Image not found or type unknown

Installation and Configuration Guide

Step-by-step instructions for installing, configuring, and setting up the Mikrotik VPN WHMCS module, including Mikrotik router preparation (RouterOS certificates, HTTPS and API-SSL, VPN server), WHMCS integration, email templates, server registration, and product configuration.

- WHMCS Installation and Update
- Product Configuration
- Setup guide: Mikrotik preparation and configuration
- Add server (Mikrotik router)

WHMCS Installation and Update

Mikrotik VPN module **WHMCS**

Order now | Download | Community

System requirements

Requirement	Minimum
WHMCS	8.x+, 9.x+
PHP	7.4, 8.1, 8.2, 8.3, 8.4
Mikrotik RouterOS	7.x or higher
ionCube Loader	v15+

> **Note:** The module uses ionCube encoding. Make sure ionCube Loader is installed and active on your server.

Installation

> **Note:** The module now uses **ionCube 15**, which provides universal out-of-the-box support for all encodings.
>
> All versions can be found at this link:
> `https://download.puqcloud.com/WHMCS/servers/PUQ_WHMCS-Mikrotik-VPN/`

> Older module versions for WHMCS 8 are available in the archive directory: `https://download.puqcloud.com/WHMCS/servers/PUQ_WHMCS-Mikrotik-VPN/archive/`

1. Download the latest version from the PUQ download page:

```
wget https://download.puqcloud.com/WHMCS/servers/PUQ_WHMCS-Mikrotik-VPN/PUQ_WHMCS-Mikrotik-VPN-latest.zip
```

2. Unzip the archive:

```
unzip PUQ_WHMCS-Mikrotik-VPN-latest.zip -d PUQ_WHMCS-Mikrotik-VPN-latest
```

3. Upload the module files to your WHMCS installation:
   - For **Server modules:** copy the `puqMikrotikVPN` directory from the unzipped folder to `whmcs/modules/servers/`

```
cp -r PUQ_WHMCS-Mikrotik-VPN-latest/puqMikrotikVPN /path/to/whmcs/modules/servers/
```

4. The module files are now in place. Proceed to the configuration chapter to set up your Mikrotik router and WHMCS product.

Update

The update procedure is the same as installation — replace the existing files with the new version:

1. Download the latest version as described in the Installation section.
2. Unzip the archive.
3. For server modules: simply overwrite the files in `whmcs/modules/servers/puqMikrotikVPN/`. No deactivation is needed.
4. Verify the version number in the module interface matches the new release.

Product Configuration

Mikrotik VPN module **WHMCS**

Order now | Download | Community

Add new product to WHMCS

Navigate to **System Settings → Products/Services → Create a New Product**

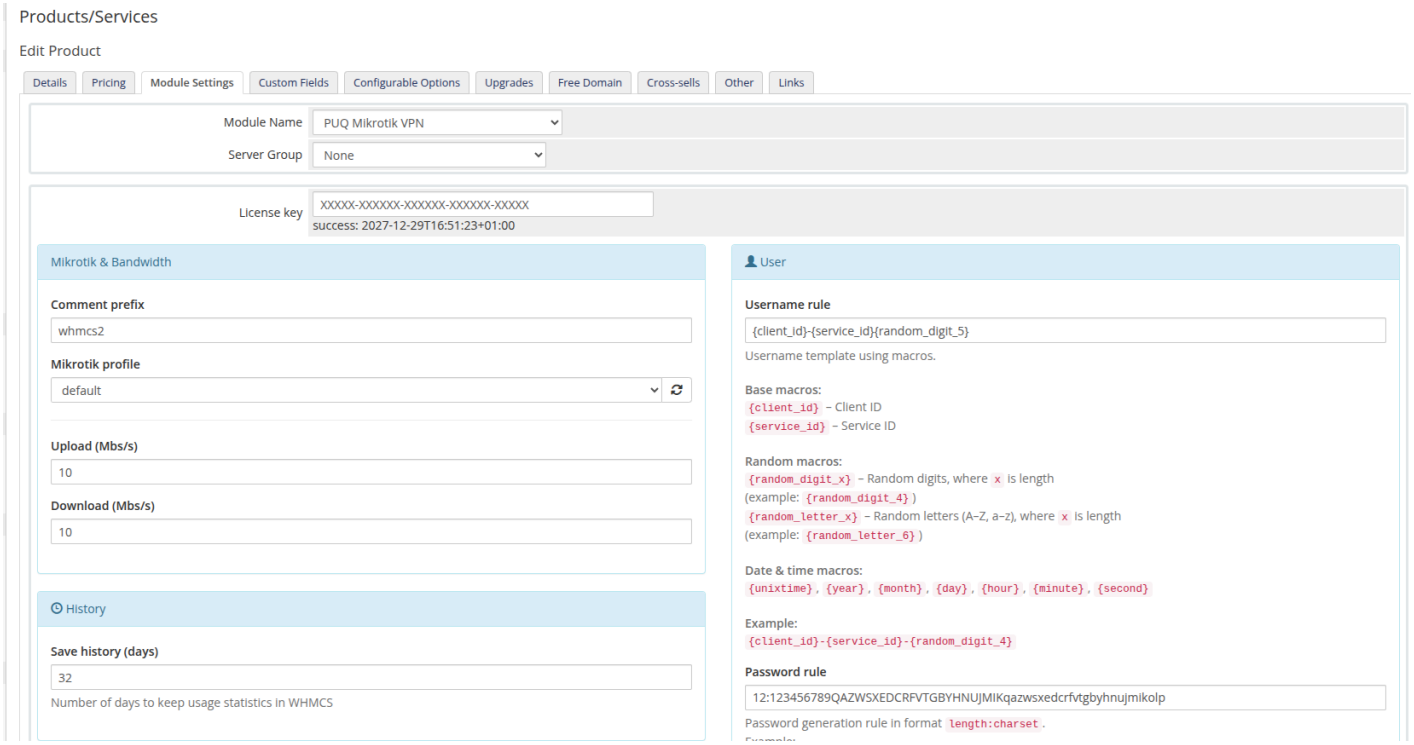
Select the **PUQ Mikrotik VPN** module in the Module settings section.

