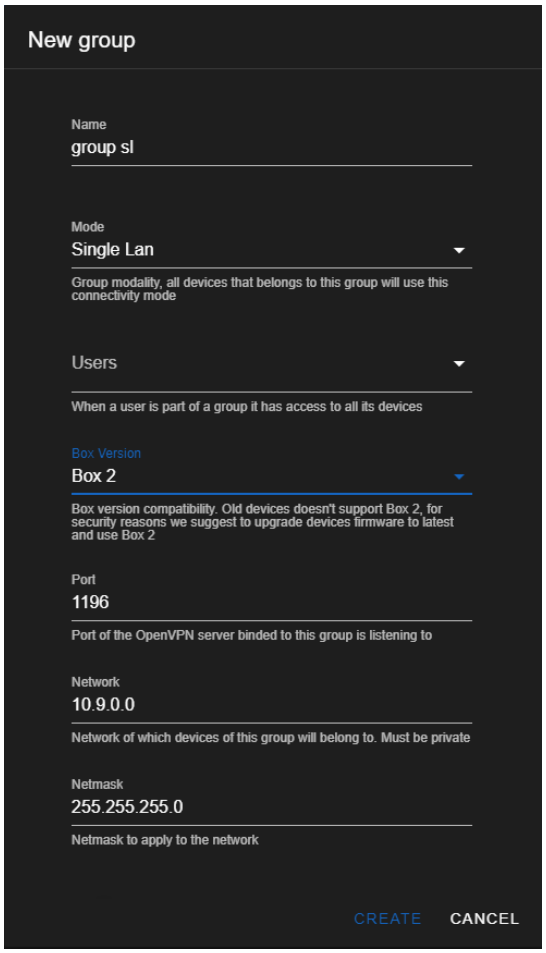
The content of the page is divided into two parts: the group list in tabular form (1) and the commands/actions area (2) with the buttons corresponding to each Group row:



By clicking on the "+ Group" button, the new user insertion pop-up will appear through which it will be possible to introduce its configuration fields and confirm the insertion with the "Create" button.

The group configuration fields depend on the VPN access mode provided for that Group (Mode). The following tables show all the possible configuration fields.

Single LAN VPN access mode (Mode = Single LAN):

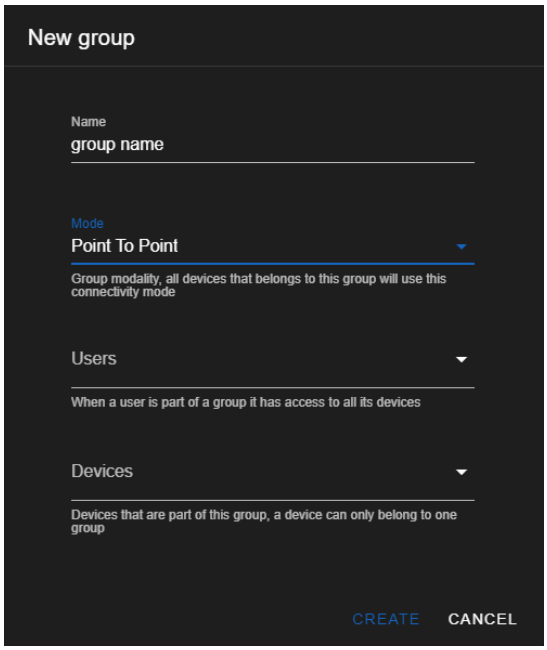


Parameter	Meaning
Name	Group name
Mode	VPN operating mode
Users	Users who are part of the Group. Expand the drop down menu and select
Box Version	Version of the communication protocol between device and vpnbox. Use Box 1 if you have devices of the Z-TWS4, Z-PASS1, Z-PASS2 type, otherwise select Box 2
Port	TCP port used for all connections of devices and users belonging to this group. Please refer to the Router Configuration paragraph in the "Vpn operating principle" chapter of the SL operating mode
Network	Indicates the virtual VPN address space that will be assigned to devices and users when connected to this group.
Netmask	Used in conjunction with the Network parameter to indicate how many IP addresses to arrange for the subnet of virtual VPN addresses.

ATTENTION!

The Network parameter must never coincide with a physical network that already exists elsewhere. In Single LAN mode it is important that a network used in the LAN of a remote device (e.g. 192.168.90.0/255.255.255.0) is never used in other devices or in the BOX2 VPN server itself.

VPN Point to Point Access Mode (Mode = Point to Point):



Parameter	Meaning
Name	Group name
Mode	VPN operating mode
Users	Users who are part of the Group. Expand the drop down menu and select
Devices	Devices that are part of the Group. Expand the drop down menu and select

7.5. NETWORKS (VPN)

This section allows you to manage the VPN Networks or the connection resources between users and devices. They are of two types too, SL and P2P like groups. In a mixed configuration where the VPN BOX2 is to be used for both SL and P2P connections, other networks will have to be created via this page.

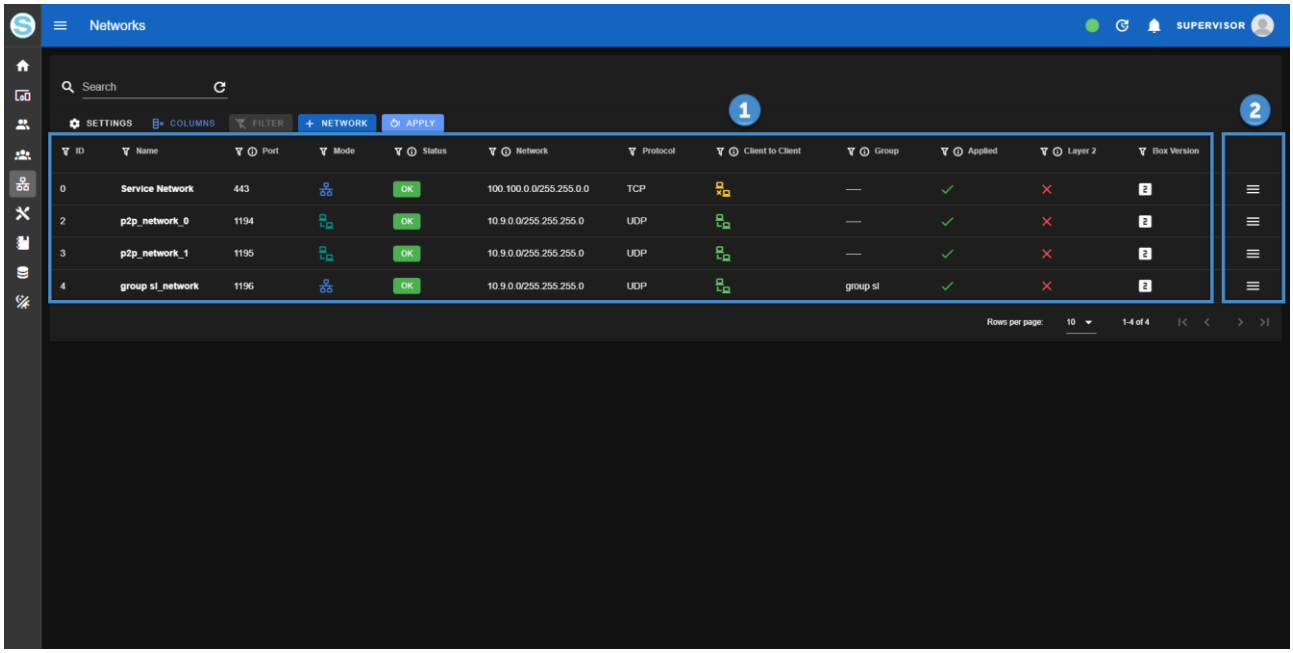
ATTENTION!

The VPN BOX2 first configuration wizard will insert all networks of the type selected in the procedure but it will always be possible to add further resources later. The only thing to bear in mind is that each network will correspond to an additional TCP/UDP port to be opened as an incoming NAT rule on the firewall where the VPN BOX2 service is exposed.

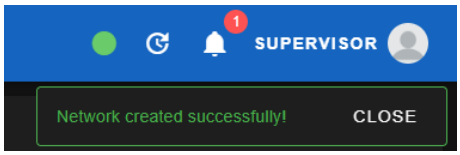
Depending on the type of network created, the following restrictions apply:

- *A SL Network can allow multiple users and devices to connect simultaneously*
- *A P2P Network allows the connection of only 1 P2P device at a time, possibly with multiple users who request it.*
- *A second device requesting access to a P2P Network will be connected to another P2P Network, the first available*
- *The monitoring and assignment of the first available P2P Network is carried out by the VPN BOX2 itself and signalled to the devices and users via the constantly active HTTPS/MQTTS service channel.*

The content of the page is divided into two parts: the list of networks in tabular form (1) and the commands/actions area (2):

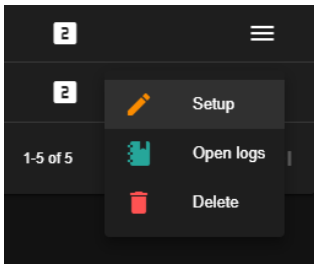


The confirmation of the operation or any error is signalled in the upper right of the notification area:

