

# PUQVPNCP installation and configuration

WireGuard Business-VPN module **WHMCS**

[Order now](#) | [Download](#) | [FAQ](#)

Official documentation:

[PUQVPNCP Documentation](#)

[PUQVPNCP Download](#)

[PUQVPNCP Order now](#)

## 1. Install the required packages

```
apt-get update
apt-get install wireguard wireguard-dkms wireguard-tools -y
apt-get install iproute2 iptables -y
apt-get install bind9 -y
```

## 2. Download the latest version of the package

<https://download.puqcloud.com/cp/puqvpncp/>

## 3. Install the puqvpncp package

```
wget https://download.puqcloud.com/cp/puqvpncp/puqvpncp_1.6.1_amd64.deb
dpkg -i puqvpncp_1.6.1_amd64.deb
```

## 4. After installation, connect to your server via a web

browser.

http://SERVER\_IP:8098

Username: admin

Password: admin

PUQVPNCP

Dashboard

VPN servers

Requirements

VPN accounts

Settings

About us

? HELP ?

ruslan (79.184.10.59)

Logout

Server Information

Hostname: dev.softkeel.com

OS Name: Debian GNU/Linux 11 (bullseye)

Architecture: amd64

CPU: Common KVM processor

CPU Threads: 4

Load: 0.02, 0.09, 0.14

Memory: 7956 MB

Used: 70%

Timezone: Europe/Warsaw

PUQVPNCP

Status: OK

Version: 1.0

WireGuards: 109

VPN Accounts: 548/550

License: 2023-11-13T18:38:43+01:00

License

Reload

WireGuard

wireguard: 1.0.20210223-1

wireguard-dkms: 1.0.20210219-1

wireguard-tools: 1.0.20210219-1

Configure

Firewall

iptables: 1.8.7-1

iproute2: 5.10.0-4

Configure

DNS server

bind9: 1:9.16.33-1~deb11u1

Running: PID: 3092940

Configure

In order for the system to start the procedure for obtaining an SSL certificate from Let's Encrypt, it is necessary.

The active domain name that resolves the server's IP address.

• Port 80 and 443 are always open, and not busy with another process

In the configuration file, enable the use of SSL and enter the domain name.

nano /etc/puqvpnncp/puqvpnncp.conf

LetsEncryptSSL=yes

Domain=XXXXXX.XXX

Restart the PUQVPNCP service

service puqvpnncp restart

After these steps, the first time you connect to the server via the https protocol, the system will request an SSL certificate and automatically renew it if necessary.

ATTENTION. After activating SSL, the system will only work in the https protocol on port 443. A redirect is also set from port 80 to port 443.

To connect to the server via the https protocol, use only the domain that was set in the configuration file. Otherwise, you will get an error that SSL is not working correctly.

The screenshot displays the PUQVPNCP web application interface. At the top, there's a navigation bar with the site name "PUQVPNCP" in large purple letters, followed by links for "? HELP ?", "ruslan (79.184.10.59)", and "Logout". Below this, a sidebar menu on the left contains links for "Dashboard", "VPN servers", "VPN accounts", "Settings", and "About us". The main content area shows the "API Access Hashes" page. A green banner at the top of this section reads "Successfully". Below it, a message states: "Everything went well. Please save the hash. It has only been shown once." Underneath the message, an "Access hash" field displays a long alphanumeric string, with a "Copy hash" button next to it. To the right of the hash field are two buttons: "Delete" (highlighted with a red box) and "Check now" (highlighted with a green box). Below this, a table lists existing API access hashes.

Name	IP	Created data	Last Login
test2	1.1.1.1	2022-11-18T10:38:37+01:00	
TEST	79.184.10.59	2022-11-15T15:23:05+01:00	2022-11-17T09:36:57+01:00
piotr2	79.184.10.59	2022-11-17T14:26:40+01:00	2022-11-17T14:42:08+01:00
Piotr	79.184.10.59	2022-11-16T14:23:48+01:00	

Accept the fact that once the Access Hashs API is created, it will only be shown once. Each API Access Hash only works from a specific IP address.

---

Revision #15

Created 24 November 2022 09:37:16 by Ruslan

Updated 11 June 2024 10:00:52 by Yuliia Noha