

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
 Bandwidth 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 answer OK

Interface name (MTU)	private-key/public-key	IP	Disabled	Running
puq-5-2-116 (1420)	2L/qBwzJOpz00UJSdjQH6CVyDuWRsKdldDP7WzDSY1U= /m6YpP8ntqO6Ec8xkJlIMi1F0THoTxHeyHlfwFSDIn0=	192.168.101.1/24	false	true

10

Show Record

Search

Name	private-key/public-key	Disabled	IP	Endpoint	Latest handshake	RX/TX
2	INM55FMf1xf1VUzmEakZq9TaQYxyc1nZcFk6TNsEmFQ= o9YruWqkf5dHBC2z9FaOY8Hx3LQ2YJ3sMeDF1f2rqF4=	false	192.168.101.2/32	213.134.190.109:13435	16h8m28s	54606980/498508584
cam1	uj3WfVHEaBgk6Eycor1ifaQeQPNchsluse6yfS/ScWA= phpQP0pL6mEAA1nQGchJJlae6DnrrPIYbMKBmyGyHHs=	false	192.168.101.4/32	N/A	N/A	0/0
cam2	aDn7gaRNIBT8gzIO4SL7yTk+x8kbFTzIXsOaKrByB1k= Od+fnZQWgPyXcHvGM21p5NDTG7u04biFYCKXdguGAgY=	false	192.168.101.5/32	N/A	N/A	0/0
server1	EDaXOQjBucf4XC65Rxt43+RChTTEYWbWKhcaNo0OqIU= 7QBUpU3hLS2KU2TbEMbgTHsbxlfXtxXCmGJZxGqb5kc=	false	192.168.101.3/32	N/A	N/A	0/0

Showing records from 4 to 1 - 4

Prev1Next

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](#)

v1.1 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/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

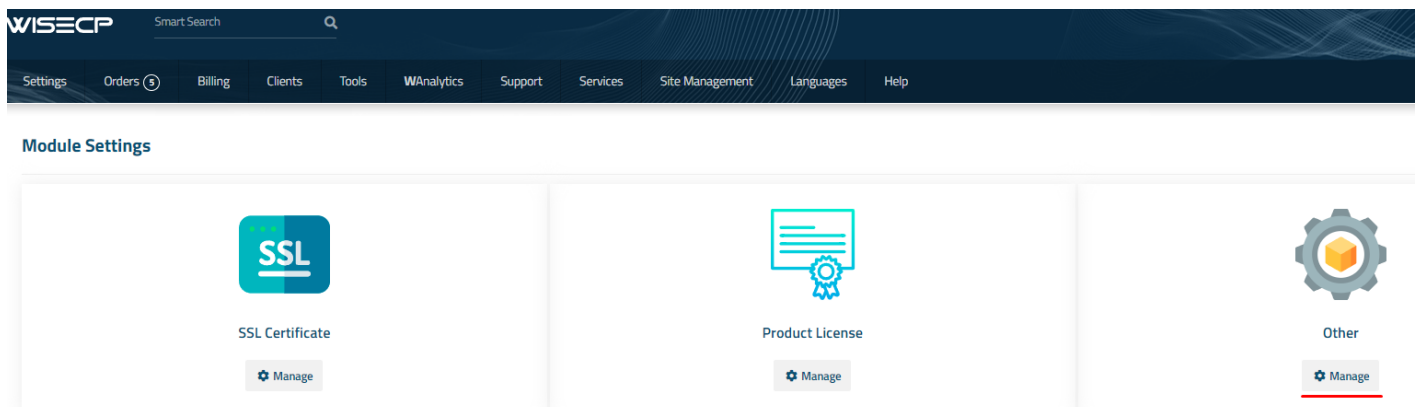
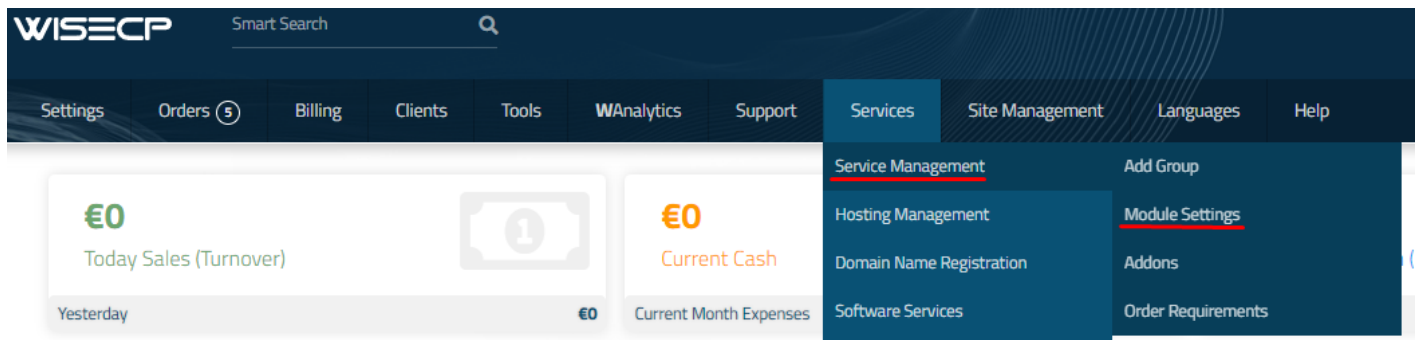
Mikrotik WireGuard Business-VPN module

