MANUALE UTENTE

VPN BOX2 Hardware

VPN BOX2 Virtual Machine

VIRTUAL PRIVATE NETWORK SERVER

SENECA s.r.l.

Via Austria, 26 - 35127 - PADOVA - ITALIA

Tel. +39.049.8705355 - 8705359 Fax. +39.049.8706287

Sito web: www.seneca.it

Assistenza tecnica: supporto@seneca.it (IT), support@seneca.it (Altro)

Riferimento commerciale: commerciale@seneca.it (IT), sales@seneca.it (Altro)

Data	Revisione	Note	Autore
02/05/2023	1	Prima uscita	AS
12/05/2023	2	Traduzione	AZ
10/07/2023	3	Cambiata intestazione	AZ
16/02/2024	4	Fix vari, Aggiunta procedure per connessione IOS/Android	FT/MM

INDICE

1. SENECA VPN BOX2

ATTENZIONE!

IN NESSUN CASO, SENECA S.R.L. O I SUOI FORNITORI SARANNO RESPONSABILI PER LA PERDITA DI DATI/REDDITI DI REGISTRAZIONE O PER* DANNI CONSEGUENTI O ACCIDENTALI DOVUTI A NEGLIGENZA O A UN USO IMPROPRIO E SCONSIDERATO *DEL PRODOTTO, ANCHE SE SENECA SRL È A CONOSCENZA DI QUESTI POSSIBILI DANNI.

SENECA, LE SUE CONTROLLATE, LE SUE AFFILIATE, LE SOCIETÀ DEL GRUPPO, I SUOI FORNITORI E I SUOI RIVENDITORI NON GARANTISCONO CHE LE FUNZIONI SODDISFINO COMPLETAMENTE LE ASPETTATIVE DEL CLIENTE O CHE IL PRODOTTO, IL FIRMWARE E IL SOFTWARE NON PRESENTINO ERRORI O FUNZIONINO IN MODO CONTINUO.

2. SOFTWARE OPEN SOURCE

Il prodotto Seneca VPN BOX2 contiene software Open Source distribuito secondo licenza GPL. In ottemperanza alla sezione 3b di tale licenza, Seneca fornisce i sorgenti di tale software. È possibile fare richiesta del codice scrivendo una email al contatto del supporto tecnico support@seneca.it .

3. INTRODUZIONE

VPN Box è un dispositivo server che consente di realizzare in modo semplificato delle connessioni sicure VPN (Virtual Private Network) tra Impianti e Server/PC geograficamente distanti tra loro mantenendo una gestione centralizzata di tutti i dispositivi SENECA abilitati all'utilizzo di una VPN.

Le connessioni remote basate su tecnologia VPN permettono di comunicare in modo trasparente utilizzando i protocolli TCP/IP più diffusi nel mondo industriale. Trattandosi di connessioni basate su IP (Internet Protocol) è possibile veicolare tramite VPN più protocolli di comunicazione contemporaneamente. Ad esempio sarà possibile comunicare in Modbus TCP/IP con un dispositivo remoto mentre si effettua manutenzione sul software di un PLC appartenente allo stesso impianto.

I dispositivi SENECA compatibili con VPN BOX2 permettono connessioni dall'impianto sia su rete Ethernet che direttamente Mobile/Cellulare (solo prodotti dotati di modem).

Le tipologie di VPN realizzabili con questo prodotto sono di due tipi: VPN Single LAN e VPN Point to Point.

La tipologia Single LAN risolve i casi in cui è necessario creare una connessione che consenta la comunicazione tra dispositivi installati in siti diversi e distanti tra loro, in modo da formare un'unica rete che possa includere, volendo, anche le sottoreti dei dispositivi; questi casi sono tipici negli ambienti SCADA e Telecontrollo.

La tipologia Point to Point consente ad un manutentore di raggiungere un singolo dispositivo e, opzionalmente, la sua sottorete per intervenire su di esso; l'utilizzo tipico è l'assistenza remota in campo delle macchine e la riprogrammazione di un PLC/HMI, la verifica di alcune funzioni e la risoluzione dei problemi.

VPN Box2 è un dispositivo server che necessita di essere configurato tramite interfaccia web

Per creare il tunnel VPN tra un PC remoto e la rete/dispositivo viene fornito il software VPN Client Communicator.

VPN BOX2 è compatibile solo con versioni di VPN Client Communicator > v4.0.0.0.

Tutti i software necessari all'utilizzo del prodotto VPN BOX2 sono scaricabili dalla pagina ufficiale di prodotto nella sezione SOFTWARE & APP.

Il VPN BOX2 è fornibile in due versioni: Hardware e Virtual Machine (VMware) di seguito sono riportate le caratteristiche di ciascuna versione.

3.1. SPECIFICHE HARDWARE

Per ottenere le specifiche tecniche del box pc con il quale viene fornito il prodotto in versione “hardware” si consulti il manuale installazione del prodotto VPN BOX2.

3.2. SPECIFICHE VIRTUAL MACHINE (VMWARE)

La versione Virtual Machine viene fornita in formato OVF esportato con un’indicazione di massima dei requisiti hardware dell’applicazione Virtuale. Tali requisiti dovranno poi essere opportunamente modificati dall’utente in fase di creazione della VPN BOX2 Virtual machine in modo da tener conto di:

- *Numero di dispositivi Seneca da gestire*
- *Numero di utenti da gestire*
- *Carico di lavoro al quale il server dovrà provvedere*

Per una configurazione minima si consiglia di rispettare i seguenti requisiti:

Requisito	**Valore Minimo ammesso**
CPU	64 bit / 2 core
RAM	8 GB
Disco	64 GB SSD
SO	compatibile con distribuzioni LINUX
Networking	1xETH (100/1000 Mbit)
Host/Hypervisor	Host supporto: Intel-VT o AMD-V / Hypervisor: VMware

Le configurazioni potranno essere modificate in una fase successiva alla creazione del server per garantire la scalabilità dell’applicazione.

Per ulteriori istruzioni relative all’utilizzo del formato OVF per avviare una VPN BOX2 Virtual Machine si veda il capitolo Installazione VM.

4. INSTALLAZIONE DI VPN BOX2

4.1. INSTALLAZIONE DELLA VERSIONE HARDWARE

Per effettuare l'installazione del VPN BOX2 hardware procedere come segue:

- *Posizionare il server orizzontalmente su una superficie piana*
- *Collegare i morsetti di alimentazione del box hardware ad una sorgente di alimentazione dedicata. I requisiti per l'alimentazione sono riportati nel manuale utente*
- *Il VPN BOX2 hardware non necessita di tastiera, mouse o video per operate. Tuttavia potrebbero essere richiesti in caso di assistenza tecnica da parte del personale di Seneca.*
- *Avviare il VPN BOX2 premendo e rilasciando 1 sola volta il pulsante ON/OFF riportato sul pannello frontale del box*
- *Il led POWER si accenderà istantaneamente ma il server non sarà immediatamente operativo, necessiterà di alcuni minuti per l'avvio completo (tempo di avviamento max 5 min)*

ATTENZIONE!

il VPN BOX2 è un apparato server, necessita di essere correttamente acceso e spento evitando brusche interruzioni di alimentazione. Per questo motivo si raccomanda di installare una UPS a protezione dell'alimentazione del server.

Per lo spegnimento del server:

- *Premere e rilasciare 1 sola volta il pulsante ON/OFF*
- *Attendere completo spegnimento del led POWER*
- *In alcuni casi la procedura di arresto normale può richiedere 1 o 2 minuti.*

In caso di blocco dell'avvio del server o di mancato spegnimento procedere con un arresto forzato come segue:

- *Premere e mantenere premuto 1 sola volta il pulsante ON/OFF*
- *Mantenere il pulstante premuto fino a che il led POWER non sarà spento.*
- *Ripetere procedura di avvio*

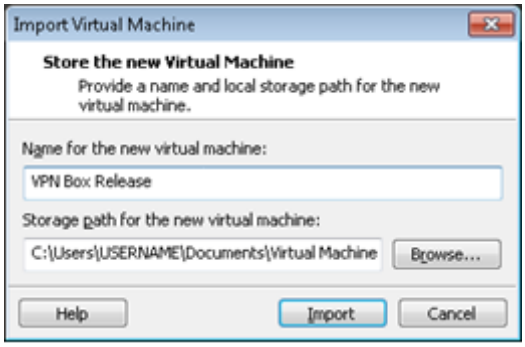
Per ulteriori dettagli sull'installazione del VPN BOX2 hardware si consulti il manuale installazione del prodotto.

4.2. INSTALLAZIONE DELLA VERSIONE VIRTUAL MACHINE

Nel caso di installazione virtual machine è necessario importare sul proprio software di virtualizzazione il file con estensione ".ovf". Tutti i file accessori forniti dovranno trovarsi nella stessa cartella del file OVF per evitare errori in fase di import e creazione della virtual machine.

Il file OVF è compatibile con il software di virtualizzazione VMware Workstation Pro, le istruzioni riportate di seguito mostrano come importare l'applicazione VPN BOX 2 virtual machine in tale software

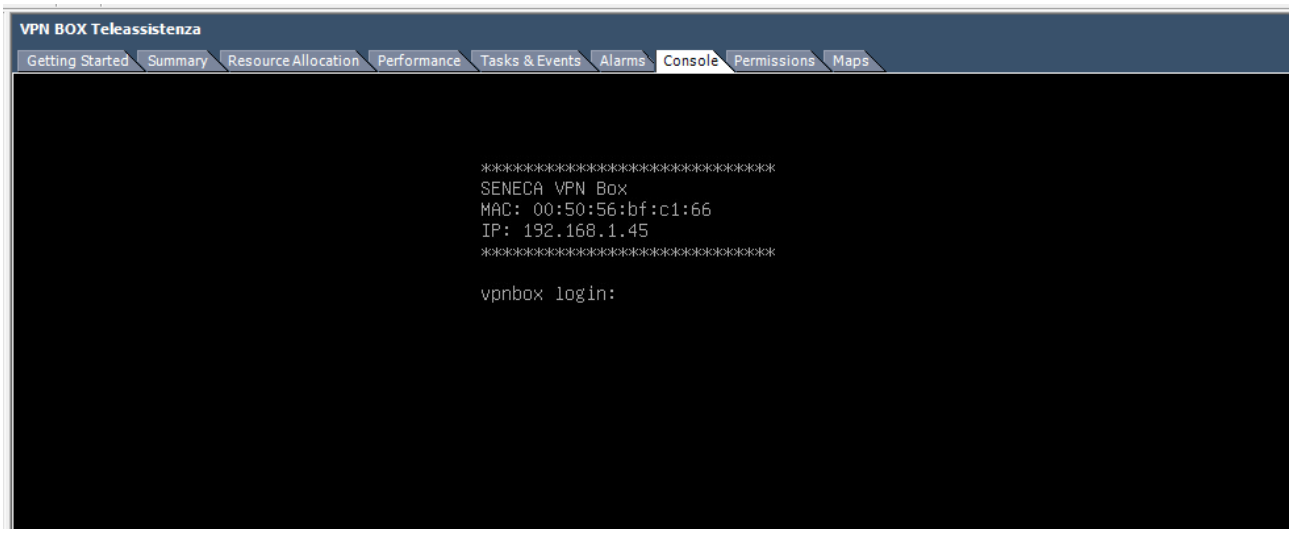
- *Effettuare doppio click sul nome del file con estesione .ovf per avviare l'import dell'applicazione*
- *Seguire il wizard di import virtual machine*



- *Avviare l'applicazione virtuale*
- *Al termine dell'avvio la schermata di login verrà mostrata a video sulla console. Come mostrato nello screenshot seguente*

ATTENZIONE!

Nessuna operazione è richiesta all'operatore in questa schermata. Semplicemente ridurre ad icona la console ed utilizzare il server VPN BOX2 tramite l'accesso web con un browser compatibile.



La compatibilità VMware è impostata come di seguito riportato:

- 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

ATTENZIONE!

La virtual machine ed il Sistema operativo Guest è di tipo 64 bit quindi il Server/PC Host dovrà essere compatibile con la tecnologia Intel-VT o AMD-V che dovranno essere preventivamente attivate nel bios.

5. CONFIGURAZIONE DI RETE ETHERNET DI DEFAULT

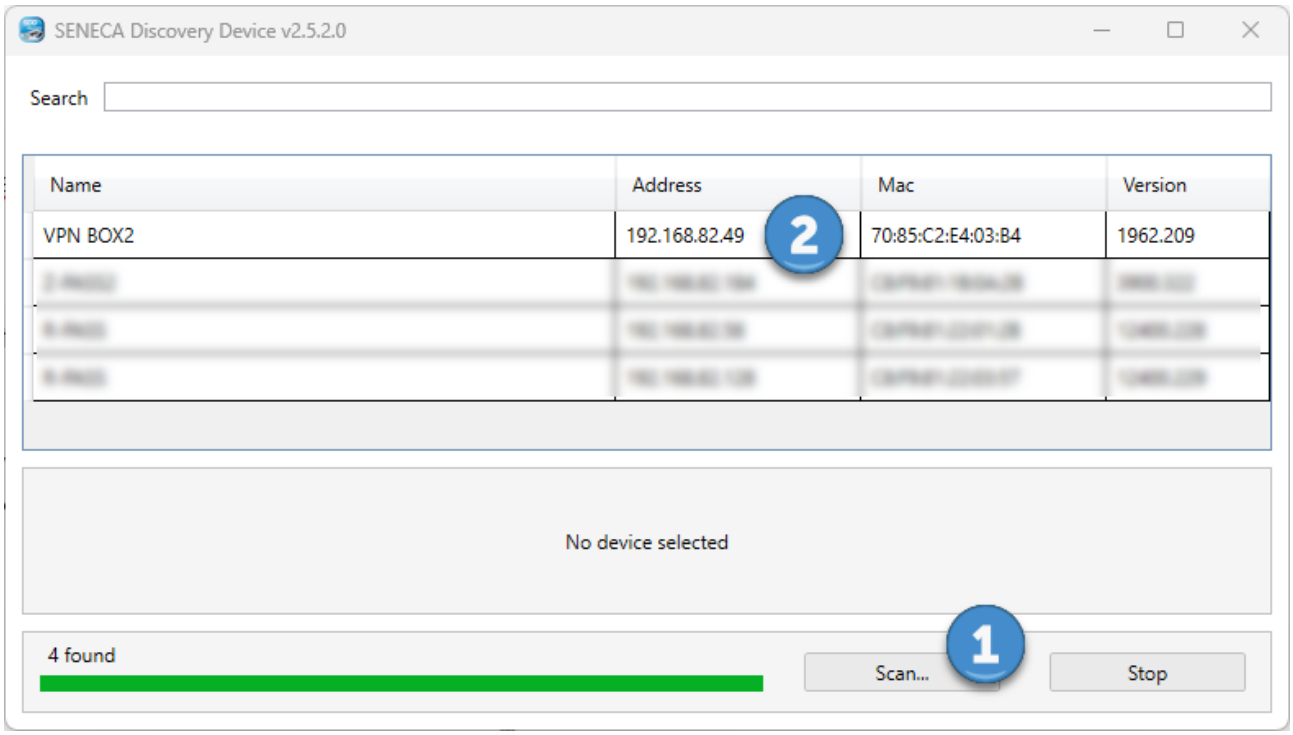
VPN BOX2 viene fornito di default con la Network/porta Ethernet impostata in DCHP (ottieni automaticamente indirizzo IP dalla rete), nel caso non sia disponibile un server DHCP verrà impostato automaticamente l'indirizzo IP 192.168.90.101.

Per rilevare l'indirizzo IP attuale del VPN BOX2 si consiglia di utilizzare il software SDD (Seneca Discovery Device) installato su un PC connesso alla stessa rete del box o direttamente in esecuzione sullo stesso server Host su cui è in funzione la Virtual Machine.

Il software SDD può essere facilmente installato eseguendo il programma di installazione disponibile al seguente link:

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

una volta eseguita la scansione della rete con il tasto “Scan…” l’indirizzo IP sarà visibile nella colonna “Address” in corrispondenza alla riga del device “VPN BOX2”:



6. PRIMA CONFIGURAZIONE DEL VPN BOX2

Per effettuare la configurazione di VPN BOX2 è necessario utilizzare un browser dello stesso tipo utilizzato per la navigazione Internet.

Una volta ottenuto l’IP attuale del server tramite SDD avviare il browser web ed inserire nella barra dell’indirizzo il seguente URL:

https://<actual-ip-address>/

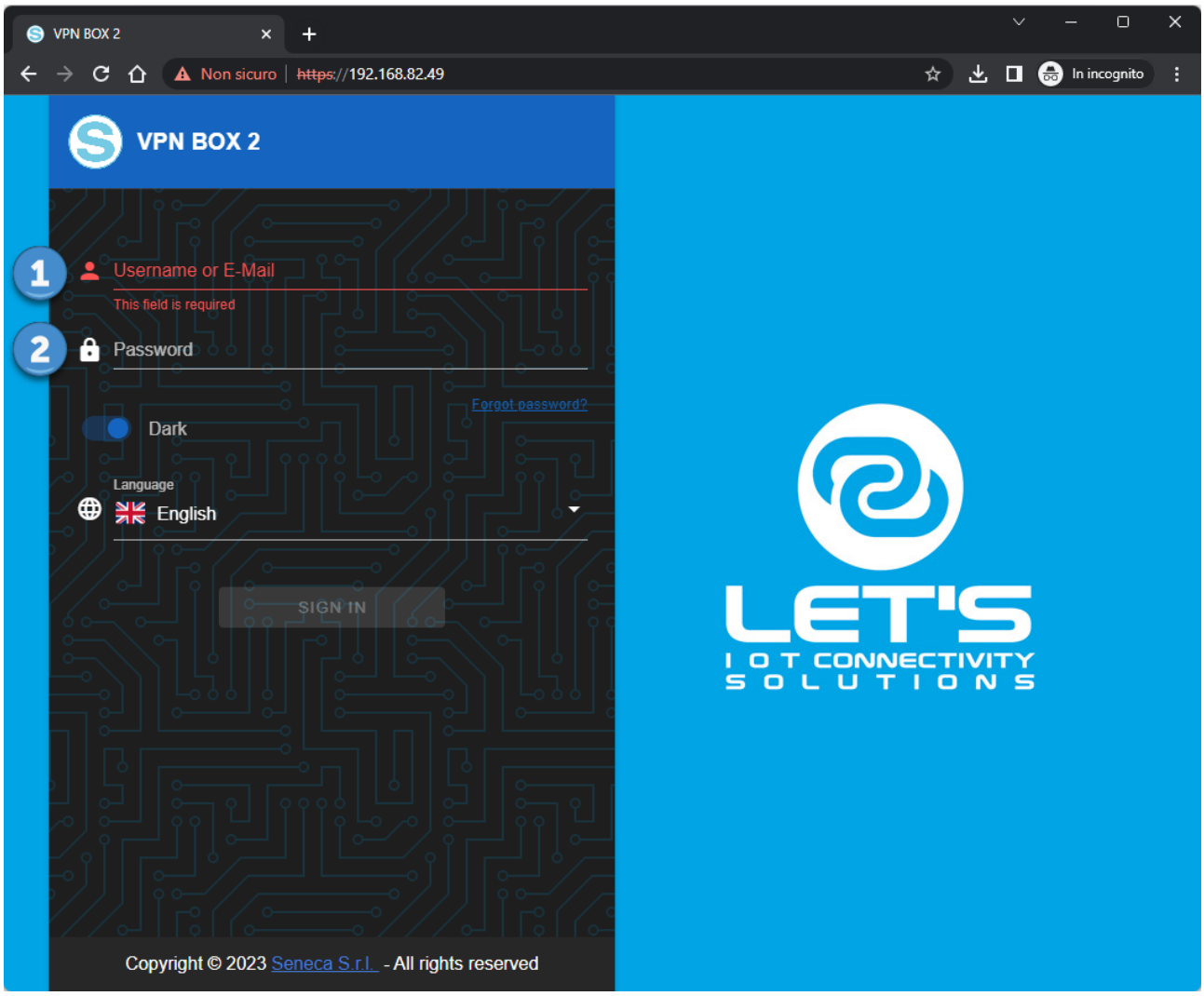
NOTA: sostituire il valore con <actual-ip-address> con l’indirizzo IP rilevato tramite SDD es. 192.168.90.101, un esempio di URL valido è il seguente:

https://192.168.90.101/

il browser a questo punto mostrerà la schermata di login.