Configuration parameters

The module settings are divided into several logical blocks.

1. Mikrotik & Bandwidth

Parameter	Description
Comment prefix	Prefix applied to the VPN user comments on the Mikrotik router (e.g. `whmcs2`). Helps identify which PPP secrets belong to WHMCS-managed accounts.
Mikrotik profile	PPP secret profile on the Mikrotik router. The dropdown is populated with the profiles configured on the selected server.
Upload (Mbs/s)	Upload speed limit applied to the VPN account.
Download (Mbs/s)	Download speed limit applied to the VPN account.



product-configuration-overview.png

2. User Credentials Generation

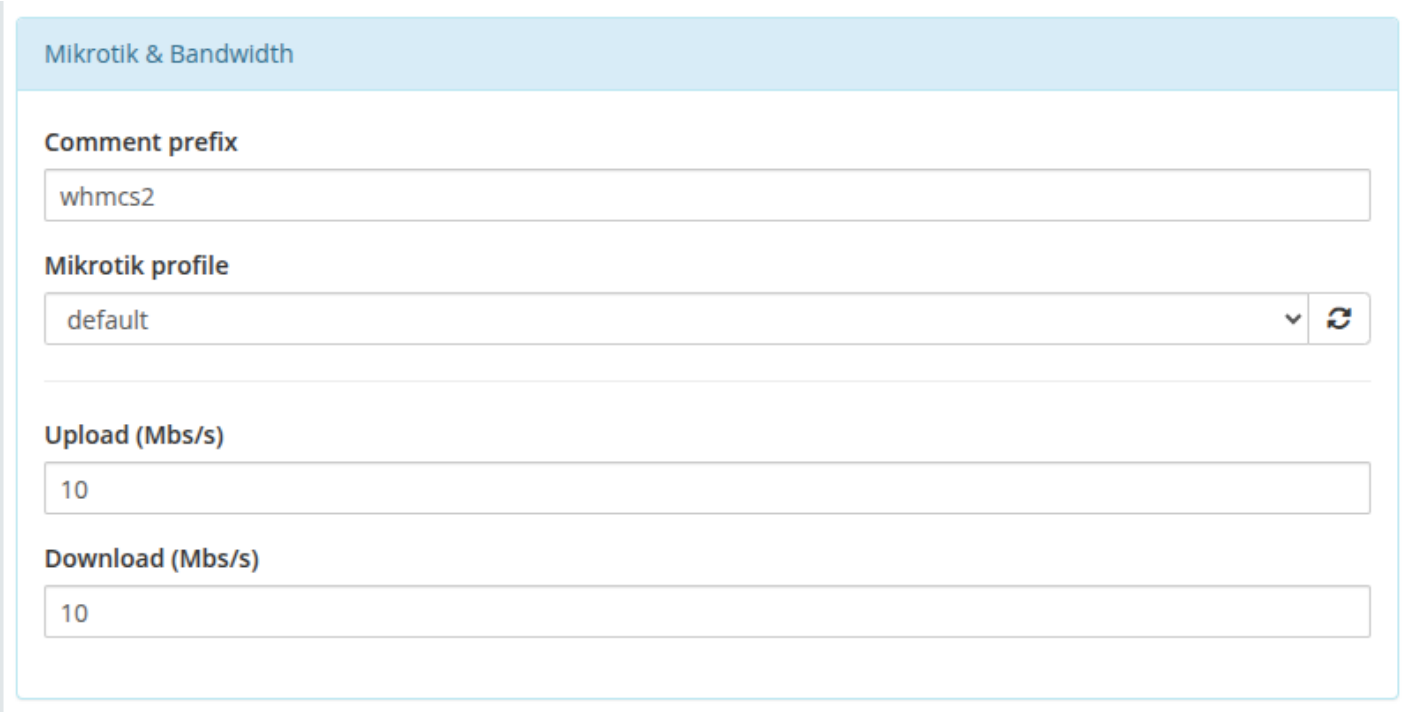
Parameter	Description
Username rule	Template for generating unique VPN usernames. You can use macros like `{client_id}`, `{service_id}`, `{random_digit_5}`, `{year}`, etc.
Password rule	Defines the format for auto-generating VPN passwords. Format: `length:charset` (e.g. `12:123456789QAZWSXEDCRFVTGBYHNUJMIKqazwsxedcrfvtgbyhnujmikol`).