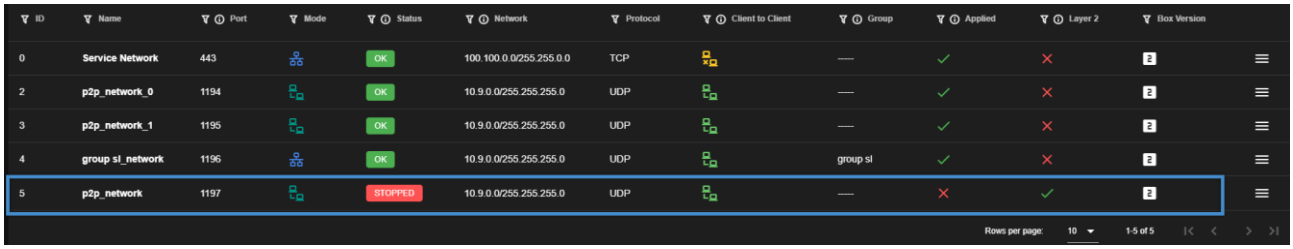


By clicking on a Network in the actions menu, you can perform the following operations:

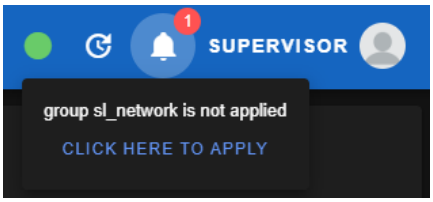
- *Setup: opens the popup with the Network settings*
- *Open logs: direct link to the logs page with the pre-set filter on the logs of the selected Network only*
- *Delete: deletion of the Network*

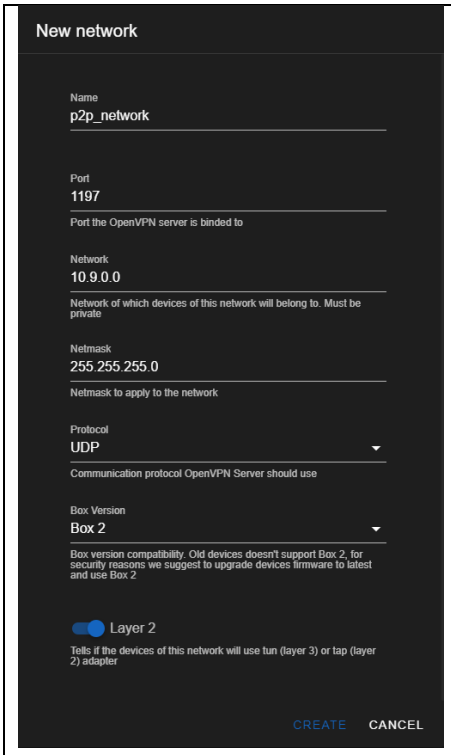


Immediately after inserting a new network, its status will be "stopped" and the network will not be operational until confirmed by the user.



It will be possible to confirm the configuration and apply the settings by clicking the "apply" button or by clicking in the notification area of the top bar and confirming the operation with "click here to apply":



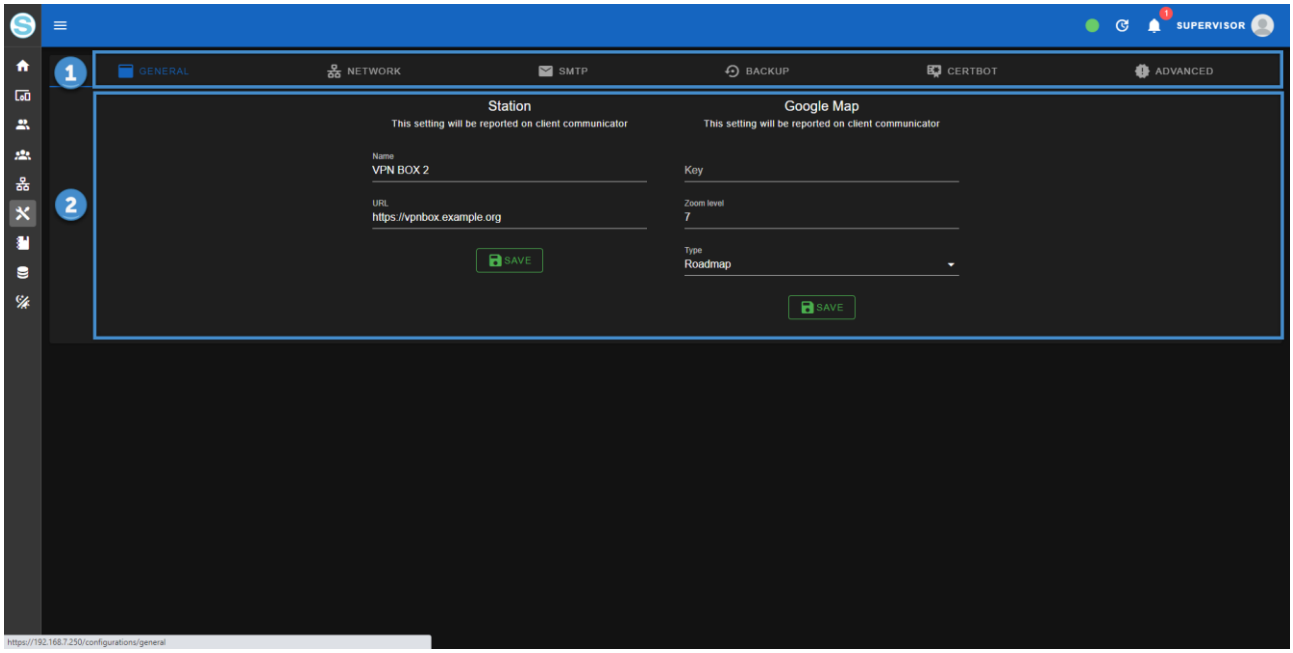


Parameter	Meaning
Name	Group name
Port	TCP or UDP port used for all connections of devices and users belonging to this group.
Network	Indicates the virtual VPN address space that will be assigned to devices and users when connected to this group.
Netmask	Used in conjunction with the Network parameter to indicate how many IP addresses to arrange for the subnet of virtual VPN addresses.
Protocol	Communication protocol used at the transport layer: possible values: TCP, UDP. TCP is recommended for stable data connections between users, devices and servers, otherwise UDP is preferable
Box Version	Version of the communication protocol between device and vpnbox. Use Box 1 if you have devices of the Z-TWS4, Z-PASS1, Z-PASS2 type, otherwise select Box 2
Layer 2	It allows you to activate a "low level" VPN where all the data traffic of the remote network is accessible from the PCs of the users who access it. It can be selected only if the Network is of the P2P type

7.6. CONFIG. GENERAL

This section allows you to manage the configurations of the VPN BOX2 server.

The content of the page is divided into two parts: the tabbed navigation bar which divides all the configurations by category (1) and the main part with the list of parameters (2).

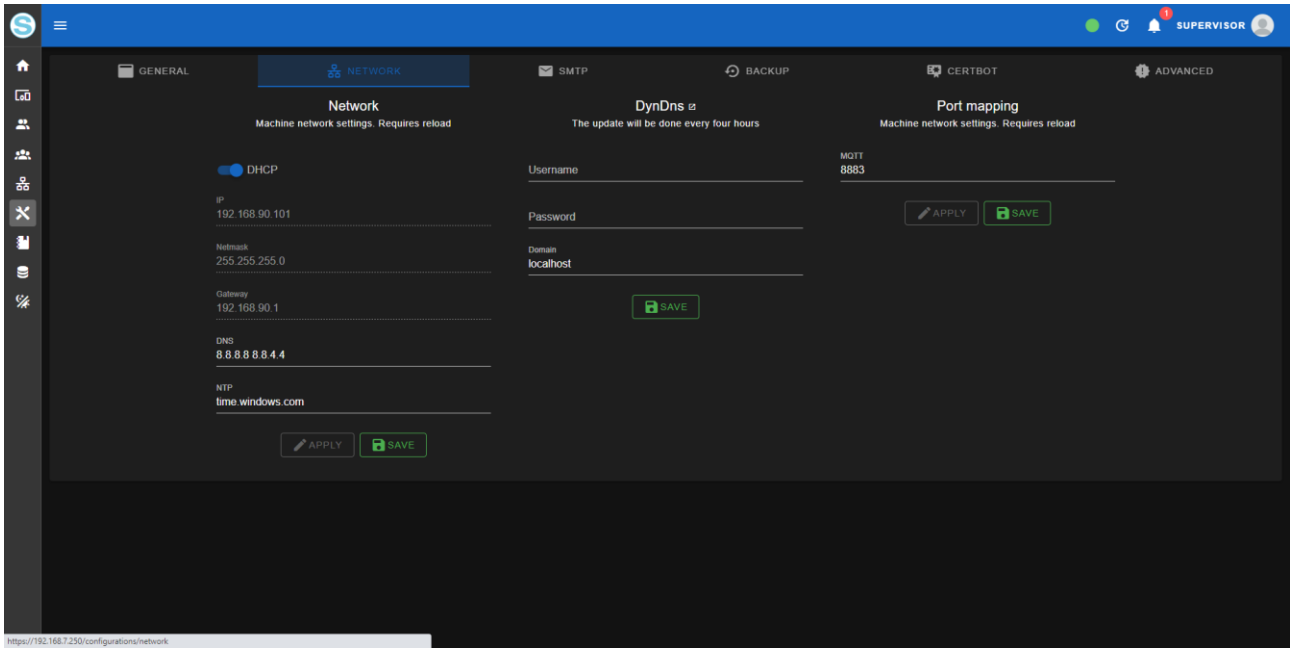


The general page contains the following parameters:

Parameter	**Meaning**
Station / Name	Server name that will be displayed in the title bar in order to identify the VPN BOX2 more easily
Station / URL	Full address of the VPN BOX2 server (the one that must be typed into the address bar of the browser)
Google Map / Key	To use this service, registration with the third-party Google Maps service is required. Once the account is active, to connect it to the VPN BOX2 server, it will be necessary to enter the API Key code in this field. For more information, consult the official website of the service: https://developers.google.com/maps/documentation
Google Map / Zoom Level	Default zoom level of the map when opening the Home window
Google Map / Type	Type/Style of map used