6.1. LOGIN

Ad ogni accesso, compreso quello di prima configurazione, il server chiede all'utente di identificarsi:



Le credenziali di accesso di default sono le seguenti:

Username: supervisor

Password: seneca

ATTENZIONE!

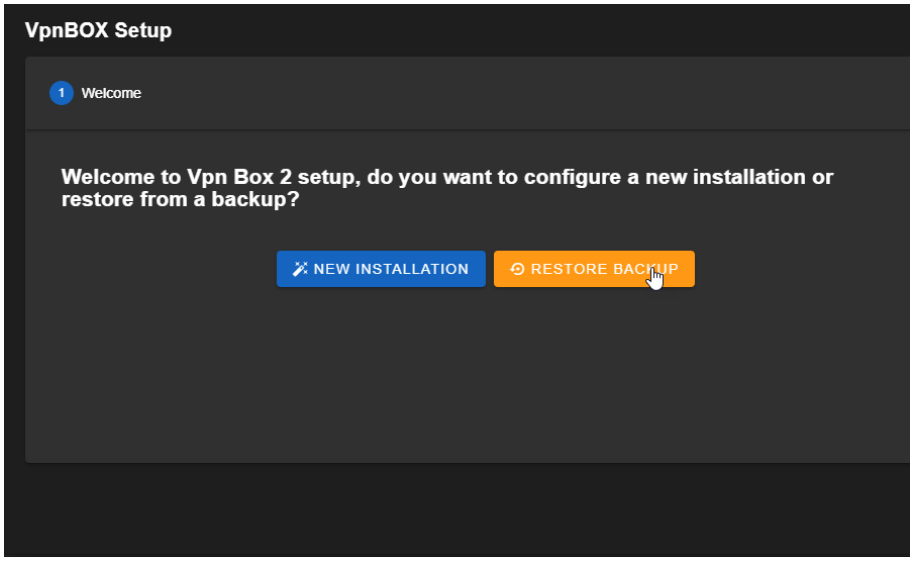
Per ragioni di sicurezza si raccomanda di modificare le credenziali di default dell'utente con i privilegi massimo "supervisor" e si suggerisce di creare un utente per ogni persona fisica che necessita di accedere al sistema.

A login verificata se il server non è mai stato configurato comparirà il wizard di prima configurazione altrimenti verrà visualizzato il pannello Home.

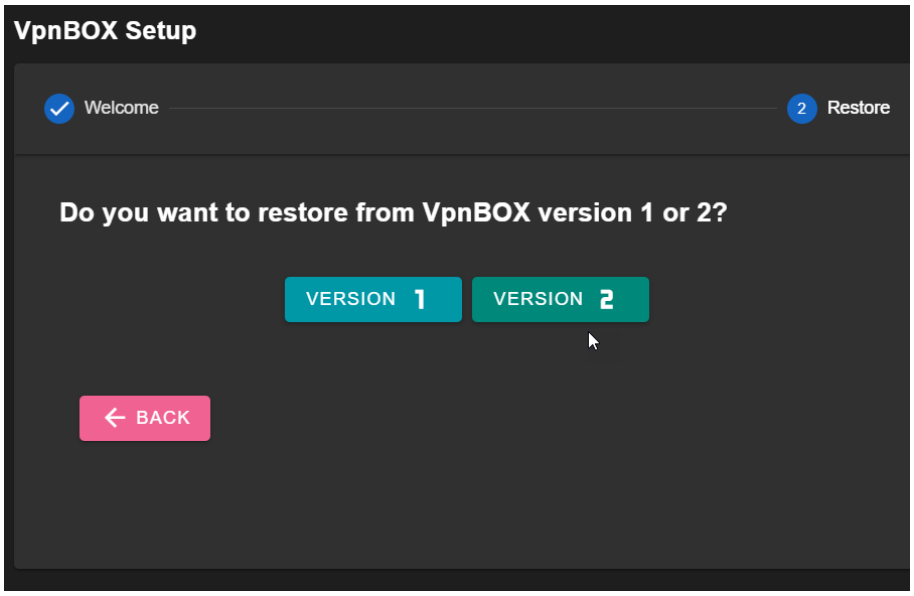
6.2. WELCOME

Al primo avvio comparirà un wizard di prima configurazione che permetterà all'operatore di scegliere tra

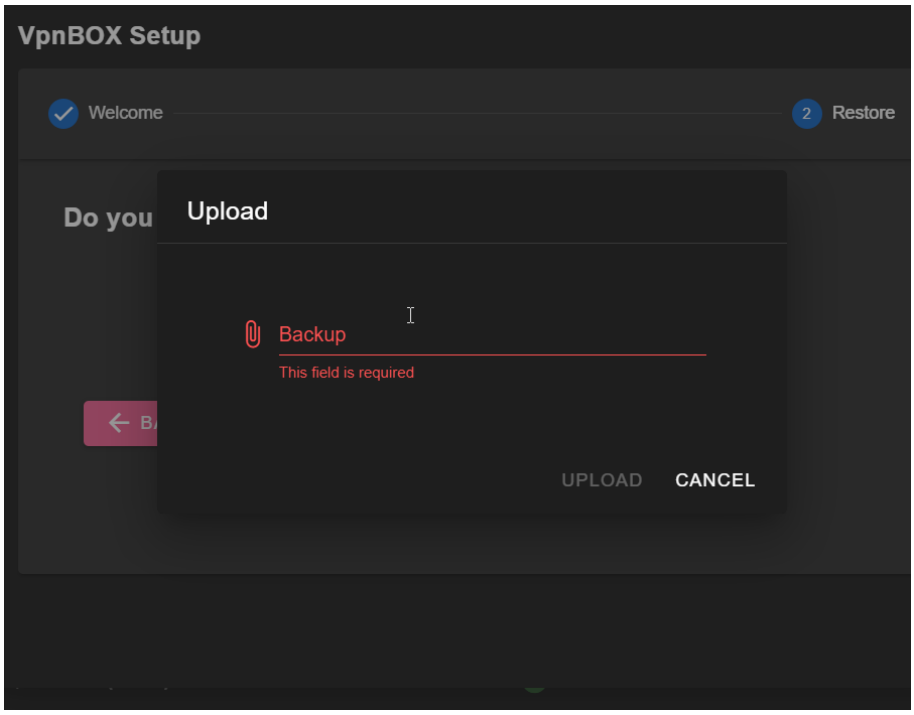
- *Creare una nuova configurazione*
- *Ripristinare un VPN BOX2 da file di backup*



Nel caso di ripristino file di backup si può scegliere se importare un file di una precedente installazione VPN BOX v1 o un file di un VPN BOX2



Cliccare sul testo “Backup”, selezionare il file di backup che si intende ripristinare e confermare cliccando su “upload”:



Al termine del caricamento del file il server VPN BOX2 verrà riavviato, attendere il completamento della procedura.

6.1. MODE

In caso di nuova installazione comparirà il popup di scelta della modalità di rete base dove sarà possibile scegliere tra le opzioni:

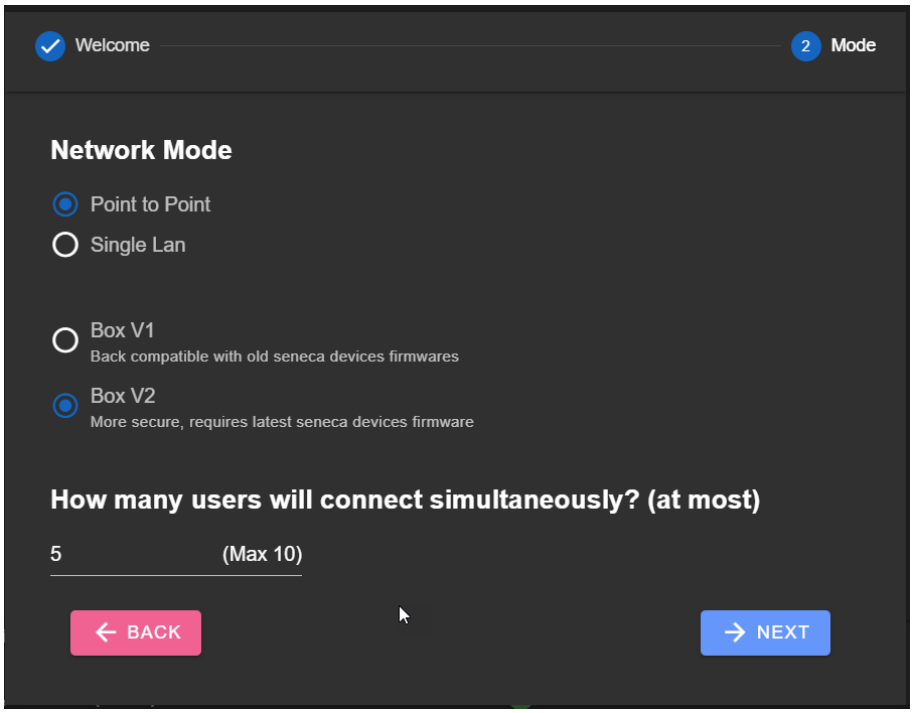
- *Point to Point*
- *Single LAN*

E tra le modalità di compatibilità con i device Seneca:

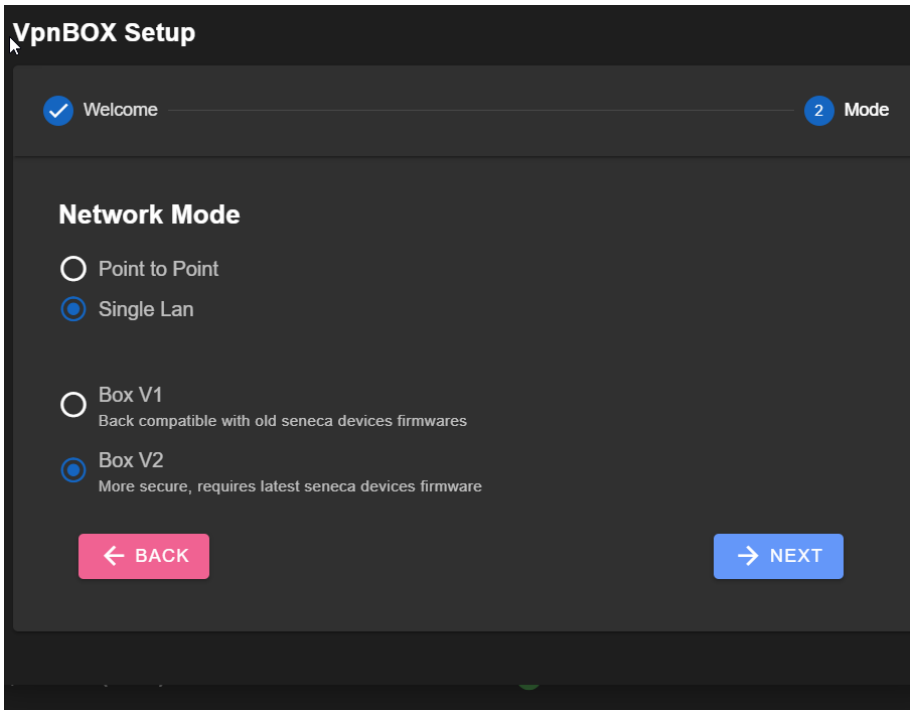
- *Box V1: tutti i device si collegheranno al VPN BOX2 credendo di accedere ad un VPN BOX precedente versione (v1). L’attivazione della connessione VPN risulta essere più lenta in quanto il protocollo utilizzato non è realtime. È l’unica possibilità se si dispone solo di device Seneca e firmware non compatibili con VPN BOX2.*
- *Box V2: i device compatibili con VPN BOX2 utilizzeranno tutte le feature disponibili sul server come ad esempio: minimizzazione dei tempi di attesa nell’attivazione della connessione VPN.*

sarà sempre possibile modificare queste impostazioni in un secondo momento tramite l’apposito menù Networks.

Nella modalità Point to Point è necessario scegliere il numero massimo di connessioni simultanee che il server VPN BOX2 in modalità P2P dovrà gestire. Da questo conteggio dovranno essere escluse le connessioni SL che saranno conteggiate a parte e meglio definite nel setup delle Networks (VPN) della sezione Amministrazione del Server:



Nella modalità Single LAN non è necessario scegliere tra il numero di utenti contemporanei in quanto tutti gli utenti appartenenti a tale rete avranno accesso simultaneo a tutti i device della rete Single LAN:

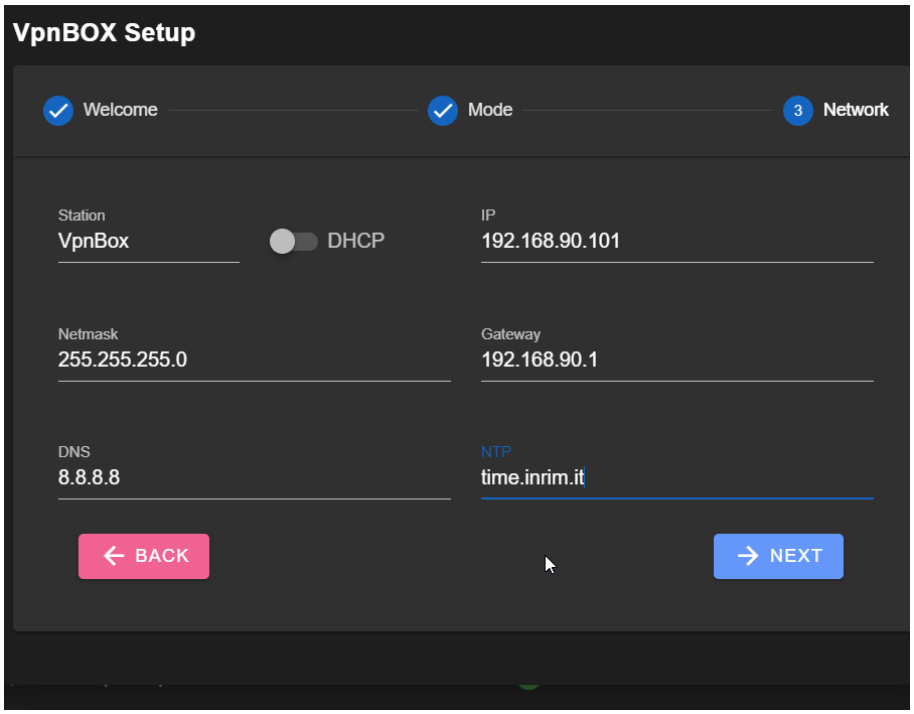


Per approfondire le differenze tra le due modalità operative Single Lan e Point to Point si vedano i rispettivi capitoli sui principi di funzionamento: “principio di funzionamento vpn network single lan” e “principio di funzionamento vpn network point to point”.

6.1. NETWORK

Il popup “network” del wizard di prima configurazione permette di settare i parametri di comunicazione del VPN BOX2.

La seguente finestra mostra le classiche impostazioni di rete di un dispositivo basato su Ethernet che possono essere statiche o dinamiche tramite l'ausilio del DHCP:



Il significato di ciascun parametro è riportato nella seguente tabella:

Parametro	**Significato**
Station	Nome del vpn box che verrà mostrato nella barra del titolo per una più facile identificazione della funzione del server. Default: VpnBox
DHCP	Indica se l’ottenimento dell’indirizzo IP per il vpn box deve avvenire in automatico dalla rete. Se viene abilitato i parametri IP, Netmask, Gateway, DNS non sono più impostabili dall’utente. Default: ON
IP	Indirizzo IP per il vpn box Default: 192.168.90.101
Netmask	Maschera di rete per vpn box Default: 255.255.255.0

Gateway	Indirizzo IP dell'Host Gateway che permette al vpn box la navigazione Internet Default: 192.168.90.1
DNS	Indirizzo del server per la risoluzione dei nomi, può essere un IP appartenente alla LAN del VPN BOX2 o anche esterno. Default: 8.8.8.8
NTP	Indirizzo IP o nome host del server NTP da utilizzare per la sincronizzazione dell'ora del server VPN BOX2 Default: time.inrim.it

ATTENZIONE!