3. History

Parameter	Description
Save history (days)	Number of days to keep daily usage statistics in the WHMCS database.

4. Client Area Settings

Parameter	Description
Link to instruction	A URL to a setup manual. This link will be displayed as a button in the client area.
Show password	Defines how the password is displayed in the client area (e.g., as a toggleable button).



product-configuration-client-area.png

---

5. VPN Protocols (PPTP, L2TP, OpenVPN, SSTP)

You can selectively enable and configure which VPN protocols are available to the client.

Parameter	Description
Enable [Protocol]	Toggles the display of connection details for the specific protocol in the client area.
Custom HTML	Allows injecting custom HTML instructions specifically for this protocol block in the client area.
L2TP IPSEC PSK KEY	*(L2TP only)* The pre-shared key for IPSec.
Profile download URL	*(OpenVPN only)* A direct link to download the `.ovpn` configuration profile.

User

Username rule

{client_id}-{service_id}{random_digit_5}

Username template using macros.

Base macros:
`{client_id}` – Client ID
`{service_id}` – Service ID

Random macros:
`{random_digit_x}` – Random digits, where `x` is length
(example: `{random_digit_4}`)
`{random_letter_x}` – Random letters (A–Z, a–z), where `x` is length
(example: `{random_letter_6}`)

Date & time macros:
`{unixtime}`, `{year}`, `{month}`, `{day}`, `{hour}`, `{minute}`, `{second}`

Example:
`{client_id}-{service_id}-{random_digit_4}`

Password rule

12:123456789QAZWSXEDCRFVTGBYHNUJMIKqazwsxedcrfvtgbyhnujmikolp

Password generation rule in format `length:charset`.
Example:
`12:1234567890`
This will generate a 12-character password using the provided characters.

product-configuration-pptp.png

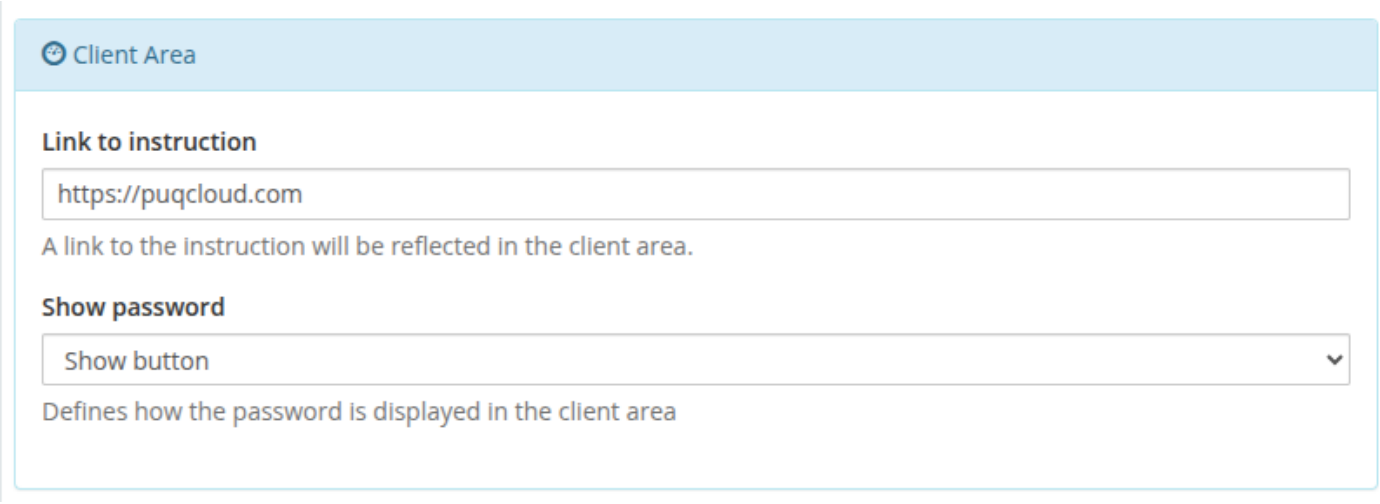
History

Save history (days)