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



Other

Other

Dashboard / Module Settings

Search Within Modules

Write something...

		<u>PUQ Mikrotik WireGuard Business-VPN</u>	

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.



PUQ Mikrotik WireGuard Business-VPN

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 address 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
```

Add server (Mikrotik) in WISECP

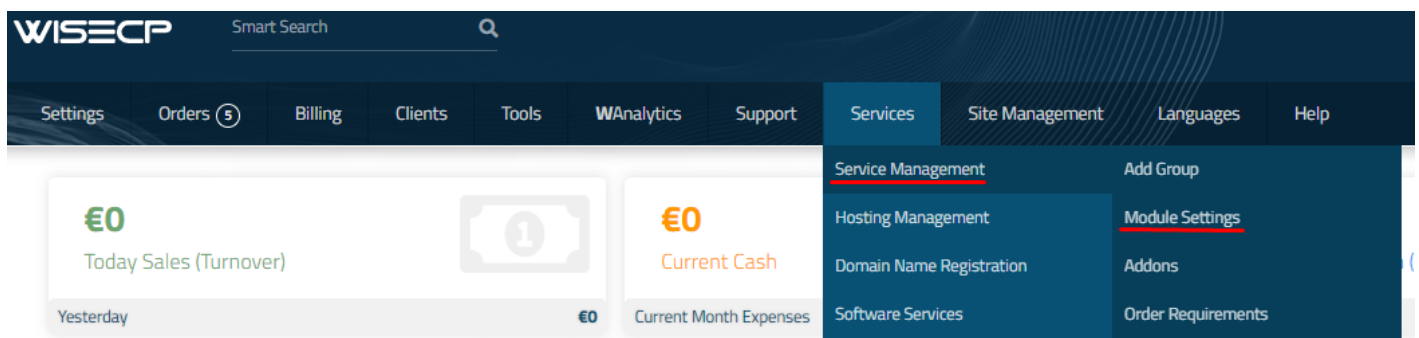
Mikrotik WireGuard Business-VPN module

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



WISECP Smart Search


Settings Orders (5) Billing Clients Tools WAnalytics Support Services Site Management Languages Help

Module Settings




SSL Certificate

Manage



Product License

Manage



Other

Manage

WISECP Smart Search

Settings Orders (5) Billing Clients Tools WAnalytics Support Services Site Management Languages Help

Other

Initial Settings

All Modules

WISECP Smart Search

Settings Orders Billing Clients Tools WAnalytics Support Services Site Management Languages Help

Other

Dashboard / Module Settings / C

Initial Settings

All Modules

Search Within Modules

Write something...

PUQ Mikrotik WireGuard VPN

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

WISSECP Smart Search Q

Settings Orders Billing Clients Tools WAnalytics Support Services Site Management Languages Help

Other Dashboard / Module Setting

Initial Settings All Modules

PUQ
cloud

PUQ Mikrotik WireGuard Business-VPN

License key R1BC6H- -YYQRKX 2023-12-20T22:17:00+01:00 [Check and Save](#)

Version: 1.0 [Web Site](#) [Documentation](#) [Changelog](#)

[+ Add New Server](#) [Server Groups](#)

Servers [MikroTik](#)

10 Show Record Search

#	Name	Status	Group	Default	IP/Domain	Usage Stats	
2	vpn-test.uuq.pl	active	Default	✓	vpn-test.uuq.pl	1/12	Edit Delete

Showing records from 1 to 1 - 1 Prev 1 Next

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 for 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	<input type="checkbox"/> Set as default server in group
DNS 1	77.87.125.10
DNS 2	77.87.125.20