È *necessario che il vpn box possa navigare in Internet per poter effettuare le seguenti operazioni essenziali al corretto funzionamento:*

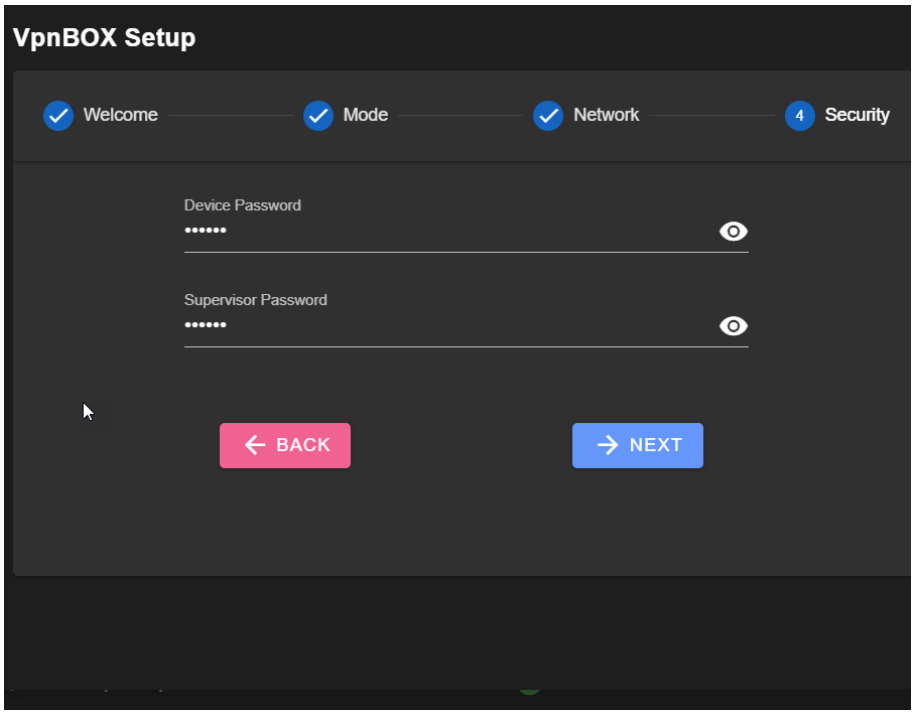
- ***per sincronizzare l'orologio di sistema (NTP) senza il quale le vpn non potrebbero essere create***
- ***aggiornamenti di sicurezza***
- ***aggiornamenti applicativi***

6.1. SECURITY

Il popup “security” del wizard di prima configurazione permette di impostare/modificare le password di default

- *dell’utente con i massimo privilegi di accesso “supervisor”*
- *dei device per l’autenticazione preliminare (da riportare nel menu di configurazione del device stesso)*

Per confronto si veda il manuale utente del device utilizzato al paragrafo “VPN configuration”:



6.1. LICENSE

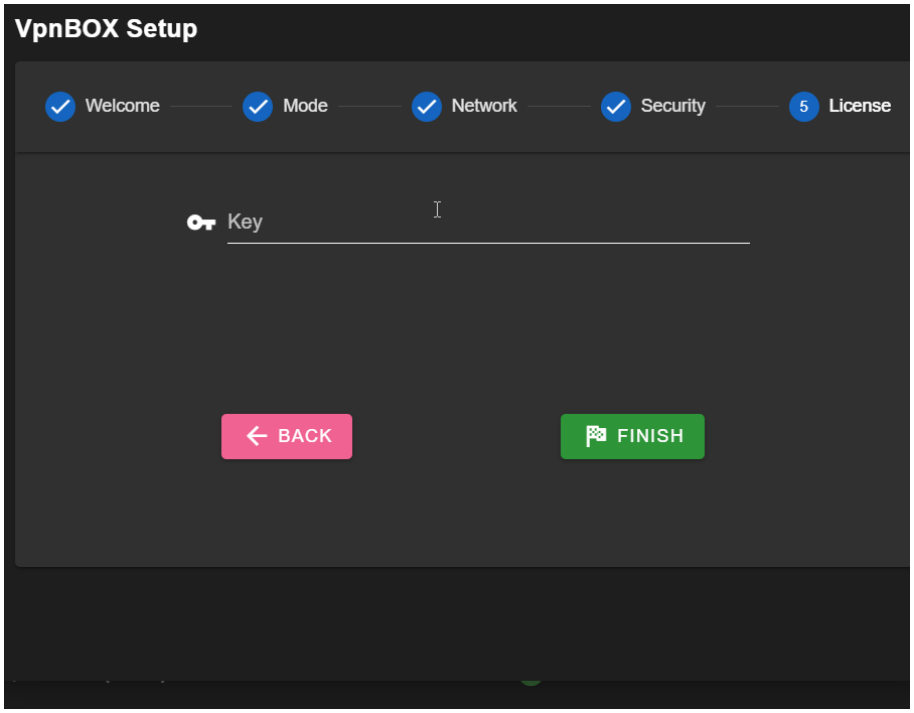
Il popup “security” del wizard di prima configurazione permette di caricare la licenza d’uso del software VPN BOX2

Il codice di licenza è presente nel coupon fornito assieme al prodotto.

La licenza è costituita da un codice alfanumerico a 4 gruppi di 4 cifre del tipo:

AAAA-BBBB-CCCC-DDDD

da introdurre nel campo “Key”:



Alla pressione del pulsante “Finish” tutte le impostazioni inserite nei precedenti popup del wizard verranno applicate al server e verrà effettuata l’attivazione della licenza associata al codice appena inserito.

Nel caso l’utente non disponesse di un codice di licenza può proseguire lasciando vuoto il campo “Key”, il VPN BOX2 risulterà comunque operativo in modalità “Demo” con le seguenti limitazioni:

Numero di utenti abilitati: 2

Numero di device collegabili: 2

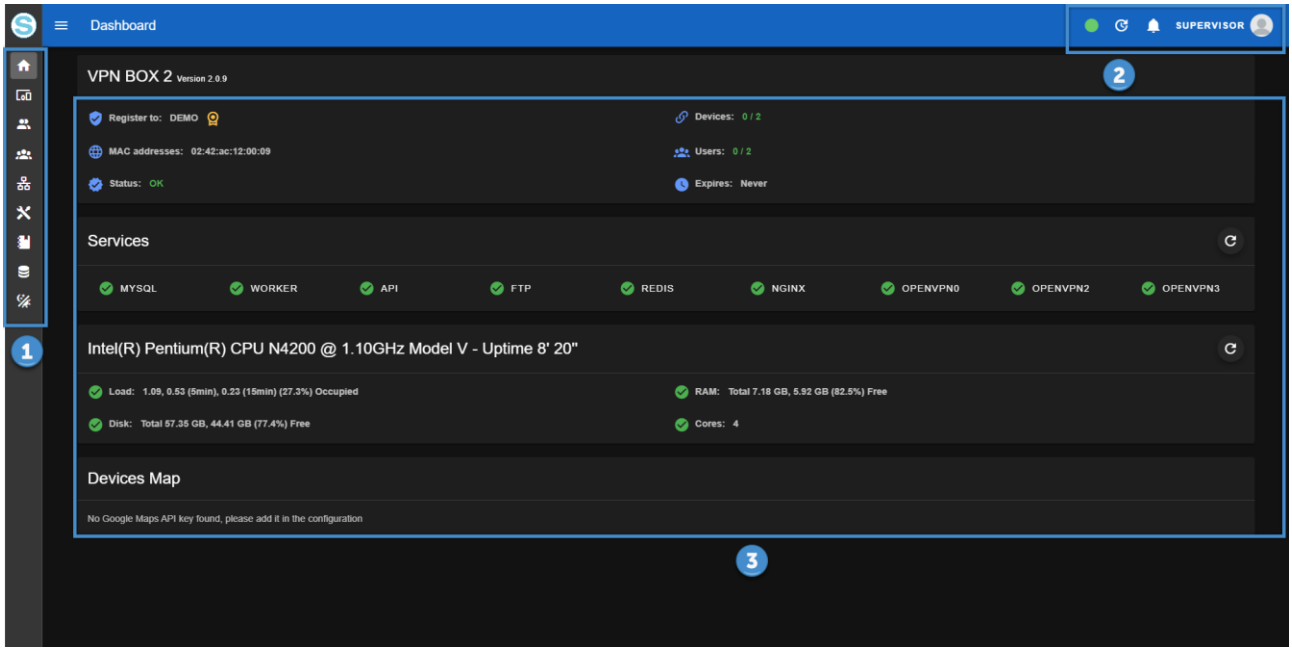
Sarà possibile introdurre la licenza in un secondo momento.

7. AMMINISTRAZIONE DEL SERVER

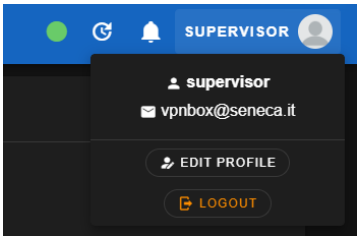
Nel presente capitolo verranno approfondite le funzionalità di ciascuna voce del menù di navigazione del server VPN BOX2.

7.1. HOME

La pagina home sarà visibile subito dopo il login dell'utente. È divisa in 3 sezioni principali: il menu di navigazione (1), la barra di gestione dell'utente con annessa area di notifica (2) ed il pannello centrale (3) divisa a sua volta in più pannelli di stato:



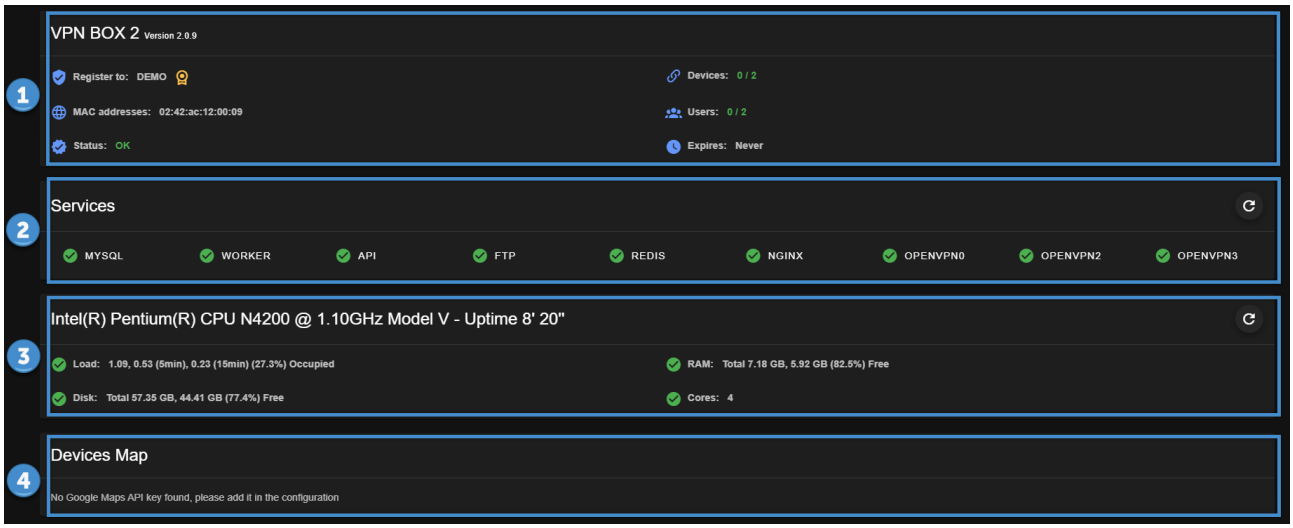
La barra di gestione dell'utente correntemente loggato permette il logout e la gestione delle preferenze dell'utente:



premendo il pulsante "Edit profile" in questa sezione sarà possibile:

- *Modificare la proria E-Mail*
- *Modificare le proprie credenziali (password)*
- *Attivare l'autenticazione a 2 fattori (2FA)*
- *Modificare la preferenza della lingua dell'interfaccia web*

I pannelli di stato della pagina home sono così composti:



La parte alta che mostra la versione dell'applicativo VPN BOX2, la licenza e le relative caratteristiche device e utenti supportati (1)

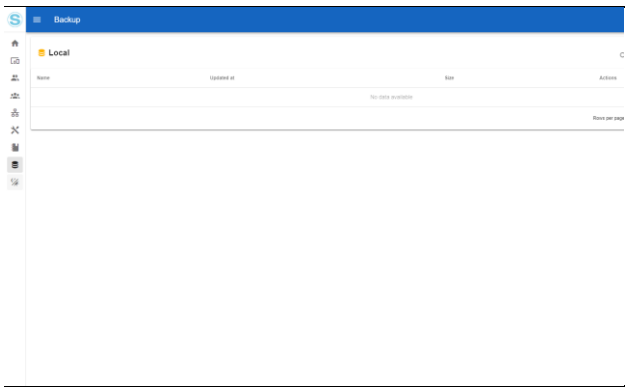
Pannello dei servizi attivi (2) che riflette l'operatività del server in quel preciso momento. Nel caso un servizio non correttamente funzionante l'icona posta a fianco sarebbe una X rossa ad indicare uno stato di errore.

Si suggerisce di consultare il menu Logs per rilevare l'anomalia che ha causato il blocco del servizio. Per una corretta operatività del server è necessario che tutti i servizi siano attivi.

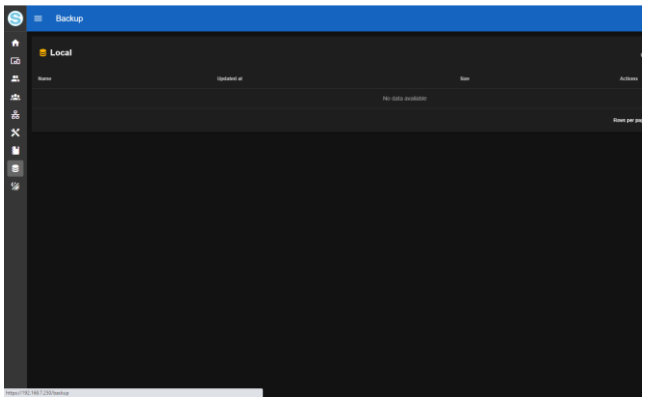
Il pannello statistiche del server (3) mostra lo stato di funzionamento della macchina fisica o virtuale che ospita l'applicazione VPN BOX. Le statistiche sono: carico della CPU, percentuale di utilizzo della RAM, disco e numero di core del processore.

In ogni pagina è possibile regolare lo sfondo dell'applicazione secondo il proprio comfort visivo cliccando sull'ultimo pulsante del menu per ottenere le seguenti:

Sfondo Chiaro

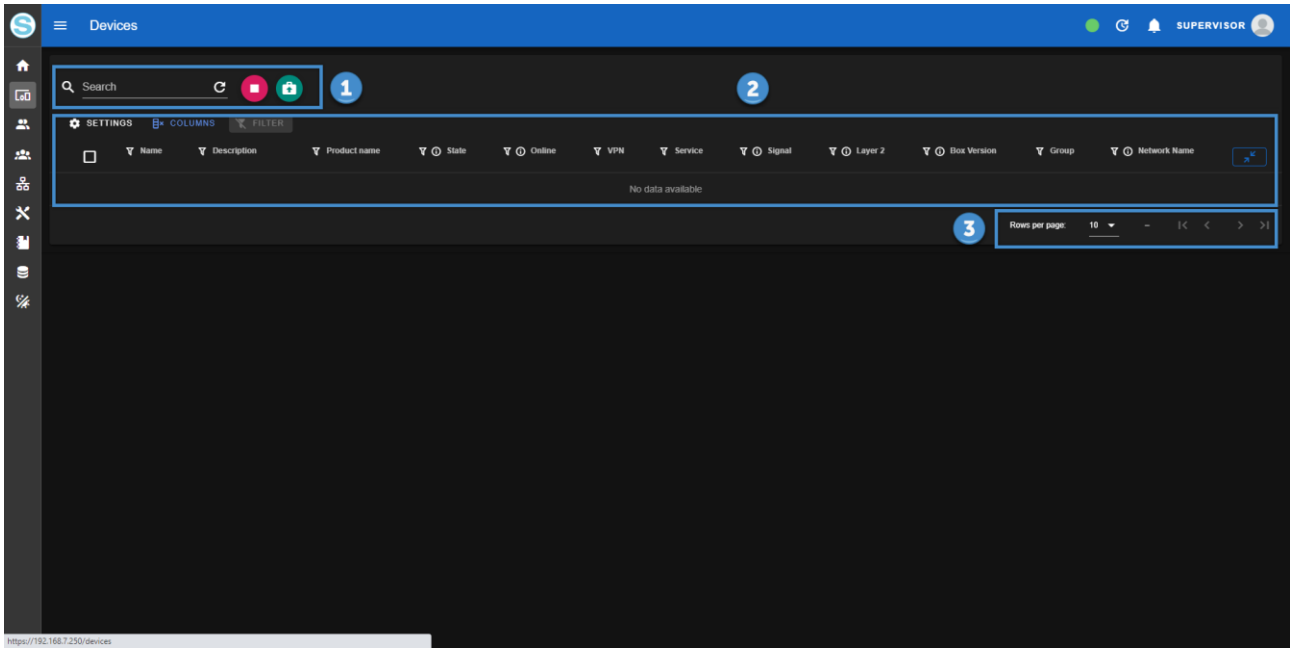


Sfondo Scuro (default)



7.2. DEVICES

La sezione Device contiene l'elenco di tutti i dispositivi Seneca connessi al VPN BOX2. Non esiste un pulsante aggiungi device in quanto è il dispositivo stesso che, opportunamente configurato, si presenterà in lista.



Una volta configurati in locale tramite il proprio Web Server, i dispositivi Seneca si registreranno sul VPN BOX2 e compariranno in questa sezione: questa operazione potrebbe richiedere fino a 2 minuti in caso di scarsa qualità del canale di comunicazione server-device.

Durante questo tempo ogni dispositivo comunicherà eventuali cambiamenti di stato e riceverà nuove configurazioni da server per la prima "inizializzazione".

La pagina Devices è dotata di un filtro di ricerca di tipo "full text" (1) dove ogni testo digitato verrà ricercato in tutti gli attributi dei device, una tabella/elenco (2) costituisce la vista centrale mentre nella parte bassa si trova il controllo della paginazione della tabella (3). Di default vengono mostrati 10 device per pagina.

Lo stato del dispositivo determina il colore del testo con cui viene visualizzato nella pagina secondo quanto riportato nella seguente tabella:

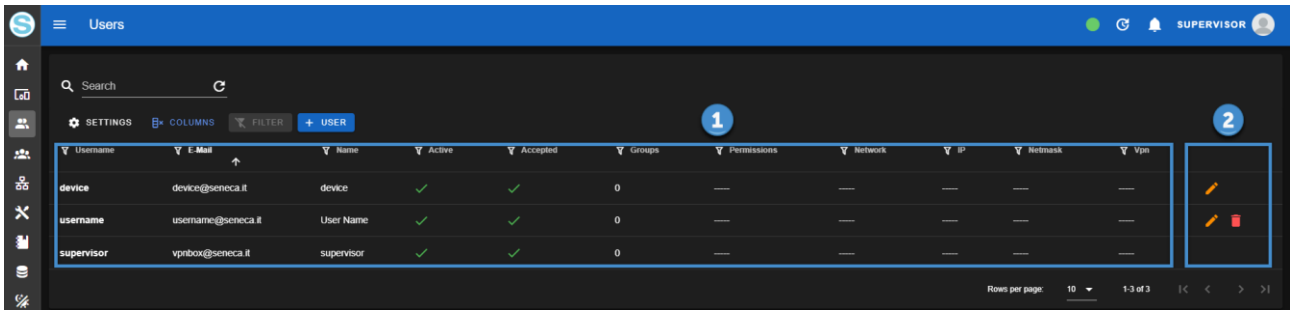
Stato	Colore
Nuovo (da assegnare ad un Gruppo)	Grigio
Configurato e connesso	Verde
Non connesso	Rosso

Subito dopo la registrazione, lo stato del dispositivo è "New" e il dispositivo stesso è in attesa di essere configurato; in questo stato il dispositivo non eseguirà alcuna operazione e non si collegherà in VPN. Durante la registrazione, il dispositivo fornisce i propri dati di identificazione:

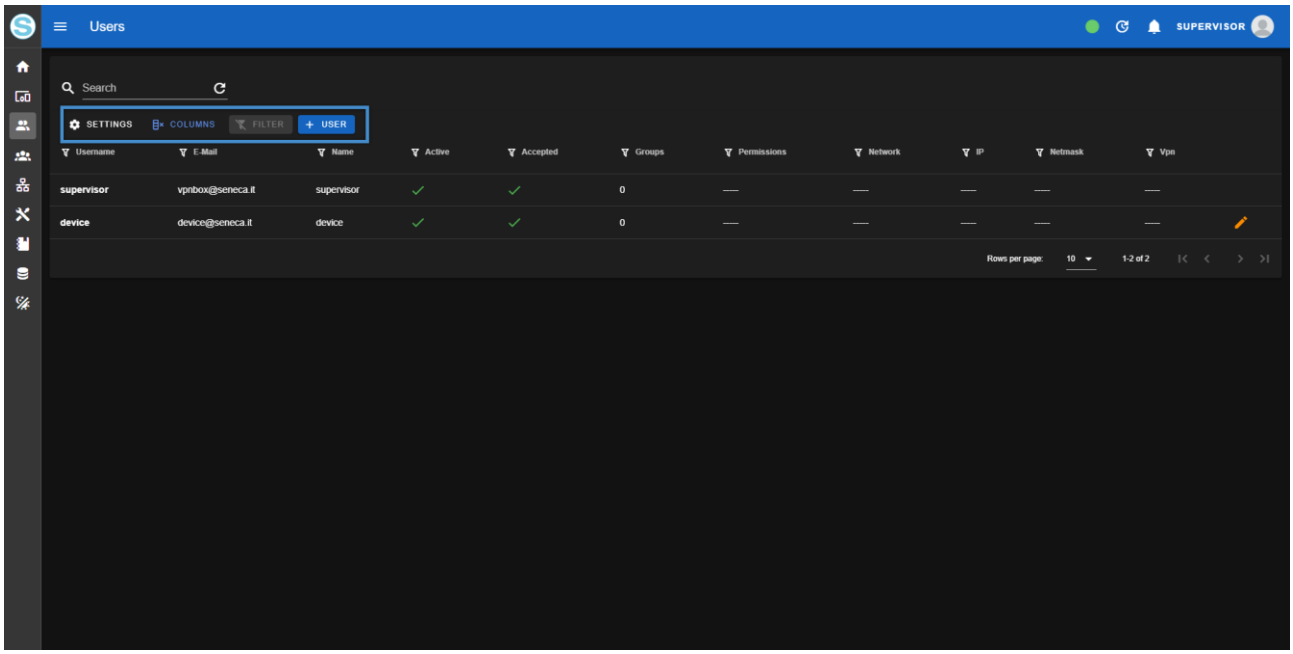
- *il suo indirizzo MAC,*
- *l'IMEI (se dotato di modem),*
- *il nome del TAG (identificativo scelto dall'utente ed inserito nella configurazione del device tramite la sua pagina web)*
- *la configurazione della rete locale LAN del device.*

