USER MANUAL

VPN Box HW

VPN BOX Virtual Machine SW

VIRTUAL PRIVATE NETWORK SERVER

SENECA s.r.l.

Via Austria, 26 – 35127 –PADOVA – ITALY

Tel. +39.049.8705355 – 8705359 Fax. +39.049.8706287

Web site: www.seneca.it

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

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

This document is the property of SENECA srl. Duplication and reproduction are forbidden, if not authorized. The contents of the present documentation refer to products and technologies described in it. All technical data contained in the document may be modified without prior notice The content of this documentation is subject to periodical revision.

To use the product safely and effectively, read the following instructions carefully before use. The product must be used only for the use for which it was designed and built. Any other use will be the user's responsibility. The installation, implementation and set-up are allowed only for authorized operators; these must be physically and intellectually suitable people. Set-up must be performed only after a correct installation and the user must perform every operation described in the installation manual carefully. Seneca will not be liable for any failure, breakdown or accident caused by ignorance or failure to apply the stated requirements. Seneca will not be liable for any unauthorized changes. Seneca reserves the right to modify the device, for any commercial or construction requirements, without the obligation to promptly update the reference manuals.

No liability for the contents of this document can be accepted. Use the concepts, examples and other content at your own risk. There may be errors and inaccuracies in this document, that may of course be damaging to your system. Proceed with caution, and although this is highly unlikely, the author(s) do not take any responsibility for that. Technical features subject to change without notice.

MI004180_102

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Date	Revision	Notes
24/11/2015	01	First revision.
12/04/2017	102	Added VM Ware Virtual Machine Appliance

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Contents

1. SOFTWARE OPEN SOURCE 6

2. INTRODUCTION 6

2.1. Hardware Specifications 6

2.2. Virtual Machine Specifications 7

3. VPN BOX INSTALLATION 7

3.1. VPN Box Hardware 7

3.2. Virtual VPN Box 8

4. DEFAULT NETWORK CONFIGURATION 9

5. FIRST CONFIGURATION WITH VPN BOX MANAGER 10

5.1. General Parameters 11

5.2. Network Setup 12

5.3. Credentials 13

5.4. Configuration Application 14

5.5. Monitoring the Operation 14

5.5.1. Configure 15

5.5.2. Backup 15

5.5.3. Restore 15

5.5.4. System Log 16

6. FACTORY RESET AND FIRMWARE UPDATE 16

6.1. VPN Box Hardware 16

6.2. Virtual VPN Box 23

7. SINGLE LAN 23

7.1. Router Configuration 24

7.2. VPN Configuration 24

7.2.1. SENECA Device Configuration 24

7.2.2. VPN Accesses 26

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

8. POINT TO POINT 27

8.1. Router Configuration 28

8.2. VPN Configuration 29

8.2.1. SENECA Device Configuration 29

8.2.1. Group Configuration 30

8.2.2. VPN Access Configuration 31

8.3. VPN Client Communicator 31

9. CONNECTION TO THE VPN NETWORK WITH VPN CLIENT COMMUNICATOR ... 32

9.1. VPN Client Connection 32

9.2. VPN Client Communicator in Service Mode 33

10. CONNECTION VIA ANDROID CLIENT (MOBILE AND/OR TABLET) 34

11. GLOSSARY 36

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Seneca VPN-BOX

ATTENTION!

UNDER NO CIRCUMSTANCES, WILL SENECA S.R.L. OR ITS SUPPLIERS BE RESPONSIBLE FOR ANY LOSS OF RECORDING DATA/INCOME OR FOR* CONSEQUENTIAL OR INCIDENTAL DAMAGE DUE TO NEGLIGENCE OR RECKLESS MISHANDLING *OF THE VPN-BOX, EVEN THOUGH SENECA IS WELL AWARE OF THESE POSSIBLE DAMAGES.

SENECA, ITS SUBSIDIARIES, AFFILIATES, COMPANIES OF THE GROUP, SUPPLIERS AND RETAILERS WILL NOT GUARANTEE THAT THE FUNCTIONS COMPLETELY SATISFY CUSTOMERS' EXPECTATIONS OR THAT THE VPN-BOX, THE FIRMWARE AND THE SOFTWARE HAS NO ERRORS OR WORKS CONTINUOUSLY.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

1. Software Open Source

The VPN Box software and firmware contain Open Source software under GPL license. In compliance with section 3b of GPL, we provide the sources of this software. It is possible to get them from SENECA s.r.l. asking for them via email to support@seneca.it.

2. Introduction

VPN Box is a server device that allows centralizing the management and connection of the SENECA devices enabled to use a VPN.

In a company's (suitably configured) LAN network, the field remote equipment can connect among themselves or to a PC (via Ethernet or 3G modem) and communicate using TCP/IP protocols. With this device it is possible to organize a VPN Single Lan (or Remote Control) or Point to Point (or Remote Service) network.

The Single LAN method solves the cases where it is necessary to create a connection allowing the communication between devices installed in different sites and far from each other, so as to form one network that can include, if so wished, also the device sub-networks; these cases are typical in SCADA and Remote control environments.

The Point to Point method allows a maintenance technician to reach a single device and, optionally, its sub-network to work on it; the typical use is field remote Service of machines and reprogramming of a PLC/HMI, verification of some functions and problem solving.

The VPN Box is a server device that needs to be configured by a software provided with: VPN Box Manager;

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

2.1. Hardware Specifications

Type of device	Industrial server
Motherboard Form Factor	Mini-ITX
Cooling	Passive (fanless)
Front I/O	2 x USB 2.0
Back I/O	2 high current USB 2.0 2 USB 2.0 1 VGA 1 HDMI 1 Gb LAN 1 Jack DC (8 V to 19 V)
Processor	Intel Atom N2800
Processor speed	1.86 GHz

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Socket	Onboard (BGA)
Number of cores	2
Chipset	Intel NM10
Type of memory	DDR3 SO-DIMM (non-ECC)
Amount of memory	2 GB 1066MHz
LAN Controller	Intel 82579L GbE
Supply voltage	8~19 V
Supply connector	Jack DC Onboard
Operating temperature	0°C ~ 40°C
Dimensions (WxHxD)	185.14 x 32 x 205 mm
Certifications	CE, FCC, RoHS
Storage	32 GB SSD Drive

2.2. Virtual Machine Specifications

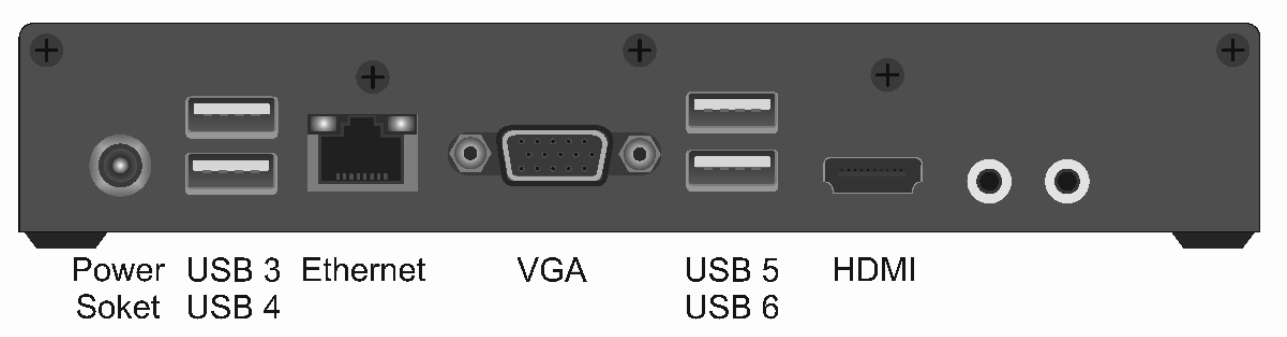
The virtual machine is supplied in OVF (see VM installation chapter) and has no specific hardware characteristics. It needs to work on an ATOM processor of at least 64 bit and 1Gb of RAM; the operating system is Debian and therefore the host must be compatible with this LINUX distribution.

3. VPN Box Installation

3.1. VPN Box Hardware



Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



Socket

To install VPN Box, proceed as follows:

Position the server horizontally on a flat surface, or use the appropriate brackets that make it possible to fit it against the wall (included in the supply).

Connect the power supply (to the round plug on the back) and the network cable. The device needs no keyboard or mouse to operate, but these are required in case of recovery or firmware update; they can therefore be left disconnected.

Start the device with the front button: nothing else is required.

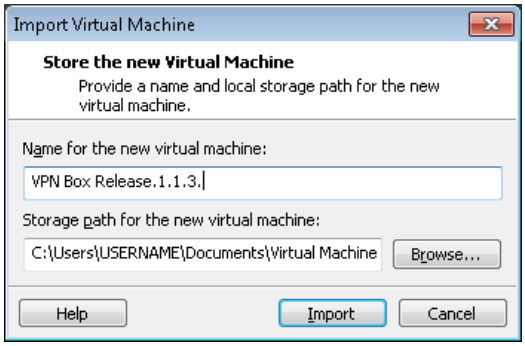
ATTENTION: this being a server, it needs to be correctly switched on and off, that is the power must not be disconnected when the server is ON. To avoid power surges and/or blackouts, we recommend a UPS is used.

The device is switched off with the front button that must be pressed only once, briefly; the prolonged pressure of this button switches the unit off immediately giving the operating system no time to close the various processes.

3.2. Virtual VPN Box

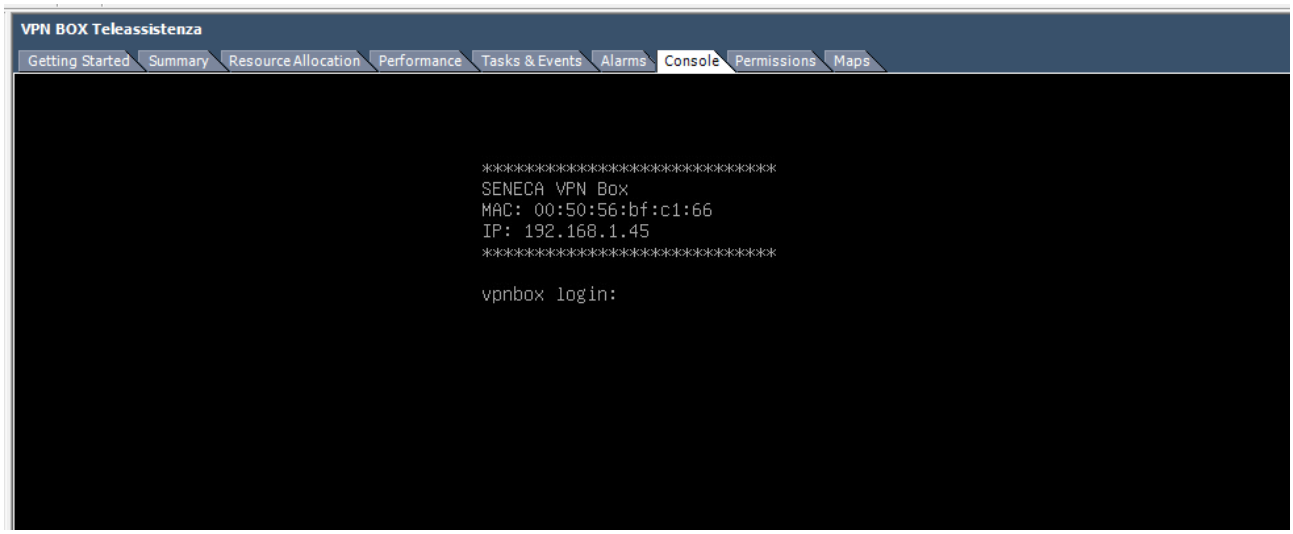
In this case, it is necessary to install the packet provided as virtual machine, consisting of an ".ovf" file saved in OVF 1.0.

This file can be imported to a virtual host such as VMWare. To start installation, double-click on the packet this will start the installation that will take up to several minutes. You will then follow a wizard and the first screen is as shown in the figure below.



Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Once the disk have been created, start the device. On first start-up, once the Login screen is displayed, the system will create the encryption keys; this operation might take some time, wait till completed (The VM restarts and the login screen representing only a maintenance terminal is displayed again: nothing else is therefore required).



The VMWare host will detect a Guest Managed machine, VMWare tools are already installed (the package is the Debian 8.x one). Compatibility is set as follow:

ESXi: 6.0, 5.5, 5.1, 5.0 - Fusion: 8.x, 7.x, 6.x, 5.x, 4.x - Workstation: 12.0, 11.x, 10.x, 9.x, 8.x

WARNING! This virtual machine is a 64 bit virtual machine this means that the host must be compatible with Intel-VT or AMD-V technology that has to be enabled on the PC bios: this feature is implemented by the CPU.

4. Default Network Configuration

The VPN Box's default configuration is the network configuration obtained via DHCP, therefore, once connected to the network it will try and acquire an IP address, gateway and DNS via the DHCP server.

If this operation is not successful, the following network parameters are set: IP address 192.168.90.101 and subnet-mask 255.255.255.0. From a functional point of view, the VPN Box must be configured since on first start-up no mode is available to be used; if a device tries to connect to the VPN Box, it will be ignored. For the VPN Box to communicate with the outside, when behind a router, the NAT must be configured on it; for any configuration details, see the section about the server's individual operating method (Remote Service or Remote Control).

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

5. First Configuration with VPN BOX Manager

To configure the VPN, the VPN Box Manager software will be used, available for Windows 7 or higher.

This software is also available on the www.seneca.it website, in the VPN BOX section.

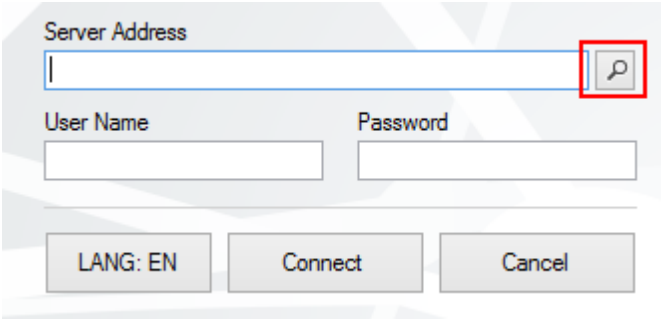
The PC you will carry out the *first configuration* from and on which the VPN Box Manager is installed, **must** be in the same LAN as the VPN Box.

Therefore, the VPN Box Manager software allows editing/modifying:

- ***Operating modes and Configuration***
- ***Device management***
- ***VPN Client accesses***

When the software starts, an access login is displayed; the first thing to do is to find out the IP address of the VPN Box for the connection.

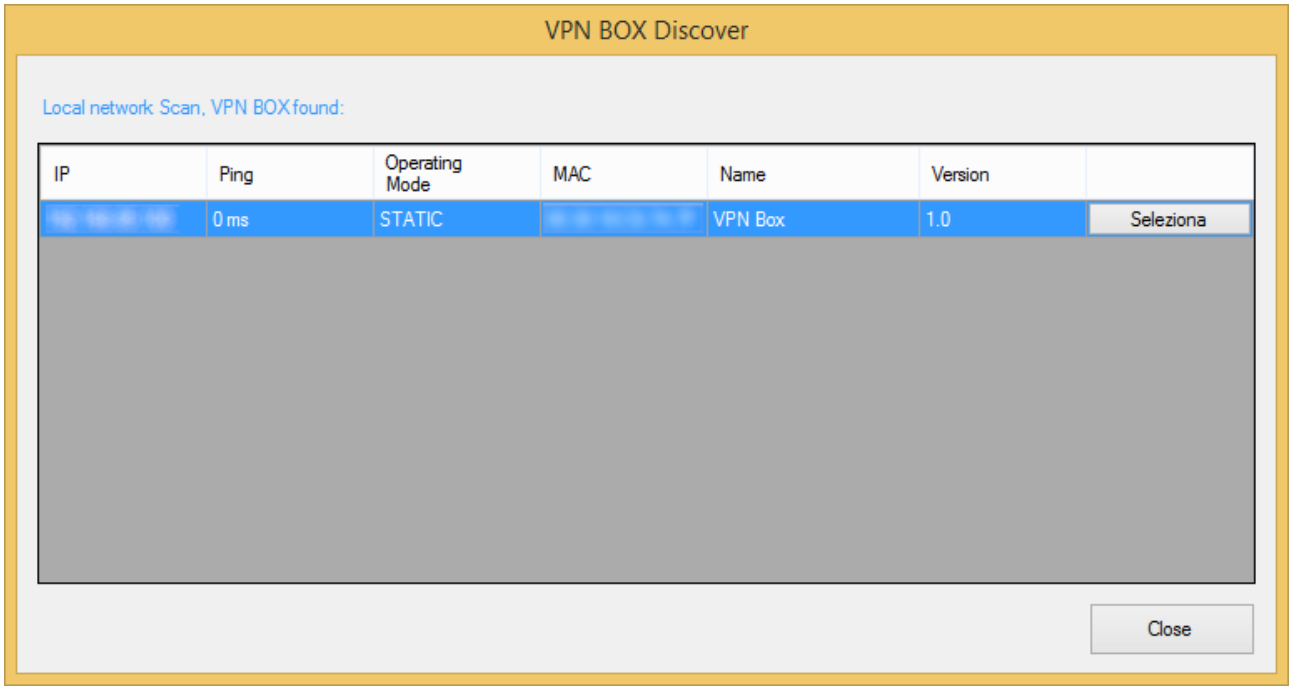
To find it, you can use the discovery system in the software that can be accessed from the login panel via the appropriate button shown in the figure:



ATTENTION! If this button is disabled, it means another process is using the UDP 49161 port. You must identify what application is using this port and close it down.

When the discovery system is started, the network is scanned to identify the VPN Box devices, their IP addresses and versions.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



By pressing Select the login screen will display the IP address found and selected.

ATTENTION: if the network configuration of the PC you connect from is not compatible with the VPN Box, you must add a compatible IP address from Windows network management.

When you connect for the first time, the device has default credentials (all in small letters):

USERNAME: supervisor

PASSWORD: seneca

More generally, these credentials are the same in case of a factory reset or firmware update. As soon as you log in, the device will display the configuration panel with all the parameters.

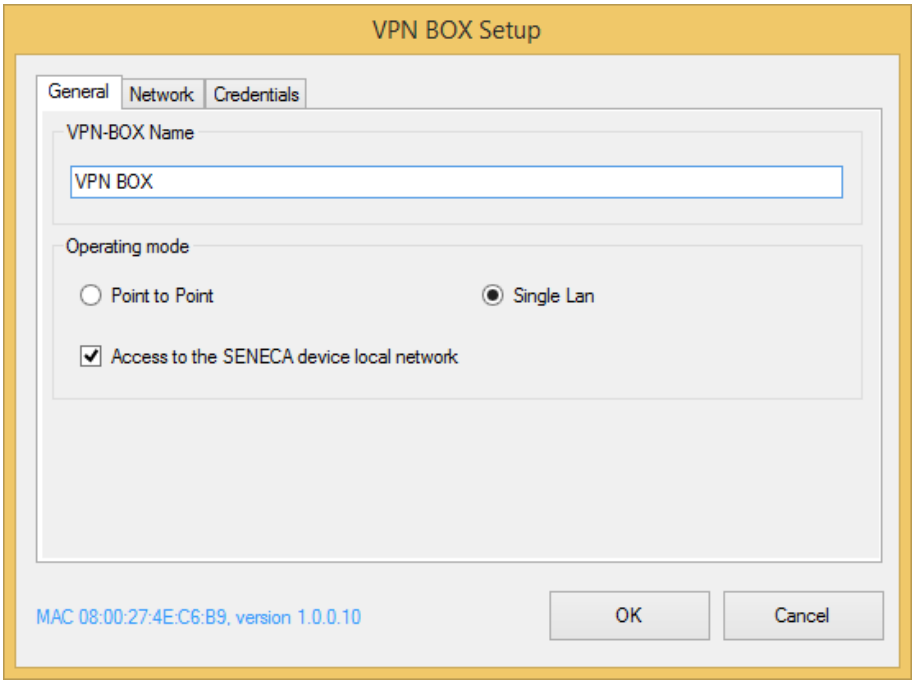
5.1. General Parameters

The section has a Name field that allows assigning a label to the VPN Box; this option is useful since the defined name will always be displayed on the VPN Box Manager and VPN Center Client softwares. The following option defines the operating mode, that is

Point to Point (also called Remote Service) or **Single Lan (called Remote Control as well).**

ATTENTION: the mode can be modified only during the first configuration, after that it will be possible to modify it only with a factory reset.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

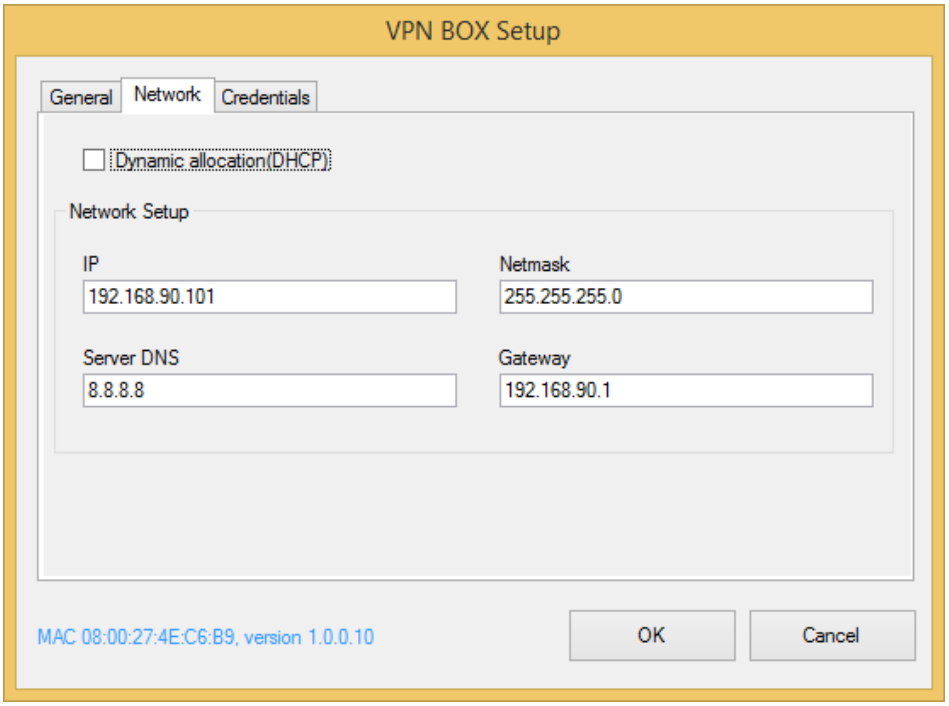


Once the mode has been selected, it is possible to check/uncheck the "Access to local network" that allows specifying if other peripherals connected to the Seneca device via Ethernet must be visible remotely to the other devices (in Single Lan Mode) or PC Clients (in both Single Lan and Point to Point modes).

5.2. Network Setup

The following window shows the classical network settings of an Ethernet-based device that can be static or dynamic through the aid of the DCHP.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



ATTENTION! On first installation it is ***highly recommended*** to provide VPN BOX with a static IP address

5.3. Credentials

In the last screen the default password for both the supervisor account and for all the Seneca devices can be modified.