Assigned IP Addresses <small>(One per line)</small>	<div>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</div> <div><interface> <public_ip>/<mask> <private_network>/<mask></div>
IP Address or Domain	vpn-test.uuq.pl
Username	wisecp-dev-MWG
Password	<div></div>
SSL	<input checked="" type="checkbox"/> Connect using SSL
Port	<div>443</div> <input type="checkbox"/> Change standard port
Test Connection	<div> Test Connection</div>

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

The screenshot displays the WISECP administrative interface. At the top, there is a dark blue header with the WISECP logo and a 'Smart Search' bar. Below the header is a navigation menu with tabs: Settings, Orders (5), Billing, Clients, Tools, WAnalytics, Support, Services (selected), Site Management, Languages, and Help. The 'Services' tab is active, showing a dropdown menu with options: Service Management, Add Group (highlighted with a red underline), Hosting Management, Module Settings, Domain Name Registration, Addons, Software Services, and Order Requirements. On the left side of the dashboard, there are two widgets: 'Today Sales (Turnover)' showing €0 for Yesterday, and 'Current Cash' showing €0 for Current Month Expenses. A third widget shows 'Current Month Expenses' with a coin icon and the number 1.

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

The screenshot shows the 'Create New Service Group' form in the WISECP dashboard. The form is titled 'Create New Service Group' and includes a breadcrumb trail 'Dashboard / Create New Service Group'. A green banner at the top states: 'Create a new service group, you can also create new categories and manage the existing one from here.' The form has tabs for 'EN', 'UK', and 'PL'. The fields are as follows:

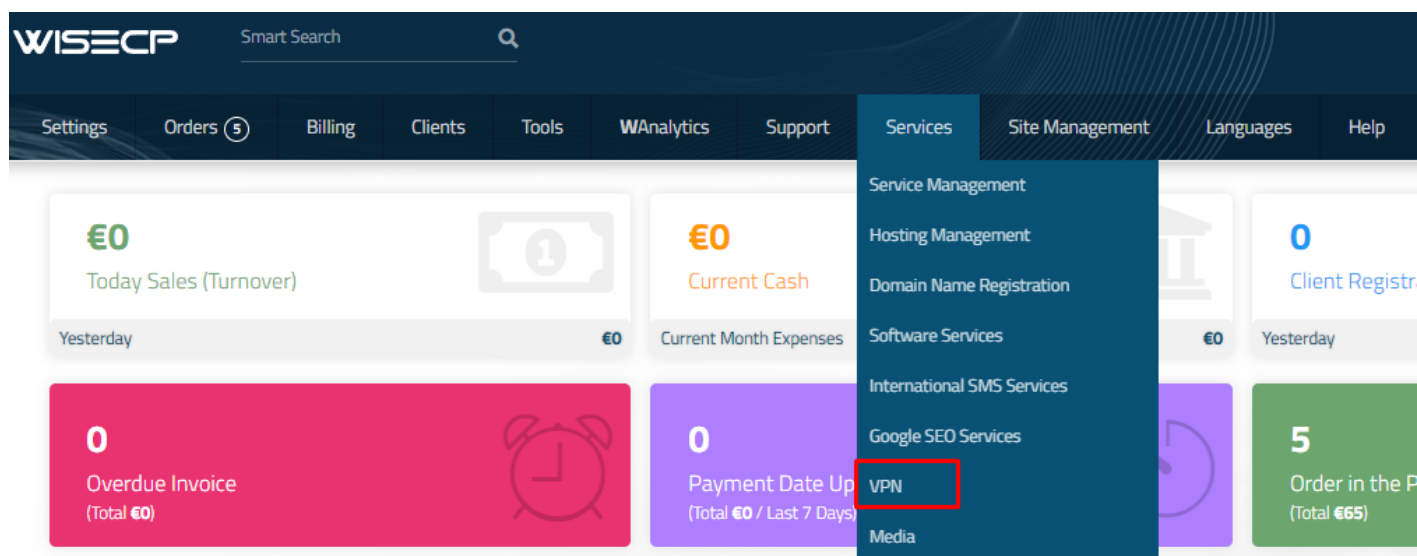
Field	Value
Title	VPN
Short Detail	Short Group Description
Listing Template	<input checked="" type="radio"/> Box List <input type="radio"/> Horizontal List
Status	Enable
Background Image	[Image placeholder]
Group Colour	#FFFFFF
