Mikrotik WireGuard Business-VPN WISECP module

The module is created to empower IT companies to enrich their service offerings through the provision of paid WireGuard VPN accounts. Once installed, the module takes care of the entire process of creating, modifying, and suspending WireGuard VPN accounts. It seamlessly integrates with the WISECP billing system, streamlining the exchange of crucial data for customer settlements, account activations, and service suspensions. In essence, the service is tailored for business clients who have the capability to manage their VPN accounts.

- Description
- Changelog
- Installation and configuration guide
  - Setup (install/update)
  - License Activation
  - Mikrotik preparation and configuration
  - Add server (Mikrotik) in WISECP
  - Service/Product configuration
- WireGuard Clients configuring
  - WireGuard Official clients
  - Mikrotik WireGuard client configuration
- Admin Area

    - Order Detail

- Client Area
    - Product Home Screen
    - Add VPN account
    - Port Forwarding

Description

Mikrotik WireGuard Business-VPN module

WISECP

Order now | Download | FAQ

The MikroTik WireGuard Business-VPN module is designed to offer a customizable Virtual Private Network service for business clients who possess the capability to independently manage their VPN accounts.

At its core, the module provides the end customer with a group of VPN account entries that the client can control. This includes the ability to add, remove, block, and perform port forwarding on these accounts. All accounts are situated within a unified network and share a common external IP address. Moreover, there is a feature that allows internal traffic to be routed among these accounts.

This innovative system empowers the end client to establish corporate private networks for their own customers. With the flexibility to manage VPN accounts and the added functionality of internal traffic forwarding, businesses can tailor their VPN service to meet the specific needs of their clientele.

> **Requirements**
> WISECP: v3.1.5+, php: v8.x, Ioncube: V12+
> MikroTik: v7+

Supports protocols:

- WireGuard

Module Functions:

- Auto create and deploy VPN account/accounts
- Suspend/Unsuspend/Delete/Change Package
- Port forwarding
- Requires a MikroTik device or MikroTik CHR.
- Possibility to set Bandwidth speed limits per client VPN account

- Module supports multilingualism (**Arabic, Azerbaijani, Catalan, Chinese, Croatian, Czech, Danish, Dutch, English, Estonian, Farsi, French, German, Hebrew, Hungarian, Italian, Macedonian, Norwegian, Polish, Romanian, Russian, Spanish, Swedish, Turkish, Ukrainian**)
- Link to instructions for setting up the service in the client area.
- Mechanism for working with servers and server groups

Available options in the admin panel:

- Create users
- Suspend users
- Unsuspend users
- Delete users
- Change Package
- VPN connection status

Available options in the client panel:

- Links in the form of buttons to the instruction and VPN clients
- General information about the service
- Option to download WireGuard configuration as a file
- QR code for WireGuard configuration
- VPN connection status

Screenshot of the client area

Add VPN account | Port Forwarding | User manual | Download VPN client

Network configuration

Dedicated IP:	77.87.125.206
Private internal network:	192.168.101.0/24
VPN Protocols:	WireGuard
Number of VPN accounts:	4/5
Bandwidtht download/upload:	5/5 M per account

VPN accounts

✓	✎	**2** (192.168.101.2/32)	WireGuard online: **yes** 213.134.190.109:13435 **RX/TX:** 54606980/498508584
✓	✎	**server1** (192.168.101.3/32)	WireGuard online: **not**
✓	✎	**cam1** (192.168.101.4/32)	WireGuard online: **not**
✓	✎	**cam2** (192.168.101.5/32)	WireGuard online: **not**

Screenshot of the Admin area

Turn Back

Port Forwarding

From 77.87.125.206: Enter port tcp

To 2 (192.168.101.2) Enter port

Add port forwarding

77.87.125.206:123 tcp	192.168.101.3:333 (server1)	Delete
77.87.125.206:356 tcp	192.168.101.5:3365 (cam2)	Delete

API Module: PUQ Mikrotik WireGuard Business-VPN

API answer OK

Interface name (MTU)	private-key/public-key	IP	Disabled	Running
puq-5-2-116 (1420)	2L/qBwzJ0pzO0UJSdjQH6CVyDuWRsKdIdDP7WzDSY1U= /m6YpP8ntqO6Ec8xkTJIMi1FOTHoTxHeyHIfwf5DIn0=	192.168.101.1/24	false	true

10 Show Record

Search

Name	private-key/public-key	Disabled	IP	Endpoint	Latest handshake	RX/TX
2	INMSSFMf1xf1VUzmEAkZq9TaQYxyc1nZcFk6TNsEmFQ= o9YruWqkf5dHBC2z9FaOY8Hx3LQ2YJ3sMeDF1f2rqF4=	false	192.168.101.2/32	213.134.190.109:13435	16h8m28s	54606980/498508584
cam1	uJ3WfVHEaBgk6Eycor1ifaQeQPNchsJuse6yfSJScWA= phpQPOpL6mEAA1nQGchJJlae6DnrrPIYbMKBmyGyHHs=	false	192.168.101.4/32	N/A	N/A	0/0
cam2	aDn7gaRNIBT8gzI04SL7yTk+x8kbFTzlXsOaKrByB1k= Od+fNZQWgPyXcHvGM21p5NDTG7u04biFYCKXdguGAgY=	false	192.168.101.5/32	N/A	N/A	0/0
server1	EDaXOQi8ucf4XC65Rxt43+RChTTEYWbWKhcaNoO0qIU= 7QBUpU3hLS2KU2TbEMbgtHsbxlfXtxXCmGJZxGqb5kc=	false	192.168.101.3/32	N/A	N/A	0/0

Showing records from 4 to 1 - 4

Prev 1 Next

Server: vpn-test.uuq.pl

Dedicated IP Interface: ether1-pub

Dedicated IP: 77.87.125.206/25

WireGuard Interface Name: puq-5-2-116

Private Network: 192.168.101.0/24

Overwrite package settings: ☐ Overwriting the package settings is necessary to personalize the service if you need it.

Send changes to server: ☐ To apply the changes on the server, it is necessary to check this checkbox.

Update

Changelog

Mikrotik WireGuard Business-VPN module

WISECP

Order now | Download | FAQ

v1.2 Released 16-03-2025

- Fixed a bug with incorrect distribution of IP addresses

---

v1.1 Released 15-02-2024

- Fixed a bug with some cases where it was not possible to delete the server
- Improved security

---

v1.0 Released 06-12-2023

First version

Installation and configuration guide

Setup (install/update)

Mikrotik WireGuard Business-VPN module

WISECP

Order now | Download | FAQ

To install and update a module, you must perform one and the same action.

1. Download the latest version of the module.

```
wget https://download.puqcloud.com/WISECP/Product/PUQ_WISECP-Mikrotik-WireGuard-Business-VPN/php81/PUQ_WISECP-Mikrotik-WireGuard-Business-VPN-latest.zip
```

All versions are available: https://download.puqcloud.com/WISECP/Product/PUQ_WISECP-Mikrotik-WireGuard-Business-VPN/

2. Unzip the archive with the module.

```
unzip PUQ_WISECP-Mikrotik-WireGuard-VPN-latest.zip
```

3. Copy and Replace "puqMikrotikWireGuardBusinessVPN" from "PUQ_WISECP-Mikrotik-WireGuard-Business-VPN" to "WISECP_WEB_DIR/coremio/modules/Product/"

