Mikrotik VPN WHMCS module

WHMCS server provisioning module for Mikrotik VPN accounts (PPTP, L2TP, OpenVPN, SSTP) via RouterOS API. Features automated lifecycle, bandwidth shaping, atomic traffic statistics, post-paid metric billing, single reset interface, and multilingual admin and client interfaces.

- Description
- Changelog
- Installation and Configuration Guide
  - WHMCS Installation and Update
  - Product Configuration
  - Setup guide: Mikrotik preparation and configuration
  - Add server (Mikrotik router)
- Admin Area
  - Product Information
- Client Area
  - Client Area Home Screen
  - Traffic Statistics
  - Usage Metrics

Description

Mikrotik VPN module **WHMCS**

Order now | Download | Community

Mikrotik VPN WHMCS module

The Mikrotik VPN WHMCS module is a provisioning module that integrates WHMCS with Mikrotik routers, enabling Internet and VPN service providers to offer VPN accounts to their customers. The module automates the full lifecycle of VPN account management using the Mikrotik API only.

Main features

- **Automatic account provisioning** — auto create and deploy client VPN accounts on the Mikrotik router upon order activation
- **Account lifecycle management** — create, suspend, unsuspend, terminate, change package, change password, and reset VPN interface
- **Bandwidth control** — configurable download / upload speed limits (M/s) enforced by the Mikrotik PPP profile
- **Metric billing** — post-paid usage-based billing for incoming and outgoing traffic (GB) via standard WHMCS MetricProvider
- **Atomic traffic statistics** — daily and monthly traffic charts with Google Charts, with atomic database increments preventing race condition losses
- **Multi-language support** — 26 languages including 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
- **Client area integration** — customers can view the VPN server address, available protocols, credentials with copy-to-clipboard, connection status, bandwidth limit and traffic statistics
- **Admin area tools** — administrators can view license status, Mikrotik API connection status (with 15s timeout protection), product information and manage VPN accounts via standard WHMCS module buttons

- **IP address pool** — the module distributes IP addresses from the list specified in the WHMCS server settings; both private and public IPs are supported
- **Configurable protocol support** — independent toggles for PPtP, L2TP (with IPSec PSK), OpenVPN, and SSTP protocols with custom instruction HTML per protocol
- **Instruction and client links** — optional URLs to VPN setup manuals and client downloads displayed as action buttons in the client area
- **License verification** — built-in license system with online / offline verification and admin alerts

---

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+

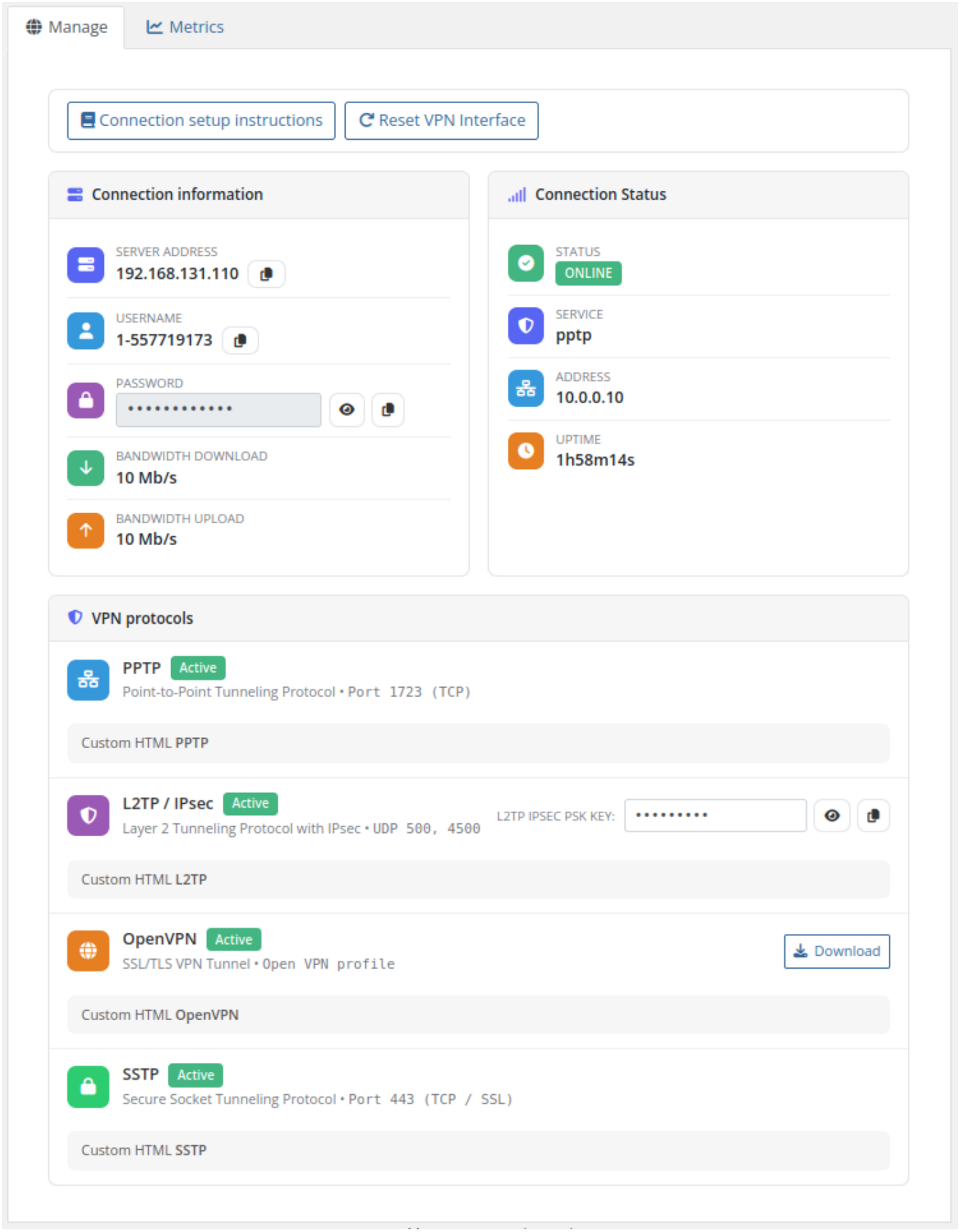
> **Important:** The module registers opposite values for upload and download speeds in the Mikrotik router compared to WHMCS settings, because Mikrotik measures incoming traffic while VPN clients experience outgoing traffic. Proper Mikrotik router configuration is essential (NAT, firewall, routing, and all required VPN server settings).

Links

- **Product page:** https://puqcloud.com/whmcs-module-mikrotik-vpn.php
- **Documentation:** https://doc.puq.info/books/mikrotik-vpn-whmcs-module
- **Support:** https://puqcloud.com/submitticket.php
- **Community:** https://community.puqcloud.com/