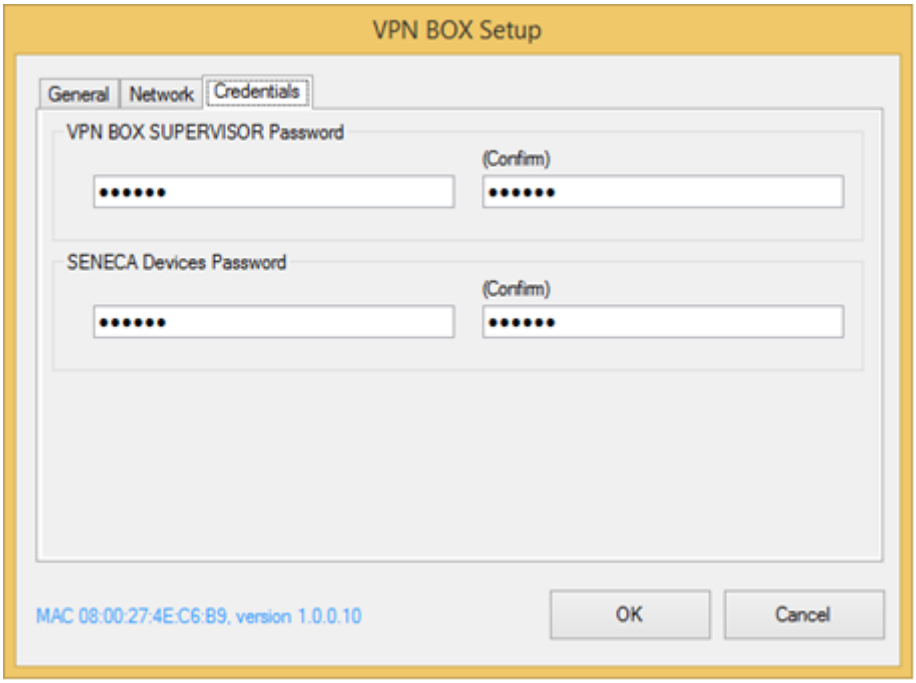
The password of the devices is necessary for the VPN configuration (i.e. Z-TWS4/Z-PASS1/2) of the devices to be registered on the VPN Box to create a network, it must coincide with the one set up on the devices.

The supervisor's default password is "seneca".

The default password of the devices is "seneca".

Take care so that the user name for the supervisor account remains always the same, that is "supervisor".

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



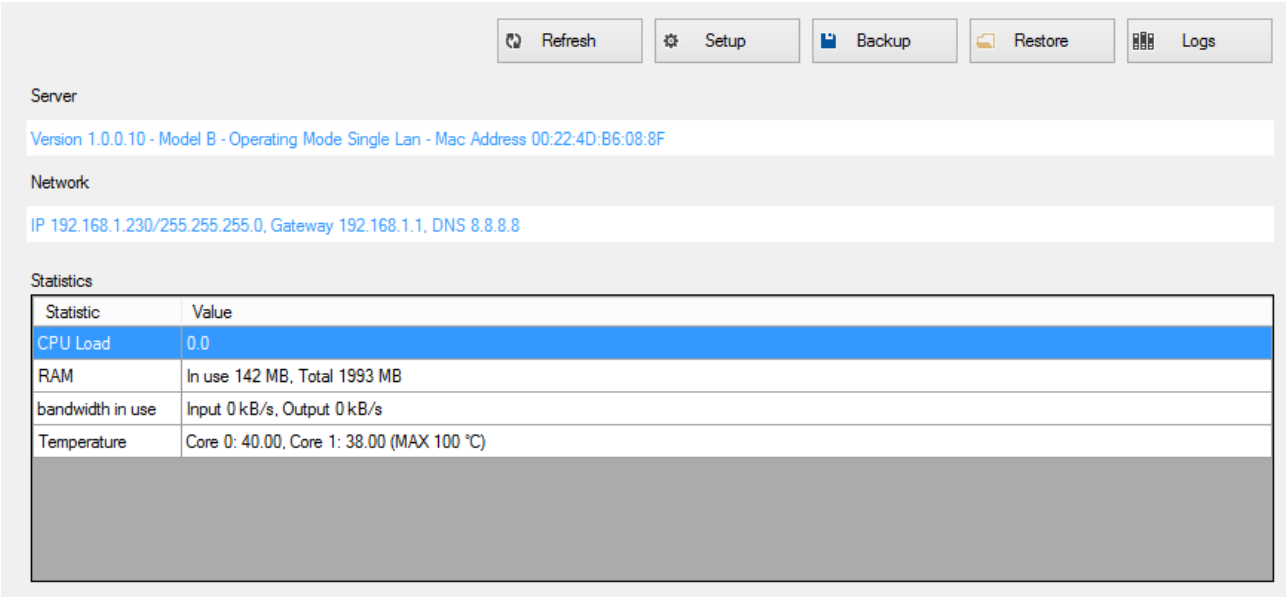
5.4. Configuration Application

When OK is pressed, the program will configure all the parameters, to do this it must restart the VPN BOX, so wait for a few minutes before reconnecting. Once the modifications are applied, the software will log out automatically.

5.5. Monitoring the Operation

This section is common to all operating modes and allows managing the device and its configuration. The central section, that can be updated with the "Refresh" button at the top, is a status panel showing the version, VPN Box model, selected operating mode; it is important to have the machine MAC address available so as to identify the devices. Immediately underneath there is the network configuration, showing what has been previously defined.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



The grid contains the status data reflecting the operation at that very moment and these are updated every minute by the machine. The first one is the CPU load, that is what the system is processing: it is a number starting from zero, that is no processing taking place, and reaching 1 or more. Between 0 and 1 the machine is within its operational limit, higher numbers mean unsuitable work loads that the machine might, sooner or later, no longer be able to process and that might cause a block; we recommend the load is kept below 0.8.

Then the following is displayed: the status of the whole memory and of the memory used by both the operating system and the services. The band shows how much the network card is working while the temperature displays the values detected by the CPU and chipset sensors.

5.5.1. Configure

This section reopens the VPN Box configuration that can be totally modified but for the mode and visibility of the device local network.

5.5.2. Backup

This function creates an image of the VPN Box configuration that can be registered as a local file, for future use. We recommend you often back up the whole configuration so as not to lose any data.

5.5.3. Restore

Restoring the Configuration data takes place by selecting the file previously created by the backup. Restoring carries out a complete rollback that needs however time to be received by the devices registered on the VPN Box. A complete reset, covering also the devices, requires a few minutes (according to the connection speed). This to allow each device to reload all the credentials.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

5.5.4. System Log

The logging window is useful to check the status of the services in case of errors. It is divided into system (SYSLOG) and application logs. The first one shows the status of the VPN services while the second one filters only the application part of the VPN Box. Both are useful only to check any errors or malfunctions. Please remember that VPN Box keeps these logs only for the current day and then deletes them.

6. Factory Reset and Firmware Update

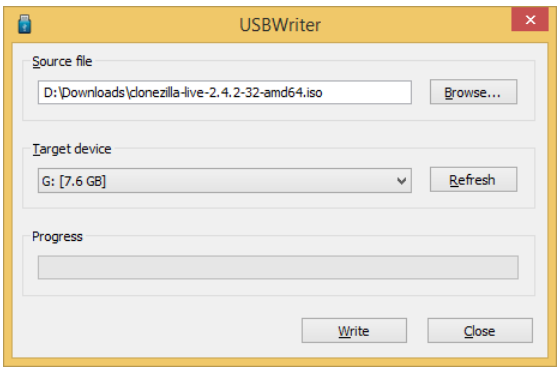
6.1. VPN Box Hardware

The factory reset and firmware update are carried out the same way, that is by resetting a factory image. In both cases, do a configuration backup first to be used for the reset. To perform these operations, the following material is required:

- ***USB keyboard and Monitor with HDMI socket (ATTENTION!! The monitor must support HD 1920 x 1080 resolutions and 72Hz refresh frequencies at least)***
- ***1 x 2Gb (at least) USB stick for the UPDATE software***
- ***1 x 2Gb (at least) USB stick for the firmware***

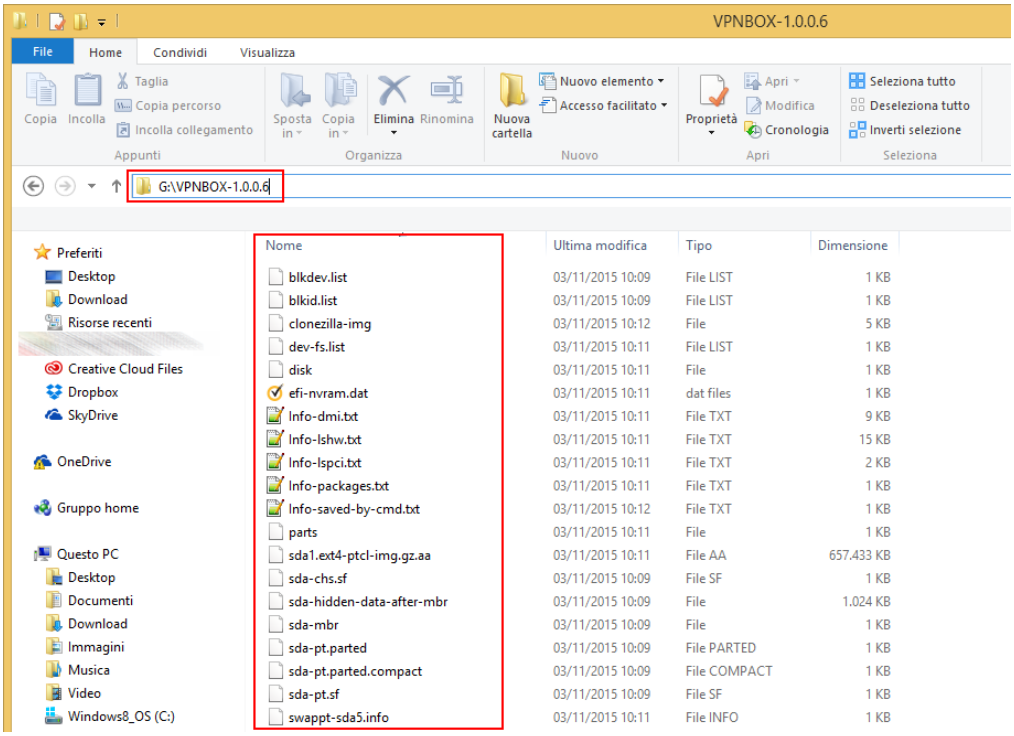
We recommend you connect to VPN Box Manager first and carry out a backup, since the procedure will clear the whole disk, configuration data included. The software required for the update is Clonezilla and can be downloaded from http://clonezilla.org/downloads.php, paying attention to download the Debian version in ISO 64bit format. To prepare the first USB stick with the Clonezilla reset program, download the program used to create the stick http://sourceforge.net/projects/usbwriter/. Now insert the USB stick, the previously downloaded USBWriter program opens, select the ISO image and the unit the stick is connected to.

ATTENTION! All the data on the stick will be deleted.