License Activation

Mikrotik WireGuard Business-VPN module

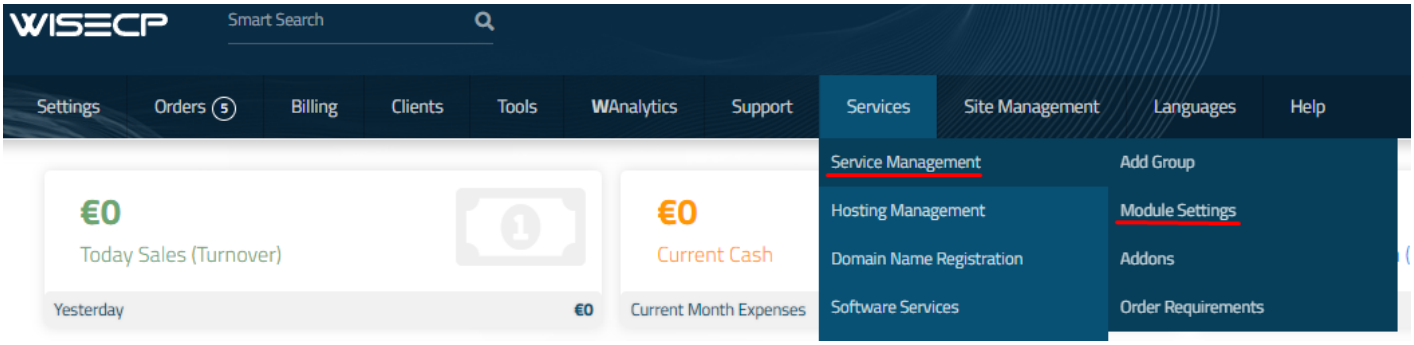
WISECP

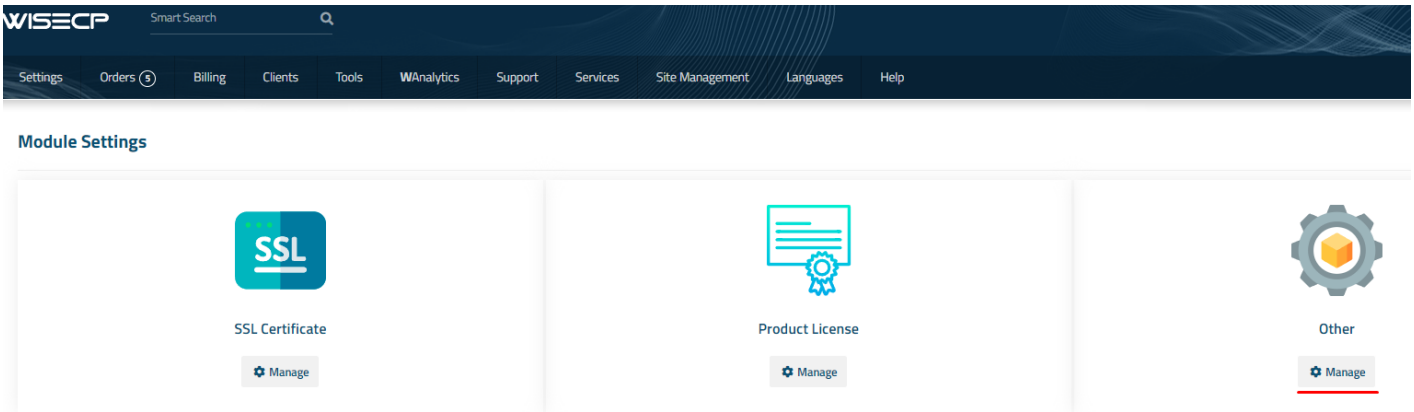
Order now | Download | FAQ

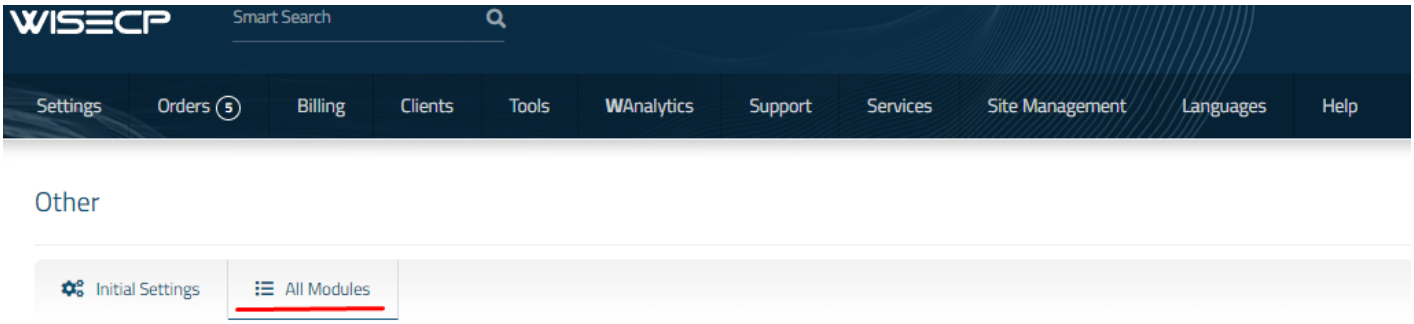
1. Log in to the administrative area of your **WISECP**.

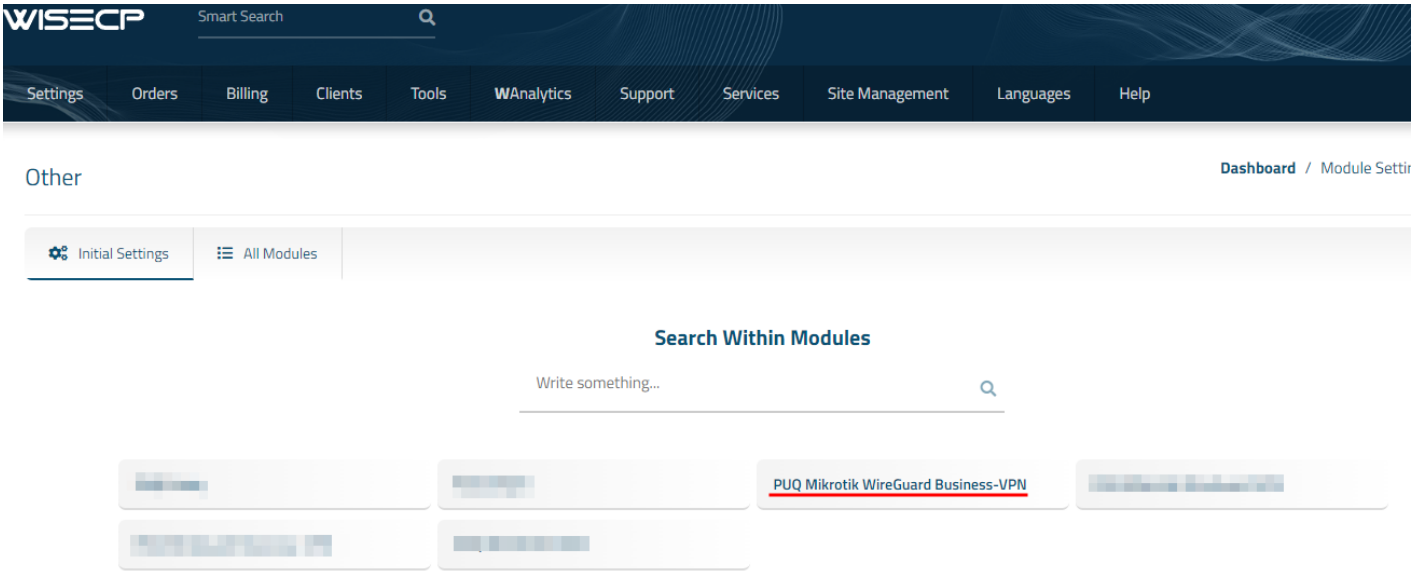
2. Go to module configuration.

```
Services -> Service Management -> Module Settings -> Other -> All Modules -> PUQ Mikrotik WireGuard Business-VPN
```

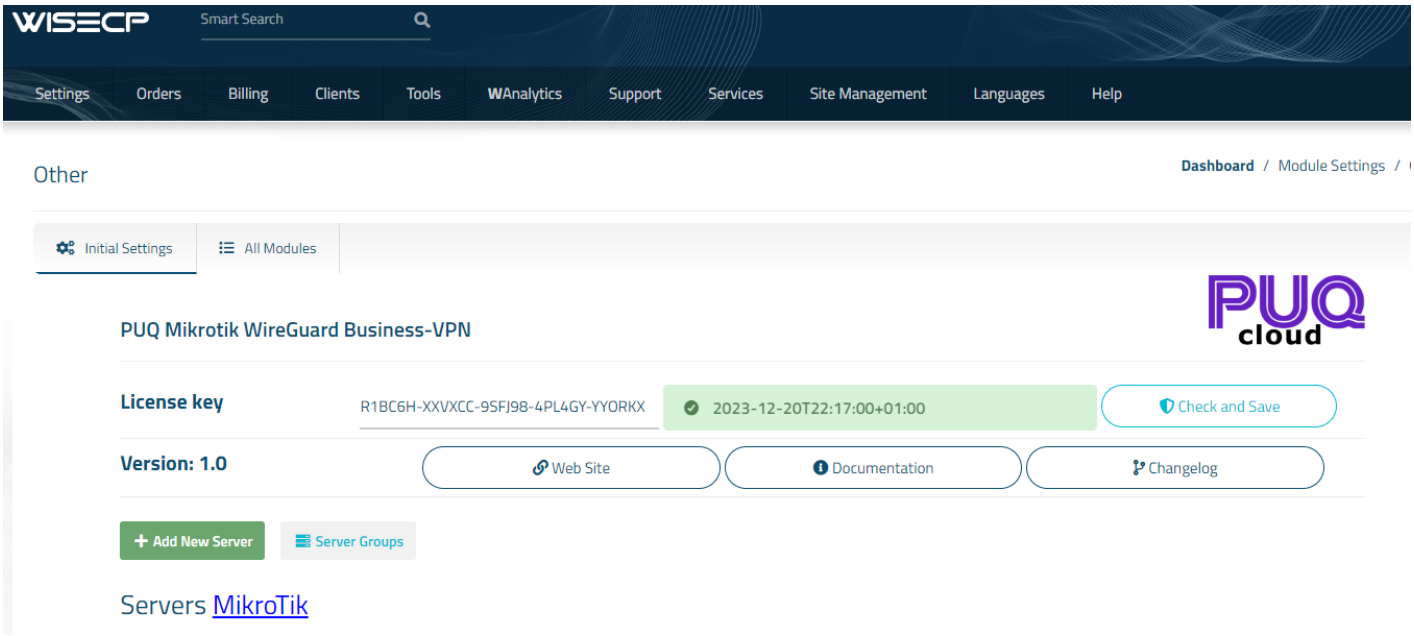








3. On the open page, enter the purchased license key for this product and click the '**Check and Save**' button to validate the key and save it.


WISECP
Smart Search
Settings
Orders
Billing
Clients
Tools
WAnalytics
Support
Services
Site Management
Languages
Help
Other
Dashboard / Module Settings /
Initial Settings
All Modules
PUQ Mikrotik WireGuard Business-VPN
PUQ cloud
License key
R1BC6H-XXVXCC-9SFJ98-4PL4GY-YYORKX
2023-12-20T22:17:00+01:00
Check and Save
Version: 1.0
Web Site
Documentation
Changelog
+ Add New Server
Server Groups
Servers MikroTik

Mikrotik preparation and configuration

Mikrotik WireGuard Business-VPN module

WISECP

Order now | Download | FAQ

> Note: **Enter the following commands one by one and wait for the command to complete.**

Check RouterOS version

> **Make sure that the version of RouterOS is 7+**

```
system/package/print
```

Enabling HTTPS Create your own root CA on your router

```
/certificate
add name=LocalCA common-name=LocalCA key-usage=key-cert-sign,crl-sign
```

Sign the newly created CA certificate

```
/certificate
```

```
sign LocalCA
```

Create a new certificate for Webfig (non-root certificate)

> Note: as common-name=XXX.XXX.XXX.XXX You enter public IP adddress of the router.

```
/certificate
add name=Webfig common-name=XXX.XXX.XXX.XXX
```

Sign the newly created certificate for Webfig

```
/certificate
sign Webfig ca=LocalCA
```

Enable SSL (*www-ssl)* and specify to use the newly created certificate for Webfig

```
/ip service
set www-ssl certificate=Webfig disabled=no
```

Enable api-ssl and specify to use the newly created certificate for Webfig

```
 /ip service
 set api-ssl certificate=Webfig disabled=no
```