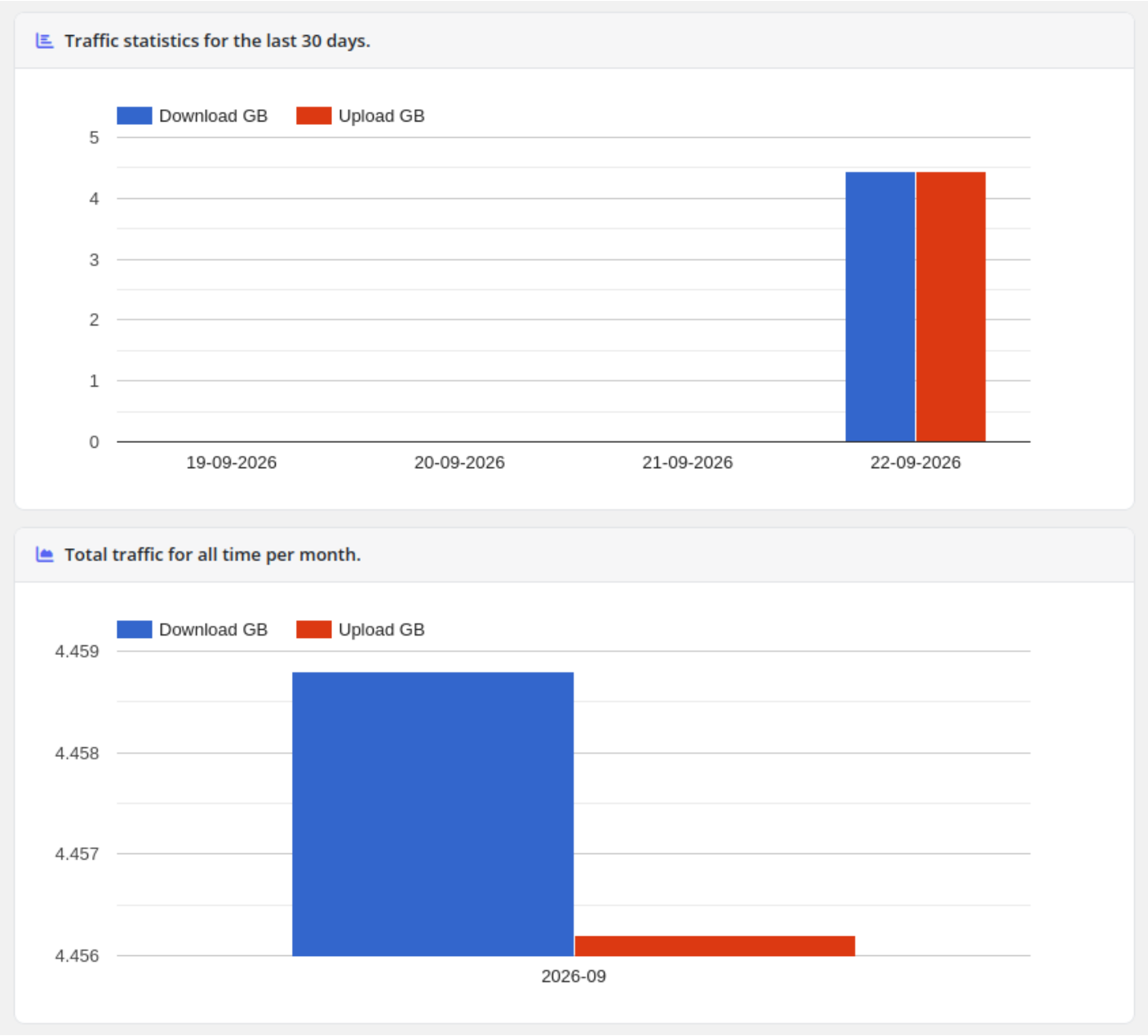
Screenshots

Client area — Home screen



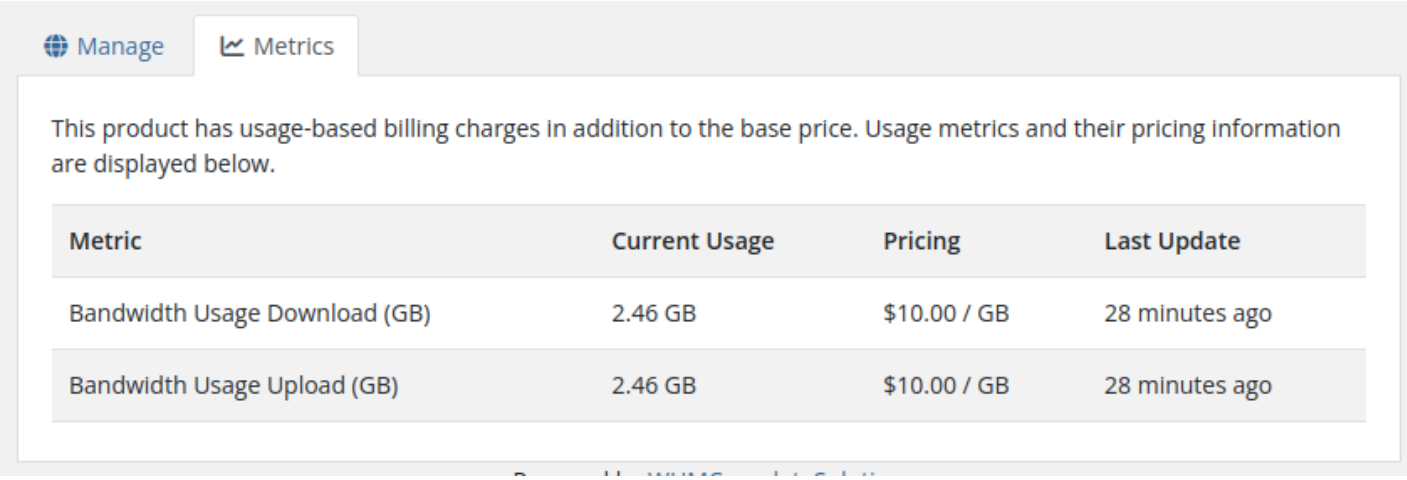
client-area-home.png

Client area — Traffic statistics



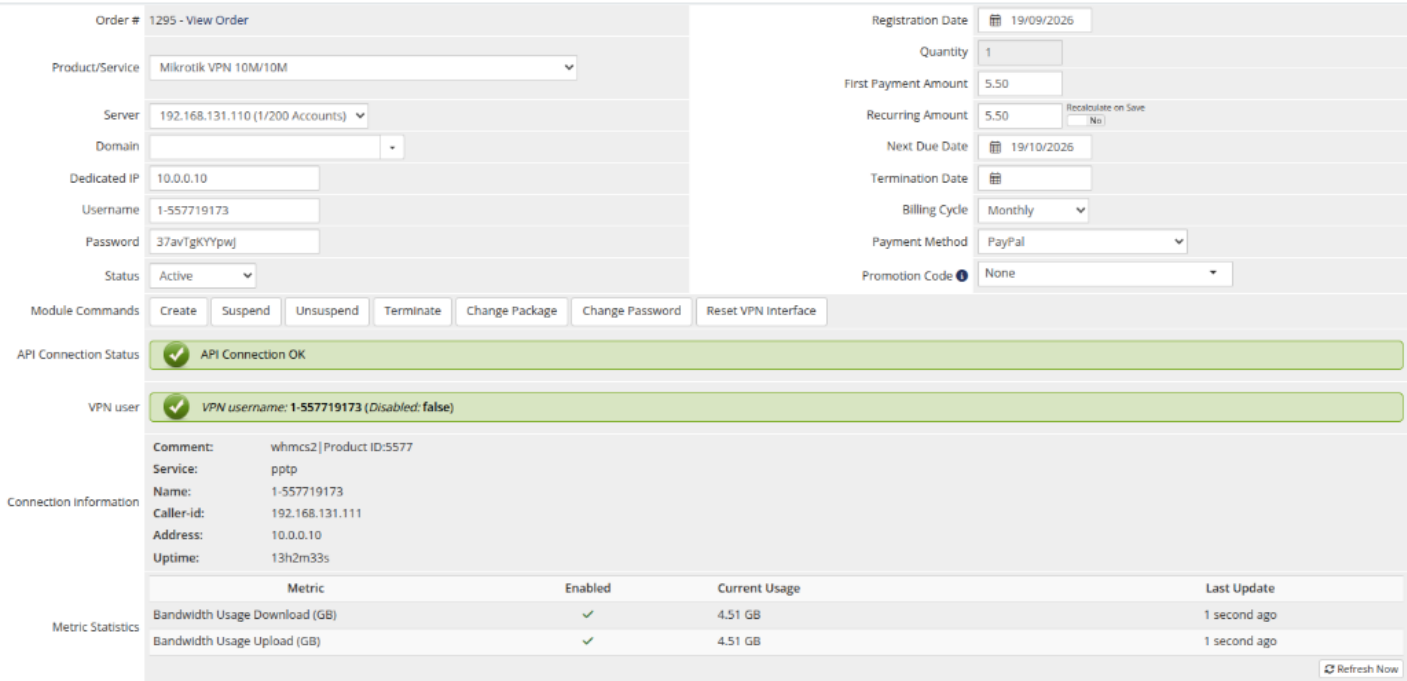
client-area-traffic.png

Client area — Usage metrics



client-area-metrics.png

Admin area — Product information



admin-product-info.png

Changelog

Mikrotik VPN module **WHMCS**

Order now | Download | Community

v4.1.0 — 2026-09-30

- **Resilient Daily Cron & Usage Synchronization.** Usage updates and traffic metric collection during WHMCS automation runs are now completely isolated per account with comprehensive diagnostic logging. A temporary connection hiccup or offline router will never interrupt the billing run for your other customers.
- **Strict PHP 8.2+ Compatibility & Type Hardening.** Resolved typed property assignment issues across package speed and bandwidth configurations, ensuring seamless and crash-free execution on modern PHP 8.1, 8.2, and 8.3 environments.
- **Zero-Touch Configuration Auto-Migration.** Existing products configured on previous versions automatically upgrade their parameters into the modern unified settings format directly in the database upon editing, eliminating manual reconfiguration.
- **Enhanced WHMCS 9 Admin Experience.** Refined dynamic module settings detection for Select2 interfaces, providing instant and responsive controls in the WHMCS 9 administrator panel.
- **Clean Module Logging.** Excluded local database license verification checks (`License_Verification(db)`) from the WHMCS Module Log, recording exclusively online verification calls to keep diagnostic logs clean.