7.3. USERS

La sezione Users contiene l'elenco di tutti gli utenti abilitati ad effettuare il login sul server VPN BOX2. Il contenuto della pagina è diviso in due parti: la lista utenti in forma tabellare (1) e l'area comandi/azioni (2). Comparirà un pulsante di modifica e di elimina in corrispondenza a ciascuna riga utente ad eccezione dei due account di sistema "device" e "supervisor":

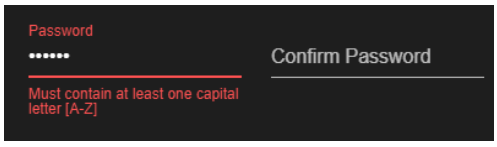


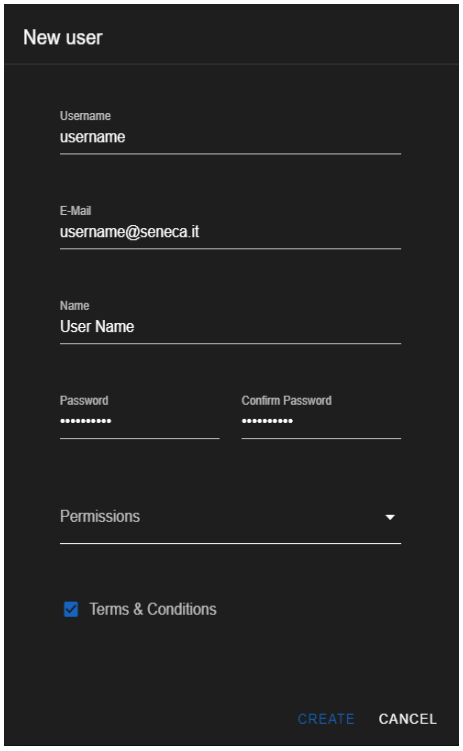
La parte alta della pagina permette di filtrare gli utenti con ricerca full text:

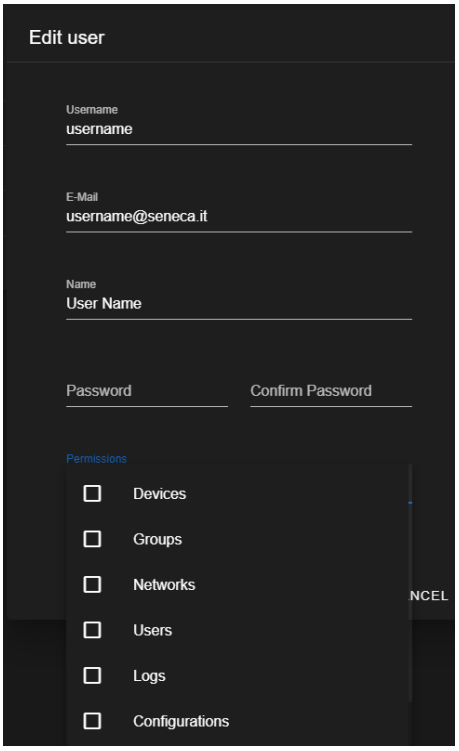


Cliccando sul pulsante "+ User" comparirà il popup di inserimento nuovo utente tramite il quale sarà possibile introdurre i suoi dati e credenziali. Confermare l'inserimento con il pulsante "Create".

In caso di errore di inserimento o di vincoli non rispettati sul campo (es. Password che non rispetta i requisiti minimi di sicurezza) il valore verrà evidenziato con colorazione rossa del testo e subito sotto il campo editabile comparirà un suggerimento per guidare l'utente nella correzione.





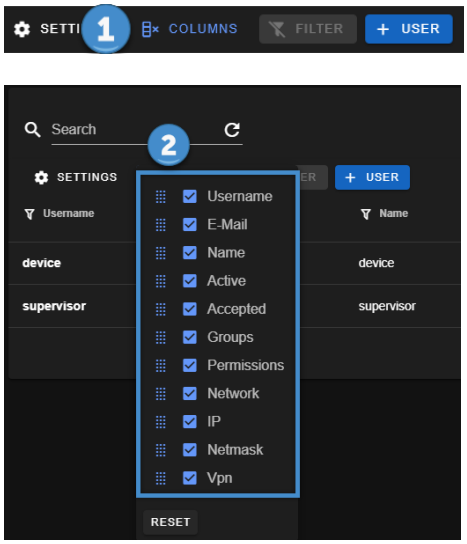


Il significato di ciascun parametro è riportato nella seguente tabella:

Parametro	**Significato**
Username	Nome breve dell'utente
E-Mail	Indirizzo E-Mail dell'utente. Può essere valido o non valido. È richiesto un indirizzo valido nel caso di attivazione del servizio di autenticazione 2FA con relativa abilitazione del servizio di invio mail: Amministrazione del server > Config. Snmp
Name	Nome dell'utente esteso
Password/Confirm Password	Password dell'utente da digitare 2 volte per verifica corretta introduzione da tastiera
Permissions	Elenco da spuntare per selezionare tutti i privilegi da assegnare all'utente. I privilegi disponibili e relativa funzione sono di seguito riportati **Devices**: permette di gestire i dispositivi e di visualizzare la relativa pagina del menù **Groups**: permette di gestire i gruppi e di visualizzare la relativa pagina del menù **Metworks**: permette di gestire le reti VPN e di visualizzare la relativa pagina del menù **Users**: permette di gestire gli utenti e di visualizzare la relativa pagina del menù **Logs**: permette di visualizzare la pagina dei log di sistema dell'applicazione VPN BOX2 **Configurations**: permette di gestire le configurazioni del server VPN BOX2. Si vedano capitoli Amministrazione del server > Config.

	System: crea una replica dell'utente "supervisor" assegnando all'utente che si sta creando i massimi privilegi sul sistema.
Term & Conditions	Da spuntare per accettare i termini di servizio del software VPN BOX2

Cliccando sul pulsante "Columns" (1) è possibile controllare le impostazioni di visualizzazione della tabella quali ordinamento delle colonne e quali visualizzare/nascondere (2):



Ogni utente creato avrà la possibilità di accedere al VPN BOX2 tramite la Login via browser ma non ha ancora la possibilità di collegarsi con la VPN ai dispositivi. Per fare ciò è necessario creare un Gruppo di accesso che metterà in relazione un certo numero di utenti con i device ai quali potrà accedere e soprattutto con la relativa modalità di accesso da utilizzare SL o P2P.

Per procedere nella configurazione si veda il paragrafo Amministrazione del server > Groups.

Gli utenti possono essere aggiunti, modificati ed eliminati a piacere; chiaramente, se un account viene cancellato mentre è in uso, questo verrà effettivamente chiuso solo nel momento in cui si disconnette dalla VPN.

ATTENZIONE!

Username e password fanno distinzione tra maiuscole e minuscole.

7.4. GROUPS

Questa sezione rappresenta l'elemento di connessione tra utenti, dispositivi e modalità di accesso VPN (SL o P2P). Ogni gruppo può contenere un sottoinsieme di dispositivi ed utenti. In particolare valgono le seguenti regole:

- *Un utente può appartenere a più gruppi*
- *Un dispositivo può appartenere ad uno e un solo gruppo però può essere spostato di gruppo all'occorrenza*
- *Il gruppo di appartenenza definisce la modalità di accesso VPN al dispositivo*

Esempio:

Supponiamo di avere due utenti chiamati X e Y e 4 dispositivi Seneca Z, X, Q, K. Vogliamo configurare il server VPN BOX2 in modo che l'utente X possa vedere tutti i device mentre l'utente Y solo Q e K.

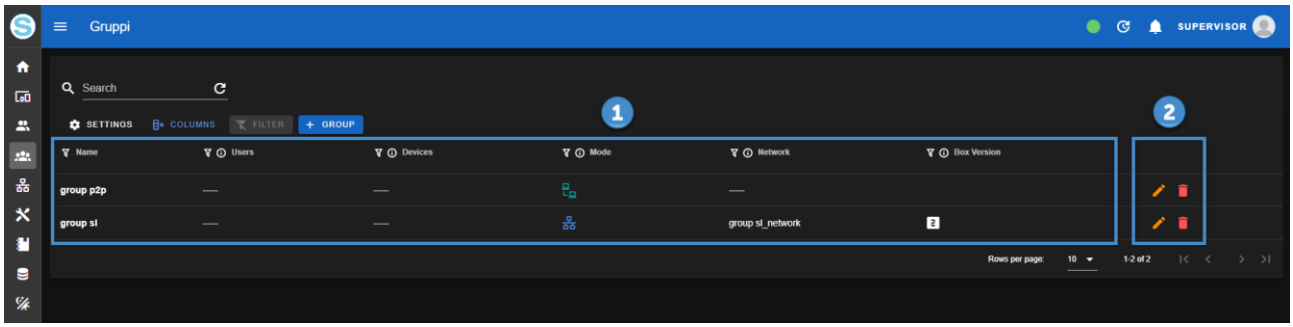
Per fare ciò dovremo creare due gruppi:

- *Un gruppo 1 contente i device Z, X*
- *Un altro gruppo 2 con solo Q e K.*

l'assegnazione utenti-gruppi dovrà essere effettuata nel seguente modo:

- *Utente X appartenente ad entrambi i gruppi 1 e 2*
- *Utente Y appartenente solo al gruppo 2*

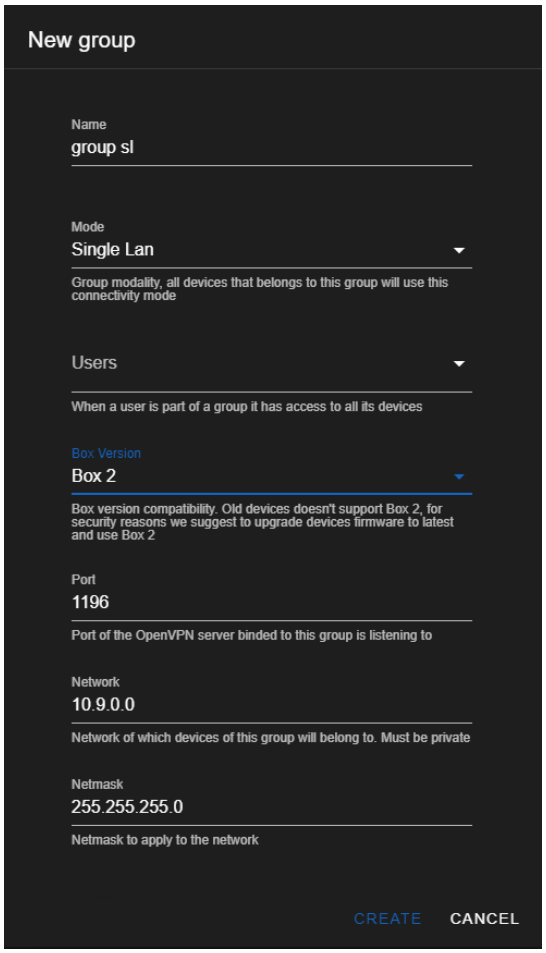
Il contenuto della pagina è diviso in due parti: la lista gruppi in forma tabellare (1) e l'area comandi/azioni (2) con i pulsanti in corrispondenza a ciascuna riga Gruppo:



Cliccando sul pulsante "+ Group" comparirà il popup di inserimento nuovo utente tramite il quale sarà possibile introdurre i suoi campi di configurazione e confermare l'inserimento con il pulsante "Create".

I campi di configurazione del gruppo dipendono dalla modalità di accesso VPN prevista per tale Gruppo (Mode). Nelle tabelle che seguono sono riportate tutti i possibili campi di configurazione.

Modalità di accesso VPN Single LAN (Mode = Single LAN):

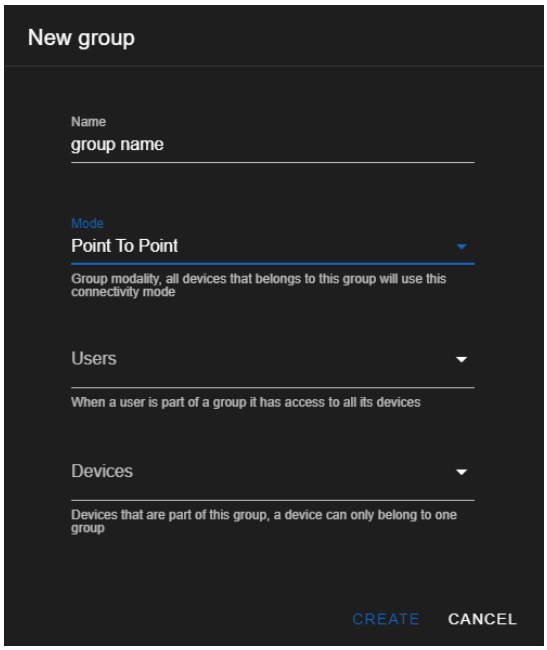


Parametro	Significato
Name	Nome del Gruppo
Mode	Modo operativo della VPN
Users	Utenti che fanno parte del Gruppo. Espandere il menù a tendina e selezionare
Box Version	Versione del protocollo di comunicazione tra device e vpnbox. Utilizzare Box 1 se si dispone di device del tipo Z-TWS4, Z-PASS1, Z-PASS2 viceversa selezionare Box 2
Port	Porta TCP utilizzata per tutte le connessioni dei device e utenti appartenenti a questo gruppo. Si rimanda al paragrafo Configurazione del Router nel capitolo “Principio di funzionamento vpn” del modo operativo SL
Network	Indica lo spazio degli indirizzi VPN virtuali che verranno assegnati a dispositi e utenti quando saranno connessi a questo gruppo.
Netmask	Utilizzata insieme al parametro Network per indicare quanti indirizzi IP predisporre per la sottorete. di indirizzi virtuali VPN.

ATTENZIONE!

Il parametro Network non dovrà mai essere coincidente con una rete fisica già esistente altrove. Nel modo Single LAN è importante che una rete utilizzata nella LAN di un dispositivo remoto (es. 192.168.90.0/255.255.255.0) non venga mai utilizzata in altri dispositivi o nel server VPN BOX2 stesso.

Modalità di accesso VPN Point to Point (Mode = Point to Point):



Parametro	**Significato**
Name	Nome del Gruppo
Mode	Modo operativo della VPN
Users	Utenti che fanno parte del Gruppo. Espandere il menù a tendina e selezionare
Devices	Dispositivi che fanno parte del Gruppo. Espandere il menù a tendina e selezionare

7.5. NETWORKS (VPN)

Questa sezione permette di gestire le Network VPN ovvero le risorse di connessione tra utenti e dispositivi. Sono anch'esse di due tipologie SL e P2P come i gruppi. In una configurazione mista in cui il VPN BOX2 deve essere utilizzato sia per connessioni SL che P2P dovranno essere create altre reti tramite questa pagina.

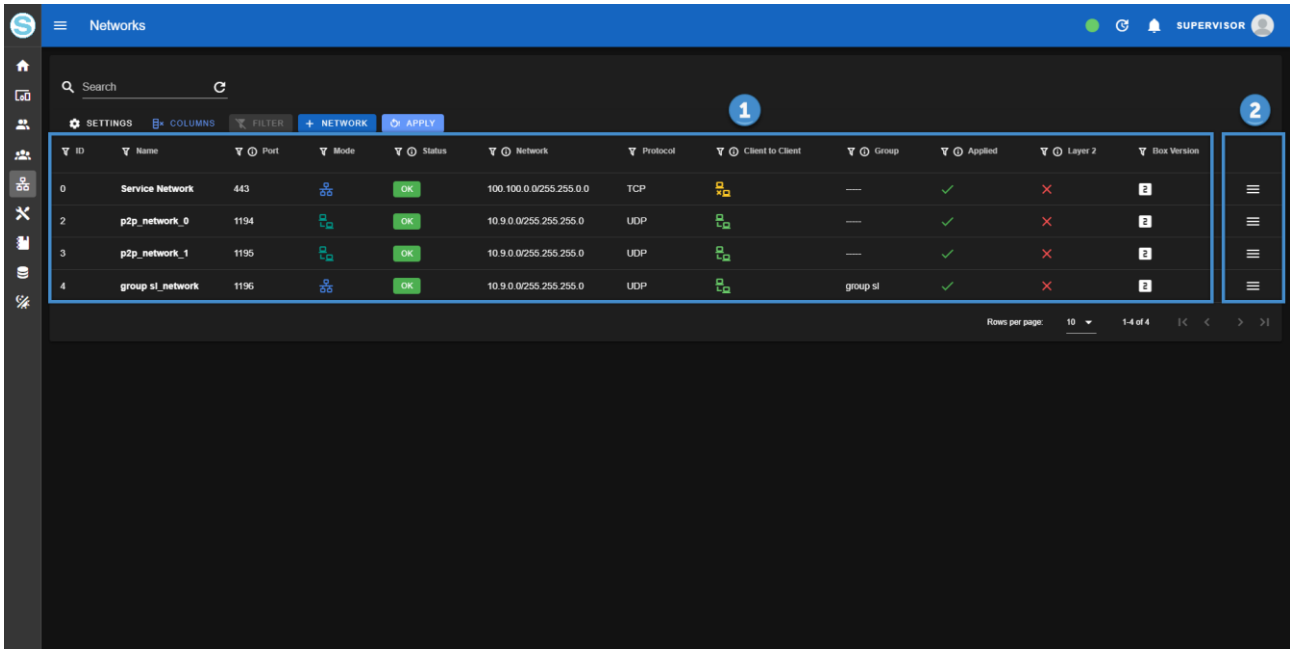
ATTENZIONE!

Il wizard di prima configurazione del VPN BOX2 inserirà tutte network della sola tipologia selezionata nella procedura ma sarà sempre possibile in seguito aggiungere ulteriori risorse. L'unica cosa da tener presente è che ad ogni network corrisponderà una porta TCP/UDP aggiuntiva da aprire come regola di NAT in ingresso sul firewall dove è esposto il servizio VPN BOX2.