Installation and configuration guide

Add server (Mikrotik) in WISECP

Mikrotik WireGuard Business-VPN module

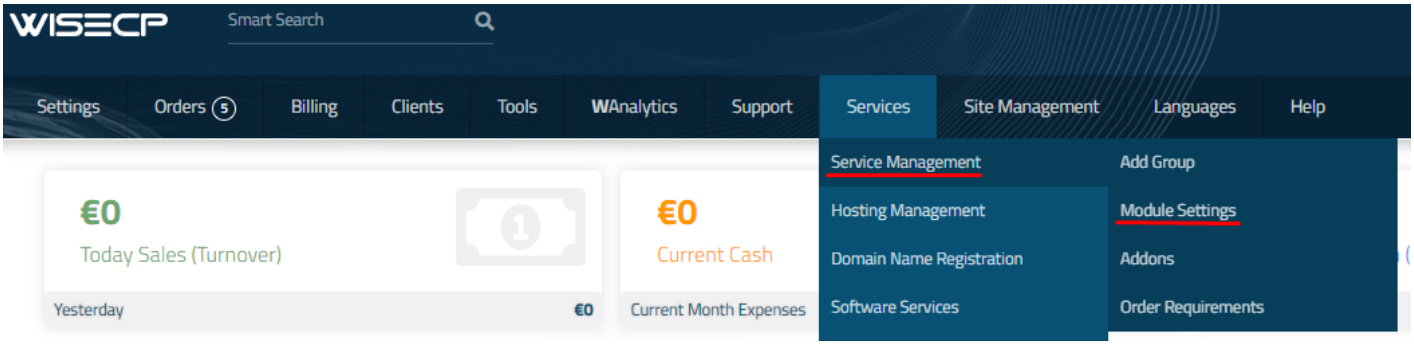
WISECP

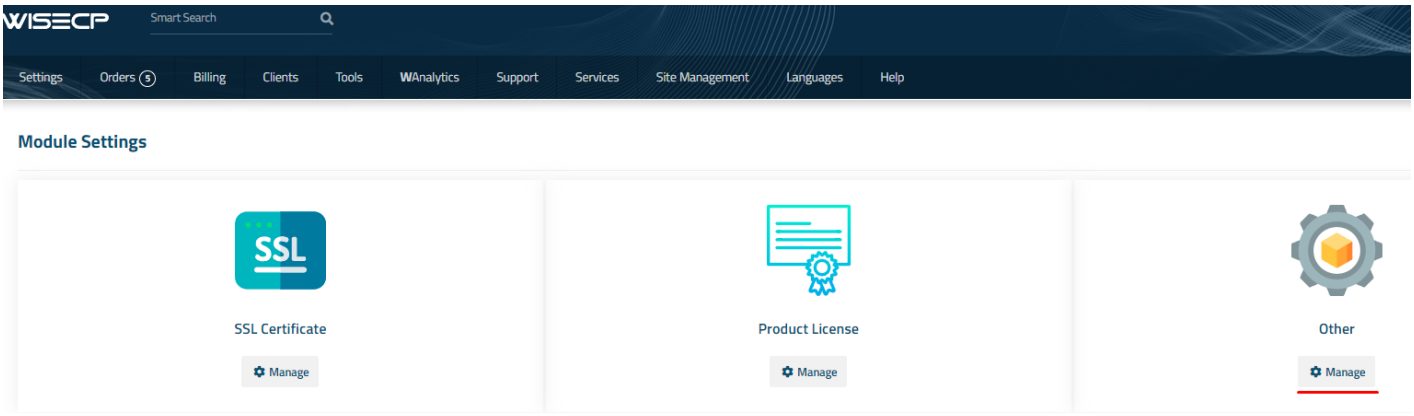
Order now | Download | FAQ

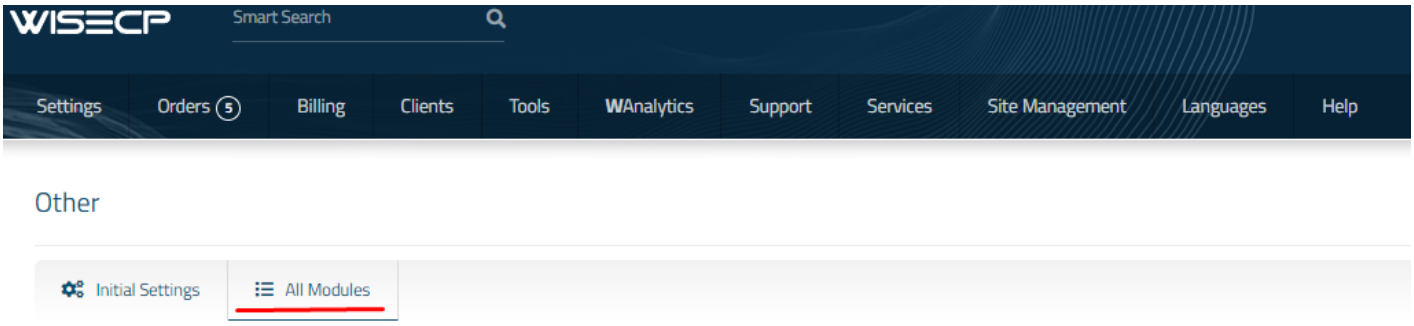
1. Log in to the administrative area of your **WISECP**.

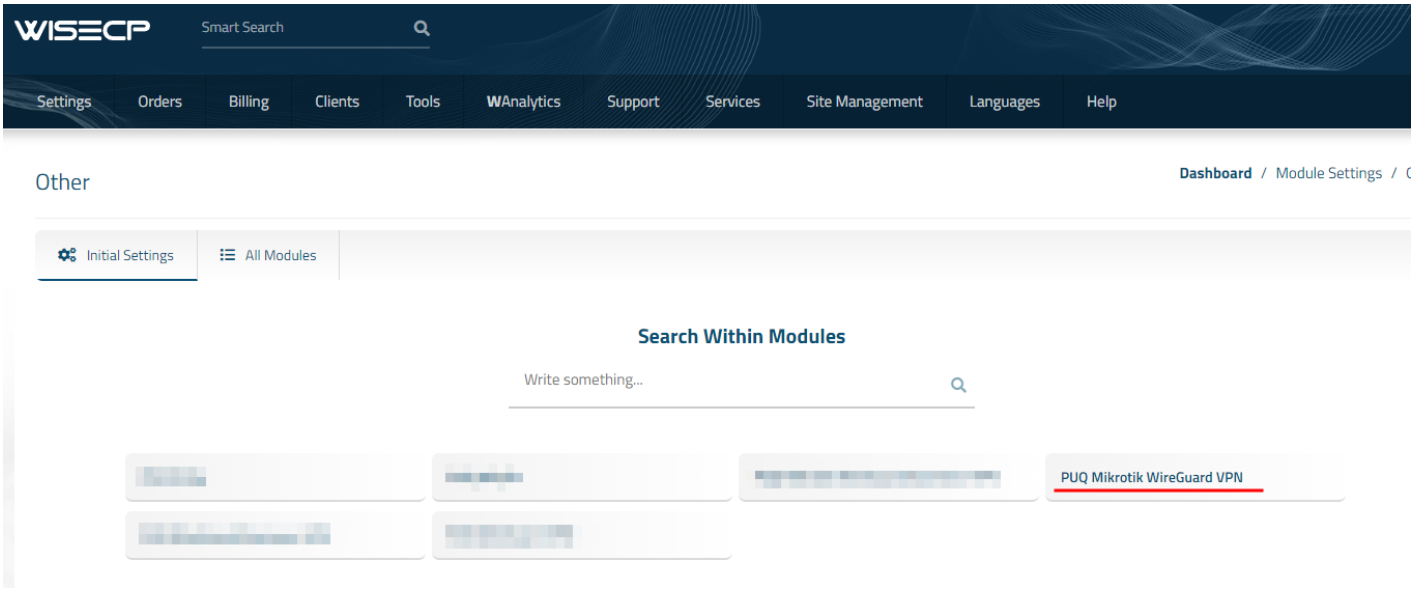
2. Go to module configuration.

```
Services -> Service Management -> Module Settings -> Other -> All Modules -> PUQ Mikrotik WireGuard Business-VPN
```