---

v4.0.0 — 2026-09-22

- **Atomic traffic statistics collection.** Replaced read-modify-write logic with atomic SQL increments (`Capsule::raw`) in `StatisticsSaveTraffic()` , eliminating race conditions and traffic data loss during concurrent WHMCS cron jobs and metric queries.
- **WHMCS Usage Billing MetricProvider fix.** Resolved zero-traffic reporting so that `Usage(0.0)` is reliably returned when usage is 0 GB, preventing "No usage data" statuses in WHMCS.
- **Unified interface reset action.** Removed redundant `resetConnection` action and

button, standardizing on a single, clean `Reset VPN Interface` button across admin and client interfaces.
- **Admin API connection timeout.** Enforced a strict 15-second timeout on router status checks with offline circuit breaker, eliminating admin panel hangs on unreachable Mikrotik routers.
- **Guzzle HTTP Client integration.** Migrated all external API and license verification requests from legacy cURL to `\GuzzleHttp\Client` with exponential backoff and retry mechanism.
- **ionCube 15 & PHP 8.2+ architectural upgrade.** Transitioned `hooks.php` to an unencoded lightweight bootstrap delegating logic to `lib/puqMikrotikVPNHooks.php` for seamless ionCube 15 compatibility.
- **Automated usage cleanup on termination.** Local usage statistics in `puqMikrotikVPN_statistics` are now automatically purged when a service is terminated.
- **Enhanced Client Area UI.** Integrated standard PUQ client area UI toolkit with `header.tpl`, dynamic copy-to-clipboard buttons, toast notifications, CSRF protection, and streamlined responsive layout.
- **Legacy configuration fallback.** Added transparent backward compatibility for products migrating from older configuration slots (`configoption2..11`).
- **Comprehensive localization.** Standardized translation strings across all 26 supported languages with safe typographic apostrophes and full Ukrainian language support.

---

v3.1.1 (02-06-2026)

- **Full support for the latest RouterOS 7.21.4.** The module has been verified end-to-end against the newest Mikrotik firmware, so you can confidently run your VPN services on up-to-date, secure routers.
- **Rock-solid router communication.** Connections to your Mikrotik devices are now even more reliable — requests that could previously stall on certain firmware versions complete instantly, keeping provisioning and management fast and dependable.
- **Stay current with peace of mind.** Whether you are deploying brand-new routers or upgrading existing ones to the latest RouterOS, your VPN automation keeps working smoothly out of the box.
- **PHP 7.4 support is back.** The module runs flawlessly on PHP 7.4 once again, so customers on established hosting stacks can keep their proven setup without rushing a server upgrade. We will continue to support PHP 7.4 for as long as it remains technically possible.

---

v3.1 (20-04-2026)

- **Improved stability across the WHMCS admin area.** Rare page-loading errors that could appear on some admin screens (for example when opening a support ticket on installations with non-standard file layouts, symlinks or custom hosting paths) have been eliminated. The admin panel now loads smoothly in every environment.
- **Greater compatibility with complex hosting setups.** The module is now fully resilient to WHMCS installations using symlinked directories, multi-domain hosting and custom include paths.
- **Smoother day-to-day operation for administrators.** Fewer interruptions, no unexpected "Oops!" pages, and a more predictable experience when working with tickets, clients and services — so your team can focus on customers, not on troubleshooting.

---

v3.0 (01-02-2026)

- Support for WHMCS 9+
- Redesigned product module settings
- Updated client area interface design
- Remote ability to have traffic-based packages has been removed; instead, a post-paid traffic billing model has been implemented using standard WHMCS metrics

> **Note:** Product reconfiguration is required after update.

---

v2.2 (23-01-2025)

- The product configuration method has been redesigned
- Added a configuration option in the product settings to display custom HTML in the client panel based on the VPN protocol

> **Important:** After the update, all products using this module must be completely reconfigured.

---

v2.0 (23-09-2024)

- Module coded with ionCube v13
- Supported PHP versions: 7.4, 8.1, 8.2
- Compatible with WHMCS 8.11.0+
- Client area more adapted for mobile
- Copy-to-clipboard buttons added for login and password

---

v1.3.5 (11-10-2023)

- Support for WHMCS v8.8.0
- Translations added/updated: 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

---

v1.3 (04-02-2023)

- Redesigned client side with intuitive icons
- Improved PHP 8.1 compatibility
- Bug fix: "Attempt to assign property bytes_upload on string" in puqMikrotikVPN.php

---

v1.2 (04-01-2023)

- Support for WHMCS v8.6
- Support for IonCube PHP Loader v12
- PHP 8.1 support
- Template improvements
- Added configurable frequency for traffic statistics collection (daily cron and per cron)
- Traffic counters on Mikrotik are reset to zero after each statistics collection
- Email template selection changed from text input to dropdown menu

---

v1.1 (28-10-2022)

- Client area design improvements
- Ukrainian and Persian translations added
- PPP secret profile selection in product settings changed from text input to dropdown

---

v1.0 (01-08-2022)

- First release

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

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**

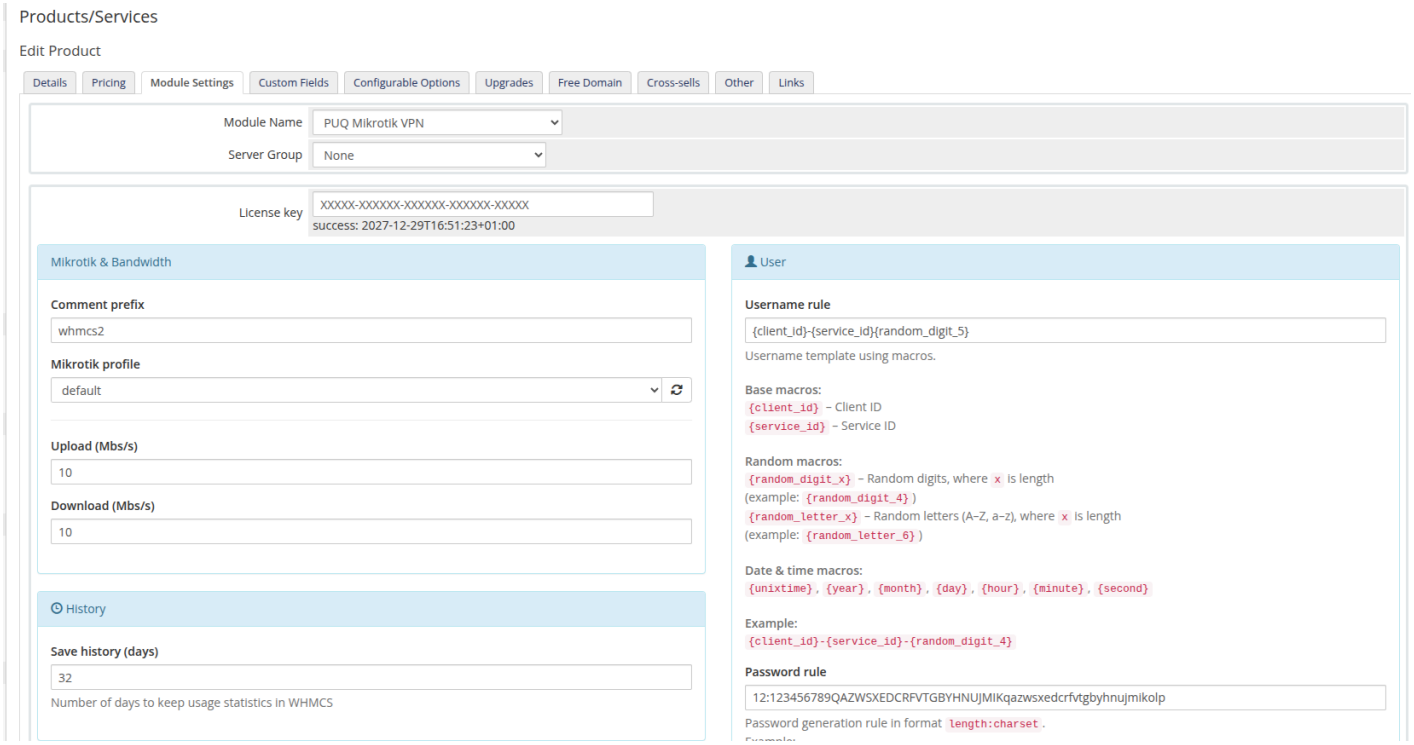
Select the **PUQ Mikrotik VPN** module in the Module settings section.