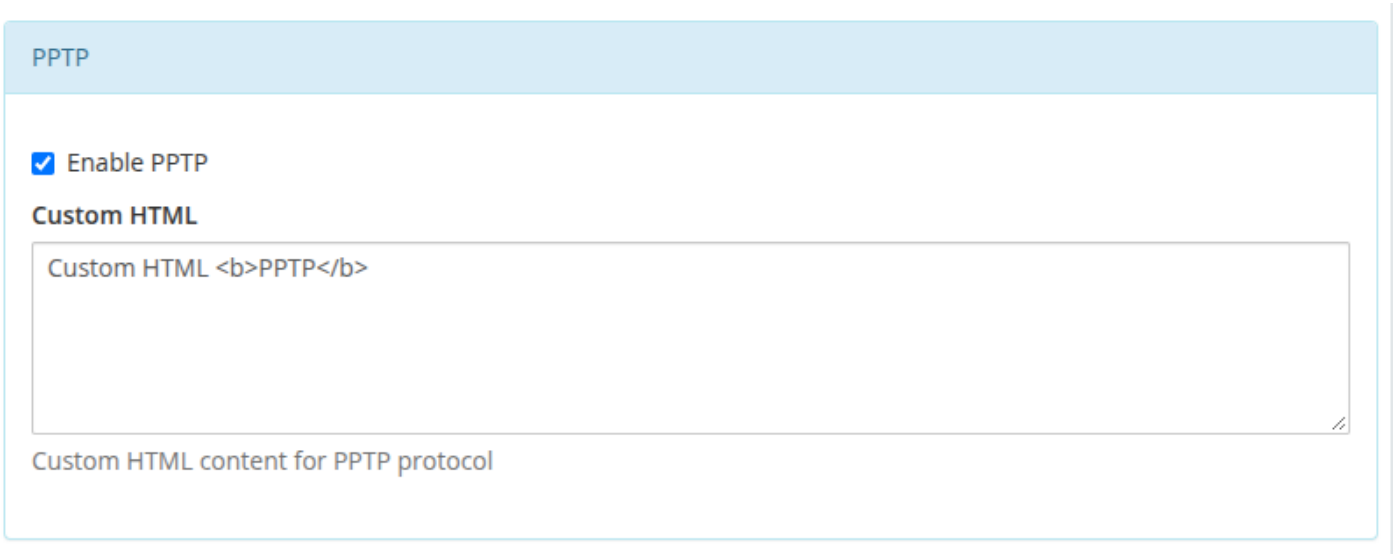
32

Number of days to keep usage statistics in WHMCS

product-configuration-l2tp.png



product-configuration-openvpn.png



product-configuration-sstp.png

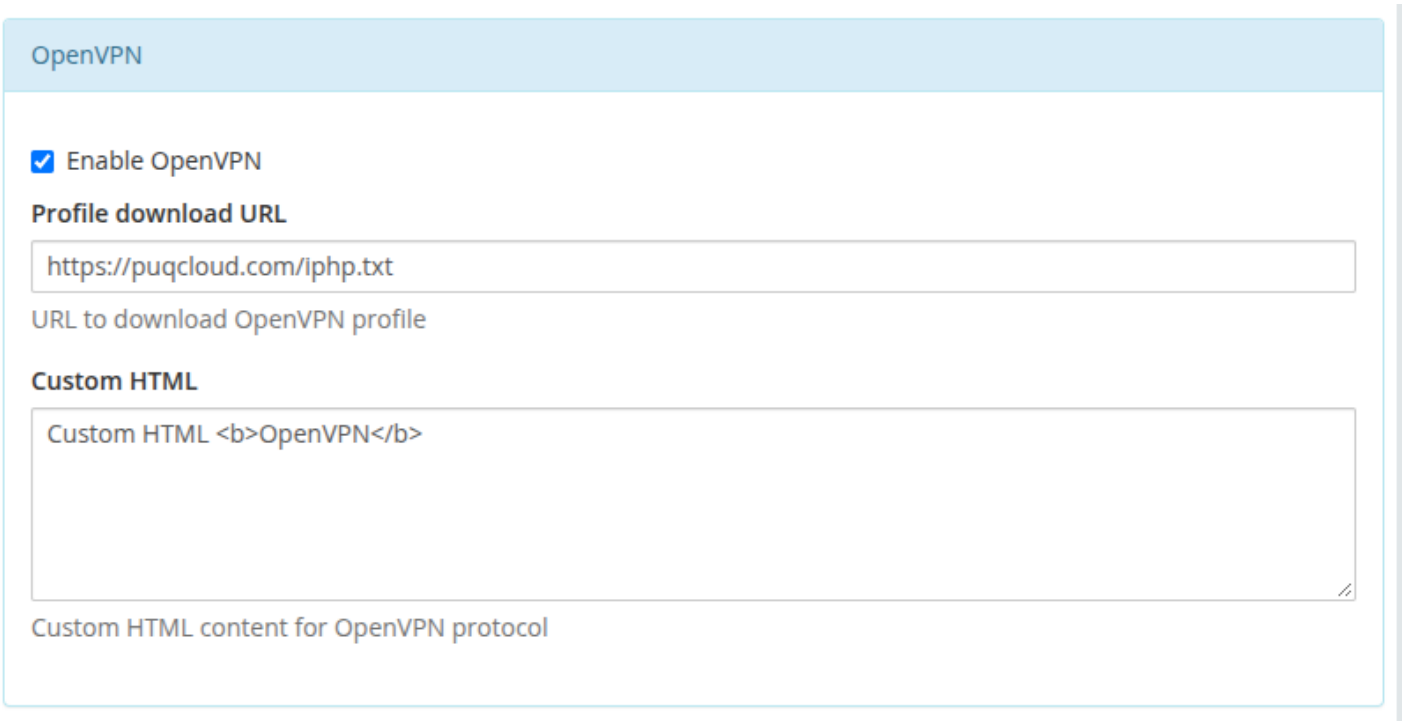
Metric Billing Configuration

The PUQ Mikrotik VPN module supports WHMCS **Metric Billing**, allowing you to charge clients post-paid based on their actual traffic usage.

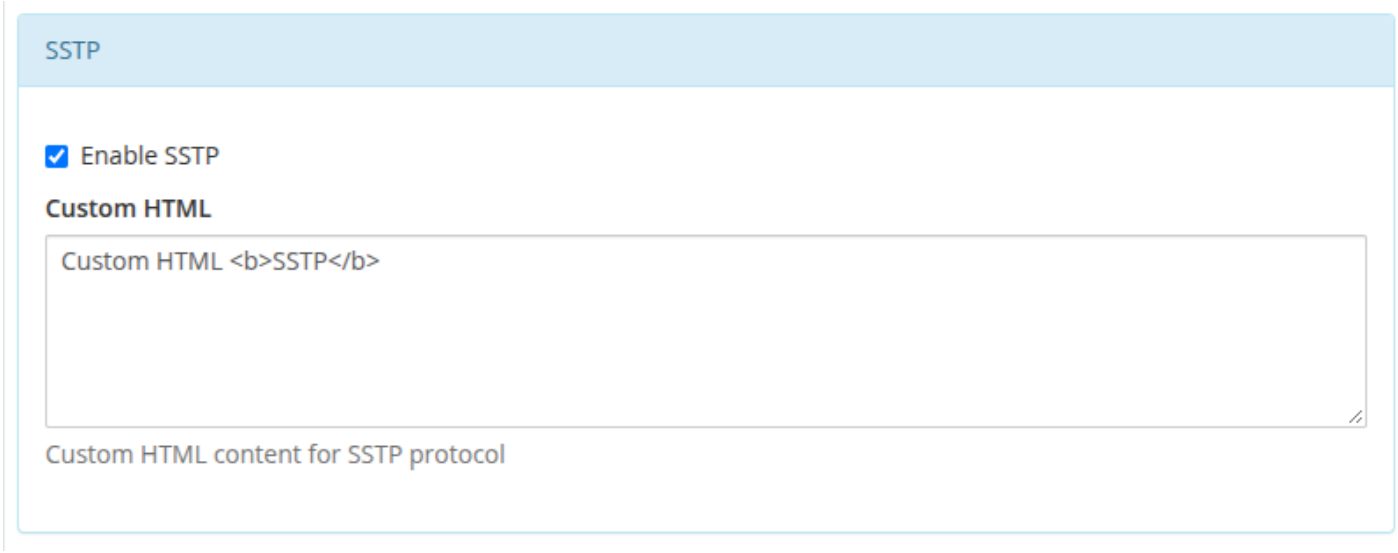
1. Navigate to the **Metric Billing** section in your product settings.
2. Toggle the switches to **ON** for **Bandwidth Usage Download (GB)** and **Bandwidth Usage Upload (GB)**.
3. Click **Configure Pricing** to set your rates per GB across your supported currencies.



product-configuration-metric-billing.png



metric-billing-download.png



metric-billing-upload.png

> **Important Note on Mikrotik Bandwidth:** The module intentionally registers opposite upload/download values on the Mikrotik router compared to WHMCS, because Mikrotik measures incoming traffic while VPN clients experience outgoing traffic.