7.7. CONFIG. NETWORK

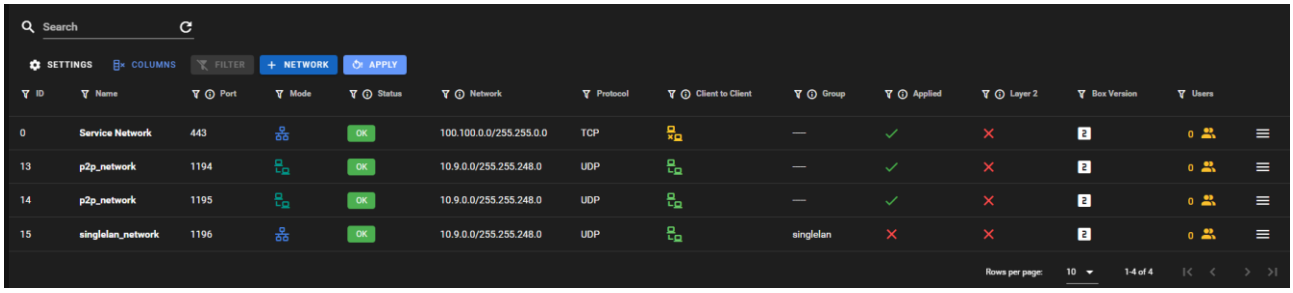
The network page contains the parameters relating to the Ethernet port of the server plus some services that simplify the accessibility of the server via the public IP such as the Dyndns service



The meaning of each parameter is shown in the following table:

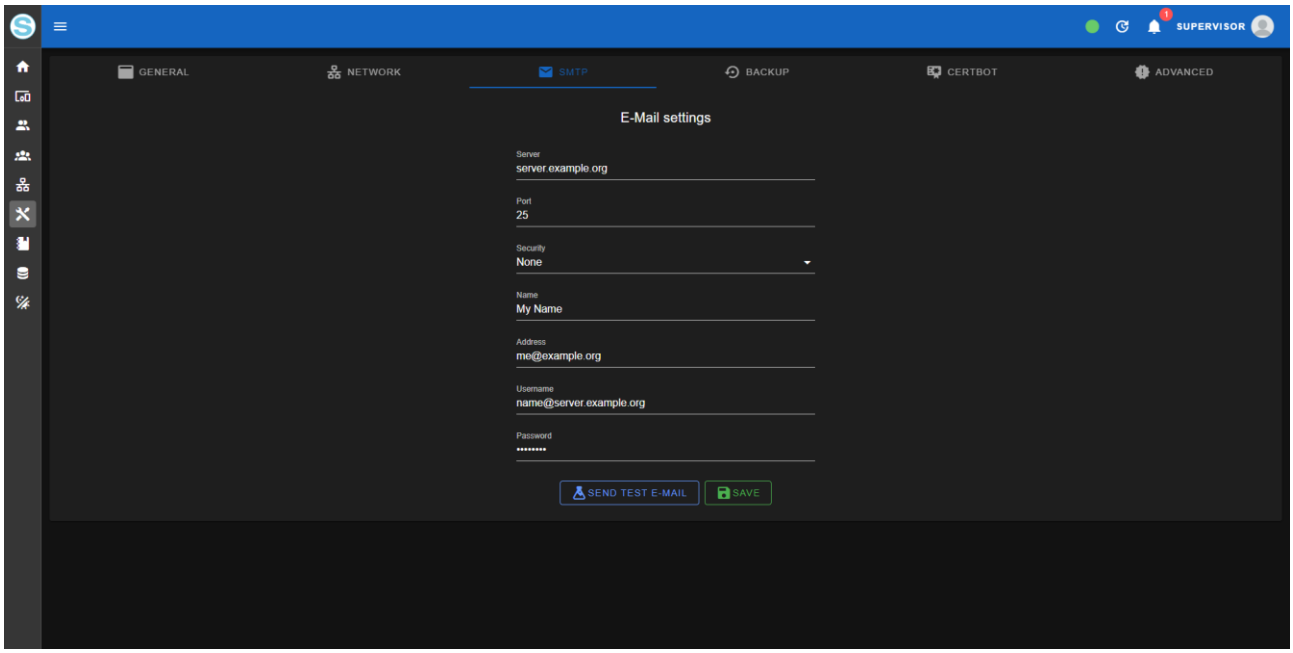
Parameter	**Meaning**
Network / *	See the section “first configuration of vpnbox2 > network” the parameters are of the same type
Dyndns / Username	To use this service, registration on the third-party portal DynDns.IT is required. Once the account is active, to connect it to the VPN BOX2 server, it will be necessary to enter the DynDns account credentials in this field. For more information, consult the official website of the service: https://dyndns.it/
Dyndns / Password	Password of the DynDns.IT account to be connected to the VPN BOX2 server
Dyndns / Domain	the domain name created in DynDns.IT for instance: myvpnbox2.ns0.it
Port mapping / MQTT	Devices compatible with the VPN BOX2 realtime service protocol use a dedicated port for real-time communication with the server. If the port indicated here is not available or is already busy on the perimeter firewall, it can be changed to one chosen by the IT manager. In any case, if the device does not find the port indicated here open, it will try to use the 443/TCP which must always be open for the application to function correctly.

Using the yellow icon it is possible to check the users currently connected to the network:



7.8. CONFIG. SNMP

The snmp page contains the parameters for setting the sending of notification emails to System users:



The meaning of each parameter is shown in the following table:

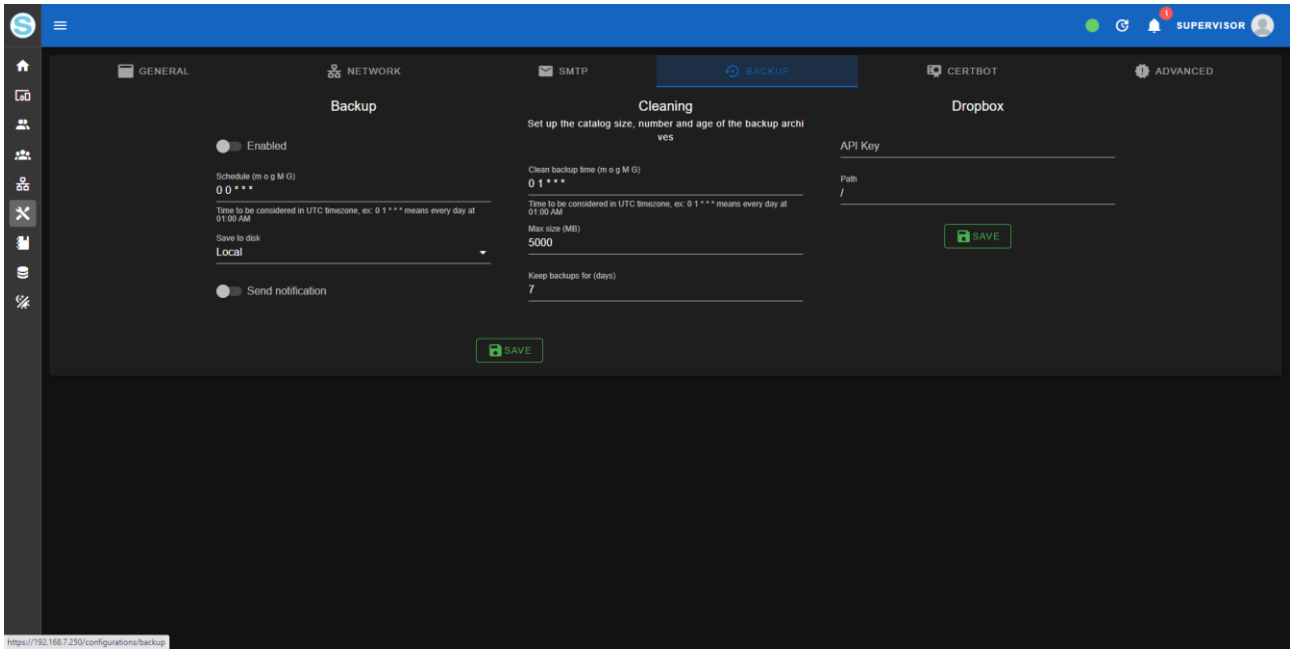
Parameter	**Meaning**
Server	To use this function, you need to register with a third-party email service or have an email account with a provider that uses the SMTP or SMTPS protocol for sending emails.
Port	Port used by the provider's mail server.
Security	Level of security used for communication with the mail server, possible values: NONE, SSL, TLS.

Name	Username of the account created with the provider. Tip: in many cases it coincides with the Username. In any case, refer to the technical support documentation available on the email provider's website.
Address	Email address of the account created with the provider. It will be the sender of all Emails sent by the VPN BOX2 server to the user.
Username	Username of the account created with the provider.
Password	Password of the account created with the provider.

7.9. CONFIG. BACKUP (AUTOMATICI)

This feature creates an image of the VPN Box configuration which can be saved as a local file or sent to a customer's Dropbox service for future use.