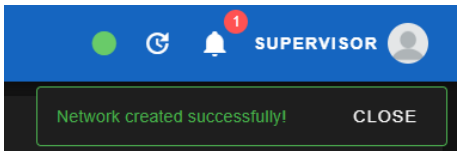
A seconda della tipologia di network creata valgono le seguenti restrizioni:

- *Una Network SL può permettere la connessione più utenti e device contemporaneamente*
- *Una Network P2P permette la connessione di solo 1 device P2P alla volta, eventualmente con più utenti che lo richiedono.*
- *Un secondo device che richiede l'accesso ad una Network P2P verrà connesso ad un'altra Network P2P, la prima disponibile*
- *Il monitoraggio e l'assegnazione della prima Network P2P disponibile viene effettuata dal VPN BOX2 stesso e segnalato ai device e utenti tramite il canale di servizio HTTPS/MQTTS sempre attivo.*

Il contenuto della pagina è diviso in due parti: la lista delle network in forma tabellare (1) e l'area comandi/azioni (2):

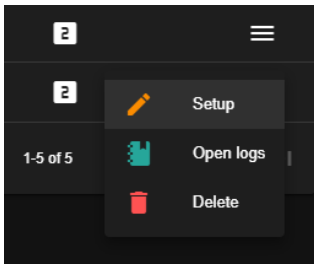


La conferma dell'operazione o un eventuale errore viene segnalato in altro a destra nell'area di notifica:

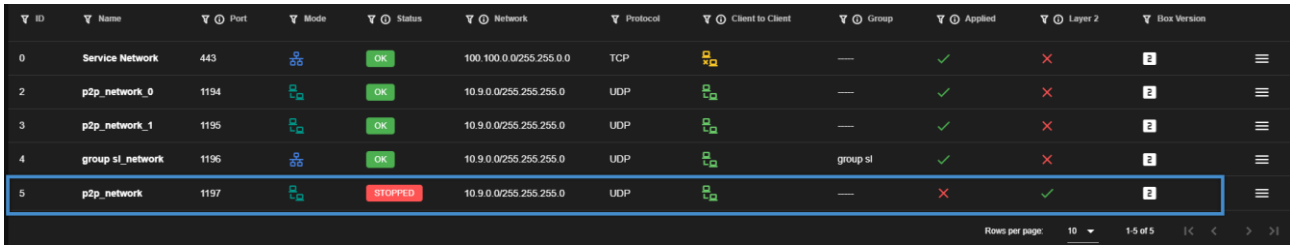


Cliccando nel menu azioni in corrispondenza ad una Network è possibile eseguire le operazioni di:

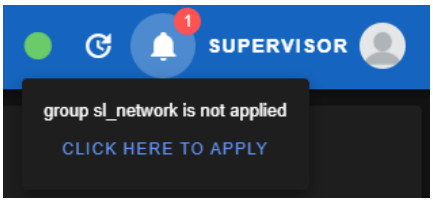
- *Setup: apre il popup con le impostazioni della Network*
- *Open logs: link diretto alla pagina logs con il filtro preimpostato sui log della sola Network selezionata*
- *Delete: cancellazione della Network*

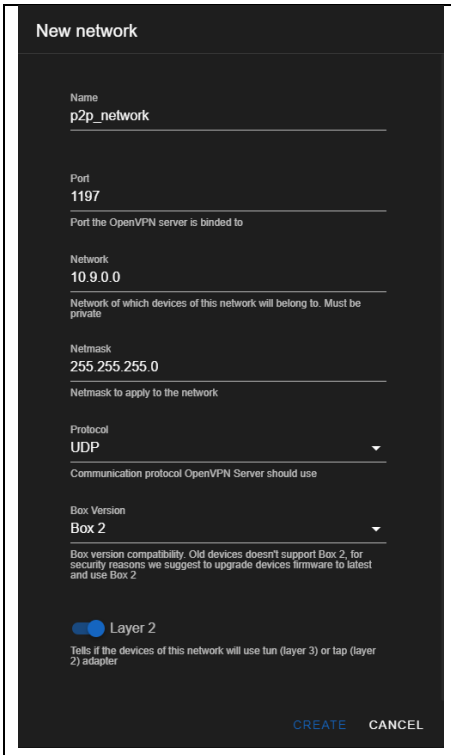


Subito dopo l'inserimento di una nuova network il relativo stato sarà "stopped" e la rete non sarà operativa fino ad avvenuta conferma da parte dell'utente.



Sarà possibile confermare la configurazione ed applicare le impostazioni cliccando il pulsante "apply" oppure cliccando nell'area di notifica della barra alta e confermando l'operazione con "click here to apply":



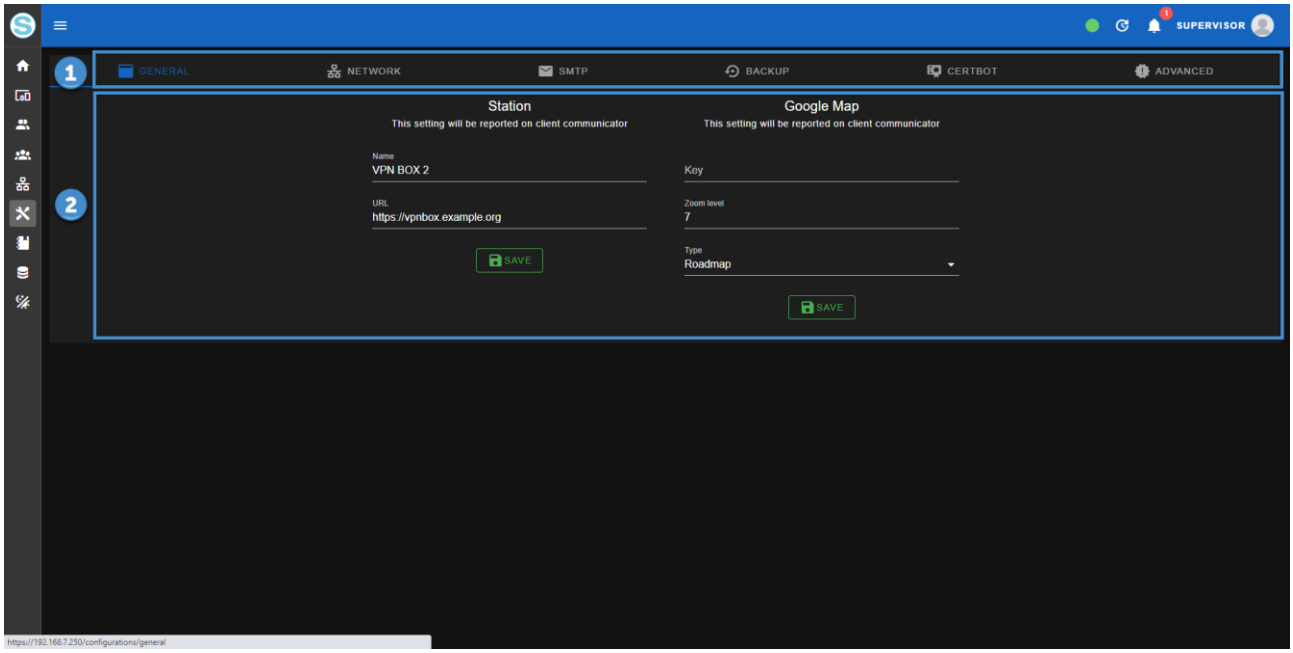


Parametro	Significato
Name	Nome del Gruppo
Port	Porta TCP o UDP utilizzata per tutte le connessioni dei device e utenti appartenenti a questo gruppo.
Network	Indica lo spazio degli indirizzi VPN virtuali che verranno assegnati a dispositivi e utenti quando saranno connessi a questo gruppo.
Netmask	Utilizzata insieme al parametro Network per indicare quanti indirizzi IP predisporre per la sottorete. di indirizzi virtuali VPN.
Protocol	Protocollo di comunicazione utilizzato a livello di trasporto: valori possibili: TCP, UDP. Si consiglia TCP in caso di connessioni dati stabili tra utenti, device e server, viceversa è preferibile UDP
Box Version	Versione del protocollo di comunicazione tra device e vpnbox. Utilizzare Box 1 se si dispone di device del tipo Z-TWS4, Z-PASS1, Z-PASS2 viceversa selezionare Box 2
Layer 2	Permette di attivare una VPN a “basso livello” dove tutto il traffico dati della rete remota risulta accessibile dai pc degli utenti che ne fanno accesso. È possibile selezionarla solo se la Network è di tipo P2P

7.6. CONFIG. GENERAL

Questa sezione permette di gestire le configurazioni del server VPN BOX2.

Il contenuto della pagina è diviso in due parti: la barra di navigazione a tab che suddivide per categorie tutte le configurazioni (1) e la parte principale con l'elenco dei parametri (2).

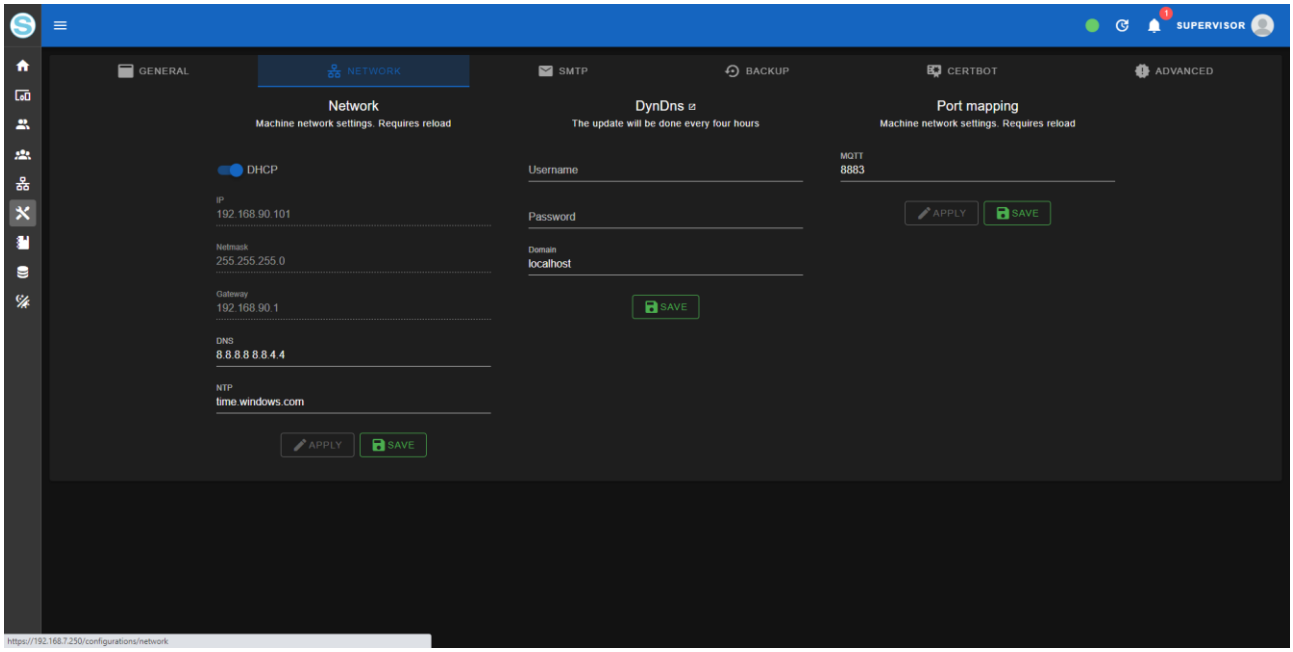


La pagina generale contiene i seguenti parametri:

Parametro	**Significato**
Station / Name	Nome del server che verrà visualizzato nella barra del titolo in modo da identificare più agevolmente il VPN BOX2
Station / URL	Indirizzo completo del server VPN BOX2 (quello che deve essere digitato nella barra degli indirizzi del browser)
Google Map / Key	Per l'utilizzo di questo servizio è necessaria la registrazione al servizio di terze parti Google Maps. Una volta attivo l'account per collegarlo al server VPN BOX2 sarà necessario introdurre il codice API Key in questo campo. Per ulteriori informazioni si consulti il sito web ufficiale del servizio: https://developers.google.com/maps/documentation
Google Map / Zoom Level	Livello di zoom di default della mappa all'apertura della finestra Home
Google Map / Type	Tipo/Stile di mappa utilizzata

7.7. CONFIG. NETWORK

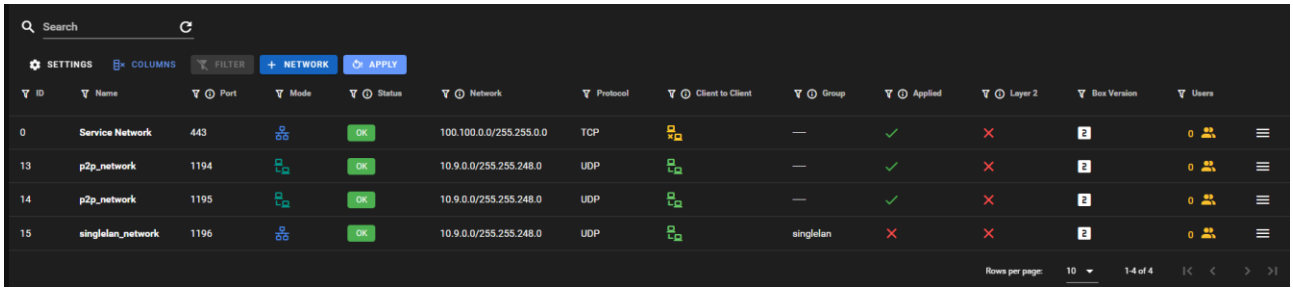
La pagina network contiene i parametri relativi alla porta ethernet del server più qualche servizio che semplifica la raggiungibilità del server tramite l'IP pubblico come ad esempio il servizio Dyndns



Il significato di ciascun parametro è riportato nella seguente tabella:

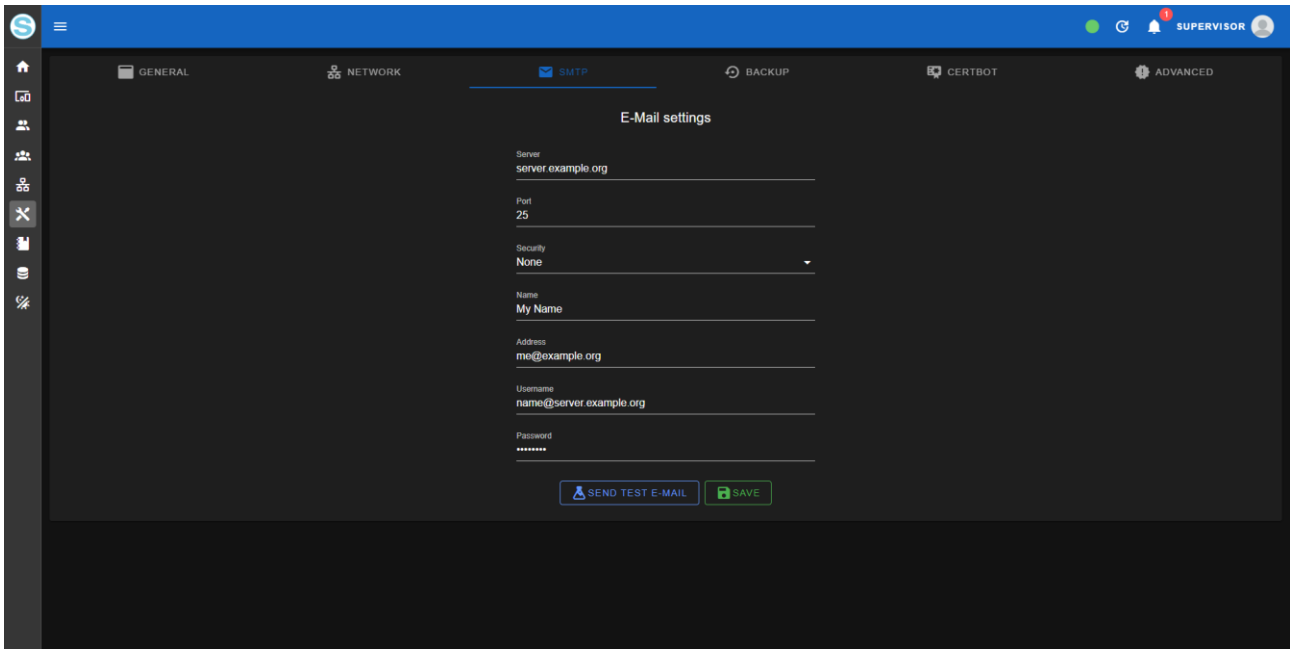
Parametro	**Significato**
Network / *	Si veda la sezione "prima configurazione del vpnbox2 > network" i parametri sono dello stesso tipo
Dyndns / Username	Per l'utilizzo di questo servizio è necessaria la registrazione al portale di terze parti DynDns.IT una volta attivo l'account per collegarlo al server VPN BOX2 sarà necessario introdurre le credenziali dell'account DynDns in questo campo. Per ulteriori informazioni si consulti il sito web ufficiale del servizio: https://dyndns.it/
Dyndns / Password	Password dell'account DynDns.IT da collegare al server VPN BOX2
Dyndns / Domain	Il nome del dominio creato in DynDns.IT ad esempio: myvpnbox2.ns0.it
Port mapping / MQTT	I dispositivi compatibili con il protocollo di servizio realtime del VPN BOX2 utilizzano una porta dedicata per la comunicazione in tempo reale con il server. Nel caso la porta qui indicata risultasse non disponibile o già impegnata sul firewall perimetrale è possibile modificarla con una a scelta dell'IT manager. In ogni caso il device se non dovesse trovare aperta la porta qui indicate tenterà l'utilizzo della 443/TCP che deve essere sempre aperta per il corretto funzionamento dell'applicazione.

Tramite l'icona gialla è possibile verificare gli uenti attualmente connessi alla network:



7.8. CONFIG. SNMP

La pagina snmp contiene i parametri per impostare l'invio email di notifica verso gli utenti del Sistema:



Il significato di ciascun parametro è riportato nella seguente tabella:

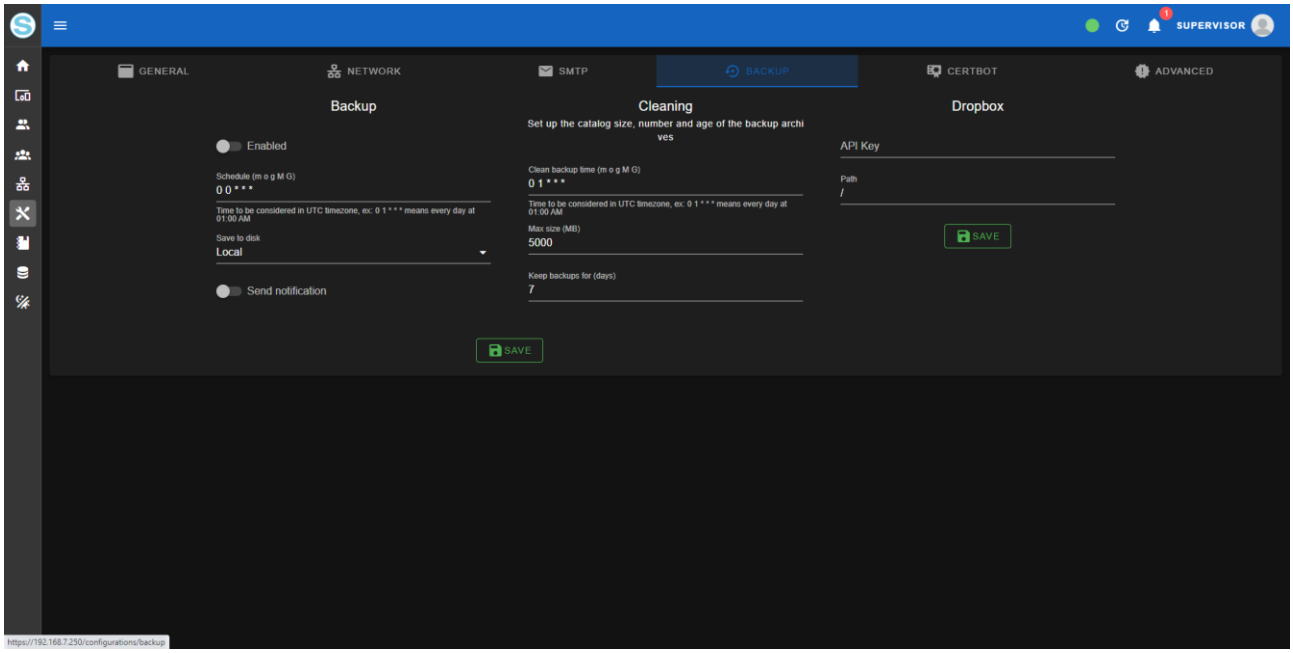
Parametro	**Significato**
Server	Per l'utilizzo di questa funzione è necessaria la registrazione ad un servizio email di terze parti o disporre di un account email presso un provider che preveda l'utilizzo del protocollo SMTP o SMTPS per l'invio delle Email.
Port	Porta utilizzata dal mail server del provider.
Security	Livello di sicurezza utilizzata per la comunicazione con il mail server. valori possibili: NONE, SSL, TLS.