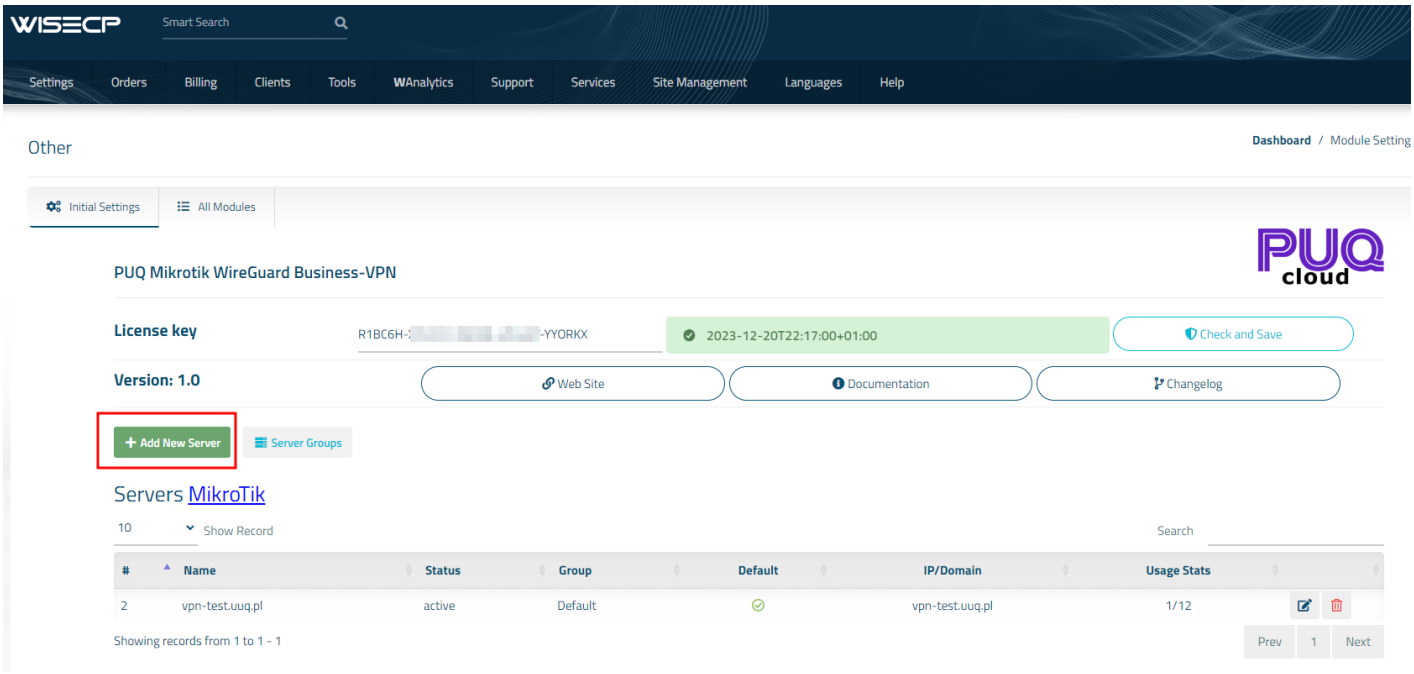








3. In the opened page, click the '**Add Server**' button.



4. On the opened page, enter all the necessary information:

- **Name**: Displayed name of the server.
- **Maximum Number of Accounts**: The number of services that can be on this server.
- **Server Group**: Optionally, choose the server group.
- **DNS 1 and DNS 2**: are DNS servers that will be specified in the configuration of WireGuard clients.
- **Assigned IP Addresses**: a list of Interface fot public IP, Public IP, Private Net that will be assigned to WireGuard VPN clients, with each address on a new line. Format:

```
<interface>| <public_ip>/<mask>| <private_network>/<mask>
```

- **IP Address or Domain**: The address of the MikroTik router you are connecting to.
- **Username:** is the username for the account on MikroTik.
- **Password:** is the password for the account on MikroTik.
- Check the **SSL** box if you want to use SSL-encrypted connection. If necessary, specify the port and perform a connection test.

< Go to Back

Add New Server

Name	vpn-test.uuq.pl
Maximum Number of Accounts	10
Server Group	Default
Default	☐ Set as default server in group
DNS 1	77.87.125.10
DNS 2	77.87.125.20
Assigned IP Addresses (One per line)	ether1-pub|77.87.125.206/25|192.168.101.0/24 ether1-pub|77.87.125.207/25|192.168.102.0/24 ether1-pub|77.87.125.208/25|192.168.103.0/24 ether1-pub|77.87.125.209/25|192.168.104.0/24 ether1-pub|77.87.125.210/25|192.168.105.0/24 ether1-pub|77.87.125.211/25|192.168.106.0/24 ether1-pub|77.87.125.212/25|192.168.107.0/24 ether1-pub|77.87.125.213/25|192.168.108.0/24 `<interface>|<public_ip>/<mask>|<private_network>/<mask>`
IP Address or Domain	vpn-test.uuq.pl
Username	wisecp-dev-MWG
Password	
SSL	☑ Connect using SSL
Port	443 ☐ Change standard port
Test Connection	Test Connection

Add New Server

Service/Product configuration

Mikrotik WireGuard Business-VPN module

WISECP

Order now | Download | FAQ

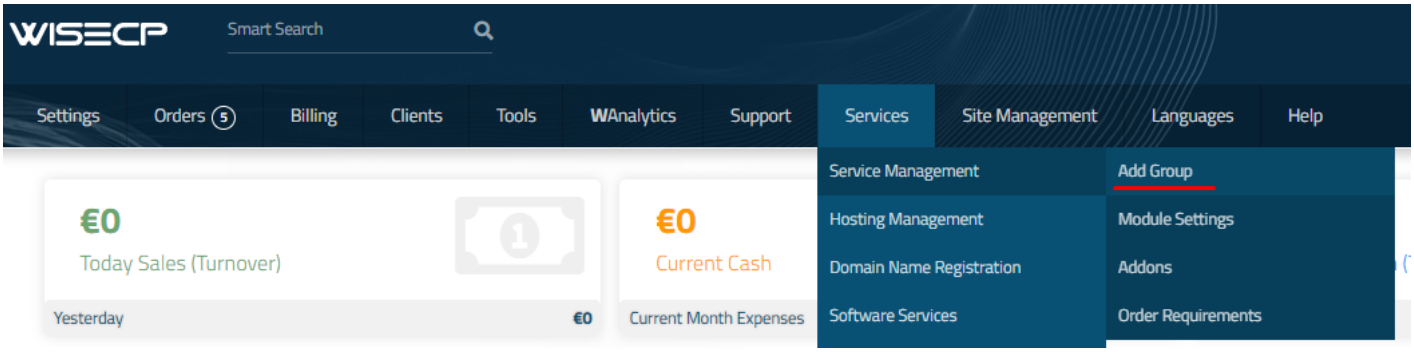
> If you do not have a **Service Group** where you want to place the new service, you need to create a new **Service Group**

1. Log in to the administrative area of your **WISECP**.

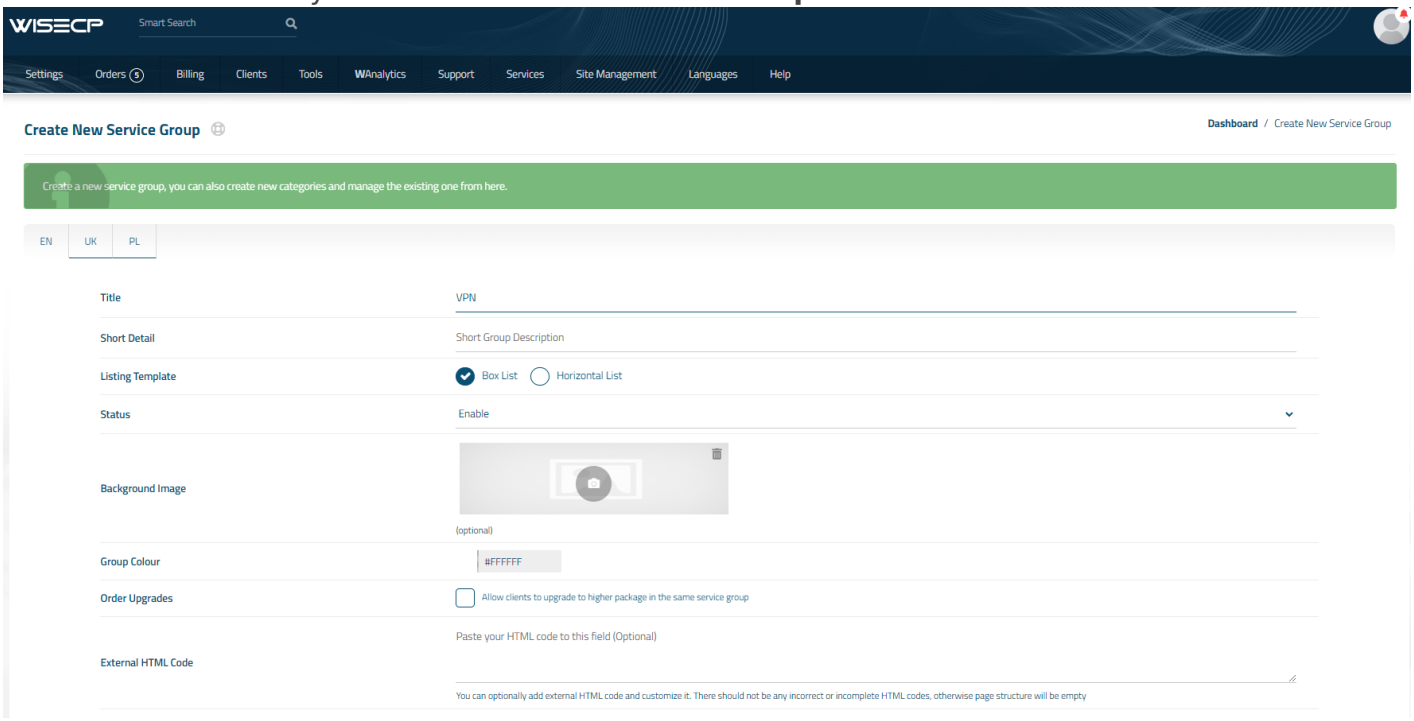
2. Create New Service Group

Go to

```
Services -> Service Management -> Add Group
```



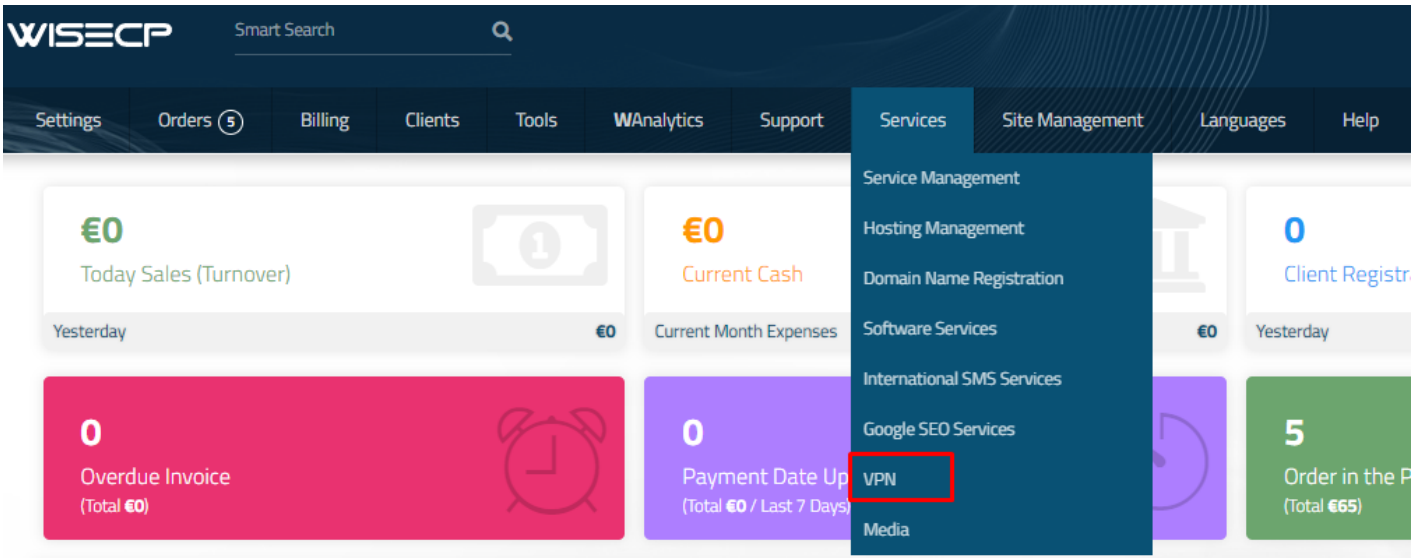
Enter all the necessary data and click the '**Create Group**' button.