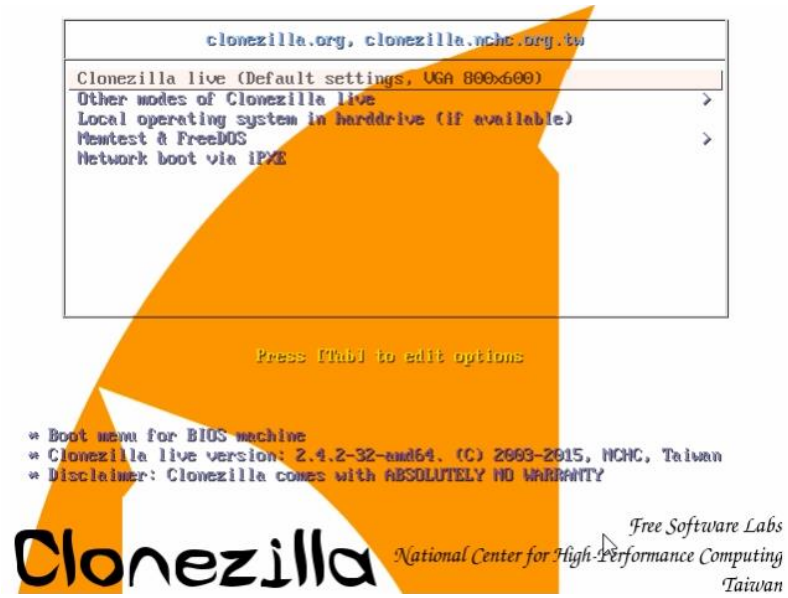


When writing is complete, close the program, disconnect the Clonezilla stick and insert the second stick. The firmware must be saved on this stick and it can be obtained from the Seneca site or server. The firmware packet must be unpacked in root, where there must be just one folder containing a series of files as per the following figure: ATTENTION! The folder must not be renamed and there must be no spaces in its name, it must be of the VPNBOX-1.0.0.6 type. Once the second stick is disconnected you are ready to reset.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

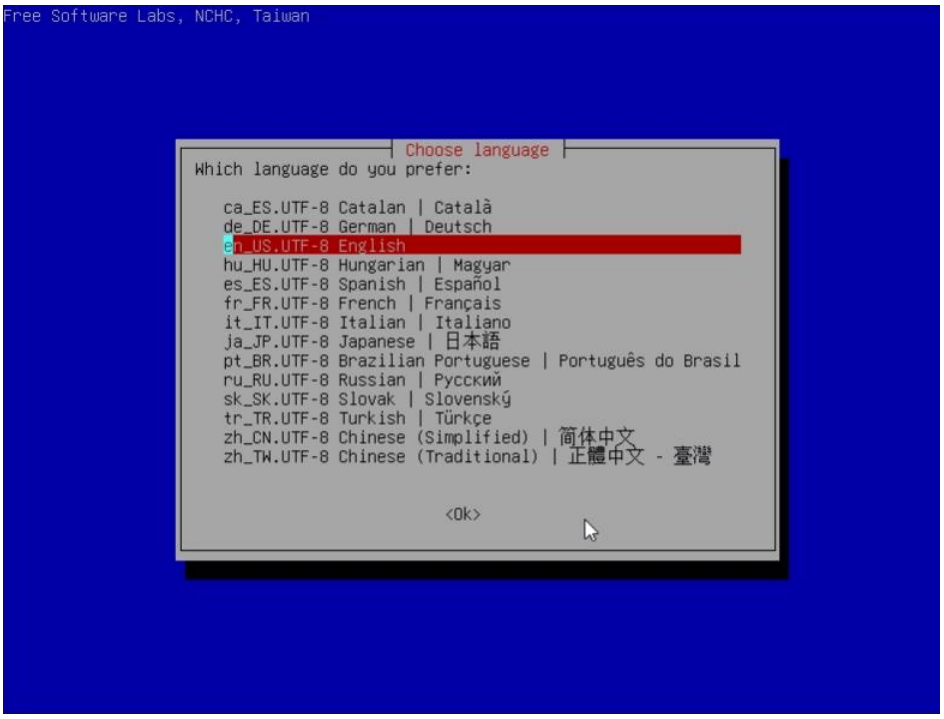


Connect the VPN Box to a monitor and to a keyboard and insert the first stick with the Clonezilla reset program into the front left port. Start the VPN Box and wait for the stick to boot, a selection screen shall be displayed, select **“Clonezilla live (default settings , VGA 800x600)”.**

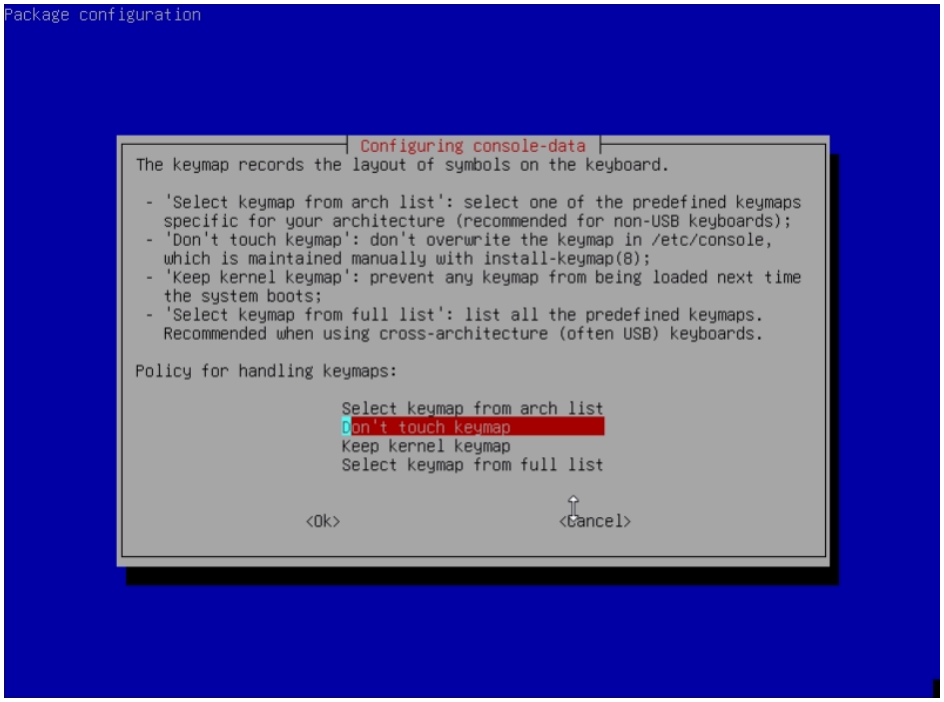


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Press Enter and wait for the operating system to boot, this might take a few minutes according to the speed of the stick used. A selection screen for the keyboard layout will be displayed first.

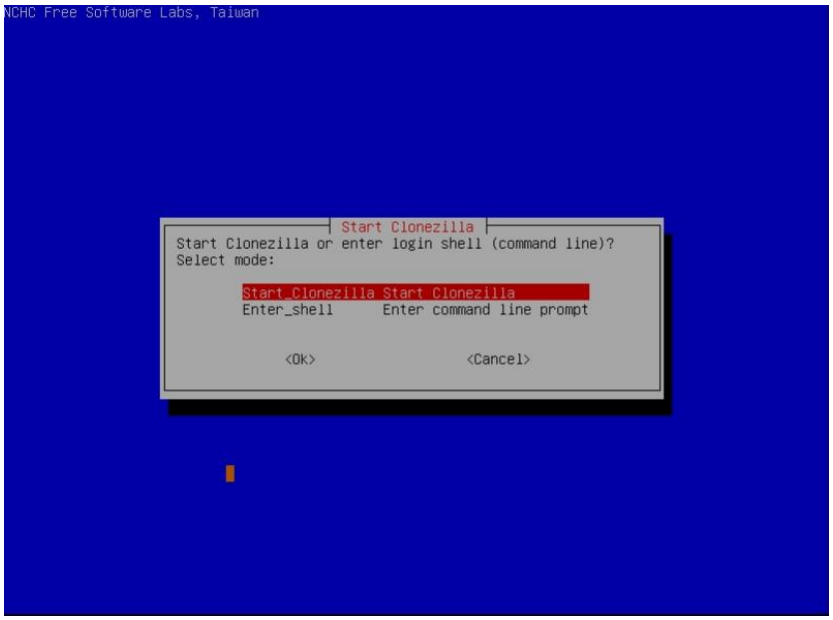


Select “en_US.UTF-8 English”, press Enter and continue with the English configuration; the system will continue asking for the keyboard to be remapped, press Enter again and continue.

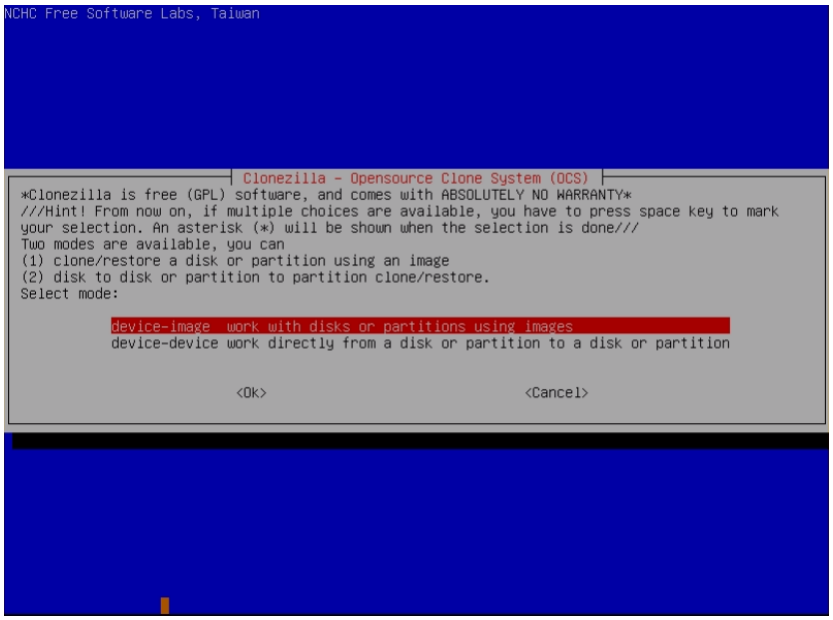


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

The system is now ready and will ask if you want to start with the wizard program or enter shell, select the first option as in the figure.

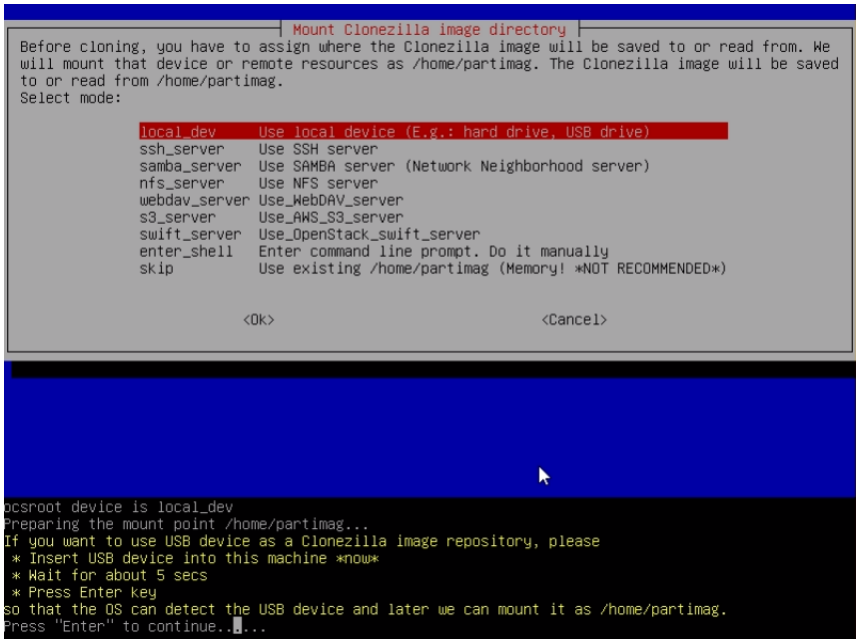


The reset is based on image, so proceed with the selection of the first item as per the following figure.