It is recommended to back up the entire configuration often so as not to lose any data:



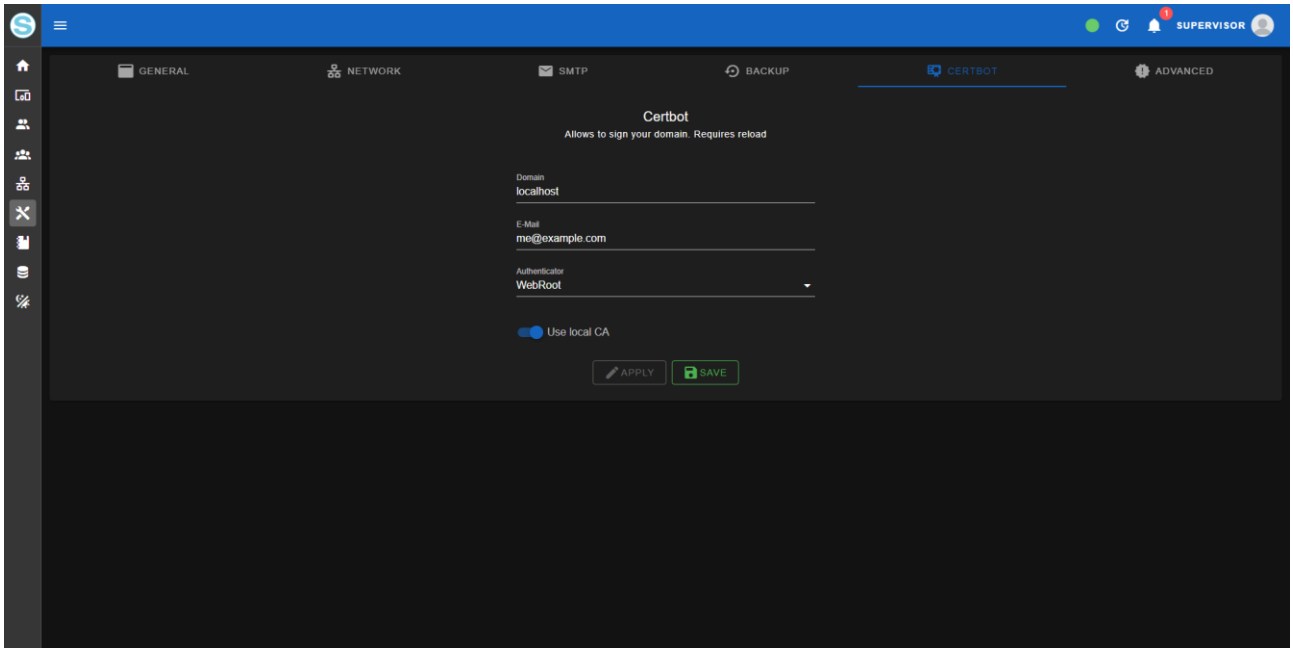
The meaning of each parameter is shown in the following table:

Parameter	**Meaning**
Backup / Enabled	Enabling of the automatic backup function
Backup / Schedule	Scheduling of the automatic start of the backup according to the format described below: * * * * * Min Hour Day of the month Month Day of the week
Backup / Save to disk	Indicates whether the backup should be saved to the internal memory or to the Dropbox service.
Backup / Send notification	At the end of the operation, it sends an Email to inform users with "System" privileges of the outcome of the operation.
Cleaning / Clean backup time	Scheduling of the periodic deletion of old backups. The format is the same used for the Backup / Schedule parameter.

Cleaning / Max size	Old backups will be deleted if the total memory used by the backup storage is greater than this parameter.
Cleaning / Keep backup for	Backups older than more than this parameter will be deleted.
Dropbox / API Key	To use this service, registration with the third-party Dropbox service is required. Once the account is active, to connect it to the VPN BOX2 server, it will be necessary to enter the apikey of the service in this field. For more information, consult the official website of the service: https://www.dropbox.com/home
Dropbox / Path	Through this parameter it is possible to specify the dedicated path where to save the backups

7.10. CONFIG. CERTBOT

The certbot page contains the parameters relating to the automated issue service of SSL/TLS certificates for accessing the VPN BOX2 from the browser via HTTPS:



The meaning of each parameter is shown in the following table:

Parameter	**Meaning**
Domain	Domain to be registered, must match what is written in the address bar of your browser to reach the VPN BOX2 server, e.g. vpn.acme.com
Email:	Email address of a server contact to be indicated to the CertBot Let's Encrypt provider to be contacted in case of reports relating to the use of the certificate for the indicated domain.
Authenticator	It is the verification method used by certbot to verify the authenticity of the server on which the secure certificate signed by Let's Encrypt will be loaded. After authentication, the browser will show the "secure connection" icon in the address bar
Use local CA	If set to ON, it uses invalid certificates, generated randomly. The browser from which you are accessing the server will show "Not secure" but the connection will still take place using TLS encryption. Setting Use local CA to ON will allow you to temporarily circumvent any problems relating to the authentication mechanism and obtaining valid signed certificates. To activate the Certbot operating mechanism it is necessary to set Use local CA to OFF and save the configuration.

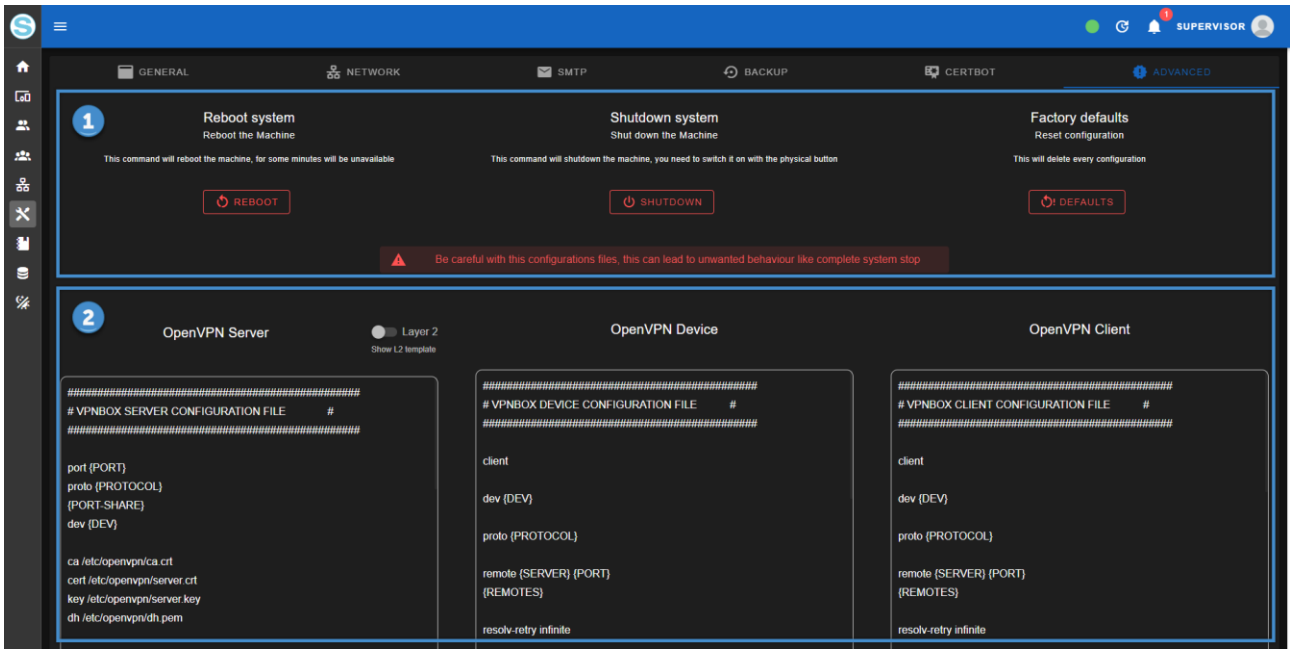
7.11. CONFIG. ADVANCED

The advanced page is divided into two sections: the upper part (1) shows the maintenance commands: System Reboot, System Shutdown and Factory Default Reset.

ATTENTION!

Before proceeding with a possible factory default reset, make sure you have a recent backup of the entire application on an external medium and NOT on the VPN BOX2 disk itself.

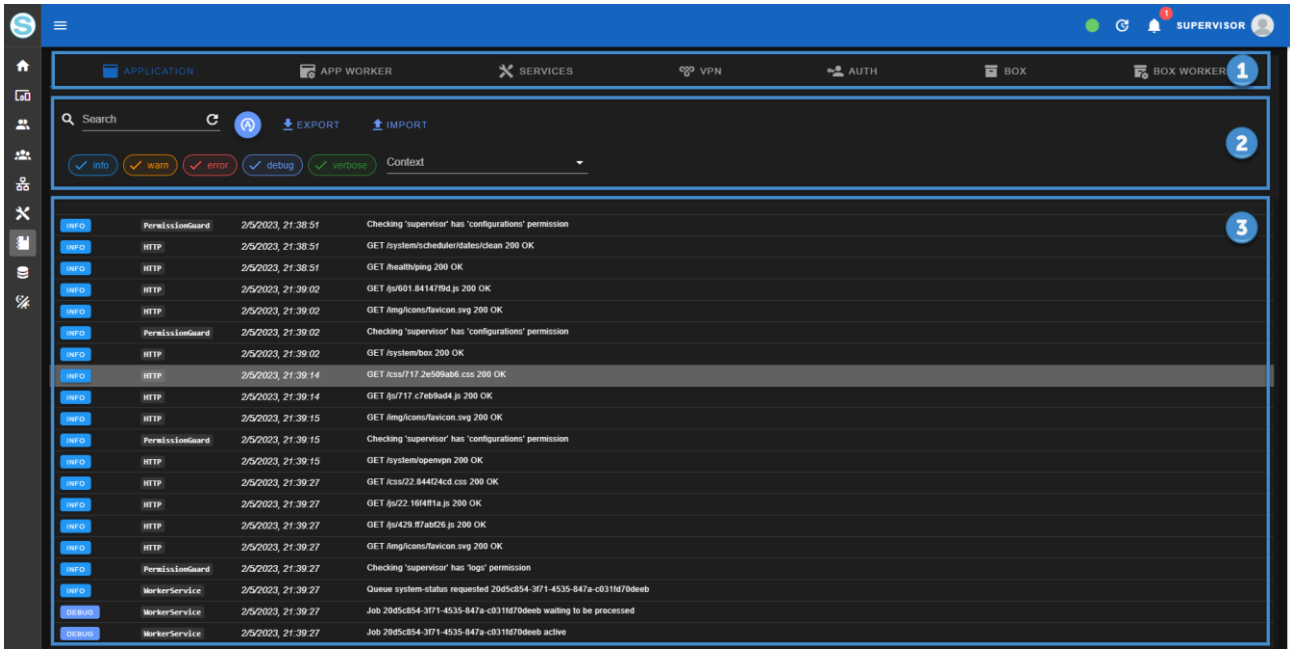
The lower part (2) contains the configurations that allow maximum flexibility in the configuration of the VPN BOX2 server but are to be used only in cases of extreme necessity. The suggested configuration templates are those that guarantee to maximize the compatibility with the devices and the stability of the communications based on both LAN/WAN and Mobile.