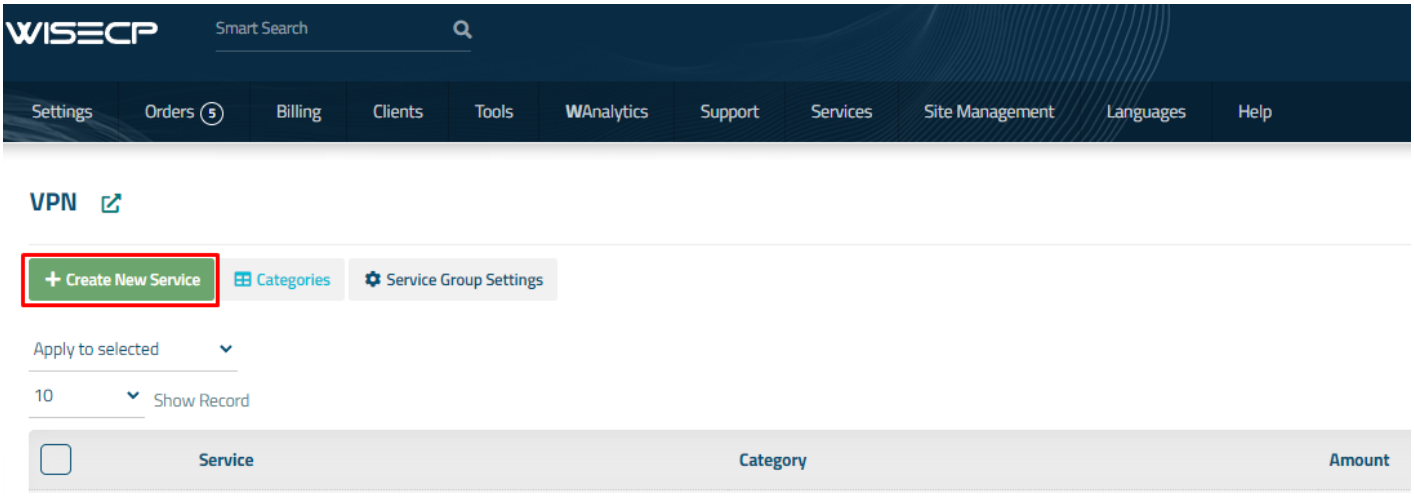
3. Adding a New Service

Go to

```
Services -> our service group where you need to add the new service.
```

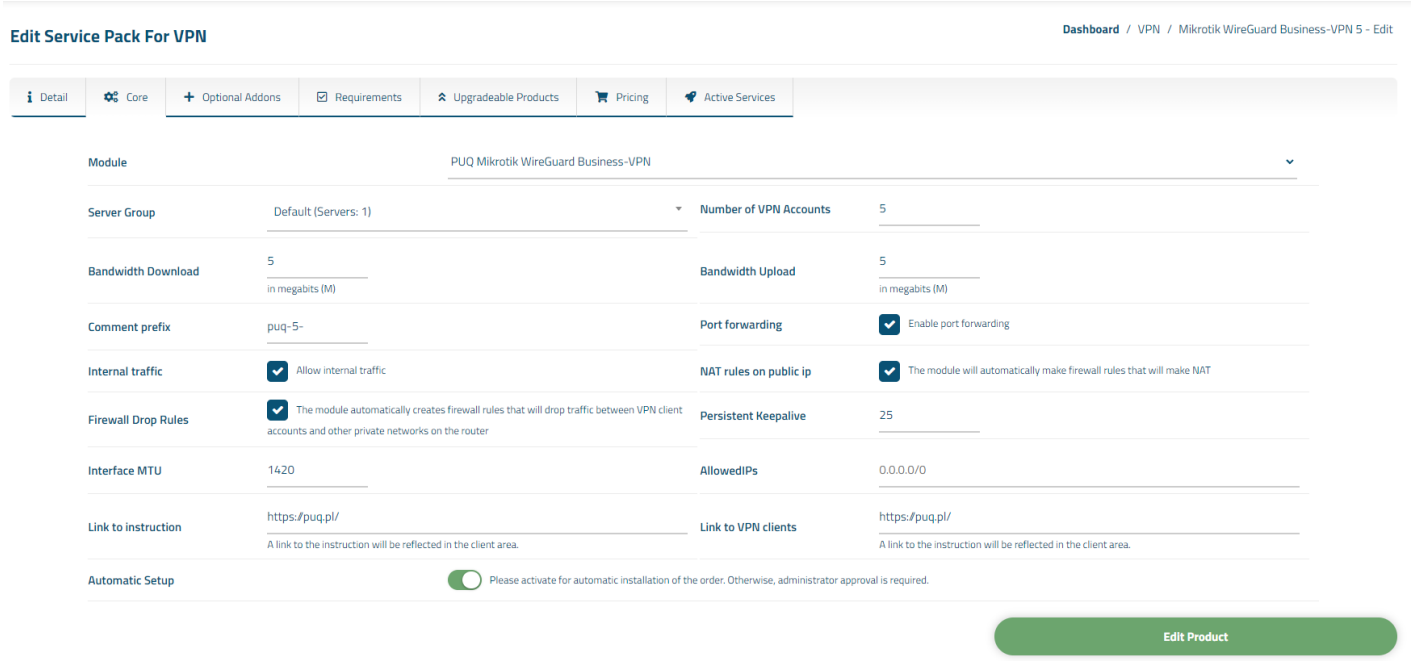


In the opened window, click the '**Create New Service**' button.



On the opened page, enter all the necessary details for your new service and navigate to the '**Core** ' tab.

Select the '**PUQ Mikrotik WireGuard Business-VPN**' module from the drop-down list of modules.



4. Fill in the configuration options according to your preferences.

- **Server Group** is the group of servers from which a server will be chosen for provisioning the service
- **Number of VPN Accounts:** the quantity of VPN user accounts a client can create within this package
- **Bandwidth Download** and **Bandwidth Upload** represent the connection speed that will be restricted by these parameters, in megabits per second, respectively.
- **Comment Prefix** will be added at the comment in **MikroTik**
- **Port Forwarding:** If the checkbox is selected, it means the client will have the ability to redirect ports from the main public address to internal addresses.
- **Internal Traffic**: If the checkbox is selected, it indicates that internal traffic between

VPN clients of the client will be allowed.

- **NAT Rules on Public IP**: If the checkbox is selected, firewall rules, specifically NAT (Network Address Translation) to the public IP address, will be created during the service deployment.
- **Persistent Keepalive/AllowedIPs:** parameters of configuration WireGuard clients
- **Interface MTU**: This parameter will be set during the creation of the WireGuard interface.
- **Link to Instruction** Provide the link to the instruction for the service, and it will be displayed in the client area as a separate button
- **Link to VPN Clients** Provide the link to the page for downloading VPN clients for the service, and it will be displayed in the client area as a separate button

WireGuard Clients configuring

WireGuard Official clients

Mikrotik WireGuard Business-VPN module

WISECP

Order now | Download | FAQ

You can download from the

https://www.wireguard.com/install/

Please always download latest versions. The following list is intended as a general direction only.

Windows [7, 8.1, 10, 11, 2008R2, 2012R2, 2016, 2019, 2022 – v0.5.3]

Download Windows Installer

Browse MSIs

---

macOS [app store – v1.0.15]

Download from App Store

Android [play store – vunknown – out of date & f-droid – v1.0.20220516]

Download from Play Store

Download from F-Droid

---

iOS [app store – v1.0.15]

Download from App Store

Debian/Ubuntu

```
$ sudo apt install wireguard
```

Mikrotik WireGuard client configuration

Mikrotik WireGuard Business-VPN module

WISECP

Order now | Download | FAQ

Make sure you have an up to date **routerOS** system.