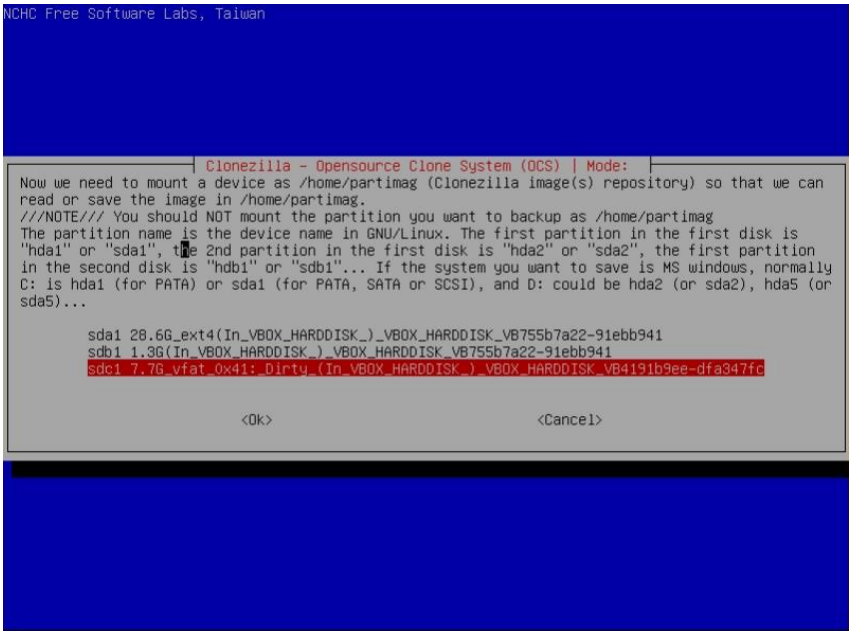


The operation carried out is a reset from local device, that is from USB peripheral, for this reason you have to select "local_dev" in the screen shown below. After pressing Enter (bottom yellow), the system will ask you to enter the peripheral you want to use for the reset. Insert the stick with the firmware into the second front right USB port, wait 5 seconds and press Enter. The connected devices will be assessed, wait for the procedure to complete.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

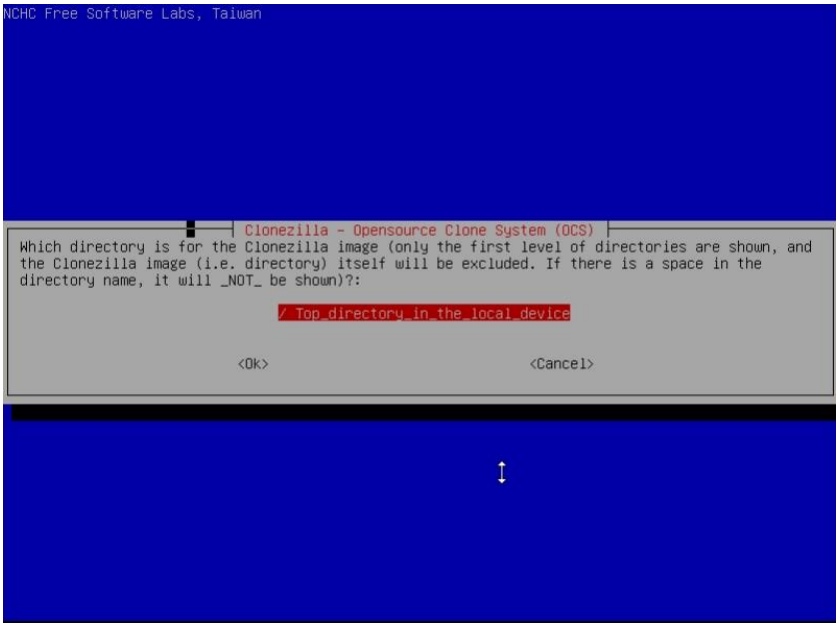


When scanning is completed, a window appears where you are asked to select the device containing the firmware. The situation should be as follows: SDA1 is the fixed disk of the VPN Box, SDB1 is the Clonezilla update program and SDC1 is the firmware. Choose the last one to carry out the reset.

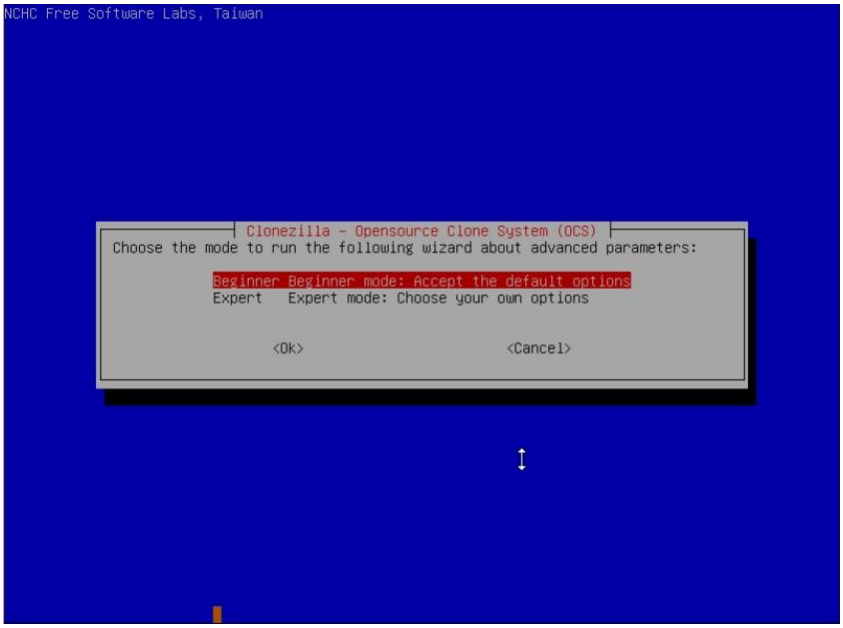


A window will then appear, as per the following picture, asking what folder must be used; since everything is in root, select “Top directory_in_the_local_device”. Once selected, press Enter and its contents will be shown, continue by pressing Enter again.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

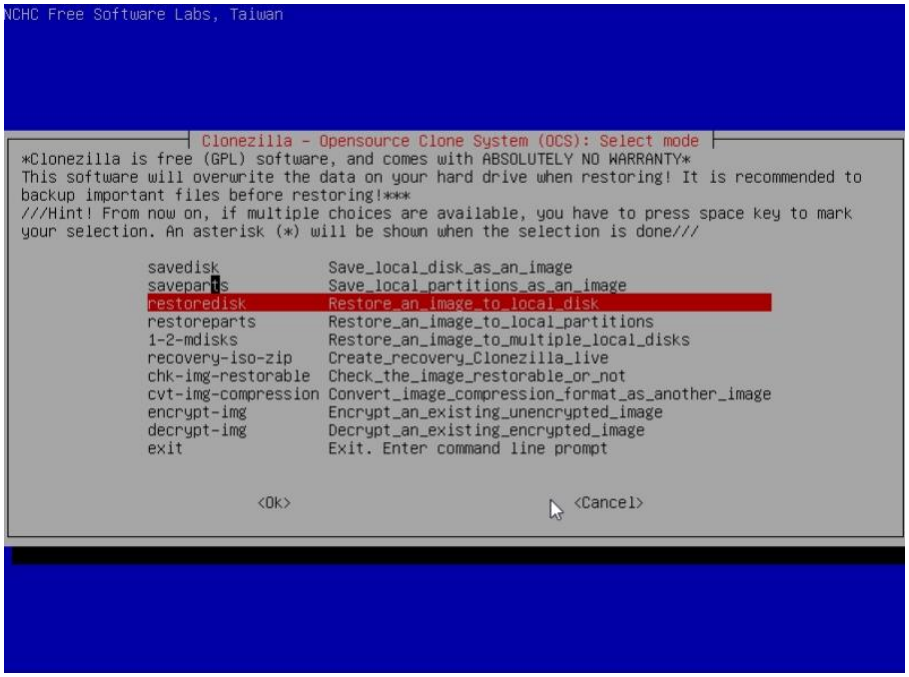


You are then asked for the level of detail of the options that, in this case, must be left as "Beginner": press Enter and continue.

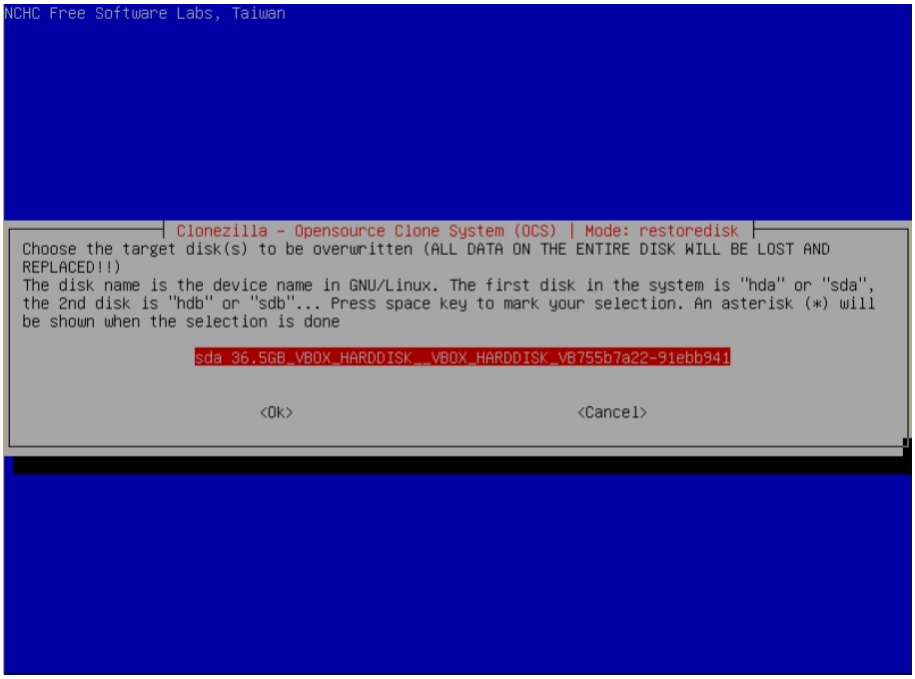


Having to reset the firmware, proceed selecting "restoredisk" followed by the unit to reset.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



The system is now ready to be reset and will ask what unit to carry it out on: the disks compatible with the restore will be displayed, as shown in the figure below; only one compatible disk should be displayed, the 32Gb system disk that is the main VPN Box disk, an SSD that should take the name SDA.



Once the disk has been selected, the procedure will start and further confirmation to proceed will be requested (by pressing y or Enter), this because this operation involves the complete loss of the previous data. At the end you will be asked how you want to proceed, select "poweroff" and then take the USB sticks out. Restart the VPN Box and wait for the machine to reboot that, once the operating system has been reloaded, will create the encryption keys: this is a long operation, so leave the VPN Box switched on until it

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

restarts automatically. *ATTENTION! The machine must not be switched off and restarted during this configuration operation.*

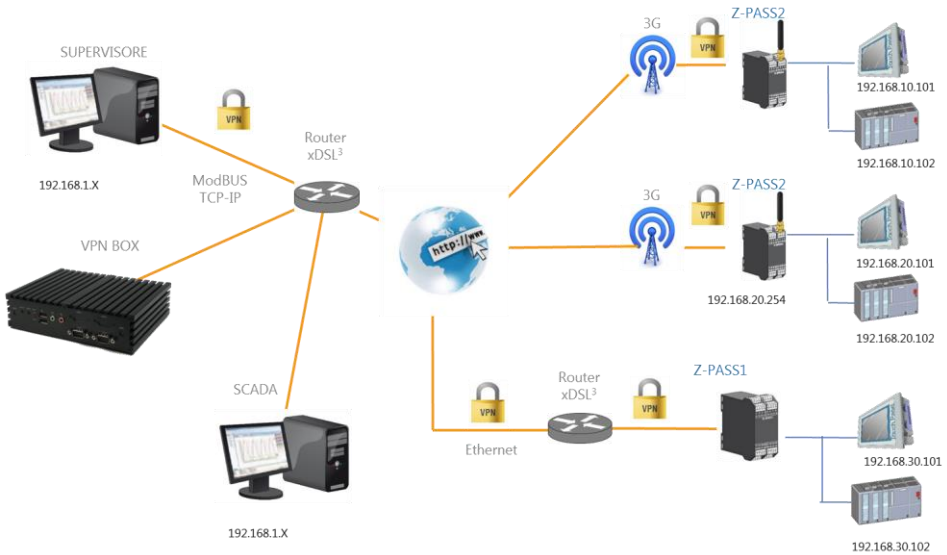
6.2. Virtual VPN Box

In the first place, back up the current VPN Box configuration. The new appliance must then be reset in the destination host machine (importing the file in OVF) and a Restore must be performed with the file created with the previous backup. Note: the reset is the same as the first installation of the Virtual VPN BOX, therefore, on first start-up, the system will calculate the encryption keys: **it must not be switched off or restarted manually**, it will restart automatically when the operation is complete. For the complete procedure, see the chapter about the first installation of the virtual machine.