7.12. LOGS

The logs section is useful to check the status of the services in case of errors. It is divided by type of Services through which it is possible to browse by selecting the respective tabs (1).

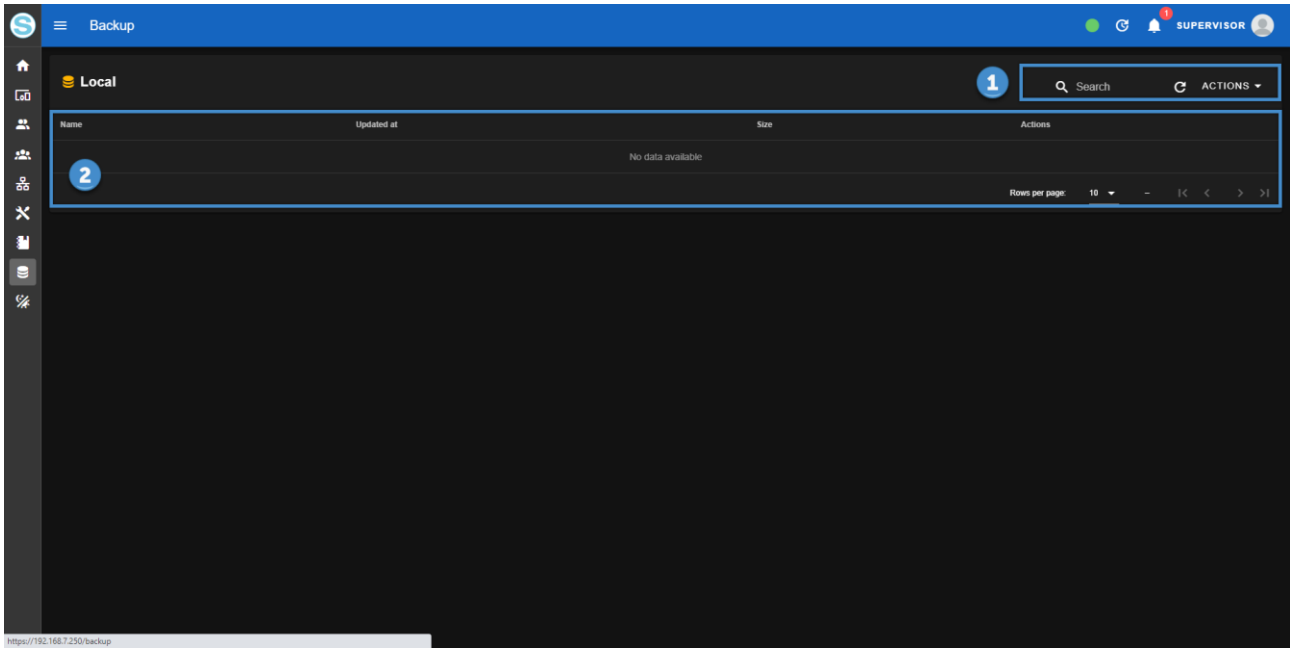
It is also possible to filter (2) the visualization by searching for a specific text or choosing the events by severity in order to obtain a less dispersive representation of the events in the content section (3).



From the current view it is possible to export the logs in CSV format.

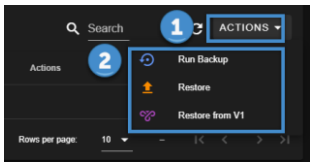
7.13. BACKUP

The backup page allows you to view all the automatic backups present in the system (2) and to perform new ones manually via the actions menu (1)



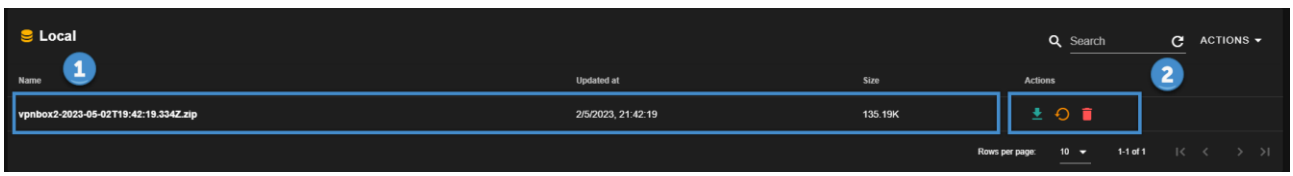
Expanding the menu (1) the possible operations (2) are:

- *Run Backup: manually start a backup which at the end will appear in the list with the others*
- *Restore: load an external backup file to restore it on the VPN BOX2 in use.*
- *Restore from V1: load a backup file of the previous VPN BOX server version and restore it with appropriate migration to the VPN BOX2 in use.*



Corresponding to each backup line, the date and time of execution and an Actions panel (2) relating to the backup itself will be recorded with which it will be possible respectively to:

- *Download the selected backup to the user's local PC*
- *Restore the selected backup*
- *Delete the selected backup*

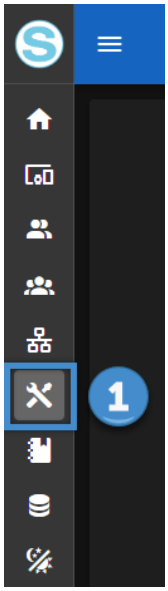


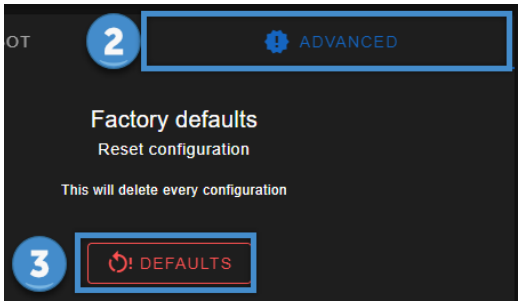
8. FACTORY RESET AND UPDATE OF THE VPN BOX2

8.1. FACTORY RESET

Restoring the factory settings is performed with a dedicated command accessible in the configuration menu section. To perform the factory reset, proceed as follows:

- *Enter the configuration menu (1)*
- *Select the "advanced" tab (2)*
- *Click on the "defaults" button (3) corresponding to the "Factory defaults" section*





8.1. VPN BOX2 UPDATE

The update of the VPN BOX2 application can be started as follows:

- *In the top bar, select the "Firmware update" icon*
- *Tick "Upload file" (1)*
- *Select the update zip file (2)*
- *Confirm by clicking on the "upload" button (3)*
- *Wait for the upload to complete and the application to restart*

9. CONFIGURATION OF THE ROUTER/FIREWALL ON THE VPN BOX2 SERVER

The network services of the VPN BOX2 are exposed on the local Ethernet interface of the server and to be accessible by remote devices and users they must be published outside the network through rules to be introduced on the perimeter firewall.

The following table lists the ports used by the various Services.

Some of these are optional as they are connected to ancillary services which can be temporarily requested and then deactivated.

It should also be noted that some, marked with (*), have a default value but via the Config. Network (VPN) page you can change the values to comply with your corporate security policies.

Port	Type	Necessary	**Input/output**	Description
443	TCP	Yes	Yes	VPN channel and, optionally, all other communications if the optional ports are closed.
1194 (*)	TCP/ UDP	Optional	Yes	VPN port dedicated to the use of the **first** VPN Network.
1195 (*)	TCP/ UDP	Optional	Yes	VPN port dedicated to the use of the **second** VPN Network.
…	…	Optional	Yes	The port configuration is dynamic to the number of simultaneous accesses requested to the server (see previous chapters).
80	TCP	Optional	Only output	Used by the Certbot service for the automatic validation procedure of the webserver's SSL/TLS certificate. It becomes mandatory only if the Certbot service is used for the VPN BOX2 server
22	TCP	Optional	Yes	If technical support is required from Seneca Service

(*) the port can be changed if necessary from the "Networks" menu if it is already used by other Services that share the same public IP as the VPN BOX2.

Initially the system will attempt to use port 443 together with ports 1194, 1195, ...

If ports 1194,1195... are closed, VPNBOX2 will only use port 443, in this case the communication overhead is higher, therefore to obtain maximum performance it is recommended to also open ports 1194, 1195, ...

These ports must be open on the router, therefore unfiltered by any firewall rule. They must then be redirected by the router, from the outside to the inside, changing the NAT and making them converge towards the local IP address of the VPN BOX: on commercial routers, this option is usually called "Virtual Server" or "Port Mapping”.

At the end of the configuration, write down the public IP address of the router, necessary (with relative password) for the VPN configuration of the SENECA devices. Refer to your system administrator on how to acquire this IP address.