Version must be at least: 7.6

```
[admin@VPN-CLIENT] > system package print
Columns: NAME, VERSION
# NAME      VERSION
0 routeros  7.6
```

Open a single-use shipment on the **WireGuard** section for the client's configuration request

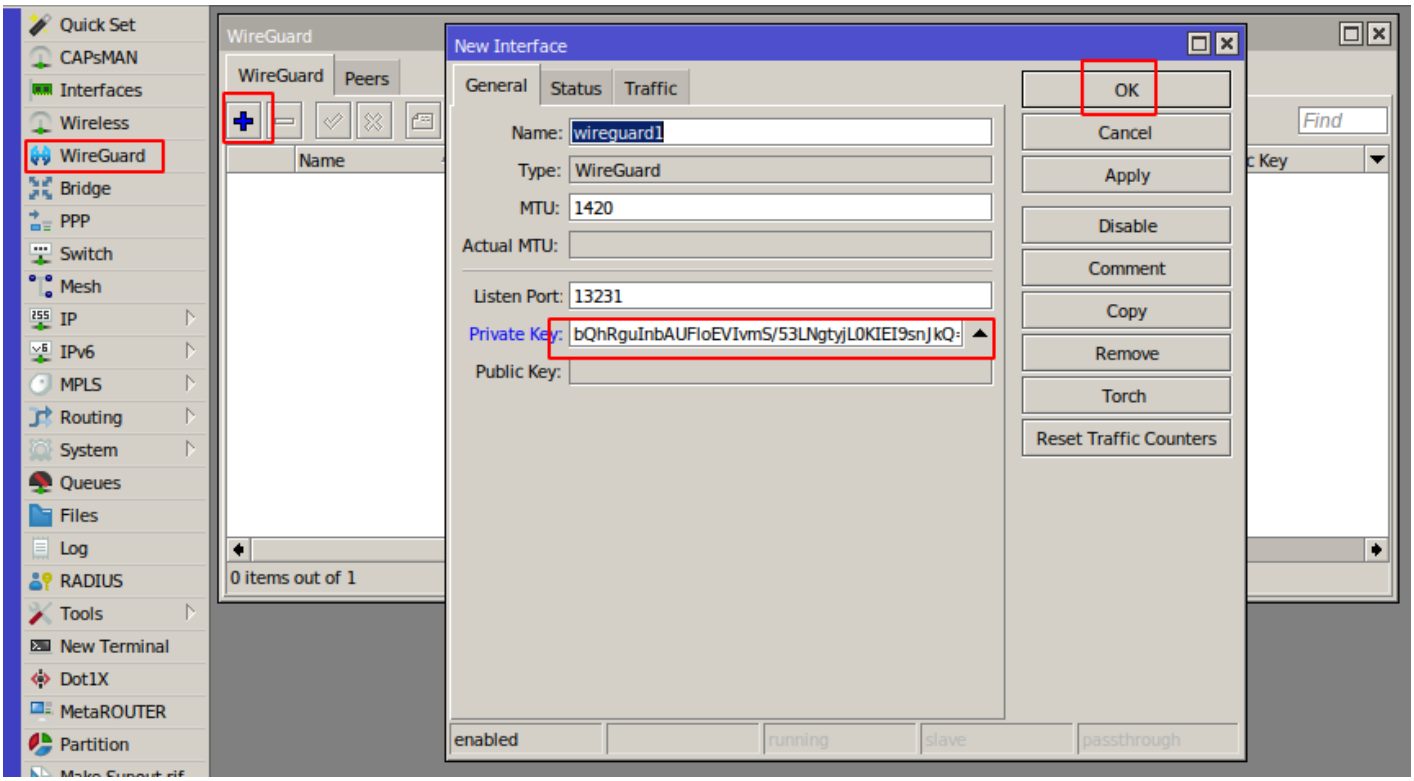
Dowload config file

```
[Interface]
        Address = 10.0.110.15/24
        DNS = 10.0.110.1,77.87.125.200
        PrivateKey = KGbQhRguInbAUFloEVIvmS/53LNgtyjL0KIEI9snJkQ=

[Peer]
        AllowedIPs = 0.0.0.0/0
        PersistentKeepalive = 5
        Endpoint = 77.87.125.200:51930
        PublicKey = xbrwVHxNZ8UsjHQyyzFwmOEy1UC+wvKQ0FG/cLoJh2w=
```

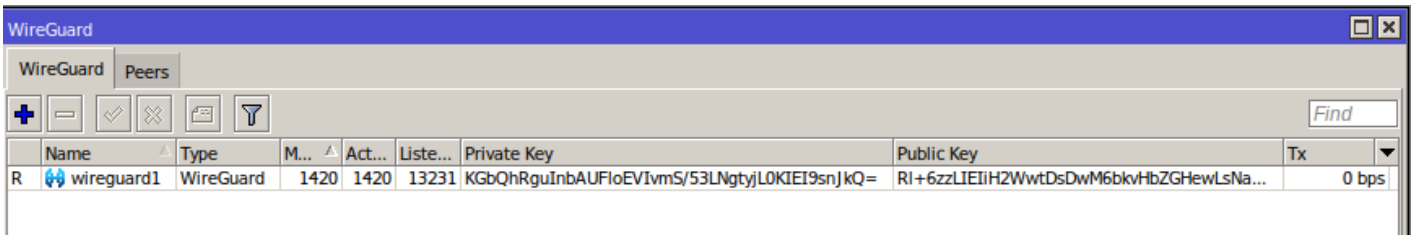
Login to **Mikrotik** via Winbox

Click on the menu item **WireGuard** In the window that opens, in the **WireGuard** tab, click the plus to add a new **WireGuard** interface

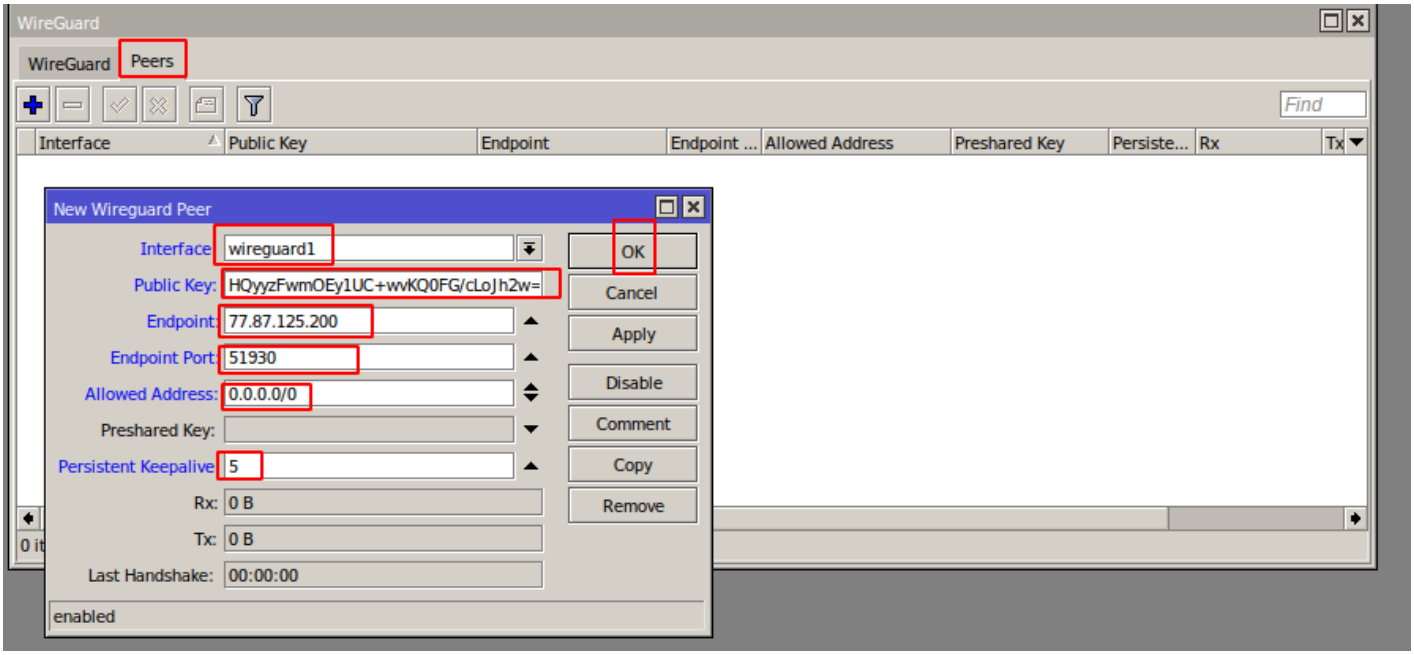


Copy the private key from the text configuration from the **[Interface]** section to the **PrivateKey** field in the **WireGuard** interface settings in **Mikrotik**

Click **OK** to create the interface



Go to the peers tab.
Click plus to add a new peer



Interface - Select the previously created **WireGuard** interface

Public key - Copy the public key from the text configuration from the **[Peer]** section to the Public key field

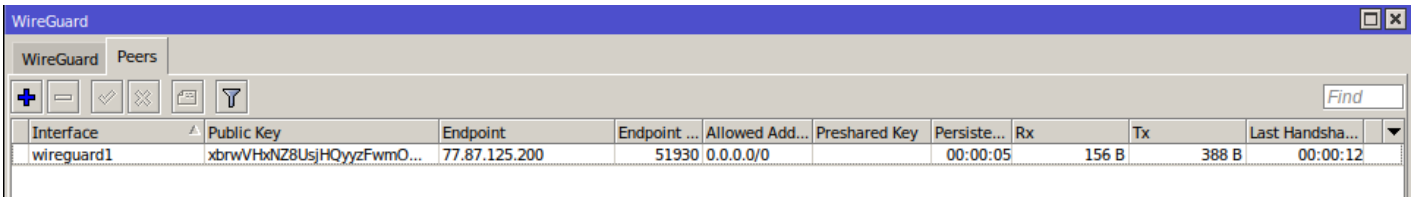
Endpoint - Copy the server **address** from the text configuration from the **[Peer]** section to the endpoint field

Endpoint Port - Copy the server **port** from the text configuration from the **[Peer]** section to the Endpoint Port field

Allowed Address - Copy **AllowedIPs** from the text configuration from the **[Peer]** section to the Allowed Address field