Name	Nome utente dell'account creato presso il provider. Suggerimento: in molti casi coincide con lo Username. In ogni caso fare riferimento alla documentazione tecnica di supporto disponibile sul sito del provider email.
Address	Indirizzo Email dell'account creato presso il provider. Risulterà come mittente di tutte le Email inviate dal server VPN BOX2 agli utente.
Username	Username dell'account creato presso il provider.
Password	Password dell'account creato presso il provider.

7.9. CONFIG. BACKUP (AUTOMATICI)

Questa funzione crea un'immagine della configurazione del VPN Box che può essere salvata come file locale o inviata ad un servizio Dropbox del cliente per uso futuro.

Si consiglia di eseguire spesso il backup dell'intera configurazione per non perdere alcun dato:



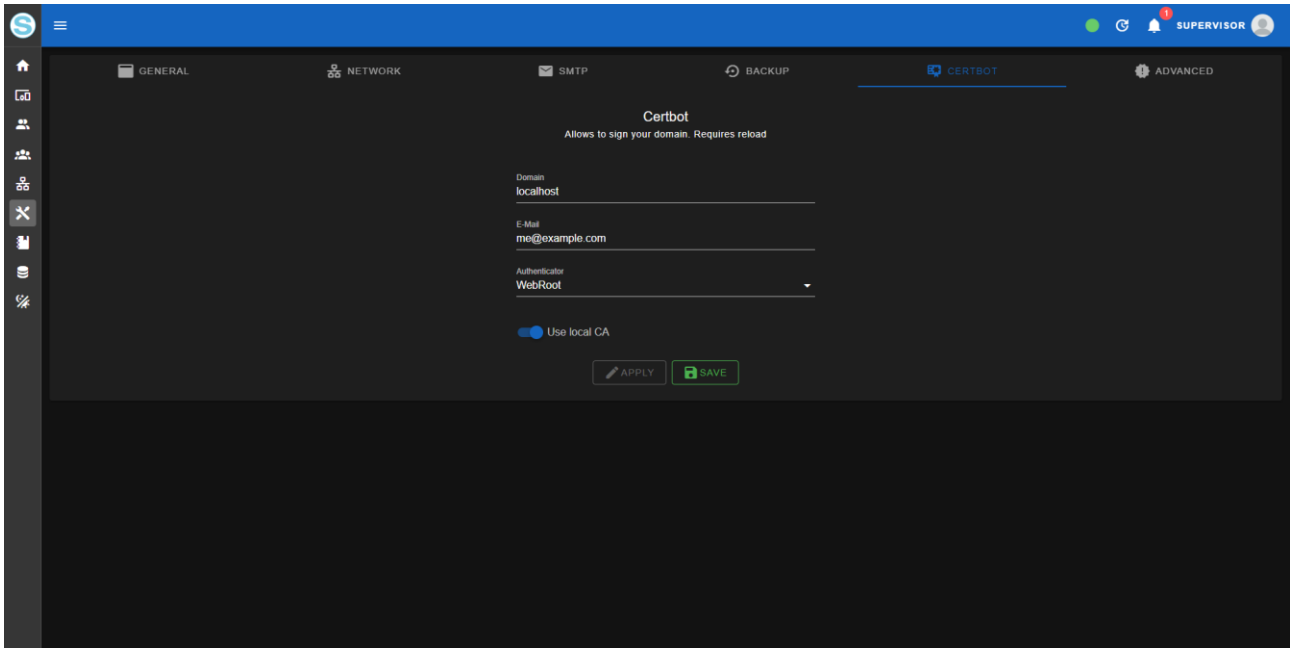
Il significato di ciascun parametro è riportato nella seguente tabella:

Parametro	**Significato**
Backup / Enabled	Abilitazione della funzione di backup automatico
Backup / Schedule	Schedulazione dell'avvio automatico del backup secondo il formato di seguito descritto: * * * * * Min Hour Day of the month Month Day of the week
Backup / Save to disk	Indica se il salvataggio del backup deve essere effettuato nella memoria interna o sul servizio Dropbox.
Backup / Send notification	Al termine dell'operazione invia una Email per informare gli utenti con privilegi "System" dell'esito dell'operazione.
Cleaning / Clean backup time	Schedulazione dell'attività periodica di cancellazione dei backup vecchi. Il formato è lo stesso utilizzato per il parametron Backup / Schedule.

Cleaning / Max size	Verrà eseguita la cancellazione dei backup vecchi se la memoria complessiva utilizzata dallo storage di backup è superiore a questo parametro.
Cleaning / Keep backup for	Verrà eseguita la cancellazione dei backup più vecchi di un numero di giorni superiore a questo parametro.
Dropbox / API Key	Per l'utilizzo di questo servizio è necessaria la registrazione al servizio di terze parti Dropbox. Una volta attivo l'account per collegarlo al server VPN BOX2 sarà necessario introdurre l'apikey del servizio in questo campo. Per ulteriori informazioni si consulti il sito web ufficiale del servizio: https://www.dropbox.com/home
Dropbox / Path	È possibile tramite questo parametro specificare il percorso dedicato dove salvare i backup

7.10. CONFIG. CERTBOT

La pagina Certbot contiene i parametri relativi al servizio di rilascio automatizzato dei certificati SSL/TLS per l'accesso dal browser via HTTPS al VPN BOX2:



Il significato di ciascun parametro è riportato nella seguente tabella:

Parametro	**Significato**
Dominio	Dominio da registrare, deve corrispondere a quanto viene scritto nella barra dell'indirizzo del proprio browser per raggiungere il server VPN BOX2 ad es. vpn.acme.com
E-mail	Indirizzo mail di un referente del server da indicare al provider CertBot Let's Encrypt per essere contattati in caso di segnalazioni relative all'uso del certificato per il dominio indicato.
Authenticator	È il metodo di verifica utilizzato da certbot per verificare l'autenticità del server su cui verrà caricato il certificato sicuro firmato da Let's Encrypt. Ad avvenuta autenticazione il browser mostrerà nella barra dell'indirizzo l'icona di "connessione sicura"
Use local CA	Se impostato a ON utilizza dei certificati non validi, generati in modo random. Il browser da cui si sta accedendo al server mostrerà la scritta "Non sicuro" ma la connessione avverrà comunque utilizzando la cifratura TLS. L'impostazione Use local CA ad ON permetterà di aggirare temporaneamente qualsiasi problematica relativa al meccanismo di autenticazione ed ottenimento dei certificati validi firmati. Per attivare il meccanismo di funzionamento Certbot è necessario impostare Use local CA ad OFF e salvare la configurazione.

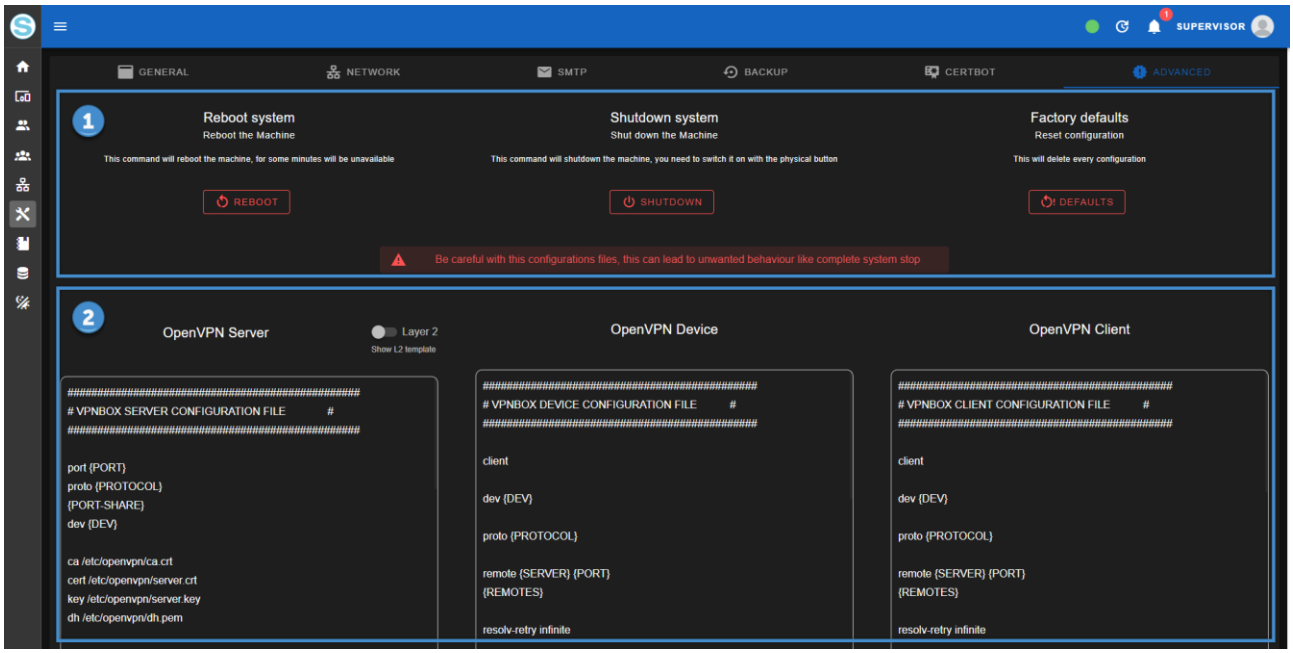
7.11. CONFIG. ADVANCED

La pagina advanced è divisa in due sezioni: nella parte alta (1) sono riportati i comandi di manutenzione: Reboot del sistema, Spegnimento del sistema e Ripristino a default di fabbrica.

ATTENZIONE!

Prima di procedere ad un eventuale ripristino a default di fabbrica verificare di disporre di un backup recente dell'intera applicazione su supporto esterno e NON sul disco del VPN BOX2 stesso.

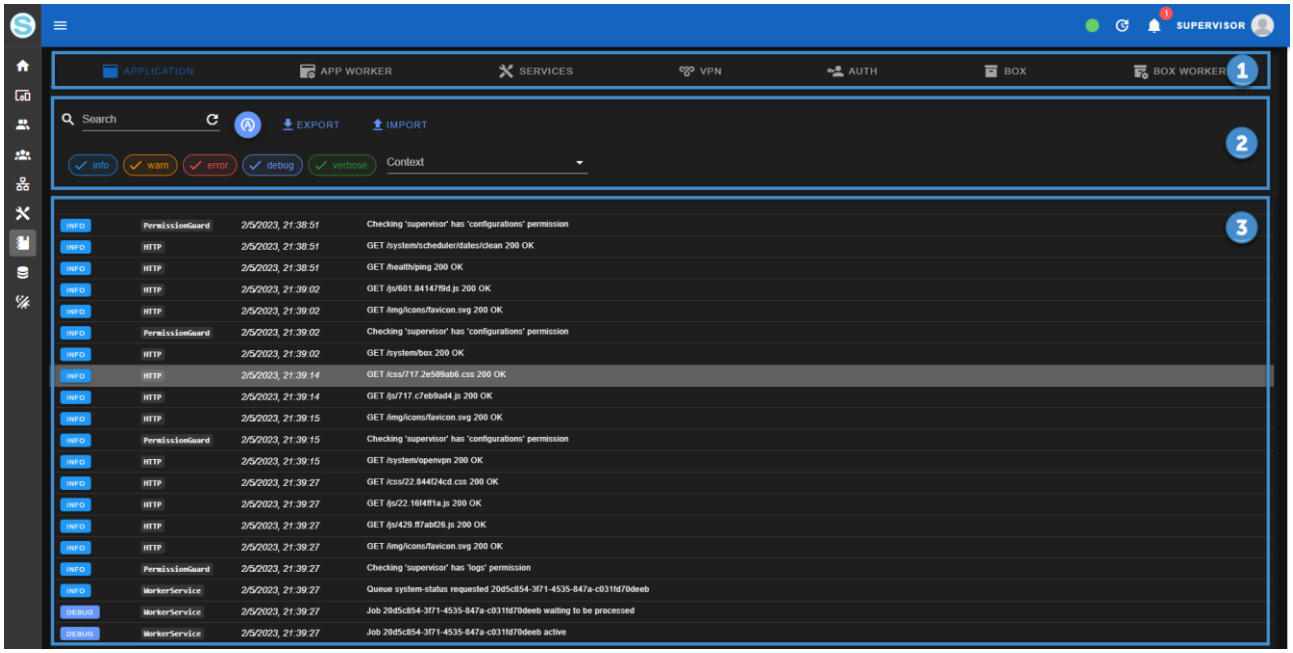
Nella parte bassa (2) contiene le configurazioni che permettono la massima flessibilità della configurazione del server VPN BOX2 ma sono da utilizzare solo per casi di estrema necessita. I template di configurazione suggeriti sono quelli che garantiscono di massimizzare la compatibilità con i device e la stabilità delle comunicazioni basate sia su LAN/WAN che su Mobile.



7.12. LOGS

La sezione logs è utile per verificare lo stato dei servizi in caso di errori. È suddiviso per tipologia di Servizi attraverso i quali è possibile navigare selezionando i rispettivi tab (1).

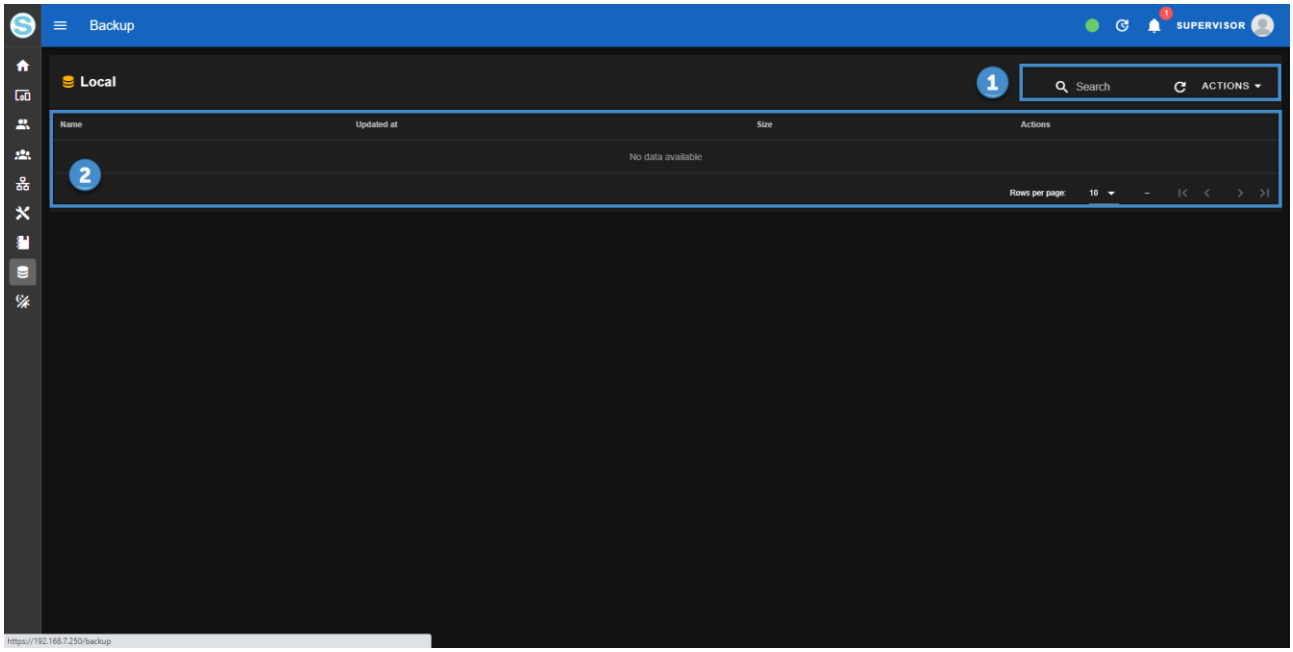
È possibile inoltre filtrare (2) la visualizzazione ricercando un testo specifico o scegliendo gli eventi per gravità in modo da ottenere una rappresentazione meno dispersiva degli eventi nella sezione dei contenuti (3).



Dalla vista corrente è possibile esportare i log in formato CSV.