Setup guide: Mikrotik preparation and configuration

Mikrotik VPN module **WHMCS**

Order now | Download | Community

This guide covers the preparation of a Mikrotik router for use with the PUQ Mikrotik VPN WHMCS module: root CA certificate, Webfig certificate, HTTPS, API-SSL and VPN server activation.

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

---

1. Check RouterOS version

Ensure RouterOS version is 7.x or higher:

```
system/package/print
```

---

2. Create a root CA on the router

Enable HTTPS by creating your own local root Certificate Authority:

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

3. Sign the root CA certificate

```
/certificate
sign LocalCA
```

4. Create a non-root certificate for Webfig

> Replace `xxx.xxx.xxx.xxx` with your router's public IP address (or the hostname you use to reach it).

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

5. Sign the Webfig certificate with the local CA

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

6. Enable HTTPS (www-ssl) with

the Webfig certificate

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

---

7. Enable API-SSL with the Webfig certificate

The PUQ Mikrotik VPN module communicates with the router through the **API-SSL** service:

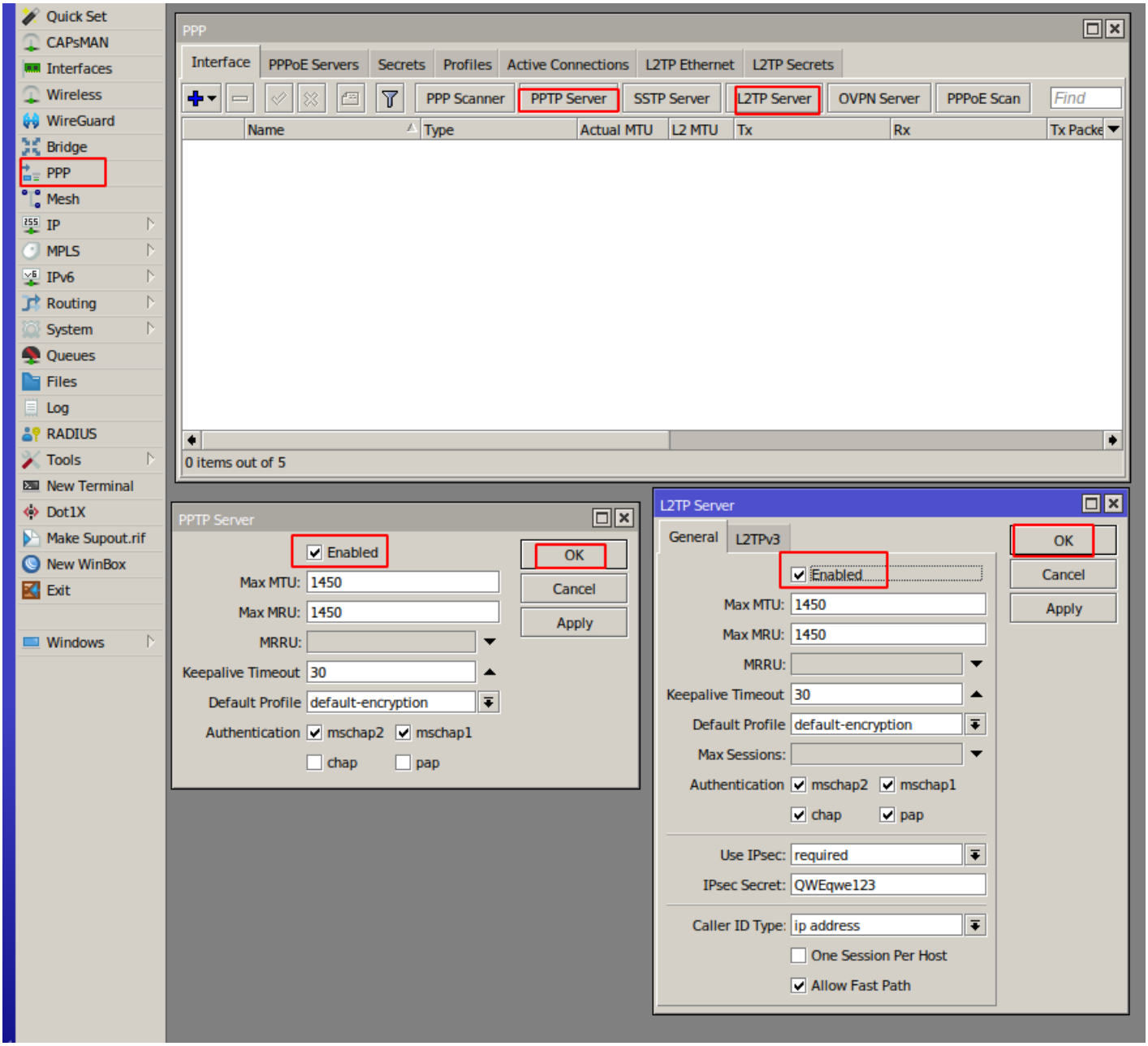
```
/ip service
set api-ssl certificate=Webfig disabled=no
```

> **Important:** The module uses the Mikrotik API only. Make sure the API-SSL port is reachable from the WHMCS server.