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

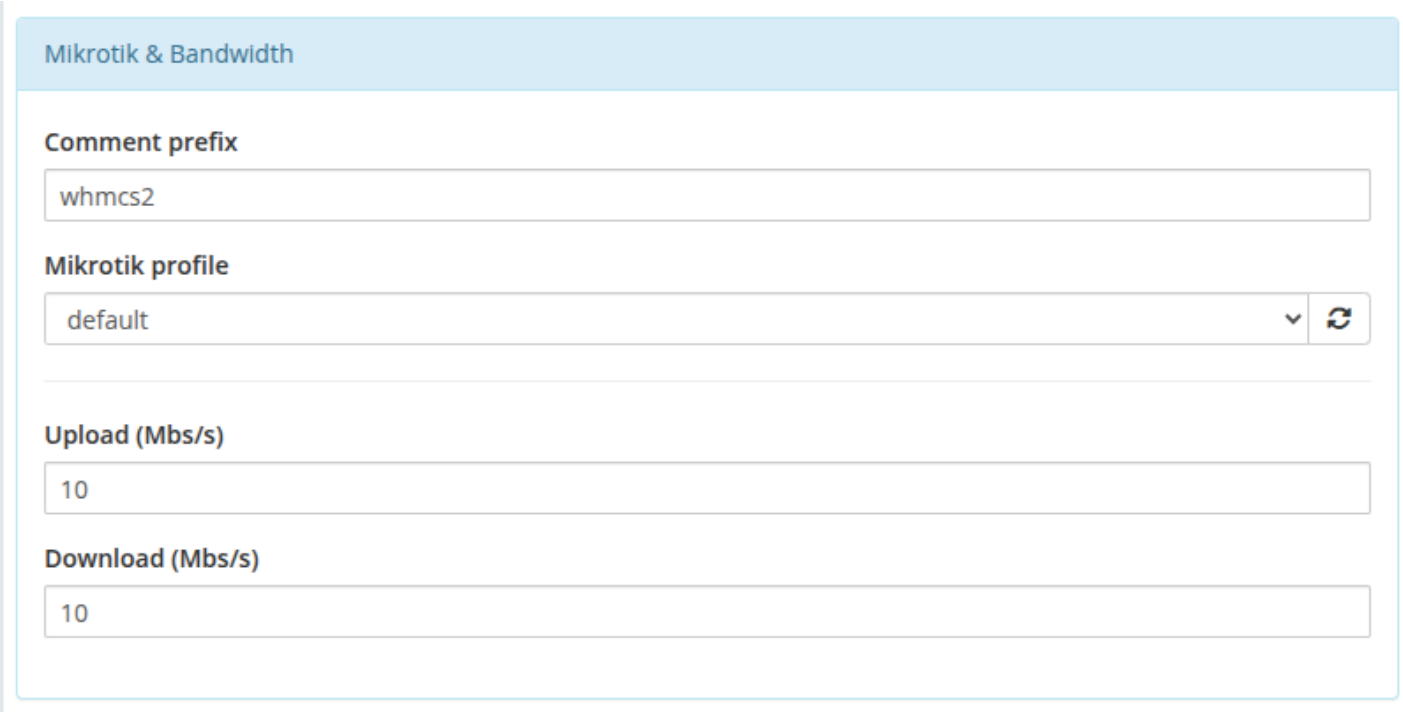
Parameter	Description
Username rule	Template for generating unique VPN usernames. You can use macros like `{client_id}`, `{service_id}`, `{random_digit_5}`, `{year}`, etc.
Password rule	Defines the format for auto-generating VPN passwords. Format: `length:charset` (e.g. `12:123456789QAZWSXEDCRFVTGBYHNUJMIKqazwsxedcrfvtgbyhnujmikol`).

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

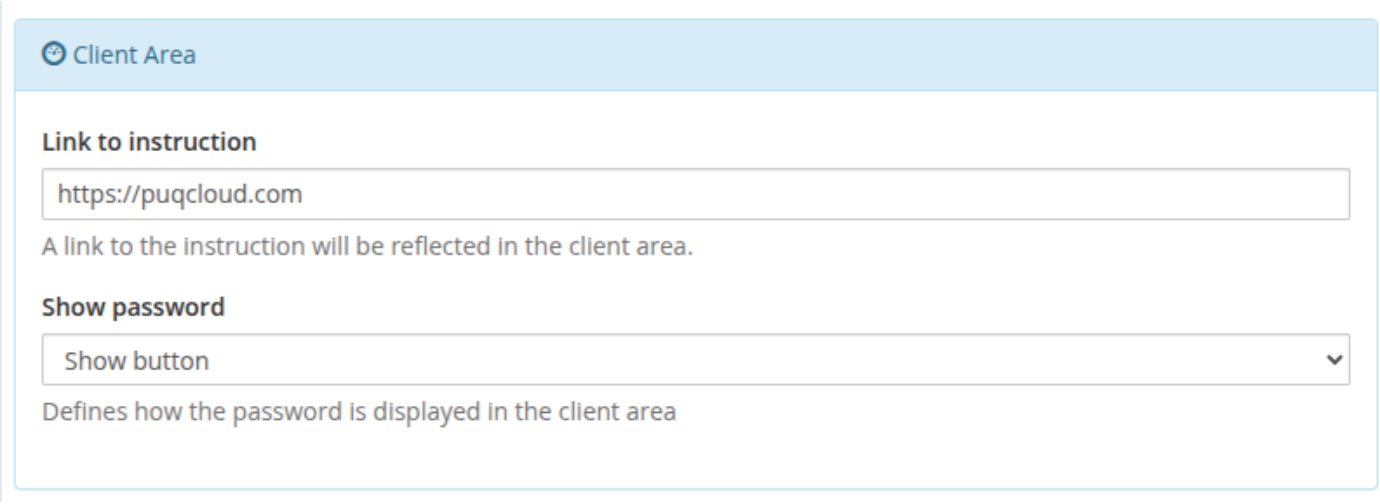
History

Save history (days)