Order Upgrades	<input type="checkbox"/> Allow clients to upgrade to higher package in the same service group
External HTML Code	Paste your HTML code to this field (Optional)

At the bottom, there is a note: 'You can optionally add external HTML code and customize it. There should not be any incorrect or incomplete HTML codes, otherwise page structure will be empty.'

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.

WISECP Smart Search

Settings Orders 5 Billing Clients Tools WAnalytics Support Services Site Management Languages Help

VPN

+ Create New Service Categories Service Group Settings

Apply to selected

10 Show Record

Service	Category	Amount
---------	----------	--------

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.

Edit Service Pack For VPN Dashboard / VPN / Mikrotik WireGuard Business-VPN 5 - Edit

i Detail Core + Optional Addons Requirements Upgradeable Products Pricing Active Services

Module PUQ Mikrotik WireGuard Business-VPN

Server Group	Default (Servers: 1)	Number of VPN Accounts	5
Bandwidth Download	5 in megabits (M)	Bandwidth Upload	5 in megabits (M)
Comment prefix	puq-5-	Port forwarding	<input checked="" type="checkbox"/> Enable port forwarding
Internal traffic	<input checked="" type="checkbox"/> Allow internal traffic	NAT rules on public ip	<input checked="" type="checkbox"/> The module will automatically make firewall rules that will make NAT
Firewall Drop Rules	<input checked="" type="checkbox"/> The module automatically creates firewall rules that will drop traffic between VPN client accounts and other private networks on the router	Persistent Keepalive	25
Interface MTU	1420	Allowed IPs	0.0.0.0/0
Link to instruction	https://puq.pl/ A link to the instruction will be reflected in the client area.	Link to VPN clients	https://puq.pl/ A link to the instruction will be reflected in the client area.

Automatic Setup ☒ Please activate for automatic installation of the order. Otherwise, administrator approval is required.

Edit Product

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

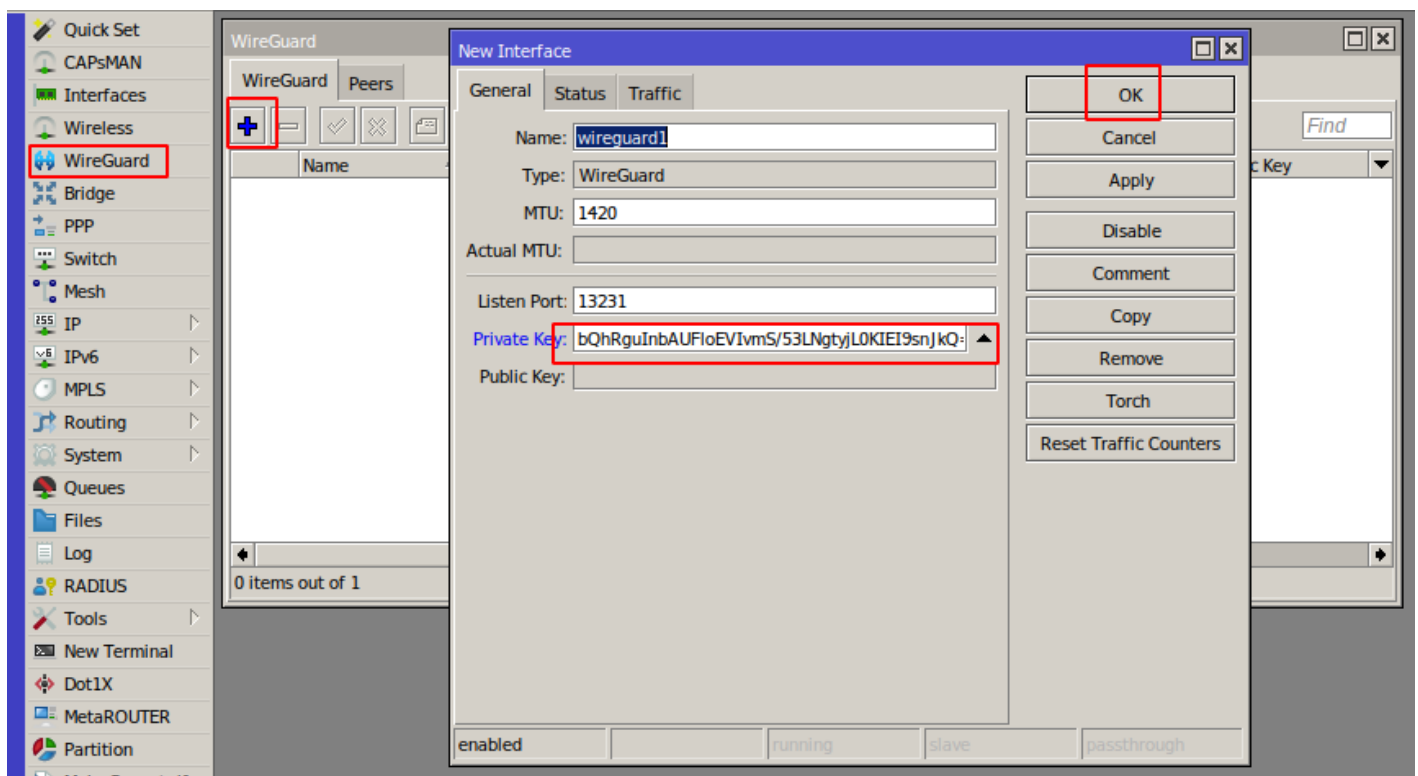
Download config file