---

8. Enable VPN server

Enable the VPN protocol(s) you plan to offer to clients (PPTP, L2TP, etc.) and configure the corresponding PPP profile, service and IP pool. The PPP profile name configured here will later be selected in the product settings on the WHMCS side.



mikrotik-vpn-setup.png

---

9. Firewall, NAT and routing

Configure NAT, firewall and routing on the Mikrotik router so that VPN clients can reach the Internet and any internal resources you want to expose. The module itself only provisions the user account (PPP secret) — the surrounding network configuration is the responsibility of the router administrator.

> **Important:** The module registers opposite values for upload and download

> speeds in the Mikrotik router compared to the WHMCS product settings, because Mikrotik measures incoming traffic while VPN clients experience outgoing traffic.

Add server (Mikrotik router)

Mikrotik VPN module **WHMCS**

Order now | Download | Community

Adding a Mikrotik router to WHMCS

Configure a Mikrotik router as a server within WHMCS using the PUQ Mikrotik VPN module.

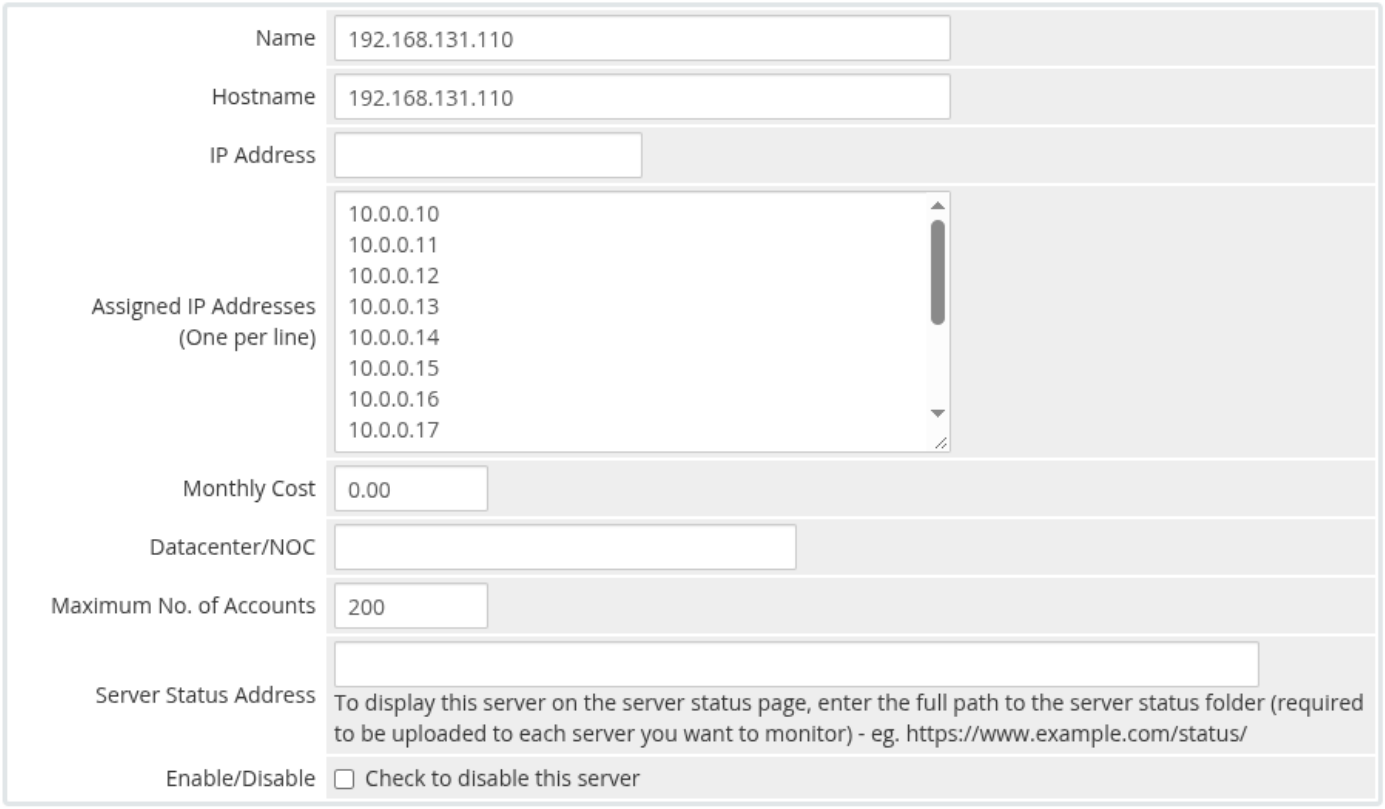
Navigate to **System Settings** → **Servers** → **Add New Server**

Step 1: General settings

Enter the correct **Name** and **Hostname** for your Mikrotik router.