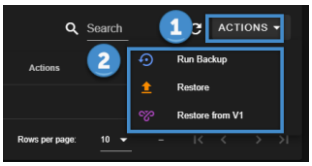
7.13. BACKUP

La pagina backup permette di visualizzare tutti i backup automatici presenti nel sistema (2) e di eseguirne di nuovi manualmente tramite il menù actions (1)



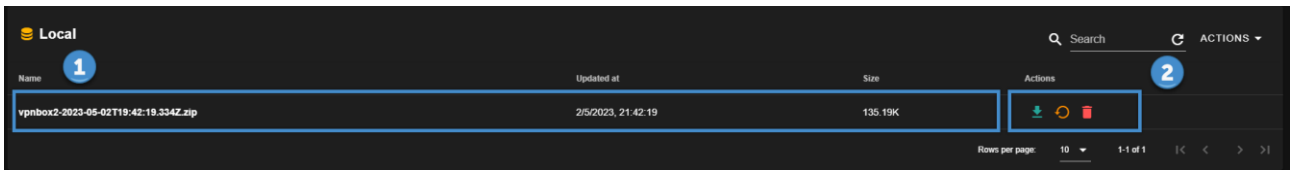
Espandendo il menu (1) le operazioni (2) possibili sono:

- *Run Backup: avviare manualmente un backup che al termine comparirà nell'elenco con gli altri*
- *Restore: caricare un file di backup esterno per ripristinarlo sul VPN BOX2 in uso.*
- *Restore from V1: caricare un file di backup della precedente versione di server VPN BOX e ripristinarlo con opportuna migrazione sul VPN BOX2 in uso.*



In corrispondenza ad ogni riga di backup verrà registrata la data ora di esecuzione ed un pannello Azioni (2) relativo al backup stesso con le quali sarà possibile rispettivamente:

- *Scaricare il backup selezionato sul pc locale dell'utente*
- *Ripristino del backup selezionato*
- *Eliminazione del backup selezionato*

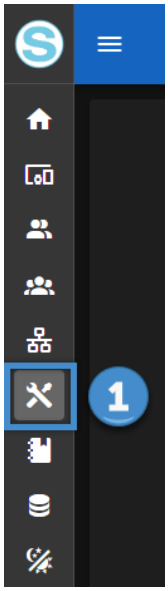


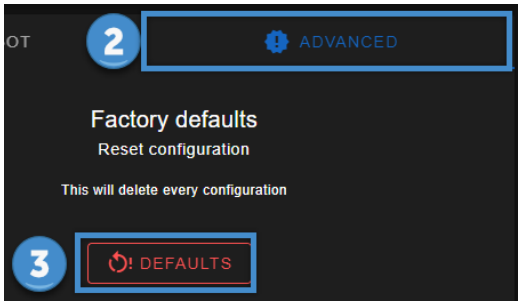
8. RESET DI FABBRICA ED AGGIORNAMENTO DEL VPN BOX2

8.1. RESET DI FABBRICA

Il ripristino delle impostazioni di fabbrica viene eseguito con comando dedicato accessibile nella sezione del menu configurazione. Per eseguire il reset di fabbrica procedere come segue:

- *Entrare nel menù configurazione (1)*
- *Selezionare la tab "advanced" (2)*
- *Cliccare sul pulsante "defaults" (3) in corrispondenza alla sezione "Factory defaults"*





8.1. AGGIORNAMENTO DI VPN BOX2

L'aggiornamento dell'applicativo VPN BOX2 si può avviare nel seguente modo:

- *Nella barra alta selezionare l'icona "Aggiornamento firmware"*
- *Spuntare la voce "Upload file" (1)*
- *Selezionare il file zip di aggiornamento (2)*
- *Confermare cliccando sul pulsante "upload" (3)*
- *Attendere completamento dell'upload e riavvio dell'applicazione*

9. CONFIGURAZIONE DEL ROUTER/FIREWALL SUL SERVER VPNBOX2

I Servizi di rete del VPN BOX2 sono esposti sull'interfaccia ethernet locale del server e per essere accessibili dai device e utenti remoti dovranno essere pubblicati all'esterno della rete tramite delle regole da introdurre sul firewall perimetrale.

Nella tabella seguente viene fatto l'elenco delle porte utilizzate dai vari Servizi.

Alcune di queste sono opzionali in quanto connesse a servizi accessori che possono essere temporaneamente richiesti e poi disattivati.

È opportuno notare inoltre che alcune, contrassegnate con (*), hanno un valore di default ma tramite la pagina Config. Network (VPN) è possibile cambiarne i valori per sottostare alle proprie policy di sicurezza aziendale.

Porta	Tipo	Necessaria	**Ingresso/uscita**	Descrizione
443	TCP	Sì	Sì	Canale VPN e, in opzione, tutte le altre comunicazioni se le porte opzionali sono chiuse.
1194 (*)	TCP/ UDP	Opzionale	Sì	Porta VPN dedicata all'uso della **prima** Network VPN.
1195 (*)	TCP/ UDP	Opzionale	Sì	Porta VPN dedicata all'uso della **seconda** Network VPN.
…	…	Opzionale	Sì	La configurazione delle porte è dinamica in funzione del numero di accessi contemporanei richiesti al server (vedi capitoli precedenti).
80	TCP	Opzionale	Solo Uscita	Utilizzata dal servizio Certbot per la procedura di validazione automatica del certificato SSL/TLS del webserver. Diventa obbligatoria solo se il servizio Certbot viene utilizzato per il server VPN BOX2
22	TCP	Opzionale	Sì	Nel caso sia richiesto supporto tecnico da parte del Service Seneca

(*) la porta può essere modificata all'occorrenza dal menu "Networks" nel caso risultasse già impegnata da altri Servizi che condividono lo stesso IP pubblico del VPN BOX2.

Inizialmente il sistema tenterà di utilizzare la porta 443 assieme alle porte 1194, 1195, ...

Nel caso le porte 1194,1195… siano chiuse il VPNBOX2 utilizzerà solamente la 443, in questo caso l'overhead della comunicazione risulta superiore, quindi per ottenere le massime prestazioni è consigliato aprire anche le porte 1194, 1195, ...

Queste porte devono essere aperte sul router, quindi non filtrate da un'eventuale regola del firewall. Devono poi essere reindirizzate dal router, dall'esterno verso l'interno, modificando il NAT e facendole convergere verso l'indirizzo IP locale del VPN BOX: sui router commerciali, questa opzione è normalmente chiamata "Virtual Server" o " Port Mapping".

Al termine della configurazione annotare l'indirizzo pubblico IP del router, necessario (con relativa password) per la configurazione VPN dei dispositivi SENECA. Fare riferimento al proprio amministratore di sistema su come acquisire questo indirizzo IP.

La modifica dei "Virtual Server" o del "Port Mapping" del router è obbligatoria solo se il VPN Box2 è in una LAN (indirizzi 192.168.x.x, 10.x.x.x e 172.x.x.x), se è installato su una rete pubblica (quindi con indirizzo IP pubblico visibile dal Internet) non sarà necessaria alcuna configurazione del router.

10. CONFIGURAZIONE DEL ROUTER/FIREWALL SUI CLIENT PC E SUI DEVICE REMOTI

La configurazione del router/firewall del device o del PC in cui viene avviato il client deve essere conforme alla seguente tabella:

Porta	Tipo	Necessaria	**Ingresso/uscita**	Descrizione
443	TCP/ UDP	Sì	Solo uscita	Canale di servizio necessario per comunicare tra device, user (VPN Client Communicator) e VPN BOX2.
1194 (*)	TCP/ UDP	Opzionale	Solo uscita	Porta VPN dedicata all'uso della **prima** Network VPN.
1195 (*)	TCP/ UDP	Opzionale	Solo uscita	Porta VPN dedicata all'uso della **seconda** Network VPN.
…	…	…	Solo uscita	La configurazione delle porte è dinamica in funzione del numero di accessi contemporanei richiesti al server (vedi capitoli precedenti).

*= numero di porta modificabile da configurazione

Generalmente nei device remoti basati su connessione cellulare (ad esempio Z-PASS2-RT) le porte sono già aperte dall'operatore telefonico della SIM utilizzata.

Inizialmente il client tenterà di utilizzare la porta 443 assieme alla porta 1194,...

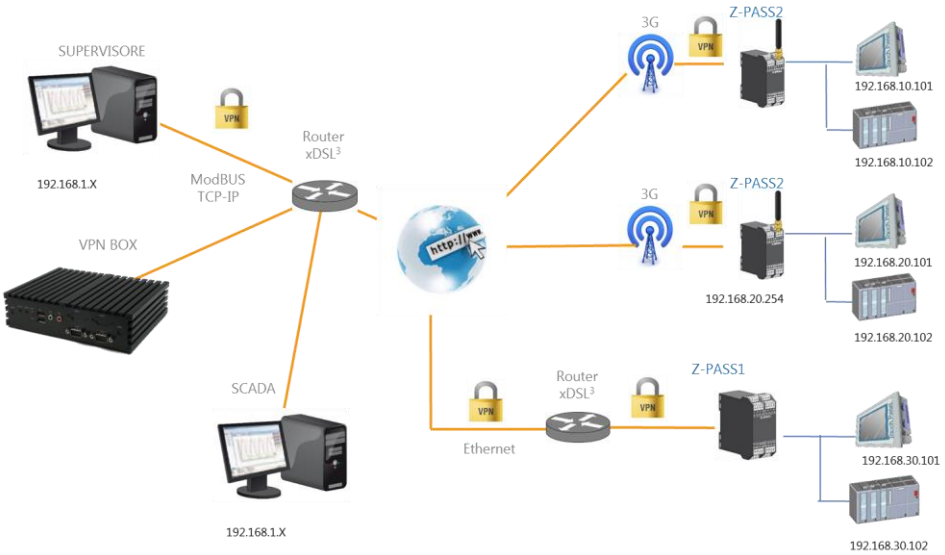
Nel caso la porta 1194,… sia chiusa il client utilizzerà solamente la 443, in questo caso l'overhead della comunicazione risulta superiore, quindi per ottenere la massime prestazioni è consigliato aprire in uscita anche la porta 1194, …

11. PRINCIPIO DI FUNZIONAMENTO VPN NETWORK SINGLE LAN (SL)

Questa modalità permette di creare una rete VPN interconnettendo due o più dispositivi con un PC, SCADA o Mobile.

ATTENZIONE!

Questa modalità configura una rete LAN virtuale richiedendo l'assegnazione di diversi IP locali su tutti i dispositivi Seneca appartenenti alla rete, in quanto i client VPN sono tutti connessi contemporaneamente e sempre visibili al resto della rete. Questo requisito è necessario soprattutto se si vuole che siano visibili le reti a valle dei device.



11.1. CONFIGURAZIONE DELLA VPN

La configurazione di un sistema di Telecontrollo (Single Lan) si articola nelle seguenti operazioni:

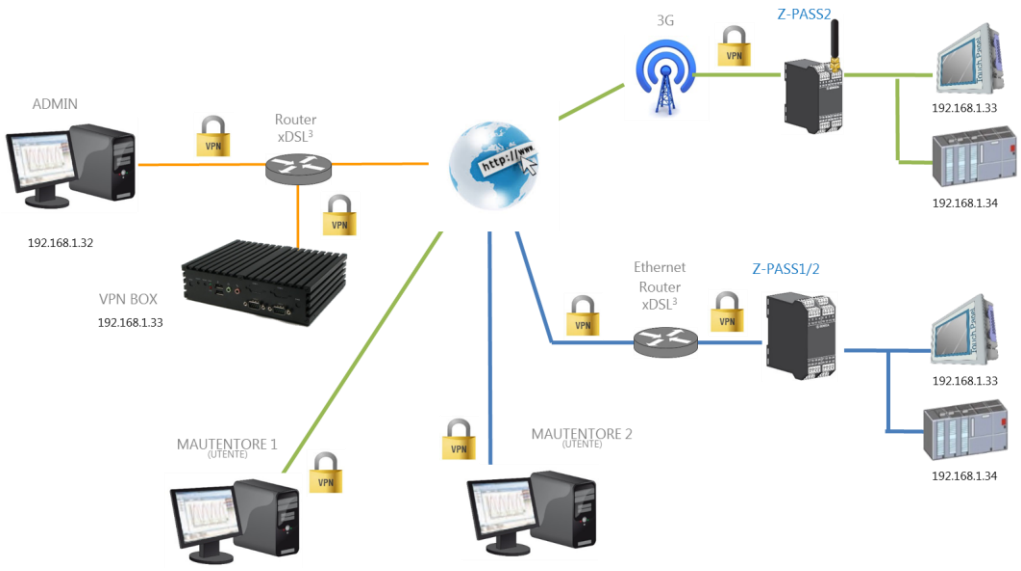
- *Creazione del gruppo Single LAN che conterrà sia gli utenti che i dispositivi*
- *Configurazione dei dispositivi Seneca entrando nelle pagine web degli stessi ed inserendo le credenziali per puntare al VPN BOX2*
- *Nel menù Devices cliccare sul menù azioni di ciascun nuovo device inserito (normalmente essendo nuovi si presentano in colore grigio) cliccare su "Setup" nella proprietà "group" selezionare come gruppo di appartenenza il gruppo Single LAN creato al primo punto*
- *Configurare gli utenti per sistema di telecontrollo*
- *Ritornare al menù gruppi ed inserire gli utenti nel gruppo Single LAN creato e che conterrà già i device*

12. PRINCIPIO DI FUNZIONAMENTO VPN POINT TO POINT (P2P)

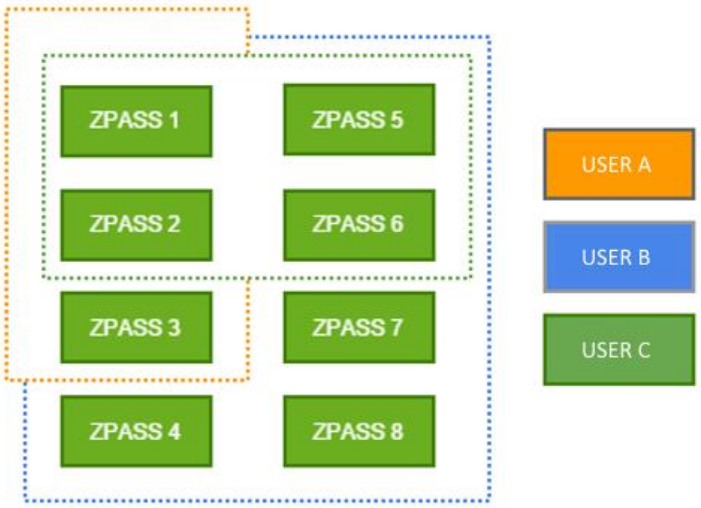
Questo scenario è tipico quando si hanno numerosi siti con sistemi e reti identiche. Poiché non è possibile creare una rete con più indirizzi IP identici, è necessario creare più reti che devono essere indipendenti.

L'utente può scegliere a quale collegarsi per effettuare l'intervento remote di manutenzione. Questa modalità è progettata per scenari di supporto on demand, non è una connessione da utilizzare in modo permanente come Single Lan.

Inoltre è possibile raggruppare i dispositivi e assegnarli agli utenti che devono connettersi: ogni utente potrà quindi connettersi solo ai dispositivi a lui assegnati.



La figura seguente mostra un esempio di utilizzo dei gruppi. Ci sono tre utenti: A, B e C ed in tutto sono a disposizione 8 device remoti a cui accedere secondo la politica di accesso schematizzata con i colori in figura:



Per realizzare questo sarà necessario creare nel VPN BOX2 uno schema di gruppi e utenti del tipo riportato in tabella seguente:

ID Device	ID Gruppo	Appartenenza degli utenti ai Gruppi		
		Utente A	Utente B	Utente C
ZPASS 1 ZPASS 2	Gruppo 1	X	X	X
ZPASS 3	Gruppo 2	X	X	
ZPASS 4 ZPASS 7 ZPASS 8	Gruppo 3		X	
ZPASS 5 ZPASS 6	Gruppo 4		X	X

12.1. CONFIGURAZIONE DELLA VPN

La configurazione di un sistema di Accesso Remoto (Point to Point) si articola nelle seguenti operazioni:

- *Creazione del gruppo P2P che conterrà sia gli utenti che i dispositivi*
- *Configurazione dei dispositivi Seneca entrando nelle pagine web degli stessi ed inserendo le credenziali per puntare al VPN BOX2*
- *Nel menù Devices cliccare sul menù azioni di ciascun nuovo device inserito (normalmente essendo nuovi si presentano in colore grigio) cliccare su "Setup" nella proprietà "group" selezionare come gruppo di appartenenza il gruppo P2P creato al primo punto*
- *Configurare gli utenti per sistema di Accesso Remoto*
- *Ritornare al menù gruppi ed inserire gli utenti nel gruppo P2P creato e che conterrà già i device*

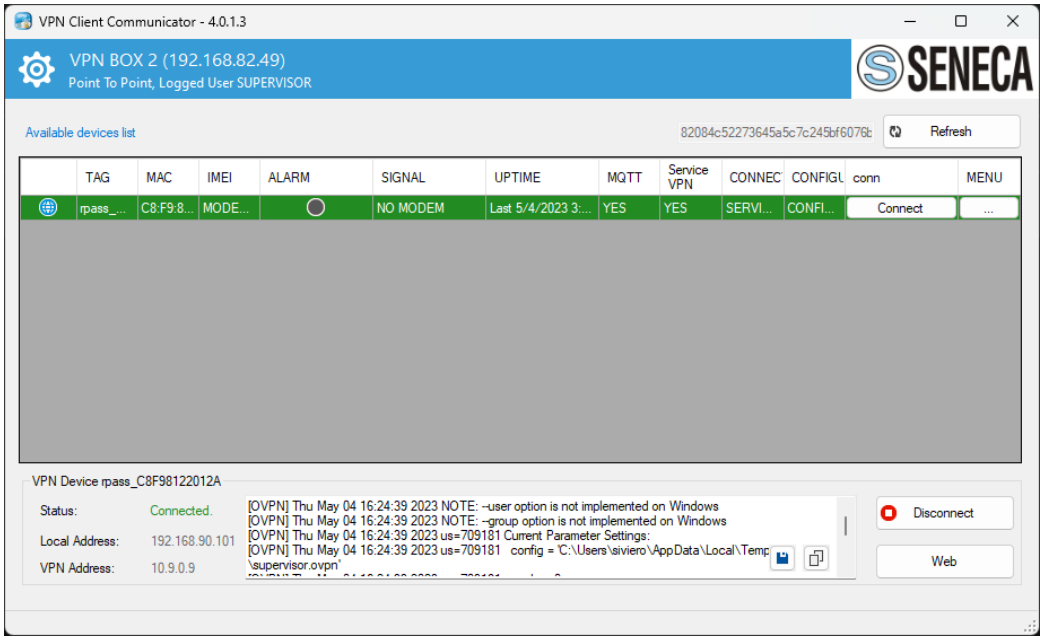
13. CONNESSIONE TRAMITE VPN CLIENT COMMUNICATOR

Questo software è un client di connessione VPN e deve essere installato sui PC che si desidera utilizzare per accedere alla rete VPN. Permette due diversi tipi di utilizzo che verranno trattati in seguito.

13.1. CONNESSIONE VPN GUI (SL o P2P)

In questa modalità l'accesso è possibile con le stesse credenziali utilizzate per collegarsi al server VPN BOX2 tramite browser. Una volta effettuato il login con l'applicazione si ottiene una vista tabellare dei dispositivi Seneca connessi e del loro stato. I dispositivi configurati che sono online sono considerati operativi, per attivare le connessioni VPN operare come segue:

- *Se connesso in modo SL: cliccare sull'unico pulsante "Connect" posto un basso a destra sull'interfaccia*
- *Se connesso in P2P: in corrispondenza a ciascun device comparirà un pulsante "Connect", cliccare su quello a cui ci si vuole connettere.*



Premendo il pulsante Connetti si entra in rete e si comunica con i dispositivi, al centro vengono registrate le operazioni di sistema durante la connessione. In basso a sinistra vengono visualizzati i dati di configurazione a livello di indirizzi VPN mentre nel pannello del dispositivo vengono visualizzati sia gli indirizzi della rete locale del dispositivo che della VPN.

ATTENZIONE!