7. Single Lan

This mode allows creating a VPN network interconnecting two or more devices with a PC, SCADA or Mobiles.

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



Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

7.1. Router Configuration

In this mode, VPN Box is a server and needs to expose the following ports on public network to work correctly:

Port	Type	Compulsory	Description
443	TCP	Yes	Service channel necessary to communicate with the devices and VPN clients.
1193	TCP	Optional	For possible Seneca support
1194	TCP	Yes	VPN data channel

These ports must be open on the router, therefore unfiltered by a possible firewall rule. They must then be re-directed from the router, from the outside towards the inside, modifying the NAT and making them converge towards the local IP address of the VPN BOX: on commercial routers, this option is normally called "Virtual Server" or "Port Mapping".

When the configuration is complete, make a note of the router IP public address, required (with the password) for the VPN configuration of the SENECA devices. Refer to your in-house system administrator about how to acquire this IP address. The modification of the router ports is compulsory **only** if the VPN Box 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 shall be needed.

7.2. VPN Configuration

The configuration of the Remote Control mode (Single Lan) is divided into two operations: Configuration of the *Seneca devices* and Configuration of the *VPN accesses* (Users). The former are clearly the connection points to various field systems and their configuration is dealt with in the specific user manual of every SENECA device compatible with the VPN Box.

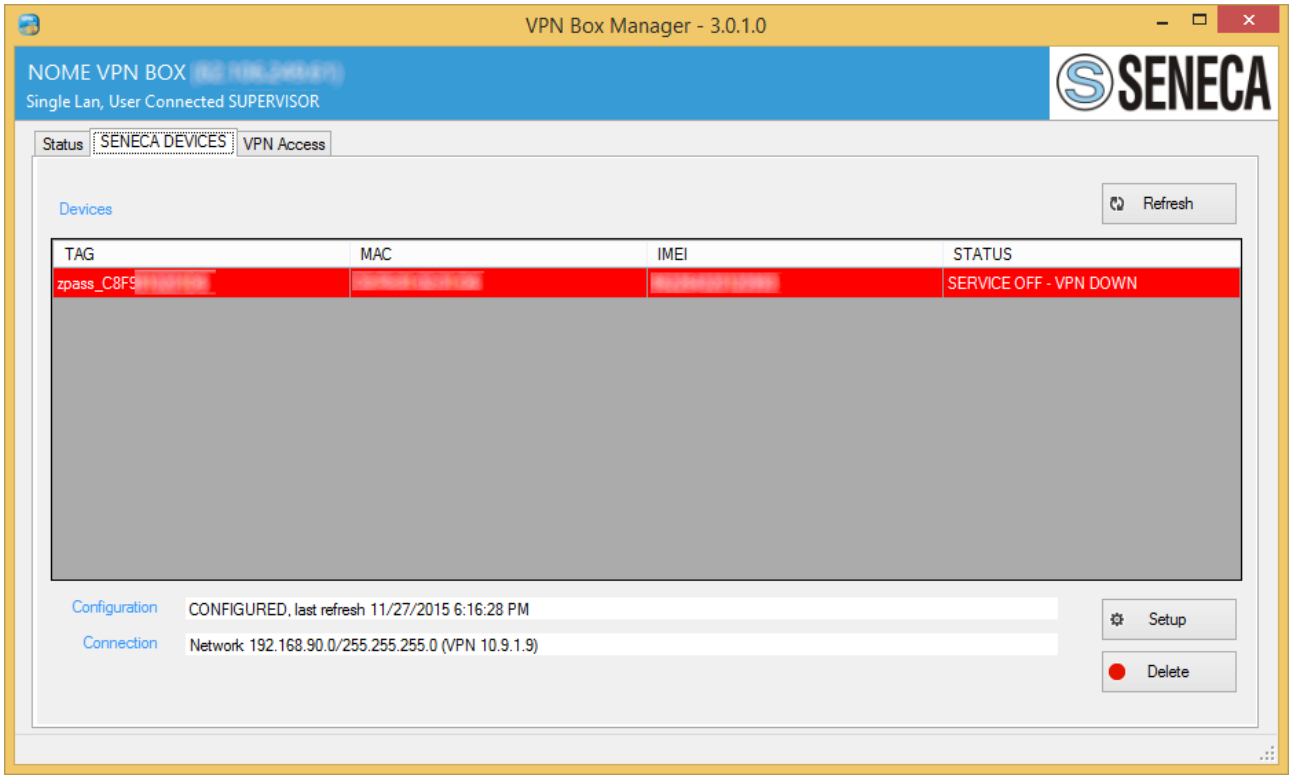
On the other hand, VPN Accesses are accounts allowing the maintenance or monitoring PCs (such as a SCADA server) to connect to the network. VPN Box Manager has a dedicated control panel for each type of operation, as shown in the figure.



7.2.1. SENECA Device Configuration

Once configured locally via their Web Server, Seneca devices will register on the VPN Box and the Device section of VPN Box Manager will start to fill up: this operation will take about 2 minutes. This time is important because each device will communicate any changes of status and receive new configurations.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



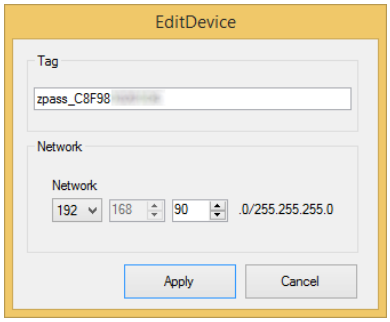
The status of the device determines its colour according to the following table, the polling offline status has priority over the machine status setting it to red.

Status	Colour
New	Orange
Configured	Green
Configuration in progress	Yellow
Service OFF	Red

Immediately after registering, the device status is "NEW" and the device itself is waiting to be configured by VPN Box Manager; in this status the device will perform no operation and will not connect to the network. While registering, the device provides various details such as its MAC address, IMEI (if provided with an integrated modem), TAG name and Local network configuration. The TAG name is the name of the installation and can be modified with the *Edit* button at the bottom so as to give it a talking name; please remember that the change of name is just an alias at VPN Box's level, the name shall remain the original one locally on the device.

Another important parameter is the network the Seneca device belongs to that, if local network visibility has been enabled, allows the device to reach the connected devices via Ethernet (for instance HMI or PLC). Exactly like the TAG name, this addressing can be modified with the Edit button, **clearly if this is modified, this configuration must be applied also locally on the device**.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

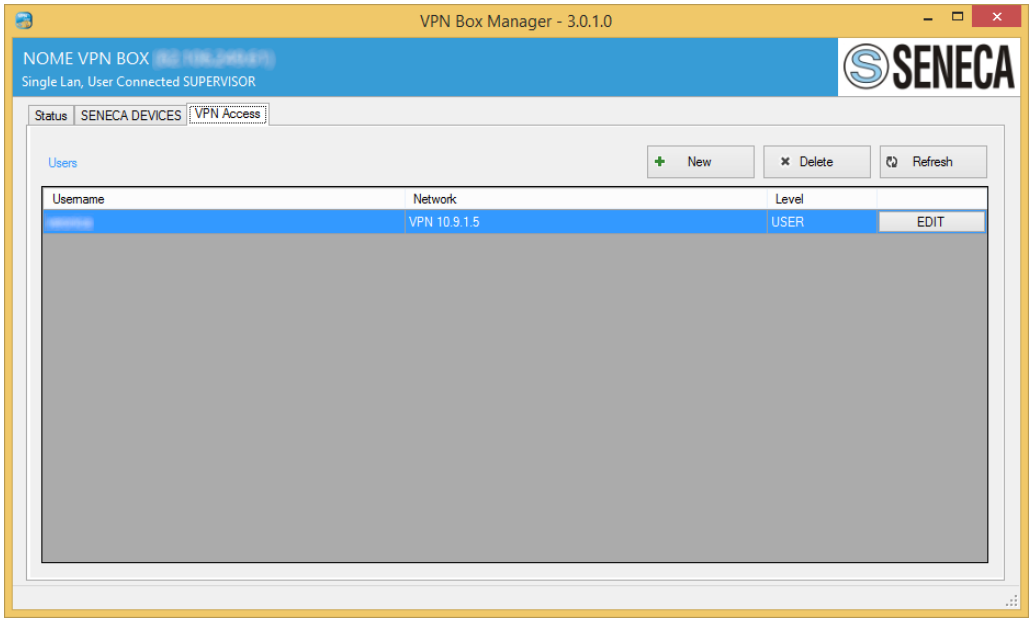


To proceed and make the device work within the VPN network, press the *Edit* button and accept the configuration with the *OK* button; polling time will be required to apply this configuration. The status of the device will pass from "NEW" to "CONFIGURATION IN PROGRESS" until the modification is applied, then it will go to "CONFIGURED" and the device will connect to the network. Devices are considered offline if no polling is carried out for over 3 minutes. The device can also be removed by pressing the *Cancel* button. If the VPN configuration on the device remains unchanged, this will try and register again.

7.2.2. VPN Accesses

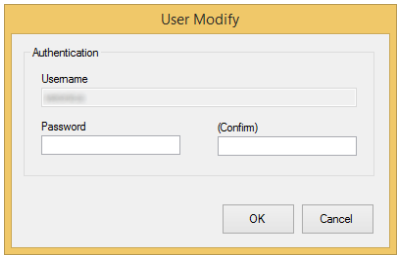
Once the devices are connected you can connect to this new network with a PC, but you need to create accesses first. Every access created is a connection to the VPN network, it is therefore necessary to define as many users as the VPN Client PCs required to monitor/maintain the Network.

ATTENTION: each access can be used by just one user at a time.



Users can be added, edited and deleted at will; clearly, if an account is deleted while it is being used, this will effectively be closed only when it disconnects.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



ATTENTION: usernames and passwords are case sensitive.

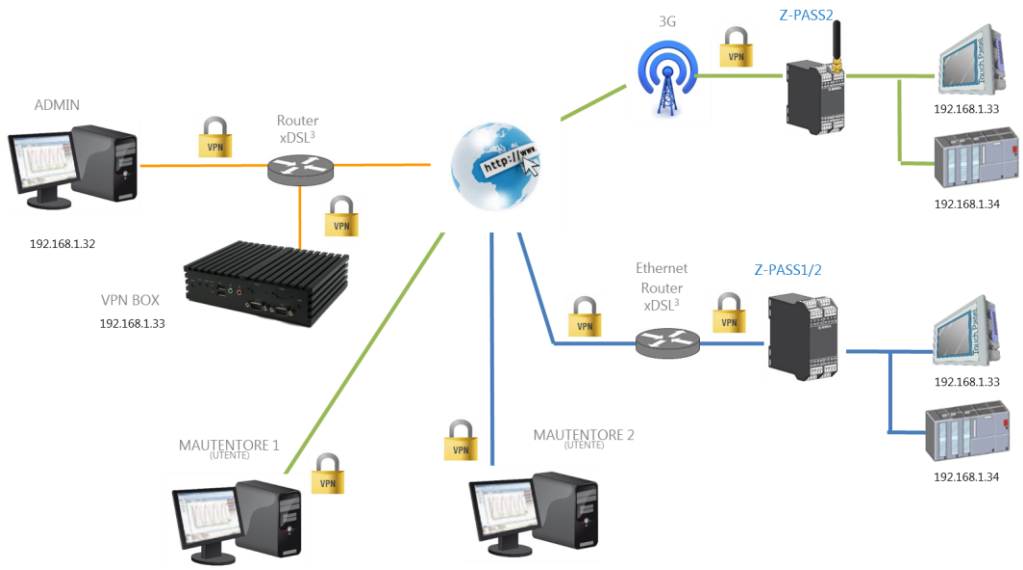
Once this is completed, the account is operational and VPN Client Communicator must be used for the connection, but we will talk about this in the appropriate section.