```
[Interface]
  Address = 10.0.110.15/24
  DNS = 10.0.110.1,77.87.125.200
  PrivateKey = KgbQhRguInbAUFloEVImS/53LNgtYjL0KIEI9snJkQ=

[Peer]
  AllowedIPs = 0.0.0.0/0
  PersistentKeepalive = 5
  Endpoint = 77.87.125.200:51930
  PublicKey = xbrwVHxNZ8UsjHQyyzFwm0Ey1UC+vvKQ0FG/cLoJh2w=
```

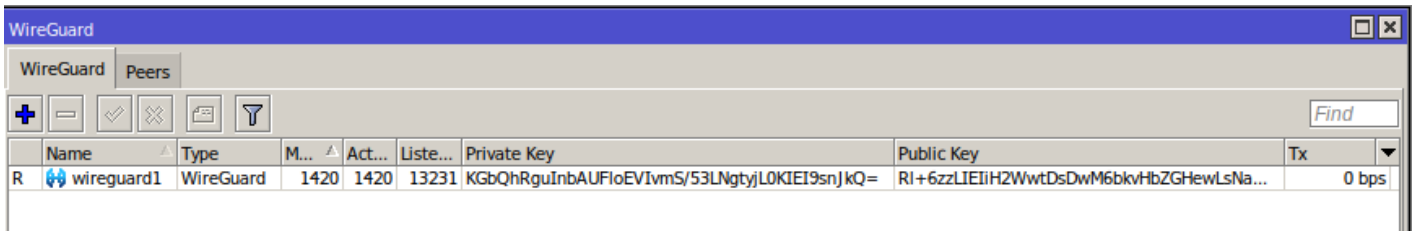
Login to Mikrotik via Winbox

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



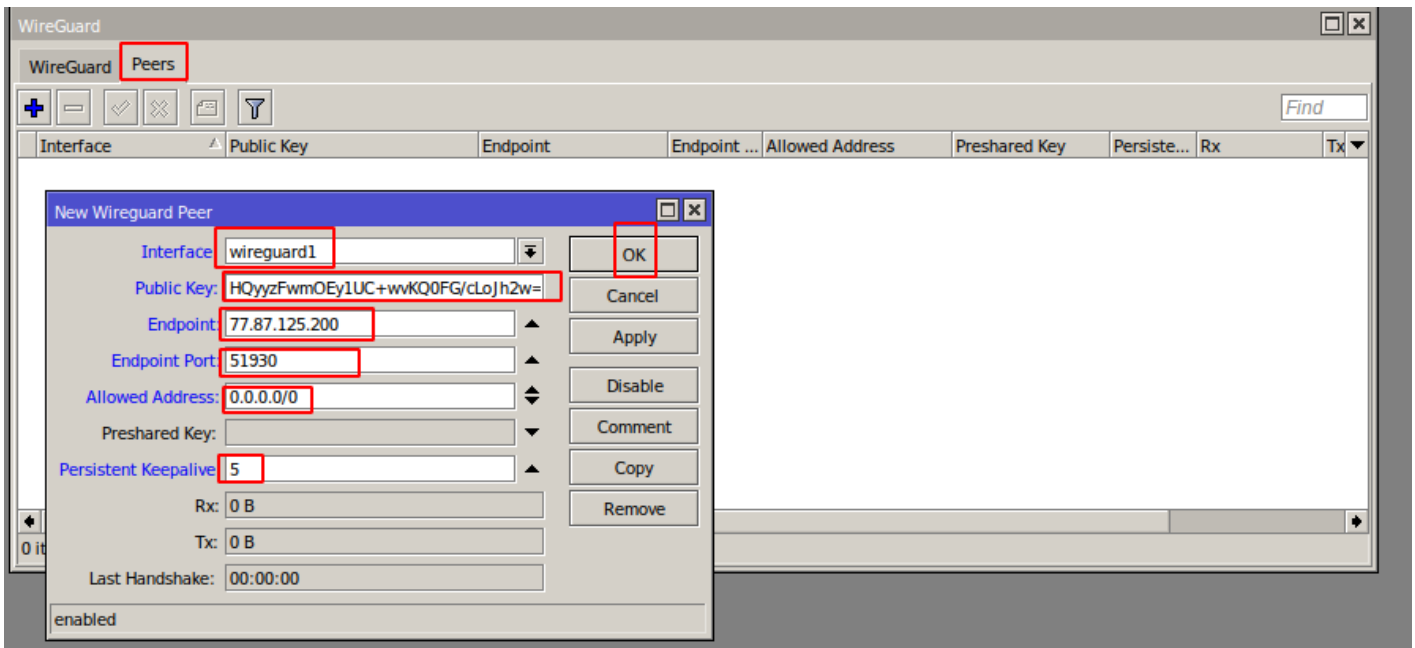
Copy the private key from the text configuration from the **[Interface]** section to the **PrivateKey** field in the **WireGuard** interface settings in **Mikrotik**

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

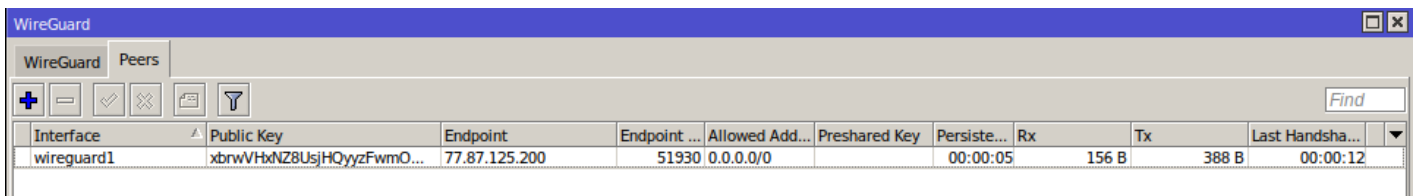
Endpoint - Copy the server **address** from the text configuration from the **[Peer]** section to the endpoint field

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

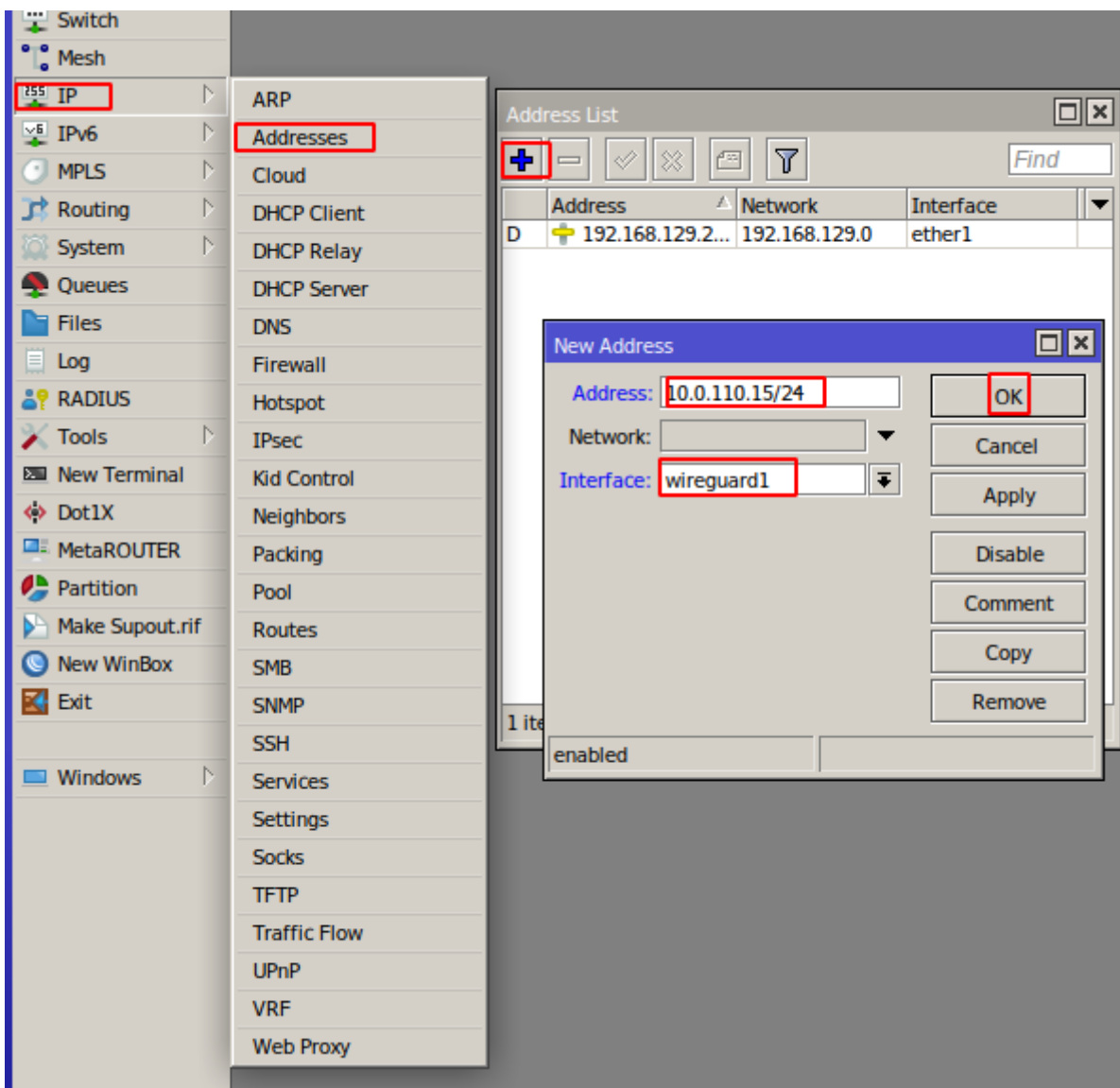


The image shows the 'WireGuard' window in a network configuration tool. It has a 'WireGuard' tab and a 'Peers' tab. Below the tabs is a toolbar with icons for adding, removing, and filtering. A table lists the configuration for the 'wireguard1' interface.