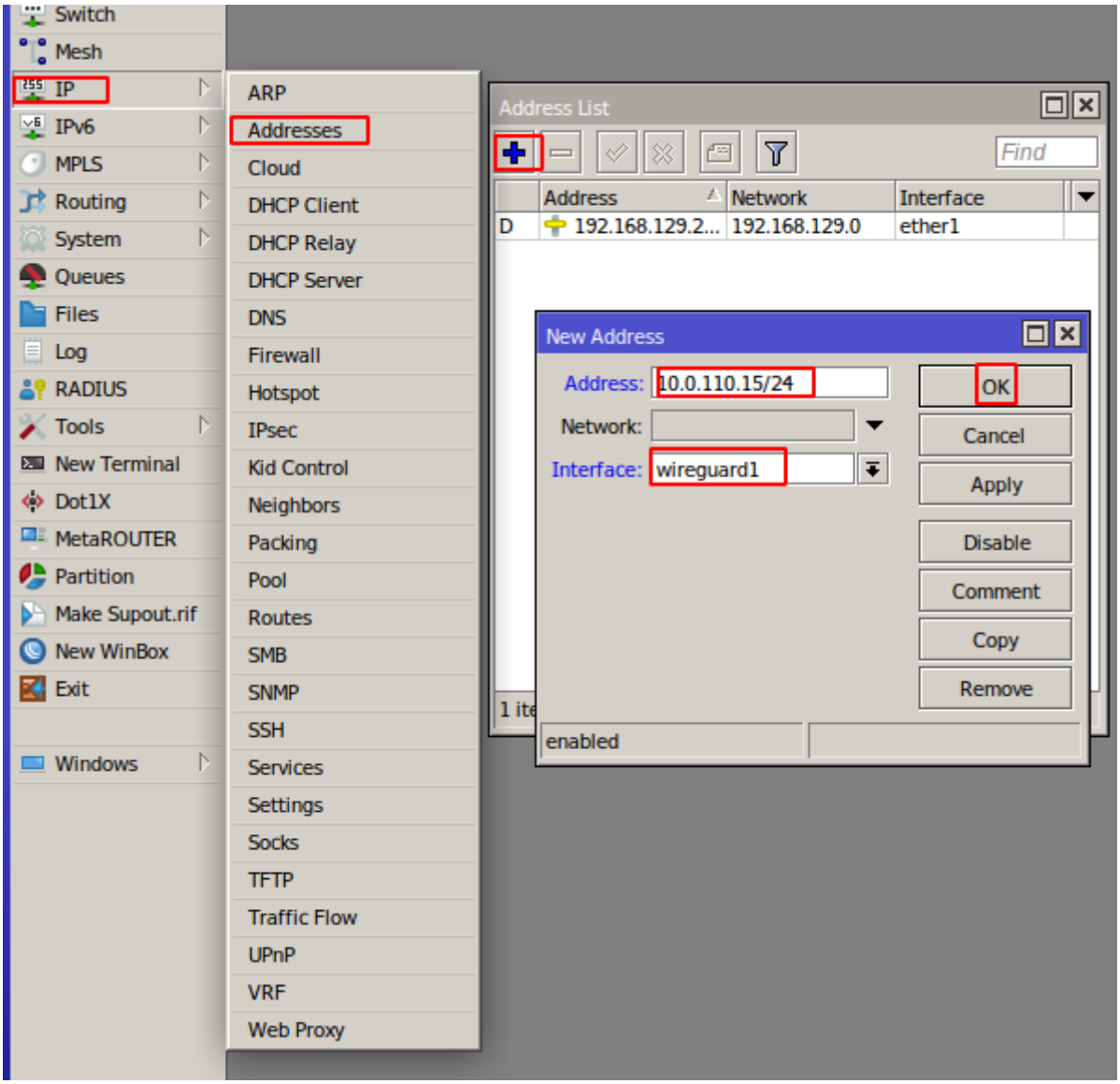
Persistent Keepalive - Copy the **PersistentKeepalive** from the text configuration from the **[Peer]** section to the Persistent Keepalive field

Click **OK** to create a peer



In order to have communication with the server, you need to set the address on the **WireGuard** interface

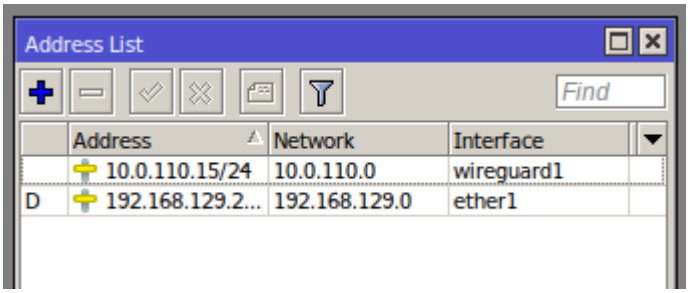
Go to the menu item **IP->Addresses** In the window that opens, click the plus to assign an IP address to the WireGuard interface



Addresse - Copy the Address from the text configuration from the **[Interface]** section to the Address field

Interface - Select the previously created **WireGuard** interface

Press the OK button to confirm



> You also need to configure the traffic routes you need at your discretion.

Admin Area

Admin Area

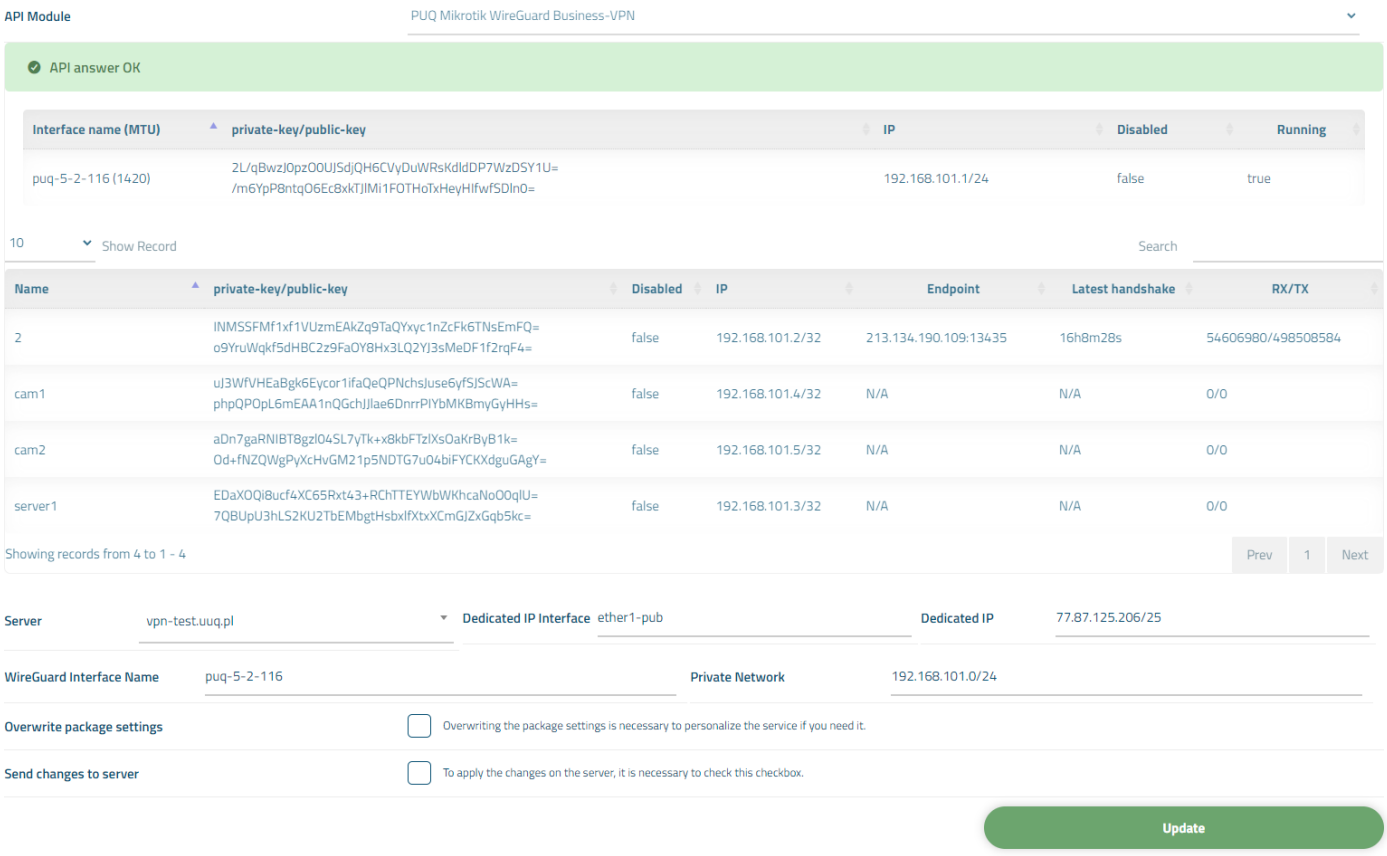
Order Detail

Mikrotik WireGuard Business-VPN module

WISECP

Order now | Download | FAQ

Navigate to the service you want to manage, then go to the '**Core**' tab.



In the opened tab, you have a view of the online status of the service. The available online information includes:

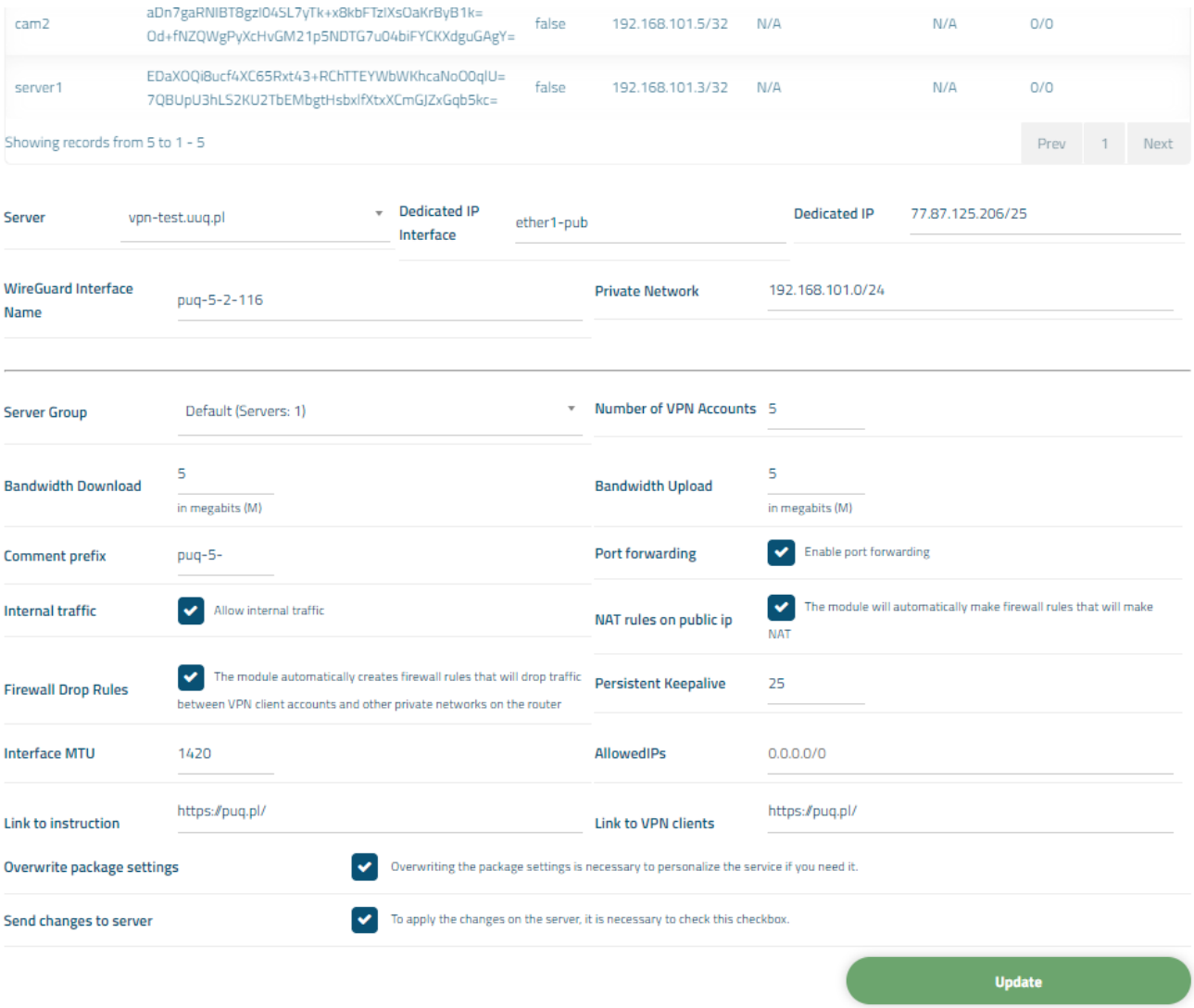
- Connection status to the API
- Information about the VPN account on the **MikroTik** router