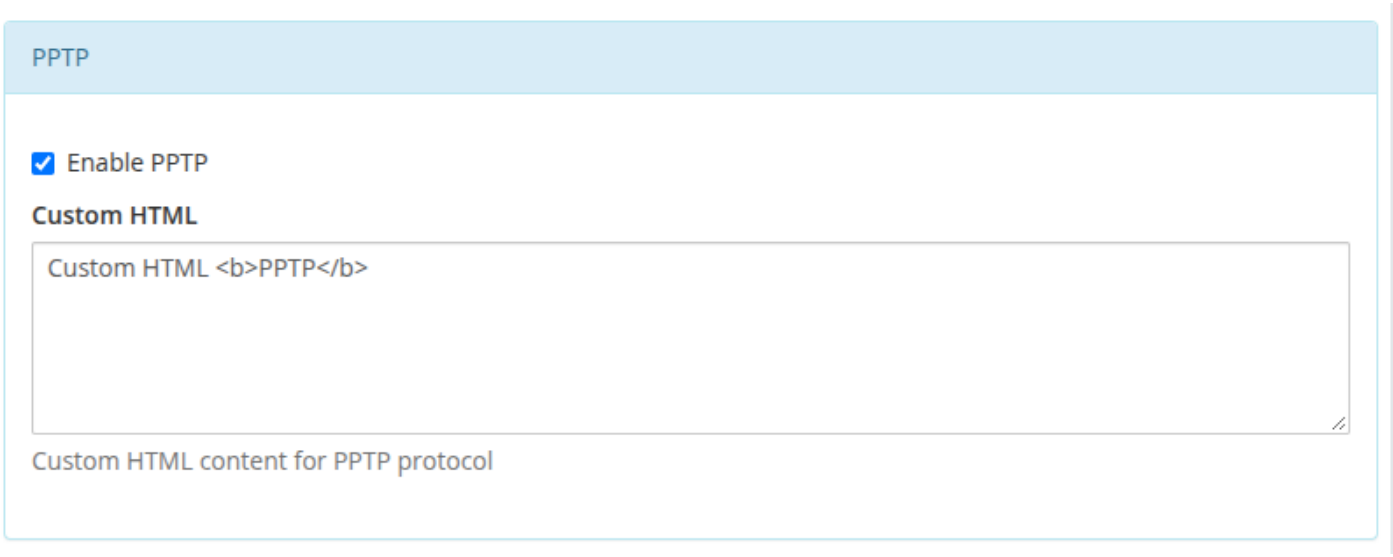
32

Number of days to keep usage statistics in WHMCS

product-configuration-l2tp.png



product-configuration-openvpn.png



product-configuration-sstp.png

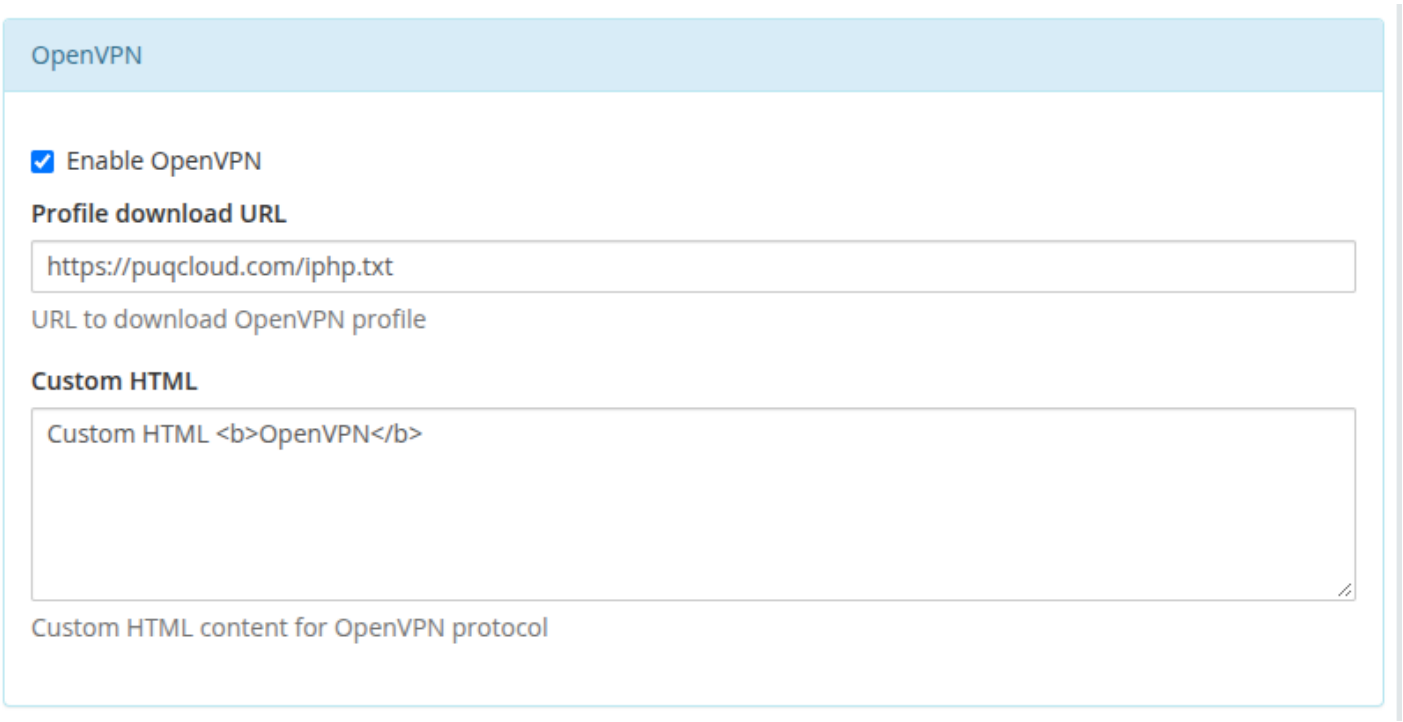
Metric Billing Configuration

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

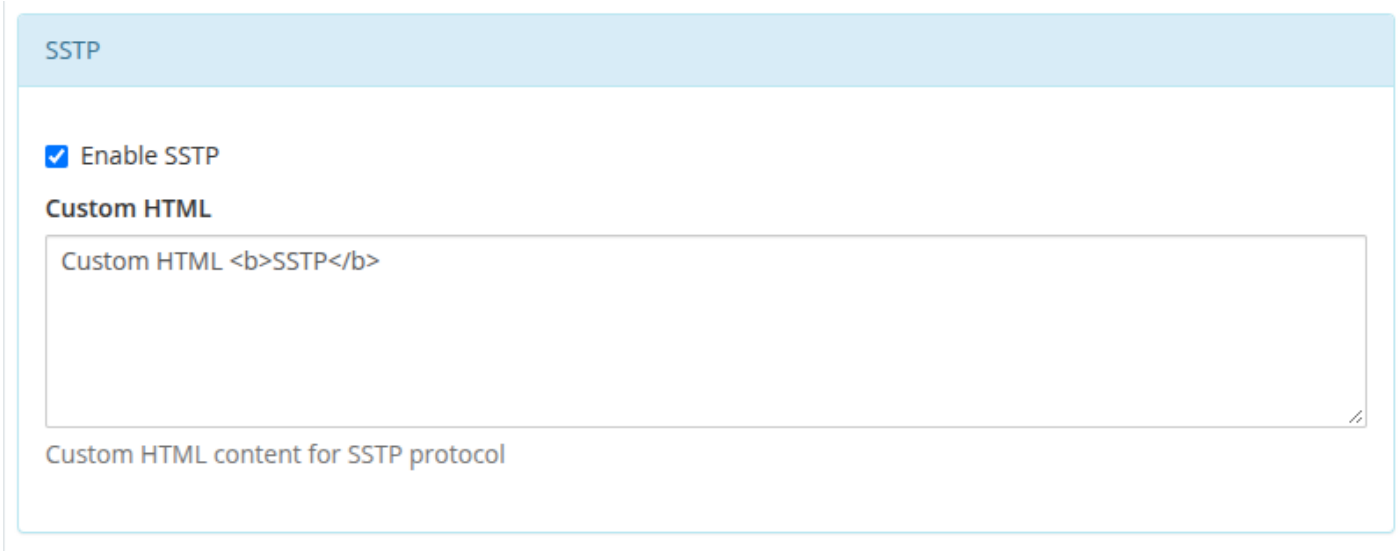
1. Navigate to the **Metric Billing** section in your product settings.
2. Toggle the switches to **ON** for **Bandwidth Usage Download (GB)** and **Bandwidth Usage Upload (GB)**.
3. Click **Configure Pricing** to set your rates per GB across your supported currencies.



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:

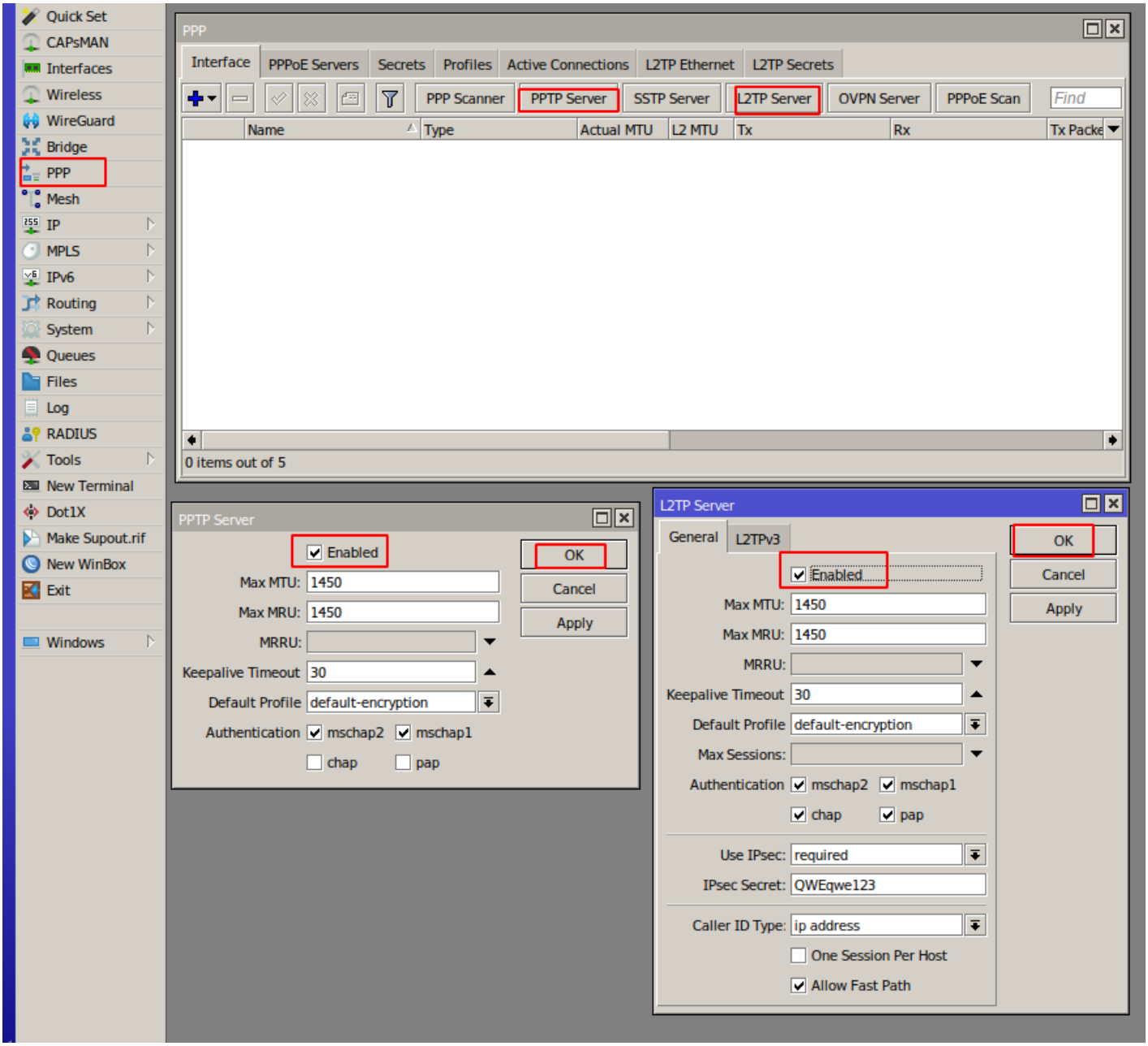
```
/ip service
set api-ssl certificate=Webfig disabled=no
```