- **Name** — an internal identification for the server (e.g. "My great Mikrotik router")
- **Hostname** — a resolvable domain pointing to the router's IP address (e.g. `vpn.mydomain.com`)

If your Mikrotik API-SSL service listens on a non-standard port, enter it in the **Port** field. Check the **Secure** checkbox (the module talks to the router through API-SSL).



add-server-general.png

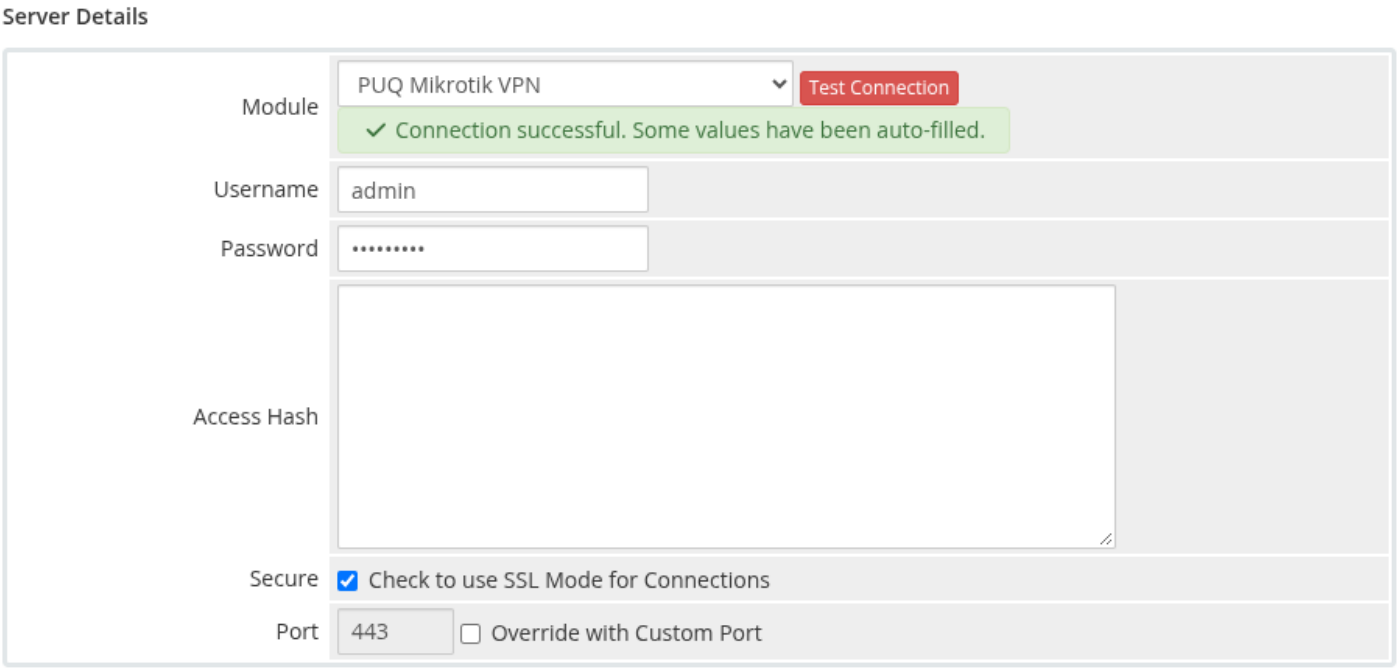
Step 2: Assigned IP addresses

In the **Assigned IP Addresses** field, enter the list of IP addresses that will be distributed to users. These IPs are consumed sequentially as new VPN accounts are provisioned. Both private and public IP addresses are supported.

Step 3: Module settings

1. In the Server Details section, select the **PUQ Mikrotik VPN** module from the dropdown
2. Enter valid Mikrotik router credentials:
   - **Username** — Mikrotik user with API access (typically with the `full` group or custom group that includes `api`, `write`, `read`, `policy`)
   - **Password** — the corresponding password
3. Click **Test connection** to verify the connection is working correctly

The test connection verifies that the module can reach the Mikrotik API-SSL service and authenticate with the provided credentials.



add-server-module-settings.png

> **Important:** The Mikrotik user must have sufficient privileges to create and manage PPP secrets, read traffic counters and reset them. The module uses the Mikrotik API only — SSH access is not used.