- Information about the account

Also, below are fields with the client's personal data.

You can also individually override package options for the client by checking the '**Overwrite package settings**' box.

> After modifying the configuration options, check the '**Send changes to server**' box to save the data to the **MikroTik** server.



Client Area

Product Home Screen

Mikrotik WireGuard Business-VPN module

WISECP

Order now | Download | FAQ

Available options in the client panel:

- VPN Account Creation Button
- Port Forwarding Management Button
- Links in the form of buttons to the instruction and VPN clients
- General information about the service
- List of VPN Users Encrypted by the Client with Status and Edit Button

Screenshot of the client area

Add VPN account | Port Forwarding | User manual | Download VPN client

Network configuration

Dedicated IP:	77.87.125.206
Private internal network:	192.168.101.0/24
VPN Protocols:	WireGuard
Number of VPN accounts:	4/5
Bandwidtht download/upload:	5/5 M per account

VPN accounts

✓	✎	**2** (192.168.101.2/32)	WireGuard online: **yes** 213.134.190.109:13435 **RX/TX:** 54606980/498508584
✓	✎	**server1** (192.168.101.3/32)	WireGuard online: **not**
✓	✎	**cam1** (192.168.101.4/32)	WireGuard online: **not**
✓	✎	**cam2** (192.168.101.5/32)	WireGuard online: **not**

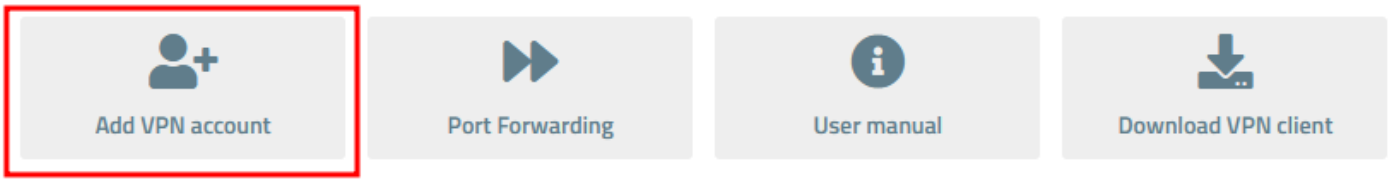
Add VPN account

Mikrotik WireGuard Business-VPN module

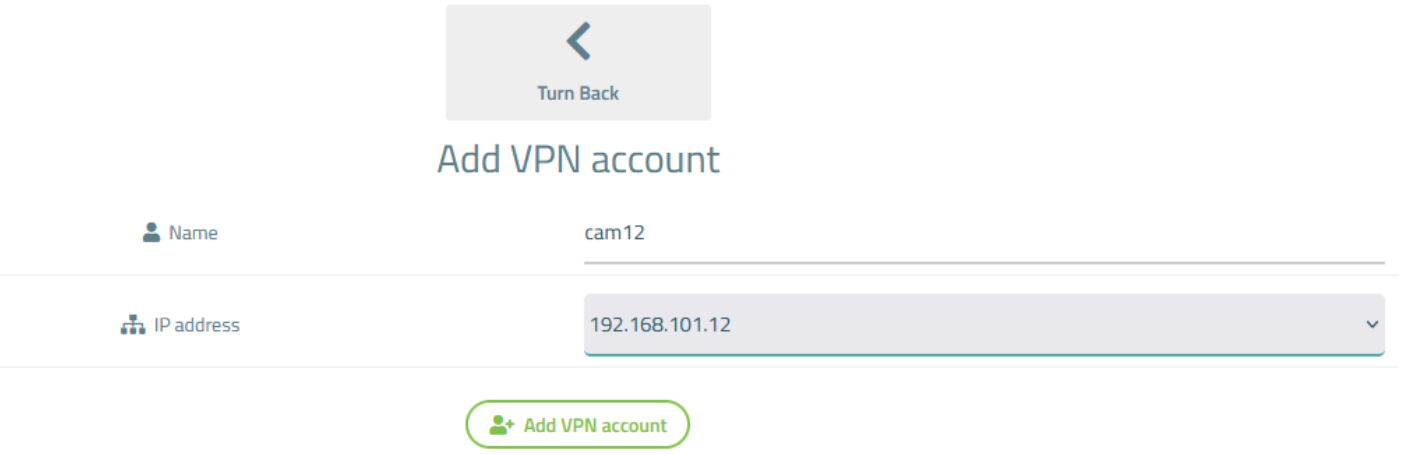
WISECP

Order now | Download | FAQ

To create a new VPN account, you need to click on the **"Add VPN Account"** button on the main screen of the product.



In the opened window, you need to enter the account name for identification, as well as select an IP address for the account that the account will use. Don't forget to click the **"Add VPN Account"** button.



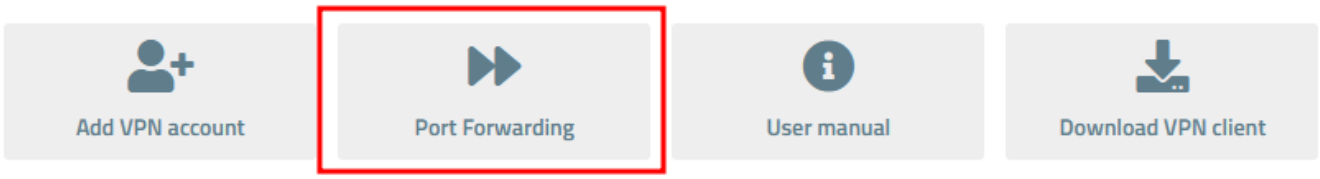
Port Forwarding

Mikrotik WireGuard Business-VPN module

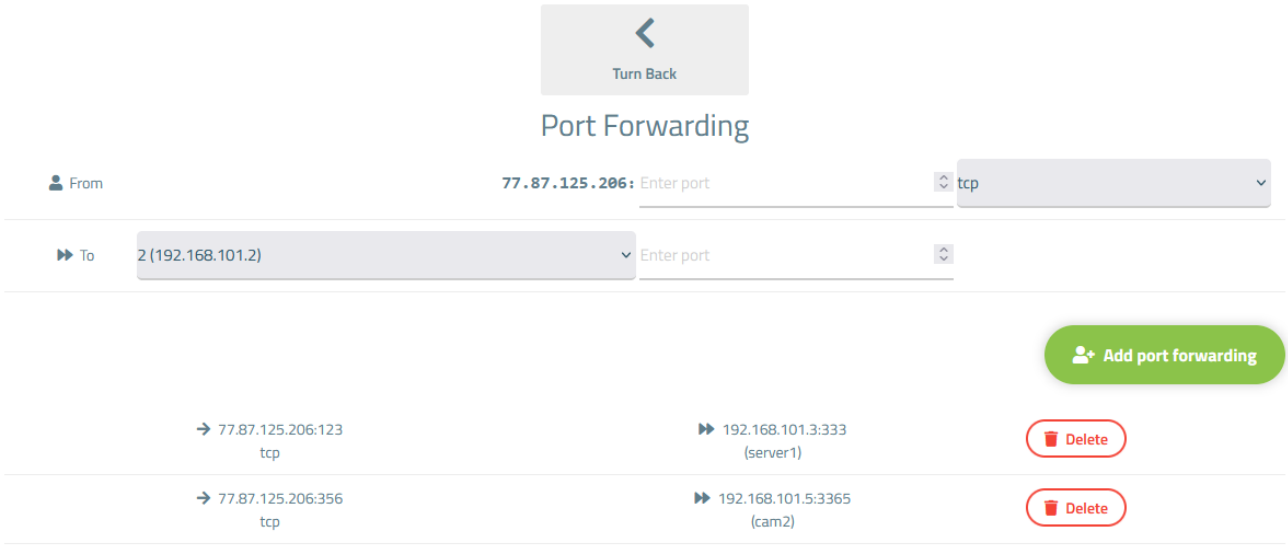
WISECP

Order now | Download | FAQ

To access the port forwarding settings, you need to click on the **"Port Forwarding"** button on the main screen of the product.



To create a new port forwarding rule, enter the port you want to forward, select the protocol, choose the VPN account from the dropdown list to which the port will be forwarded, and enter the port to which the forwarding will occur. After filling in the details, press the **"Add Port Forwarding"** button.



To delete an existing rule, you need to click the "**Delete**" button next to the rule you want to remove.