> **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.

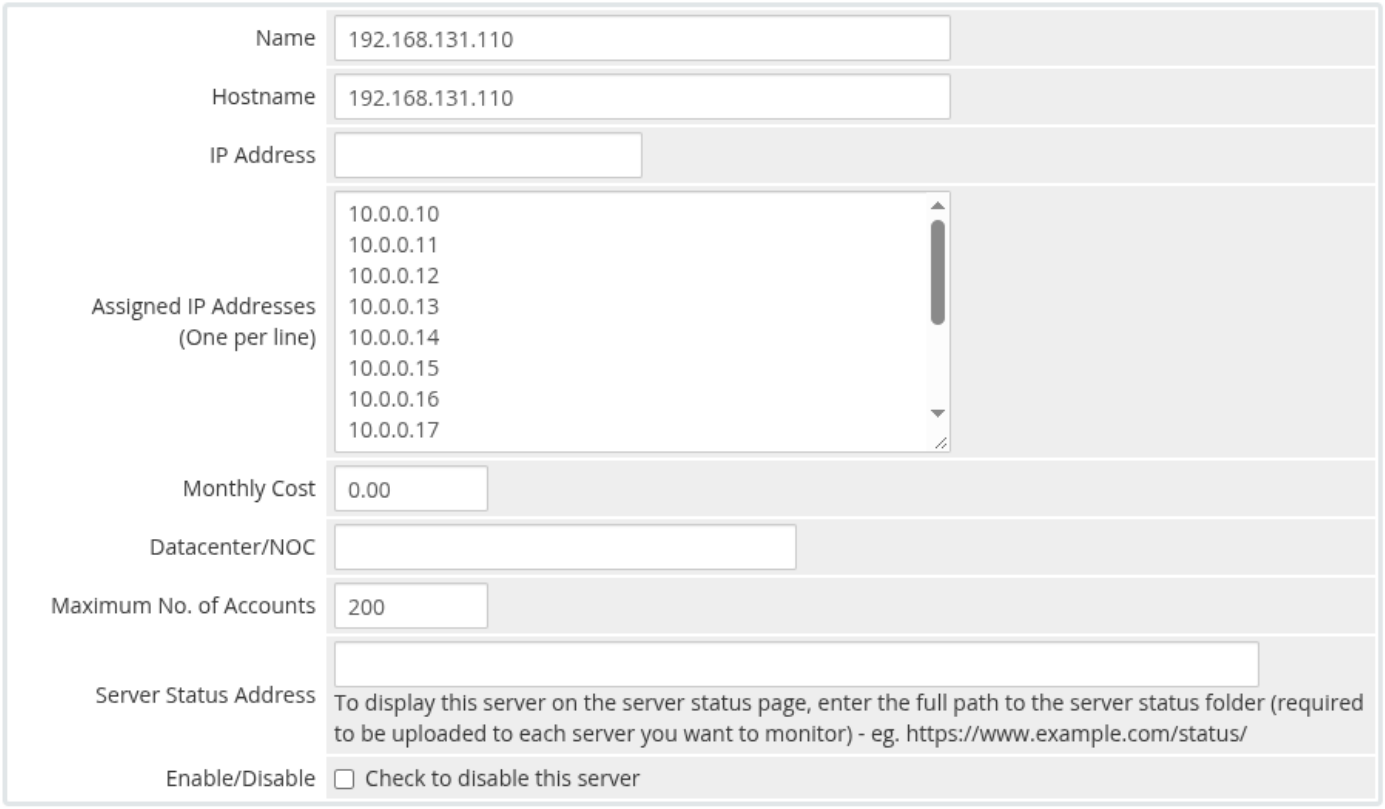
Navigate to **System Settings** → **Servers** → **Add New Server**

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

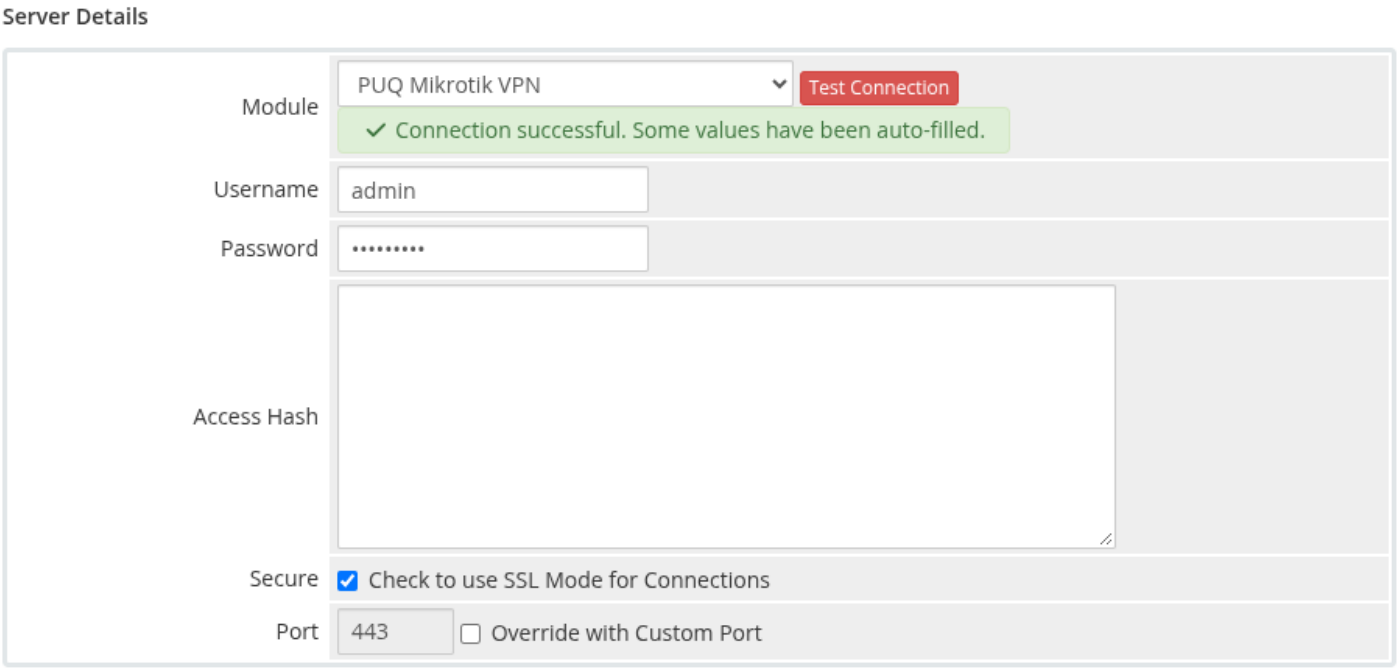
Step 2: Assigned IP addresses

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.