Interface	Public Key	Endpoint	Endpoint ...	Allowed Add...	Preshared Key	Persiste...	Rx	Tx	Last Handsha...
wireguard1	xbrwVHbNZ8UsjH0yzzFwmO...	77.87.125.200	51930	0.0.0.0/0		00:00:05	156 B	388 B	00:00:12

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

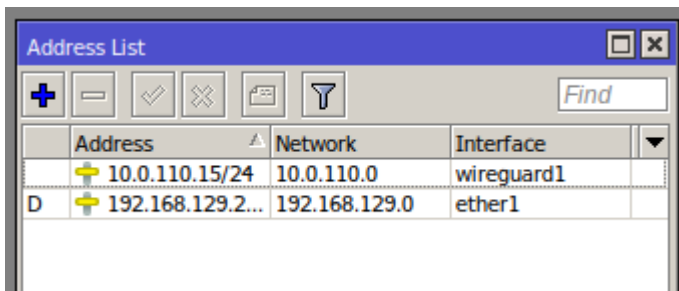
Go to the menu item **IP->Addresses** In the window that opens, click the plus to assign an IP address to the WireGuard interface



Adresse - 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

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.

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/qBwzJOpz00UJSdjQH6CVyDuWRsKddDP7WzDSY1U= /m6YpP8ntqO6Ec8xkJlMi1F0THoTxHeyHlfwFSDIn0=	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	uJ3WfVHEaBgk6Eycor1ifaQeQPNchsJuse6yfSJSWA= phpQP0pL6mEAA1nQGchJJlae6DnrrPIYbMKBmyGyHHs=	false	192.168.101.4/32	N/A	N/A	0/0
cam2	aDn7gaRNIBT8gzlO4SL7yTk+x8kbFTzIXsOaKrByB1k= Od+fNZQWgPyXcHvGM21p5NDTG7uO4biFYCKXdguGAgY=	false	192.168.101.5/32	N/A	N/A	0/0
server1	EDaXOQI8ucf4XC65Rxt43+RCHTEYwbWKhcaNo0OqIU= 7QBUpU3hLS2KU2TbEMbgTHsbxlfXtxXCmGJZxGqb5kc=	false	192.168.101.3/32	N/A	N/A	0/0

Showing records from 4 to 1 - 4