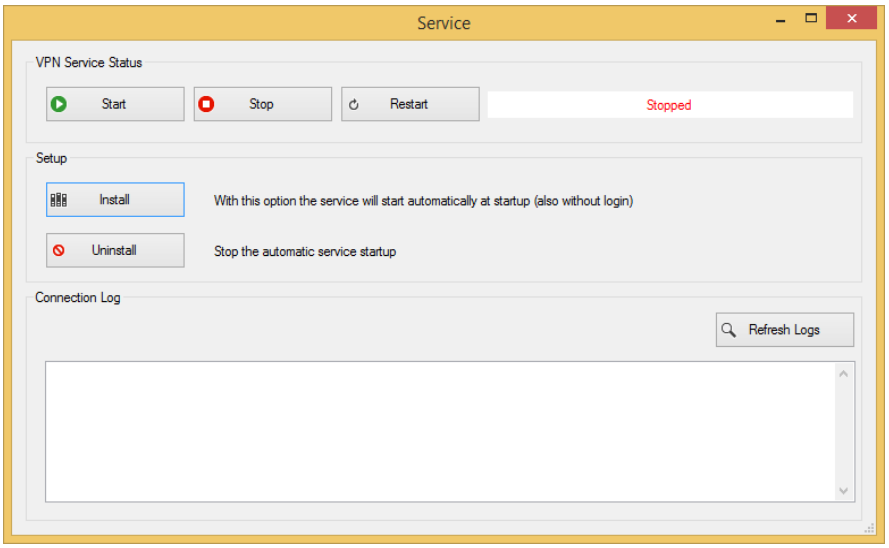
Connettendosi da un PC con indirizzi IP compatibili con quelli della rete VPN remota alcuni indirizzi IP locali potrebbero non essere più raggiungibili mentre la connessione è attiva.

13.1. CONNESSIONE VPN SERVICE MODE (SOLO SL)

Ci sono casi in cui è necessario che un PC sia automaticamente connesso all'avvio ad una rete VPN e per poterlo fare in modo autonomo ed è necessario abilitare la modalita service del VPN Client Communicator. Questi casi applicativi sono spesso collegati ad installazioni che coinvolgono sistemi di supervisione remota dotati di SCADA.

Per attivare la modalità automatica, accedi a VPN Client Communicator, fai clic sull'icona dell'ingranaggio in alto a sinistra e seleziona "Servizio" dal menu che compare.

È necessario installare la configurazione sulla macchina e per farlo premere il pulsante "Install". Il sistema eseguirà automaticamente tutte le operazioni e completerà mettendo il servizio "OpenVPN service" in "run". Nella casella in basso è possibile caricare lo storico di sistema, per verificare le operazioni effettuate o eventuali problemi di connessione.



Sempre da questo pannello è possibile arrestare e riavviare il servizio annullando anche la configurazione.

ATTENZIONE!

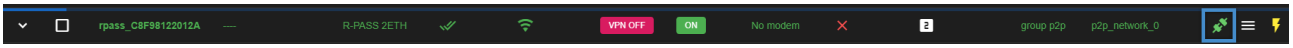
Abilitando la modalità automatica con il servizio non sarà più possibile utilizzare l'account in modalità normale.

13.2. CONNESSIONE DIRETTA DAL BROWSER

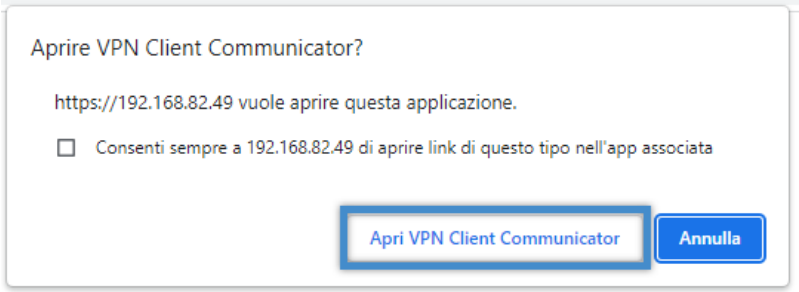
Per rendere la connessione dell'utente più rapida esiste un pulsante diretto nella pagina Devices del VPN BOX2 che permette di lanciare automaticamente l'applicazione VPN Client Communicator già loggata e parametrizzata per avviare la connessione verso il device selezionato.

Gli step da seguire sono:

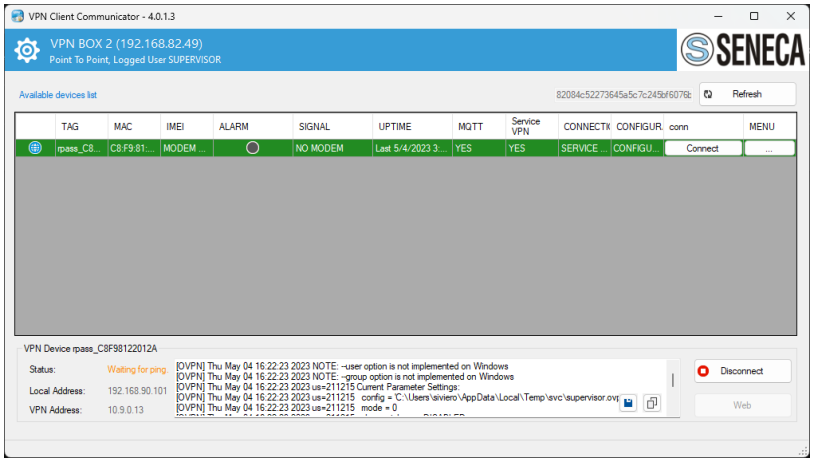
- *Individuare nella pagina il device a cui si intende connettersi e cliccare sul tasto rapido di connessione*



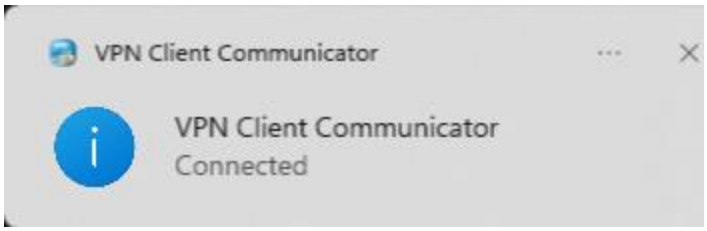
- *Il browser aprirà una pagina di conferma per l'avvio dell'applicazione esterna VPN Client Communicator*



- *L'applicazione VPN Client Communicator verrà avviata automaticamente*



- *A connessione avvenuta il VPN Client Communicator si ridurrà ad icona con un messaggio di notifica*



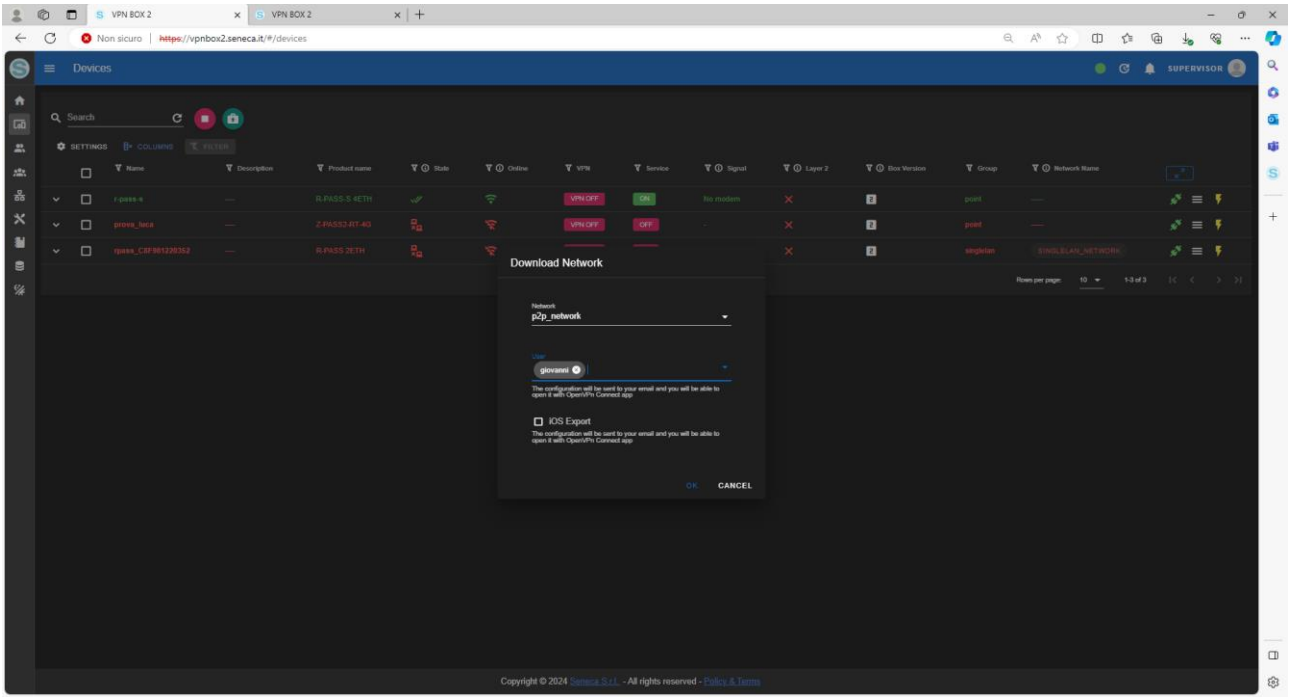
- *Anche il browser mostrerà l'avvenuta connessione vpn tramite il flag VPN ON*

14. CONNESSIONE TRAMITE CLIENT ANDROID O IOS

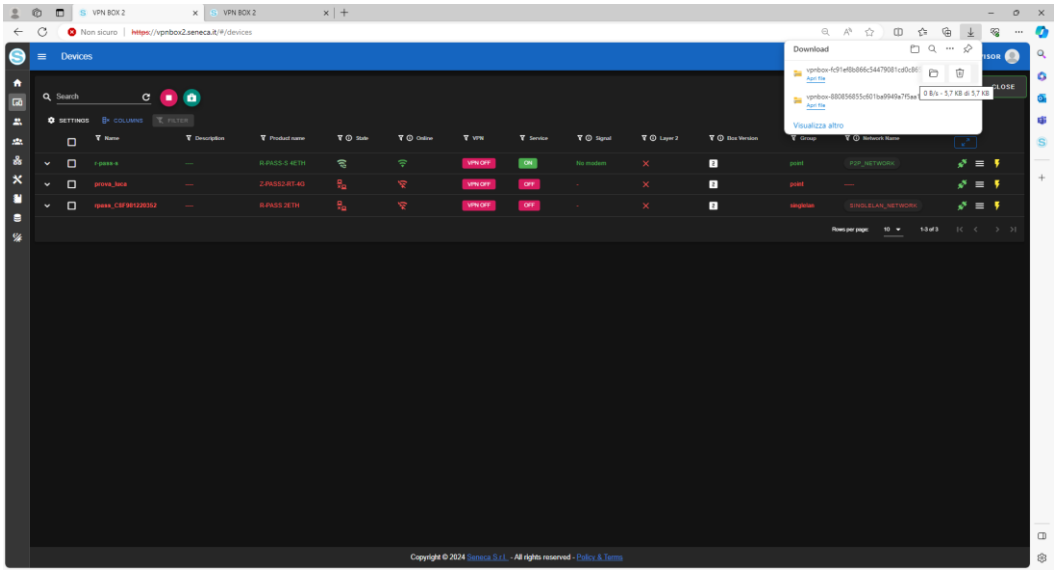
14.1. PROCEDURA PER CONNESSIONE CON CLIENT ANDROID

Importante: eseguire questa procedura collegandosi alla dashboard tramite ddns o IP pubblico (esternamente alla rete locale dove è installa la vpnbox2). Nel dispositivo Android deve essere installata la APP “OpenVPN Connect”.

1) ***Selezionare “Export”-> selezionare network e utente (in caso di più certificati sullo stesso device usare sempre stessa network). Ogni device con la propria network***

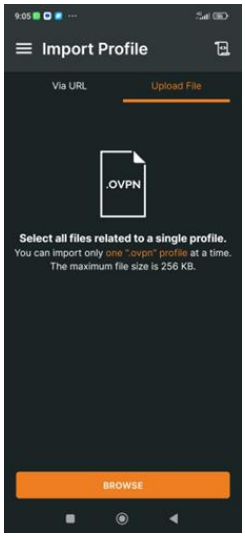


2) ***Scaricare il file zip -> inviarlo al telefono android (ad esempio via email)***

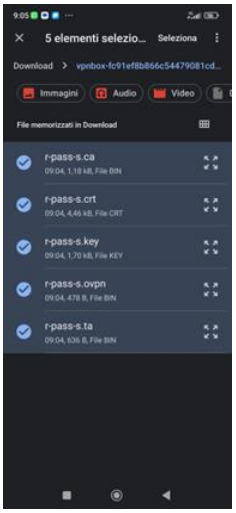


3) *Importare il file zip nel telefono*

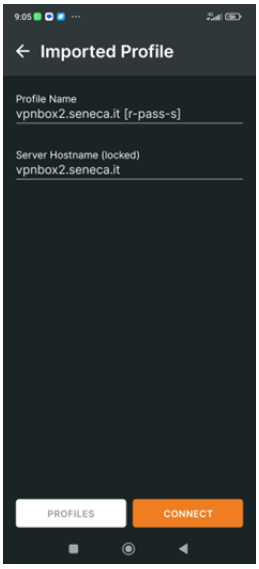
4) *Aprire openvpn nel dispositivo android e premere su upload*



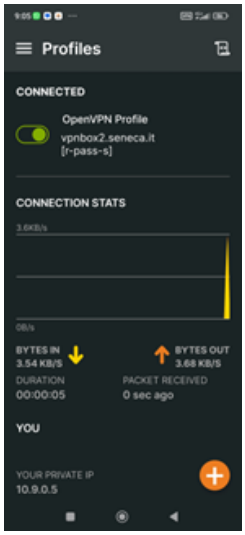
5) *Selezionare TUTTI i certificati*



6) *Dare ok e aggiungere il profilo*



7) *la connessione è funzionante*

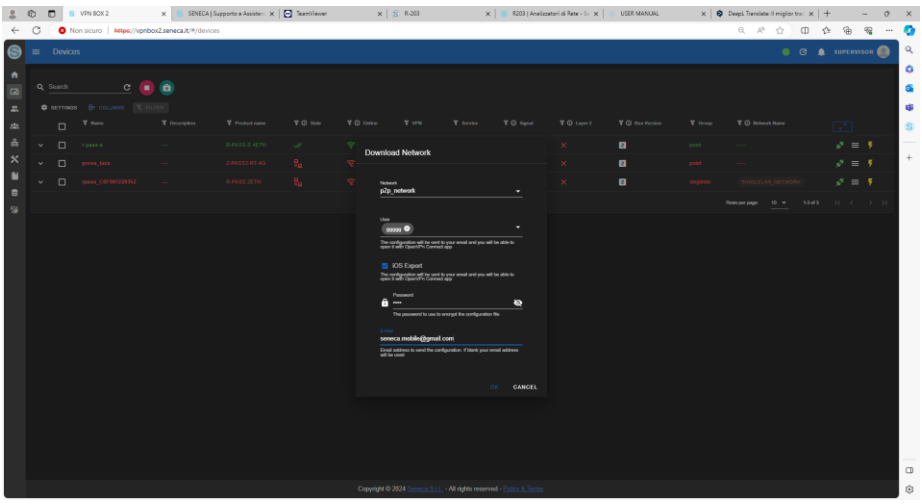


14.2. PROCEDURA PER CONNESSIONE CON CLIENT IOS

Nel dispositivo Android deve essere installata la APP “OpenVPN Connect”.

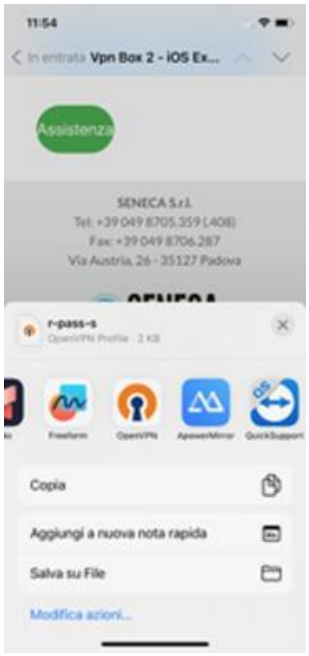
Nel server VPNBOX deve essere configurato correttamente il servizio di invio delle email nella sezione SMTP.

1) ***Selezionare “Export”-> selezionare network e utente (in caso di più certificati sullo stesso device usare sempre stessa network). Ogni device con la propria network***
   Selezionare IOS export e inserire la password per decriptare il file di configurazione. Inserire anche la mail a cui spedire i certificati

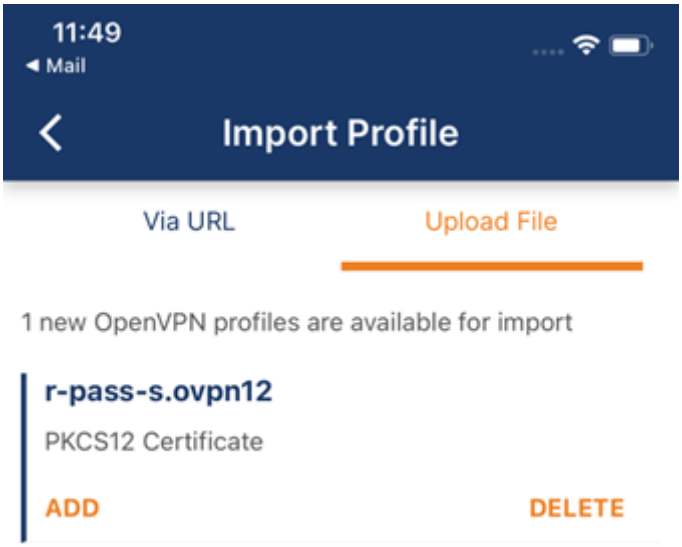


2) ***Aprire la mail nel dispositivo IOS:***

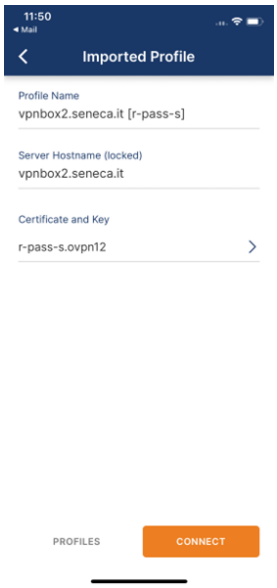
3) ***Aprire il file .ovpn12 con la App OpenVPNCONNECT (cliccare sopra il nome del file e poi selezionare APP)***



4) ***Aggiugnere il certificato e inserire la password definita in fase di export***



5) ***Aprire il file .ovpn e selezionare sul campo "Certificate and Key" il certificato precedentemente installato***



6) ***Aprire la connessione con "Connect"***

GLOSSARIO

- *VPN Client Communicator*

È il software che consente agli utenti (PC) di connettersi al VPN Box tramite VPN.

- *PTP o P2P (Point To Point)*

Questo acronimo viene utilizzato per indicare una connessione punto-punto on demand tra il PC client e il dispositivo remoto. Questa configurazione è utile quando ci sono molte reti a cui connettersi, tutte con la stessa configurazione, che non possono quindi rimanere sulla stessa LAN. Questa modalità è non permanente, cioè deve essere utilizzata per le operazioni necessarie e poi disconnessa.

- *SL (Single Lan)*

Indica la modalità VPN Box denominata Remote Control che permette di creare un'unica rete virtuale tra gli apparati e i client di connessione. È progettato per il monitoraggio di sistemi come SCADA, dove la connessione è stabile. In questa modalità i dispositivi non possono avere configurazioni di rete identiche.

- *NAT (Network Address Translation)*

Nell'ambito delle reti informatiche, il network address translation è un meccanismo che permette di modificare l'indirizzo IP dei pacchetti in transito attraverso apparati di rete - come router o firewall. Serve per esporre alla rete Internet i Servizi del VPN BOX2 che si troverà in una rete locale con a capo un firewall. Il server VPN BOX2 risulterà quindi accessibile dai device remoti Seneca tramite l'IP pubblico del firewall a cui il server è direttamente connesso.