Changing the router "Virtual Server" or “Port Mapping” is mandatory only if the VPN Box2 is in a LAN (addresses 192.168.x.x, 10.x.x.x and 172.x.x.x), if it is installed on a public network (therefore with a public IP address visible from the Internet) no router configuration will be required.

10. ROUTER/FIREWALL CONFIGURATION ON CLIENT PCs AND REMOTE DEVICES

The router/firewall configuration of the device or PC where the client is started must comply with the following table:

Port	Type	Necessary	**Input/output**	Description
443	TCP/ UDP	Yes	Only output	Service channel needed to communicate between device, user (VPN Client Communicator) and VPN BOX2.
1194 (*)	TCP/ UDP	Optional	Only output	VPN port dedicated to the use of the **first** VPN Network.
1195 (*)	TCP/ UDP	Optional	Only output	VPN port dedicated to the use of the **second** VPN Network.
…	…	…	Only output	The port configuration is dynamic to the number of simultaneous accesses requested to the server (see previous chapters).

*= port number modifiable by configuration

Generally in remote devices based on cellular connections (for example Z-PASS2-RT) the ports are already opened by the telephone operator of the SIM used.

Initially the client will try to use port 443 together with port 1194,...

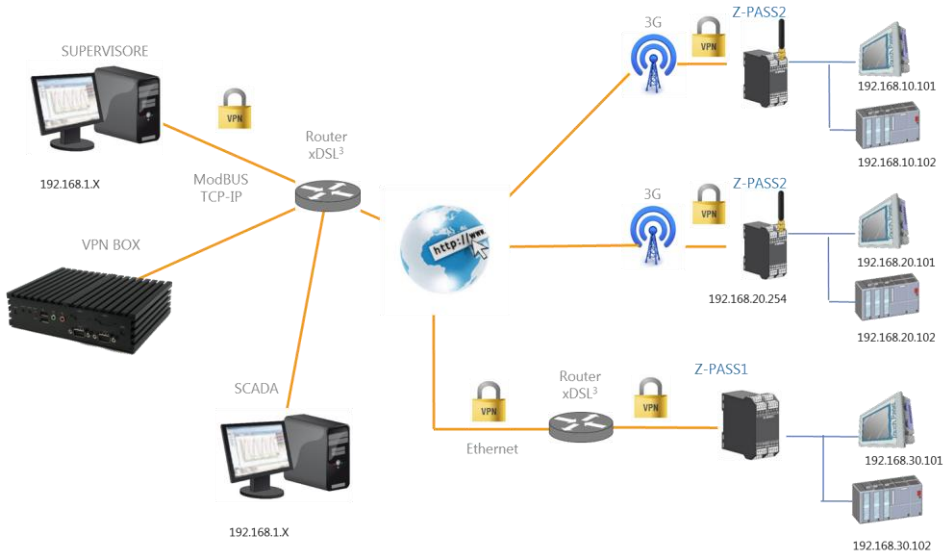
If port 1194,... is closed, the client will only use port 443, in this case the communication overhead is higher, therefore to obtain maximum performance it is recommended to also open port 1194 in output, ...

11. SINGLE LAN VPN NETWORK OPERATING PRINCIPLE (SL)

This mode allows you to create a VPN network by interconnecting two or more devices with a PC, SCADA or Mobile.

ATTENTION!

This mode configures a virtual LAN network requiring the allocation of different local IPs on all Seneca devices belonging to the network, as the VPN clients are all connected at the same time and always visible to the rest of the network. This requirement is especially necessary if you want the networks downstream of the devices to be visible.



11.1. VPN CONFIGURATION

The configuration of a Telecontrol system (Single Lan) is divided into the following operations:

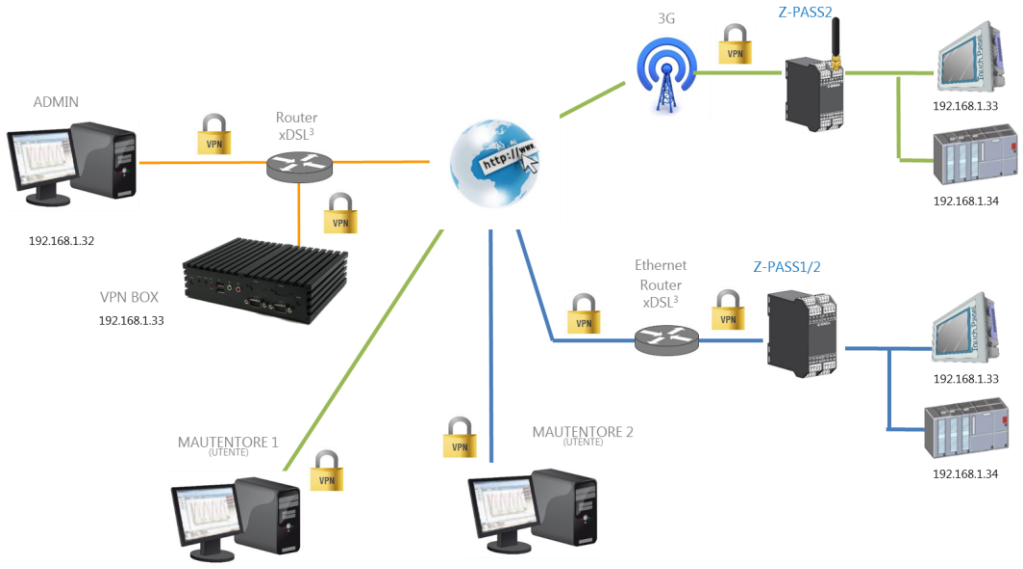
- *Creation of Single LAN group which will contain both users and devices*
- *Configuration of the Seneca devices by entering their web pages and entering the credentials to point to the VPN BOX2*
- *In the Devices menu click on the actions menu of each new device inserted (normally being new they appear in grey) click on "Setup" in the "group" property select the Single LAN group created in the first point as the group it belongs to*
- *Configure users for telecontrol system*
- *Return to the groups menu and insert the users in the Single LAN group created which will already contain the devices*

12. POINT TO POINT VPN OPERATING PRINCIPLE (P2P)

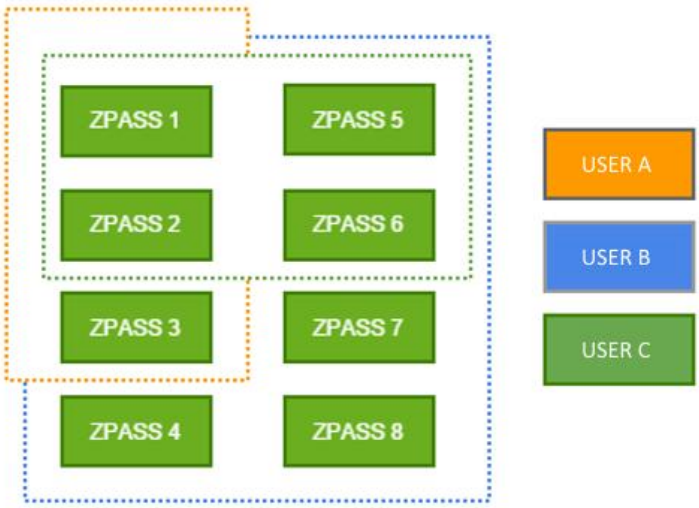
This scenario is typical when you have many sites with identical systems and networks. Since it is not possible to create a network with multiple identical IP addresses, it is necessary to create multiple networks which must be independent.

The user can choose which one to connect to to carry out remote maintenance. This mode is designed for on-demand support scenarios, it is not a connection to be used permanently as Single Lan.

It is also possible to group the devices and assign them to the users who need to connect: each user can therefore only connect to the devices assigned to him/her



The figure below shows an example of using groups. There are three users: A, B and C and a total of 8 remote devices are available to access according to the access policy shown with the colours in the figure:



To do this, it will be necessary to create in the VPN BOX2 a group and user scheme of the type shown in the following table:

Device ID	**Group ID**	**Membership of users to Groups**		
		User A	User B	User C
ZPASS 1 ZPASS 2	Group 1	X	X	X
ZPASS 3	Group 2	X	X	
ZPASS 4 ZPASS 7 ZPASS 8	Group 3		X	
ZPASS 5 ZPASS 6	Group 4		X	X

12.1. VPN CONFIGURATION

The configuration of a Remote Access system (Point to Point) consists of the following operations:

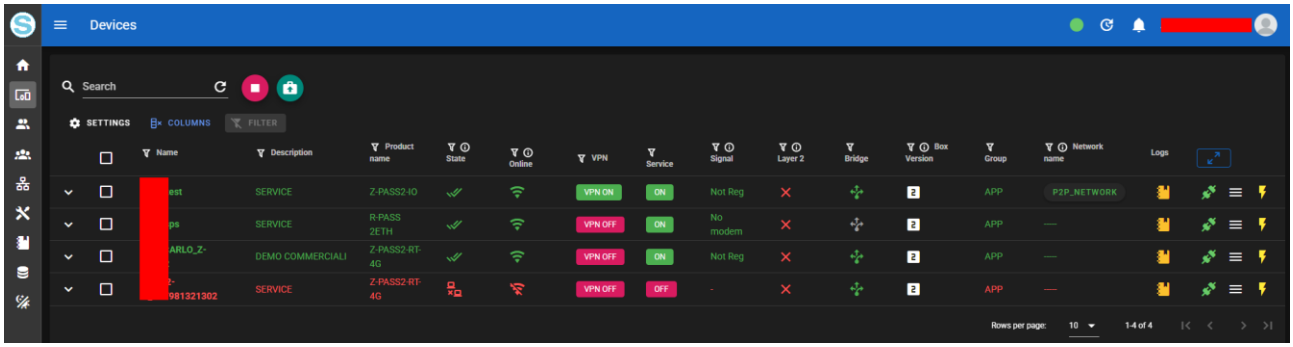
- *Creation of P2P group which will contain both users and devices*
- *Configuration of the Seneca devices by entering their web pages and entering the credentials to point to the VPN BOX2*
- *In the Devices menu click on the action menu of each new device inserted (normally being new they appear in grey) click on "Setup" in the "group" property select the P2P group created in the first point as the group it belongs to*
- *Configure users for the Remote Access system*
- *Return to the groups menu and insert the users in the created P2P group which will already contain the devices*

13. CONNECTION VIA VPN CLIENT COMMUNICATOR

This software is a VPN connection client and must be installed on the PCs you want to use to access the VPN network. It allows for two different types of use which will be covered later.