8. Point To Point

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

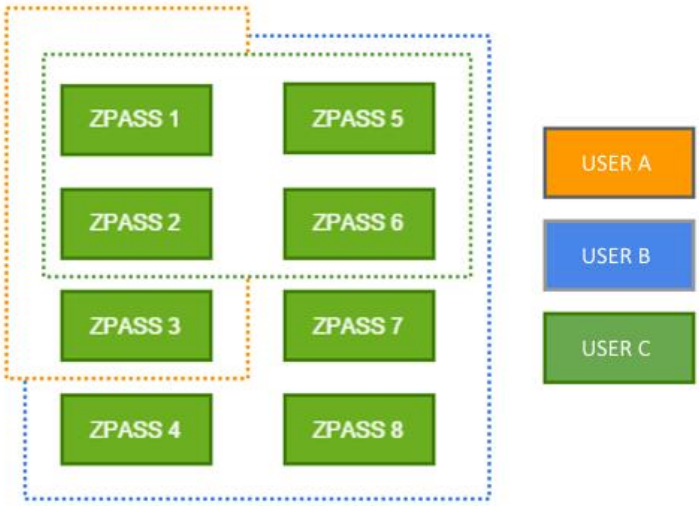
The user can choose to which one to connect (one at a time) and carry out the necessary maintenance. This mode is designed for field support scenarios, it is not a connection to use permanently like Single Lan.

Moreover it is possible to group the devices and assign them to the users that must connect: each user will therefore be able to connect only to the devices assigned to it.



The following figure shows an example of how groups are used. There are three users, A, B and C that have 8 ZPASS available and a precise access discipline is required.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



By creating a group for each user, A will see ZPASS 1, 2, 3 while B will see all the devices and C will access only 1, 2, 5 and 6.

8.1. Router Configuration

In this mode the devices create a tunnel towards the VPN Box and wait for the connection. For this reason each device is associated to a separate port. In this operating mode the VPN Box is a concentrator that sorts the connections.

Port	Type	Compulsory	Description
443	TCP	Yes	Service channel necessary to communicate with the devices and clients.
1193	TCP	Yes	Necessary to drive the tunnel
1195	TCP	Yes	Necessary for device 1
…	TCP	…	
1195+N	TCP	Yes	Necessary for device N

In this configuration the number of ports is fixed but variable according to how many devices you want to have. The system automatically assigns the port starting from 1195; if you have 10 devices, the ports from 1195 to 1204 must be opened on the router.

These ports must be open on the router, therefore unfiltered by a possible firewall rule. Once opened, they must then be re-directed from the router, from the outside towards the inside, modifying the NAT and

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

making them converge towards the local IP address of the VPN BOX: on commercial routers, this option is normally called "Virtual Server" or "Port Mapping".

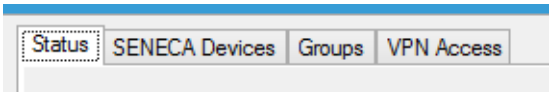
When the configuration is complete, make a note of the router IP public address, required (with the password) for the VPN configuration of the SENECA devices.

Refer to your in-house system administrator about how to acquire this IP address. The modification of the router ports is compulsory **only** if the VPN Box 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 shall be needed.

8.2. VPN Configuration

The configuration of the VPN network in Point to Point mode is divided into three parts: *Seneca device* VPN configuration, via Web Server, following which the devices will be able to register with the system to make their network available via tunnel. Configuration of the *Groups* that contain the devices and are used to isolate the VPN Accesses (Users) and make only some devices "visible" to them.

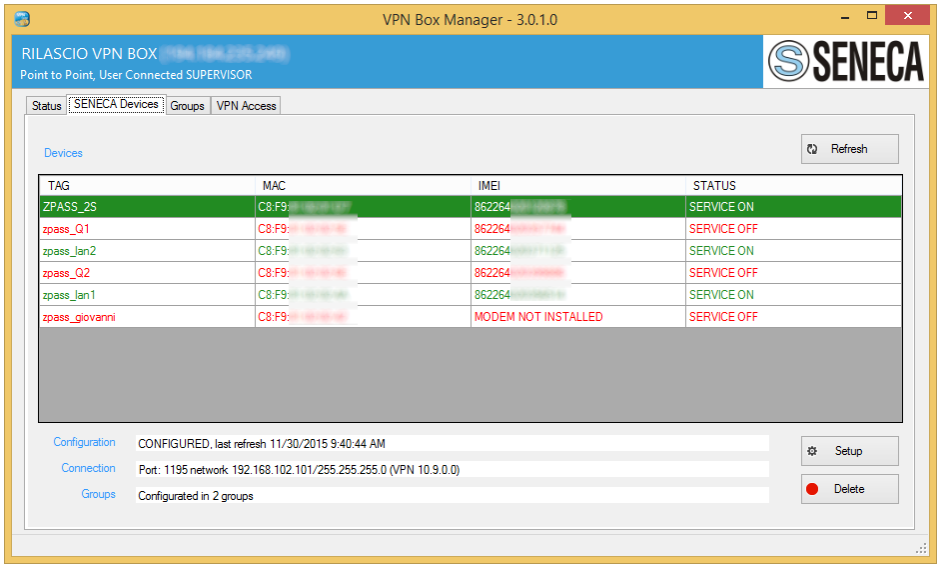
This operation allows therefore creating sets of devices and associate them to one or more VPN Accesses as a kind of access list. A device can be part of one or more groups and the same group can be associated to one or more VPN Accesses; this gives wide scope for configuration. The configuration of the *VPN Accesses* will allow maintenance technicians to access the VPN Client Communicator that, displaying just the list of the associated devices, will connect them to the required one.



8.2.1. SENECA Device Configuration

As previously mentioned, once the devices are configured locally with their web server, they will register with the VPN Box and the Seneca device section will start to fill up: the device will take about two minutes for this operation. This time is important because the device will communicate via polling any changes of status and receive new configurations.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



As shown in the figure, waiting for polling, the devices register and are immediately ready to connect. They can assume different colours according to their status as per the table shown below:

Status	Colour
Configured	Emerald green
Configuration in progress	Pea green
Service OFF	Red

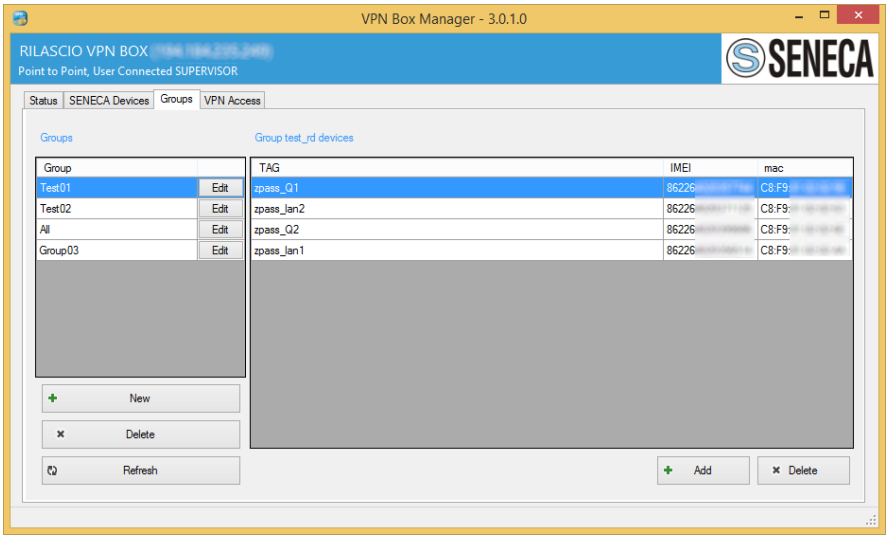
If the polling service has timed out, the system will impose the red colour to highlight an anomaly: this can be due to a loss of connection of the Seneca device or lack of synchronism. In this operating mode, the devices are always green and therefore ready to connect. A change in status takes place if a Group or User is added, edited or deleted; in fact these occurrences involve an update of the device configuration. Two operations are therefore possible on the panel: the deletion that involves the elimination of the Seneca device from the VPN Box (ATTENTION: the support must be first disabled from the VPN configuration of the web server of the device) and the change of TAG that is nothing more than the change of name of the device.

ATTENTION: Changing the TAG, this is modified only on the VPN Box, the device will keep its original name.

8.2.1. Group Configuration

This section represents the connection element between users and devices. Each group can contain all or just some devices: let's suppose there are two users (X and Y) and 4 Seneca devices (Z, X, Q, K). If user X has to see everything and Y only Q and K, two groups must be created, one with Z, X, Q and K and another one with just Q and K. Once assigned, users will see only what is applicable to them.

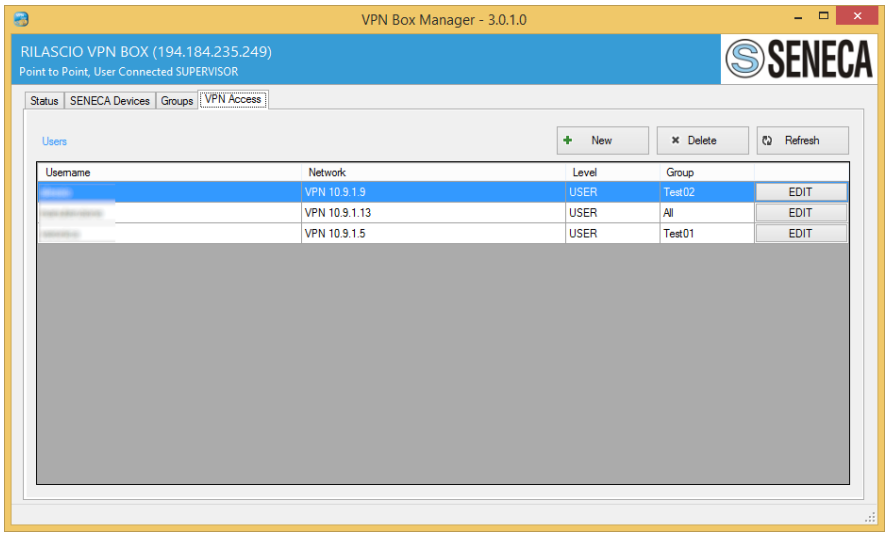
Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



The group interface is divided into two sections, the left one consists of the group lists containing also the *Edit* button and the *New*, *Delete* and *Update* buttons. On the right the content of the selected group is displayed, with the device Add and Delete buttons at the bottom.

8.2.2. VPN Access Configuration

VPN Accesses represent users that will then connect to the individual Seneca devices. They can be created by giving them a name and a password and assigning them to a group. They must be assigned to a group to access the device list; if this is not the case, no device will be seen on connection.

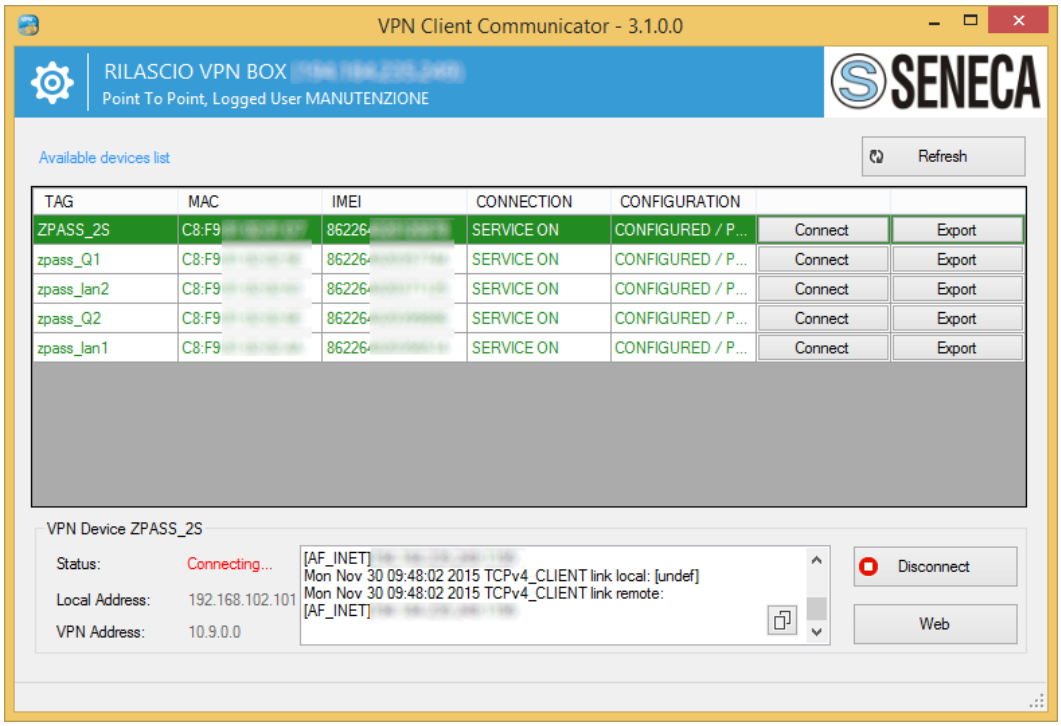


8.3. VPN Client Communicator

The connection client is used to connect to an individual Seneca device.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

ATTENTION! Each device will accept just one connection at a time, if one user is already connected, the second one will be rejected.