Prev1Next

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

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 '**Override package settings**' box.

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

cam2	aDn7gaRNIBT8gzIO4SL7yTk+x8kbFTzIXsOaKrByB1k=Od+fNZQWgPyXcHvGM21p5NDTG7u04biFYCKXdguGAgY=	false	192.168.101.5/32	N/A	N/A	0/0
server1	EDaX0Qi8ucf4XC65Rxt43+RChTTEYWbWKhcaNo00qIU=7QBUpU3hLS2KU2TbEMbgtHsbxifXtxXCmGJZxGqb5kc=	false	192.168.101.3/32	N/A	N/A	0/0
Showing records from 5 to 1 - 5						<div>Prev1Next</div>

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		
Server Group	Default (Servers: 1)	Number of VPN Accounts	5		
Bandwidth Download	5 in megabits (M)	Bandwidth Upload	5 in megabits (M)		
Comment prefix	puq-5-	Port forwarding	<input checked="" type="checkbox"/> Enable port forwarding		
Internal traffic	<input checked="" type="checkbox"/> Allow internal traffic	NAT rules on public ip	<input checked="" type="checkbox"/> The module will automatically make firewall rules that will make NAT		
Firewall Drop Rules	<input checked="" type="checkbox"/> The module automatically creates firewall rules that will drop traffic between VPN client accounts and other private networks on the router	Persistent Keepalive	25		