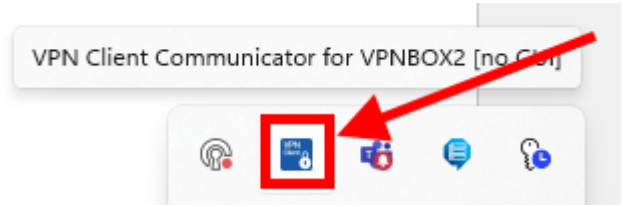
13.1. VPN CONNECTION

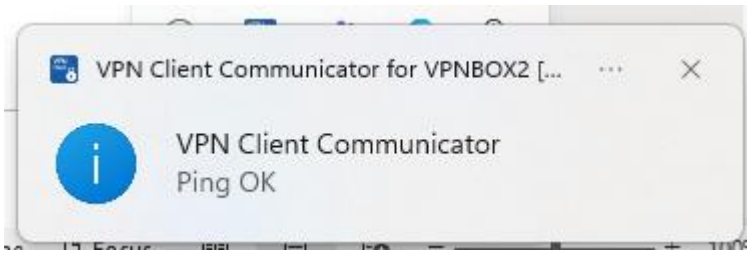
In this mode, access occurs from VPN BOX2 dashboard. Once logged in you get a tabular view of the connected Seneca devices and their status. The configured devices that are online are considered operational:



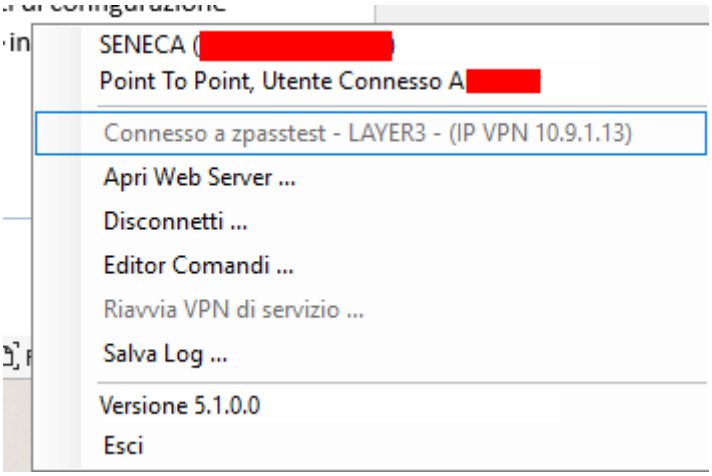
To activate VPN Connection just click of the device you want to connect to.

At this point the previously installed client communicator opens in the background on the taskbar of the Windows PC.





Context menu opens by clicking with the right button on the icon:



First three items are information related to:

- VPN BOX2 address you are connected to

- Connection mode and current user

- Remote device or network you are connected to

The other items are executable commands, for example pressing “disconnect” you get disconnection.

ATTENTION!

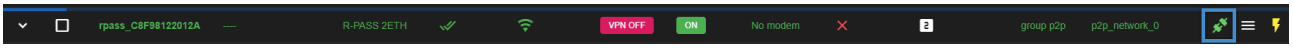
When connecting from a PC with IP addresses compatible with those of the remote VPN network, some local IP addresses may no longer be reachable while the connection is active.

13.2. DIRECT CONNECTION FROM THE BROWSER

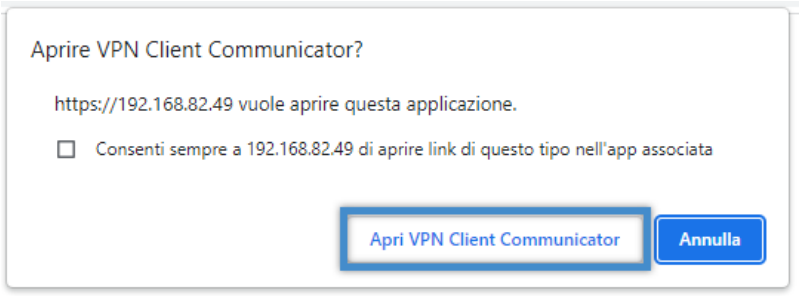
To make the user connection faster, there is a direct button on the Devices page of the VPN BOX2 which allows you to automatically launch the VPN Client Communicator application, already logged in and configured to start the connection to the selected device.

The steps to follow are:

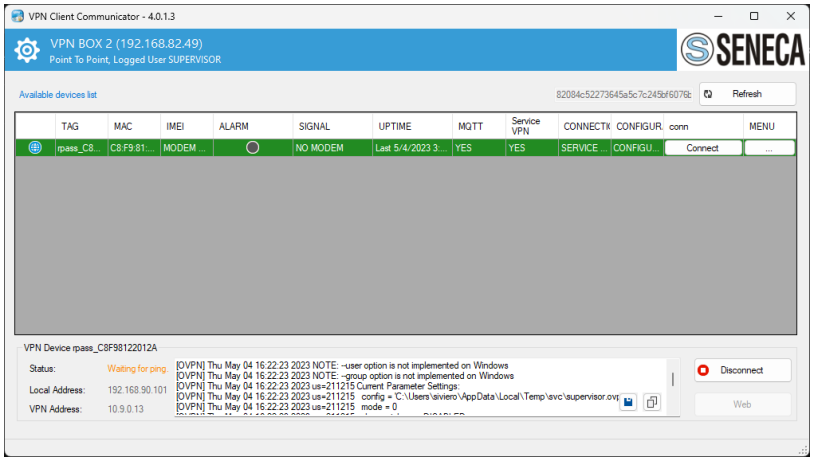
- *Identify the device to which you intend to connect to on the page and click on the quick connection key*



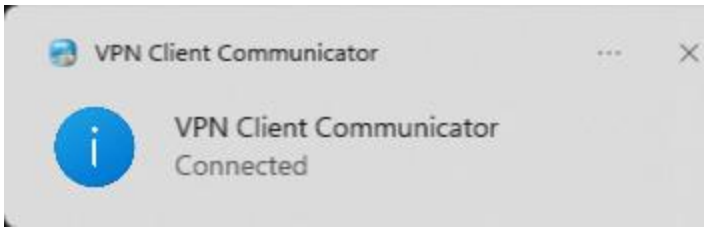
- *The browser will open a confirmation page to launch the VPN Client Communicator external application*



- *The VPN Client Communicator application will start automatically*



- *Once connected, the VPN Client Communicator will minimize itself with a notification message*



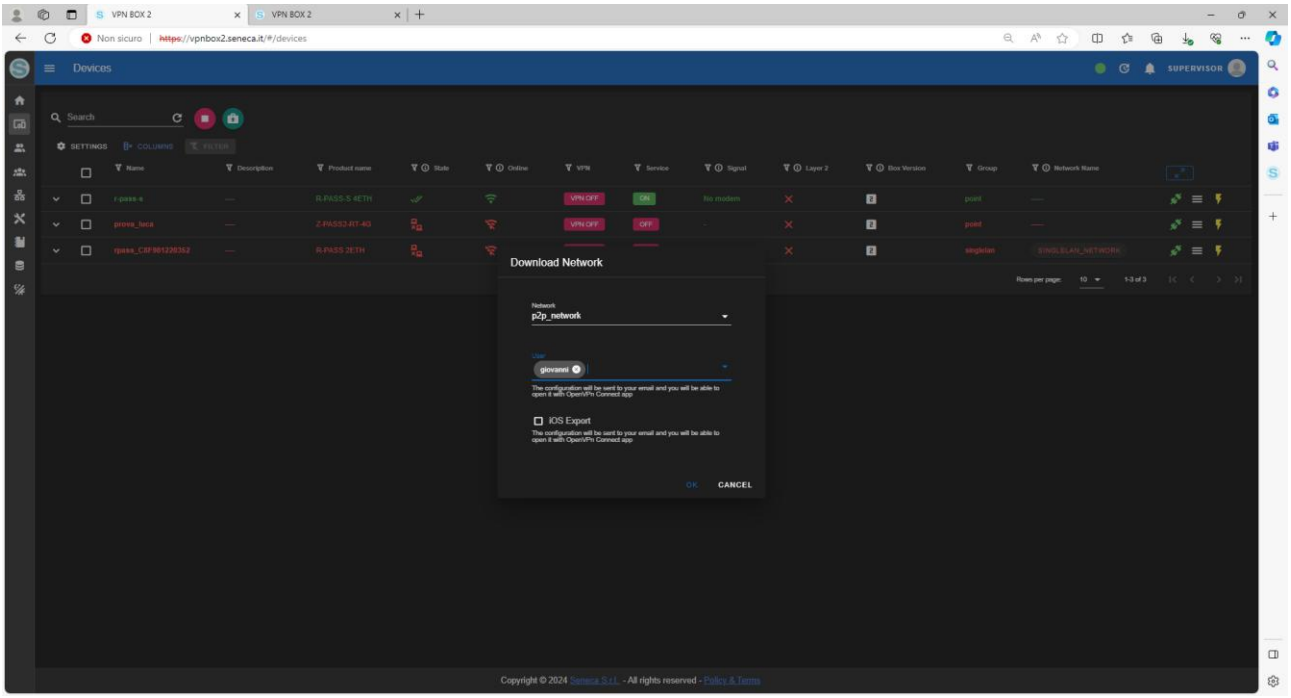
- *The browser will also show the successful vpn connection via the VPN ON flag*