Once logged in, the program will display the list of assigned devices. Each one is accompanied by its operating status and port. By pressing Connect, the system will start a session, connect to the ZPASS, projecting you into the destination network and allowing you to see also the devices downstream from the ZPASS (only if you chose this option when you first configured the device). Your configuration can be exported and used with an OpenVPN client such as an Android (for smartphone); see the paragraph on exporting.

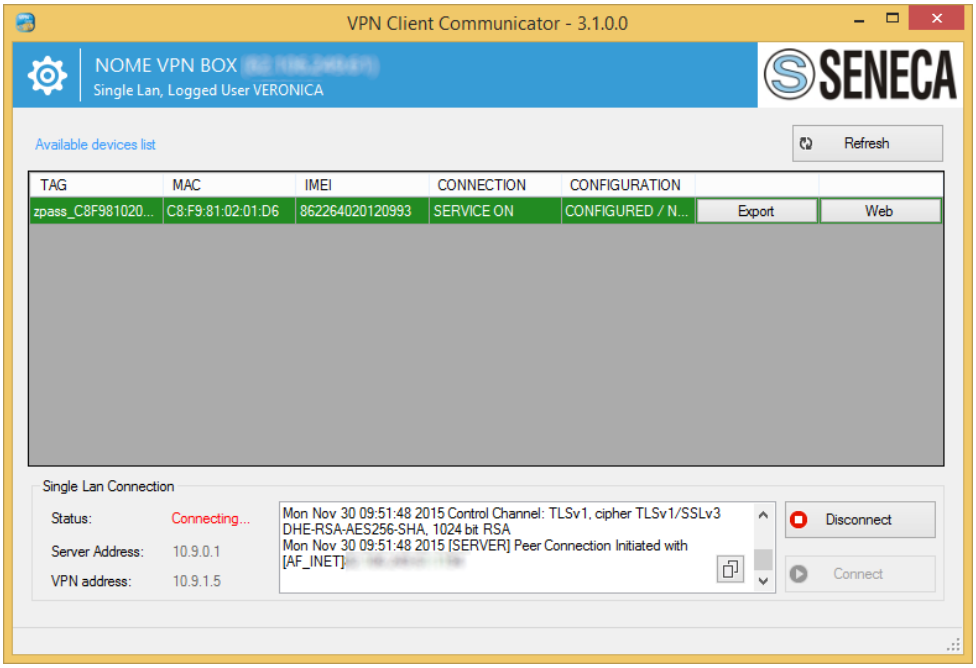
9. Connection to the VPN Network with VPN Client Communicator

This software is a VPN connection client and must be installed on the PCs you want to use to access the VPN network. It gives the possibility of three different uses, two of which will be dealt with later on.

9.1. VPN Client Connection

In this mode, access is possible with the previously created credentials, creating a VPN tunnel with the server and making the network and connected devices accessible. On entering you get a panoramic view of the connected Seneca devices and their status. The configured devices that are online are considered as operational, the network they belong to appears on each line.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



By pressing the *Connect* button you get into the network and communicate with the devices, in the centre the system operations during the connection are logged. On the bottom left-hand side, the configuration data at VPN addresses' level are displayed while on the device panel the addresses of both the device local network and of the VPN are shown. Your configuration can be exported and used with a standard OpenVPN client such as an Android (for smartphone); see the paragraph on exporting.

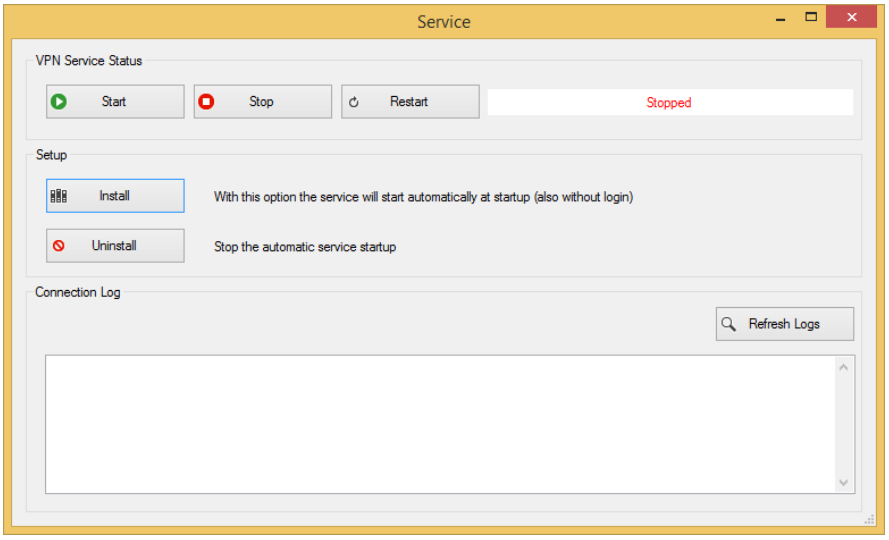
ATTENTION! If you connect from a PC with IP addresses compatible with those of the VPN network, some IP addresses might not work locally.

9.2. VPN Client Communicator in Service Mode

There are cases when it is necessary for a PC wanting to connect to the VPN network to be able to do so autonomously and automatically, without an operator logging in and starting the connection via VPN Client Communicator; these situations are often connected to SCADAs installed on servers. To activate the automatic mode, log into VPN Client Communicator, click on the gear icon in the top left-hand corner and select "Service" from the menu.

It is necessary to install the configuration onto the machine and to do it, press *Install*. The system will carry out all the operations automatically, moving the service to "run" and starting it straight away. It is possible to load the system log into the bottom box, to check the operations carried out or any connection problems.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



Always from this panel, you can stop and restart the service, cancelling also the configuration.

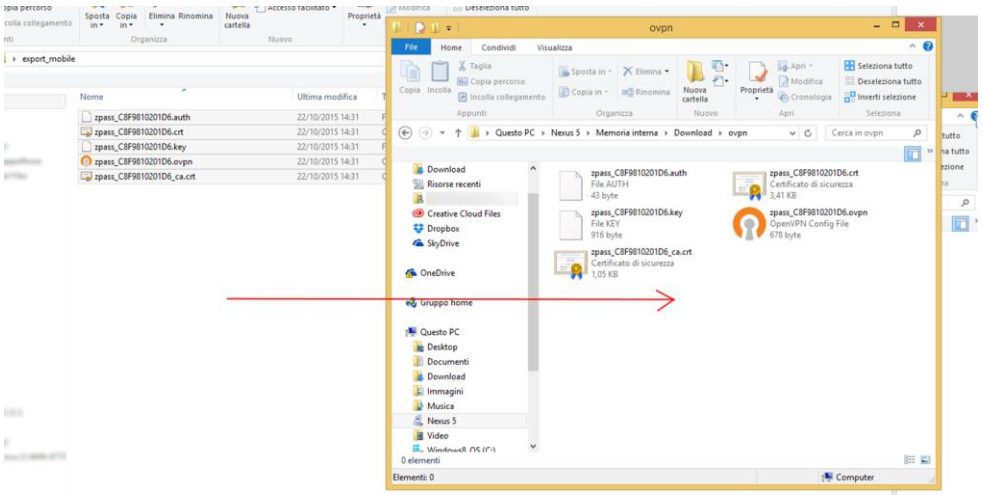
ATTENTION: if you install the automatic mode, you will not be able to use the account in normal mode.

10. Connection via Android Client (Mobile and/or Tablet)

Exporting the configuration, you can save it in a folder to be used on OpenVPN-compatible systems. An example is the configuration of a mobile for the connection, the client for Android can be found at this address:

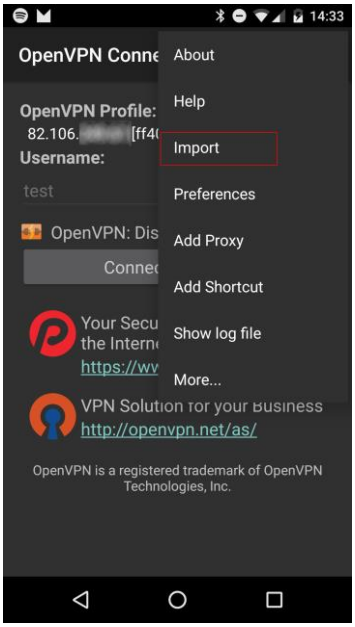
https://play.google.com/store/apps/details?id=net.openvpn.openvpn&hl=it

Connect the mobile to the computer in mass-storage mode and copy all the exported files to the device; they must be all in the same folder and must be renamed. Typically it is possible to use the Download folder, create a folder and copy the files into it.

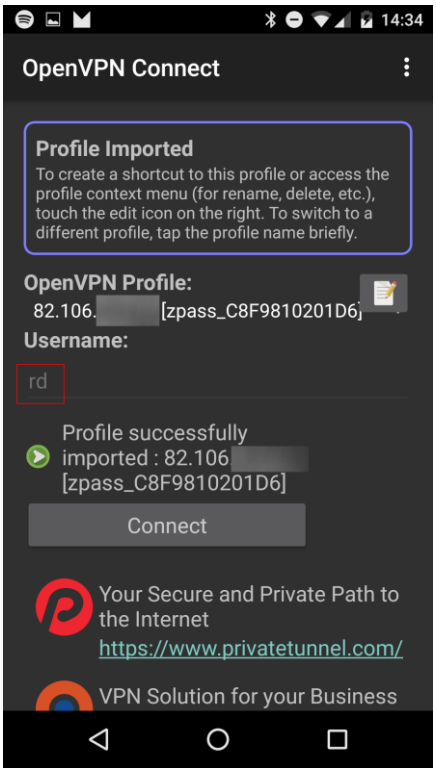


Open the application on the smartphone or tablet and open the menu in the top right-hand corner that will appear as in the figure:

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



Select "*Import Profile from SD Card*" from the menu, a window will be displayed where you can navigate your folders; look for the folder you have just created, select the .ovpn file and press "*Select*". Now the connection is ready, just press *Connect*. It is important to note that also the user created by the VPN Box, in this case "*rd*", has been imported with the profile; only the OpenVPN clients compatible with this mode can be used.





Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

11. Glossary

- *VPN Box Manager*

It is a software that allows configuring the VPN Box hardware or VPN Box Virtual Machine software.

- *VPN Client Communicator*

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

- *PTP (Point To Point)*

This acronym is used to indicate a point-to-point connection 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, that cannot therefore remain on the same LAN. This mode is non permanent, that is it must be used for the necessary operations and then disconnected.

- *SL (Single Lan)*

It indicates the VPN Box mode called Remote Control that allows creating a unique (and therefore single) virtual network between the equipment and the connection clients. It is designed for monitoring systems such as SCADAs, where the connection is stable. In this mode the devices cannot have identical network configurations.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000