Interface MTU	1420	AllowedIPs	0.0.0.0/0		
Link to instruction	https://puq.pl/	Link to VPN clients	https://puq.pl/		
Override package settings	<input checked="" type="checkbox"/> Overwriting the package settings is necessary to personalize the service if you need it.				
Send changes to server	<input checked="" type="checkbox"/> To apply the changes on the server, it is necessary to check this checkbox.				

Update

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
 Bandwidth 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

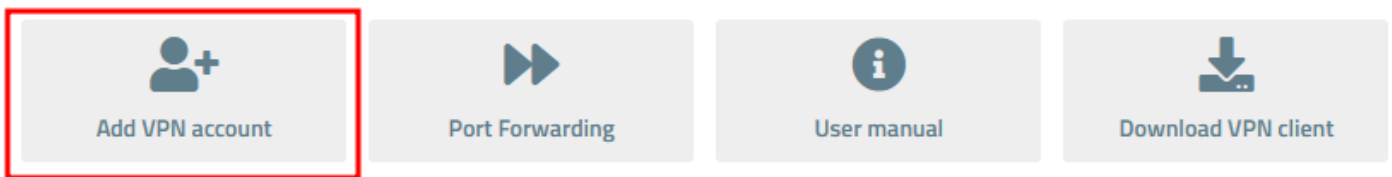
Add VPN account

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.

Turn Back

Add VPN account

Name

cam12

IP address

192.168.101.12

Add VPN account

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.


Turn Back

Port Forwarding

 From

77.87.125.206:

tcp

▼

▶▶ To

2 (192.168.101.2)

▼

↕

 Add port forwarding

→ 77.87.125.206:123 tcp	▶▶ 192.168.101.3:333 (server1)	<div> Delete</div>
→ 77.87.125.206:356 tcp	▶▶ 192.168.101.5:3365 (cam2)	<div> Delete</div>

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