14. CONNECTION VIA ANDROID OR IOS CLIENT

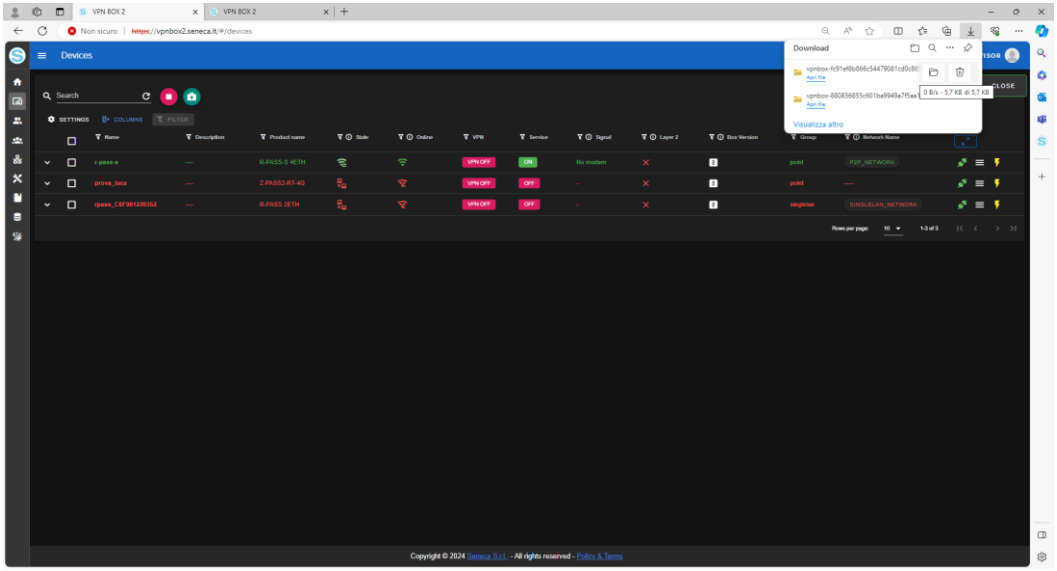
14.1. PROCEDURE FOR CONNECTION WITH ANDROID CLIENT

Important: carry out this procedure by connecting to the dashboard via ddns or public IP (external to the local network where vpnbox2 is installed). The “OpenVPN Connect” APP must be installed on the Android device.

1) ***Select “Export”-> select network and user (in case of multiple certificates on the same device always use the same network). Each device with its own network***

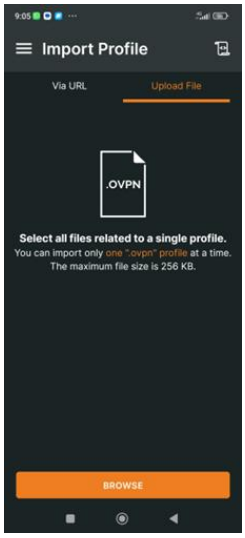


2) Download the zip file -> send it to your Android phone (for example via email)

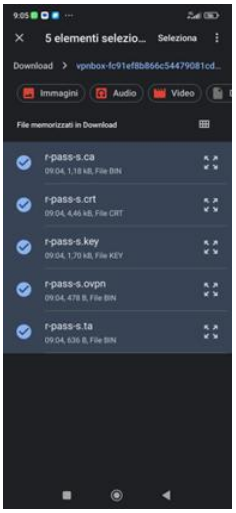


3) Import the zip file into your phone

4) Open openvpn on your android device and press upload

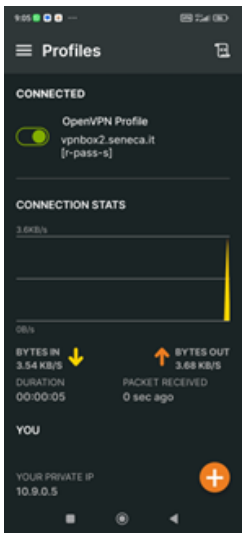


5) Select ALL certificates



6) Give ok and add the profile

7) the connection is working

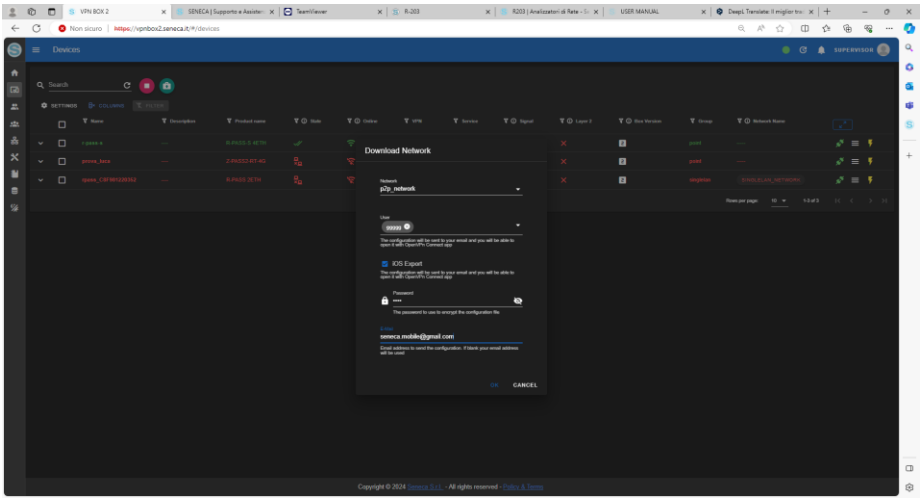


14.2. PROCEDURE FOR CONNECTION WITH IOS CLIENT

The “OpenVPN Connect” APP must be installed on the Android device.

The email sending service must be correctly configured in the SMTP section on the VPNBOX server.

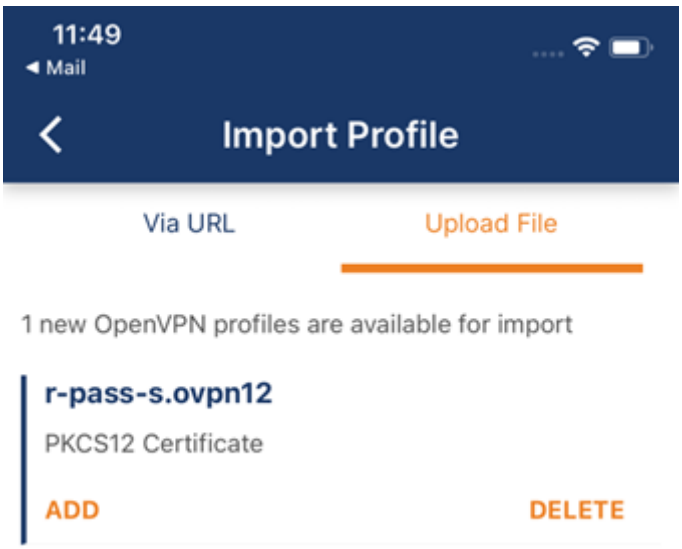
1) Select “Export”-> select network and user (in case of multiple certificates on the same device always use the same network). Each device with its own network Select IOS export and enter the password to decrypt the configuration file. Also enter the email address to which the certificates will be sent



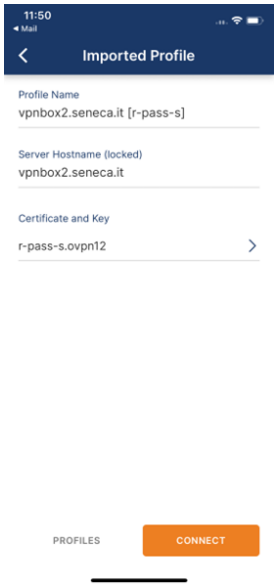
2) Open the email on the IOS device:

3) Open the .ovpn12 file with the OpenVPNCONNECT App (click on the file name and then select APP)

4) ***Add the certificate and enter the password defined during the export phase***



5) ***Open the .ovpn file and select the previously installed certificate in the "Certificate and Key" field***



6) ***Open the connection with "Connect"***

GLOSSARY

- *VPN Client Communicator*

It is the software that allows users (PC) to connect to the VPN Box via VPN.

- *PTP or P2P (Point To Point)*

This acronym is used to indicate a point-to-point connection on demand between the client PC and the remote device. This configuration is useful when there are many networks to connect to, all with the same configuration, which therefore cannot remain on the same LAN. This mode is non-permanent, i.e. it must be used for the necessary operations and then disconnected.

- *SL (Single Lan)*

Indicates the VPN Box mode called Remote Control which allows you to create a single virtual network between the devices and the connection clients. It is designed for monitoring systems like SCADA, where the connection is stable. In this mode the devices cannot have identical network configurations.

- *NAT (Network Address Translation)*

In the context of computer networks, network address translation is a mechanism that allows you to change the IP address of packets in transit through network devices - such as routers or firewalls. It is used to expose the Services of the VPN BOX2, which will be located in a local network headed by a firewall, to the Internet. The VPN BOX2 server will therefore be accessible from Seneca remote devices via the public IP of the firewall to which the server is directly connected.