Admin Area

Administrative features and tools available in the WHMCS admin panel for managing Mikrotik VPN services.

Product Information

Mikrotik VPN module **WHMCS**

Order now | Download | Community

Admin area product information

The administrator can view detailed service information in the WHMCS admin panel on the product/service page. The module adds a custom panel in the **Module Data** section with the following information:

License verification status

Displays the current license status with a colored indicator:

- **Green** — license is valid and active
- **Red** — license is invalid, expired, or missing

API connection status

Shows the result of a real-time connection test to the Mikrotik router API-SSL, confirming that the credentials entered for the server are working correctly.

VPN account information

Field	Description
Username	The VPN account username (PPP secret name) on the Mikrotik router
Enabled	Whether the VPN account is currently enabled or disabled on the router

Field	Description
Profile	The PPP profile assigned to the account
Service	The VPN service / protocol (e.g. `any`, `pptp`, `l2tp`, `pppoe`)
IP address	The IP address assigned to the account from the server's IP pool
Comment	Includes the configured Comment PREFIX and WHMCS service identifier

Connection information

- **Comment** — includes the configured comment prefix and WHMCS service identifier
- **Service** — active VPN protocol (e.g. `pptp`, `l2tp`)
- **Name** — VPN user account name
- **Caller-id** — caller identification / remote IP address
- **Address** — client IP address assigned by the router
- **Uptime** — current active session duration *(Displays "NOT ONLINE" when the client is disconnected)*

Metric Statistics

When Metric Billing is enabled, the admin view displays live metric statistics:

- **Bandwidth Usage Download (GB)** — current cumulative downloaded traffic (GB) and enabled status
- **Bandwidth Usage Upload (GB)** — current cumulative uploaded traffic (GB) and enabled status
- **Last Update** — relative time when the metric was last refreshed
- **Refresh Now** button — allows immediate on-demand metric recalculation

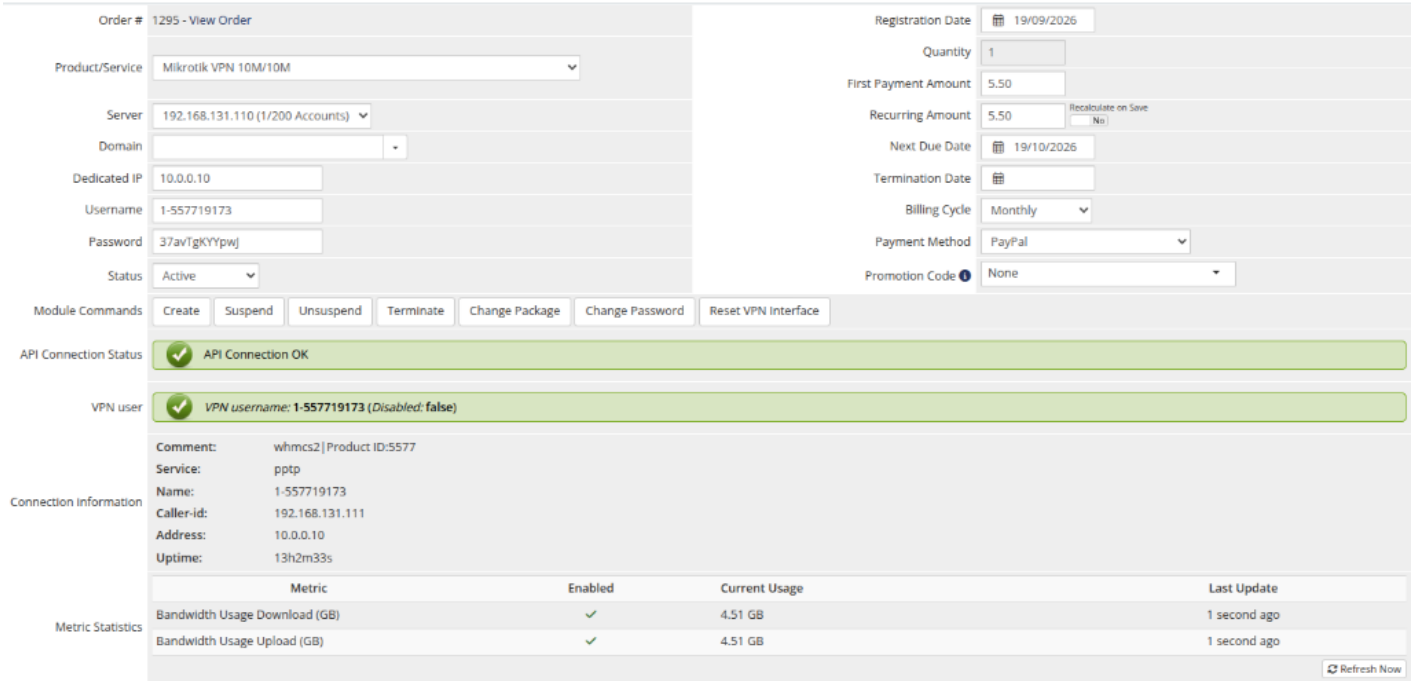
Available management actions

The standard WHMCS module command buttons are available:

- **Create** — provision a new VPN account on the Mikrotik router
- **Suspend** — disable the VPN account
- **Unsuspend** — re-enable the VPN account
- **Terminate** — permanently delete the VPN account from the router
- **Change Password** — reset the account's password
- **Change Package** — update profile, service, bandwidth limits and traffic configuration (used during upgrades/downgrades)

- **Reset VPN Interface** — force-disconnect the current active VPN session (useful when the customer needs to re-establish the tunnel)

Screenshot



admin-product-info.png

Client Area

Overview of the client-facing features available in the Mikrotik VPN WHMCS module, including the home screen (VPN server address, protocols, credentials, connection status, bandwidth limit), email notifications (traffic limit, suspension), traffic usage statistics, and usage-based billing metrics.

Client Area Home Screen

Mikrotik VPN module **WHMCS**

Order now | Download | Community

VPN Service Management Dashboard

After authenticating in the client area, the end customer sees the VPN service management page under the **Manage** tab.

Quick Actions

At the top of the dashboard, clients can find:

- **Connection setup instructions** — links to your predefined documentation (if configured).
- **Reset VPN Interface** — allows the client to manually reset their active VPN session.

Connection Information Card

Displays all the primary details needed to establish the connection:

- **Server Address** — IP address or hostname of the Mikrotik router.
- **Username** — VPN username (auto-generated or assigned).
- **Password** — masked password with an option to toggle visibility.
- **Bandwidth Limits** — the configured upload/download speeds for the account (e.g. `10 Mb/s`). *(Includes quick-copy icons next to sensitive values).*

Connection Status Card

Provides real-time information by querying the router API:

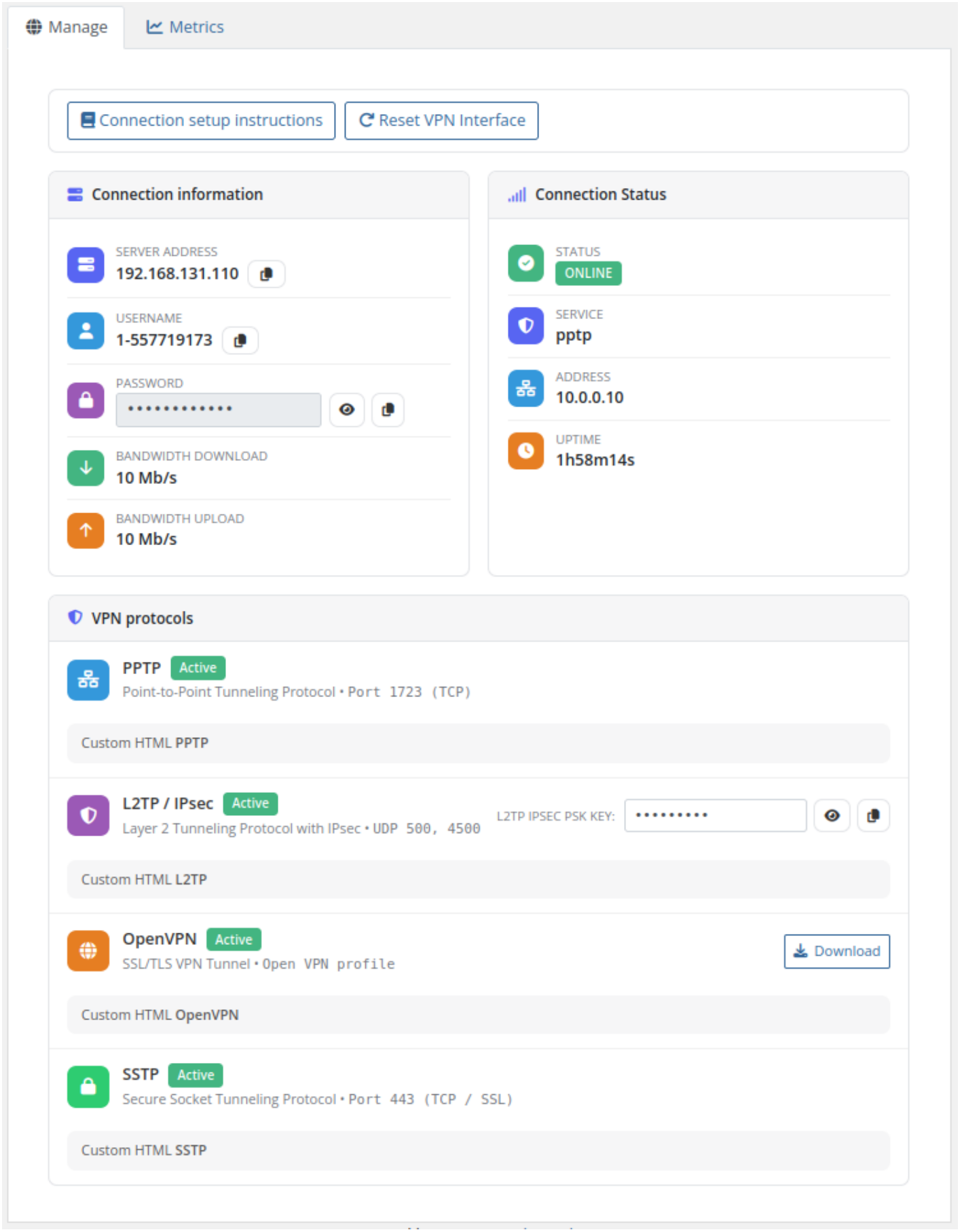
- **Status** — `ONLINE` or `OFFLINE` badge.
- **Active Service** — which protocol is currently in use (e.g. `pptp`).
- **Client IP Address** — the internal VPN IP address assigned.
- **Session Uptime** — duration of the current connection.

VPN Protocols Section

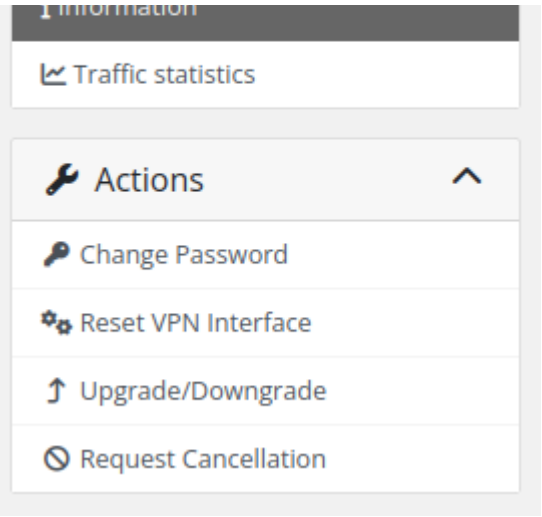
Displays the specific connection details for each VPN protocol enabled by the administrator (PPTP, L2TP, OpenVPN, SSTP). Each section contains:

- Connection port and security details.
- Custom HTML blocks with specific instructions if injected by the admin.
- Dedicated download buttons (e.g., OpenVPN profile configuration file).
- Specialized keys (e.g., `L2TP IPSEC PSK KEY`).

Screenshot



client-area-home.png



client-area-sidebar.png

Client Area

Traffic Statistics

Mikrotik VPN module **WHMCS**

Order now | Download | Community

Traffic Usage Metrics

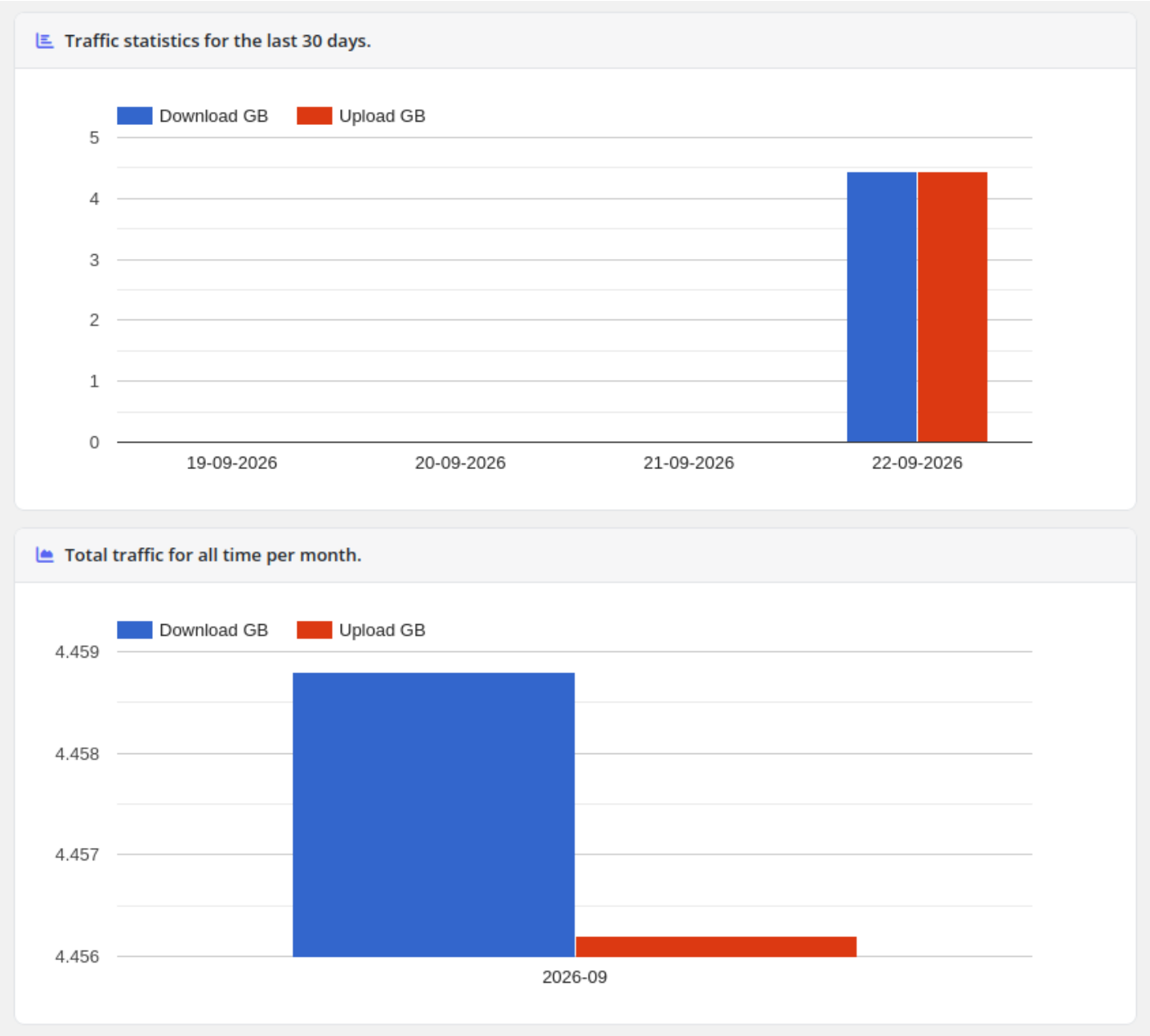
The client can view historical traffic usage statistics by navigating to the **Traffic statistics** tab in the sidebar menu of the VPN service overview.

The statistics page presents visual representations of the client's traffic usage over time, dynamically generated using charting libraries:

1. **Traffic statistics for the last 30 days:** A bar chart displaying daily bandwidth consumption, differentiating between **Download GB** (blue) and **Upload GB** (red).
2. **Total traffic for all time per month:** A bar chart providing a higher-level monthly aggregation of all downloaded and uploaded data for long-term usage tracking.

> **Note:** The data powering these charts is continuously gathered by the WHMCS Cron job and securely stored in the database according to the history retention policy defined in the module's product settings.

Screenshot



client-area-traffic.png

Client Area

Usage Metrics

Mikrotik VPN module **WHMCS**

Order now | Download | Community

Usage-Based Billing Metrics

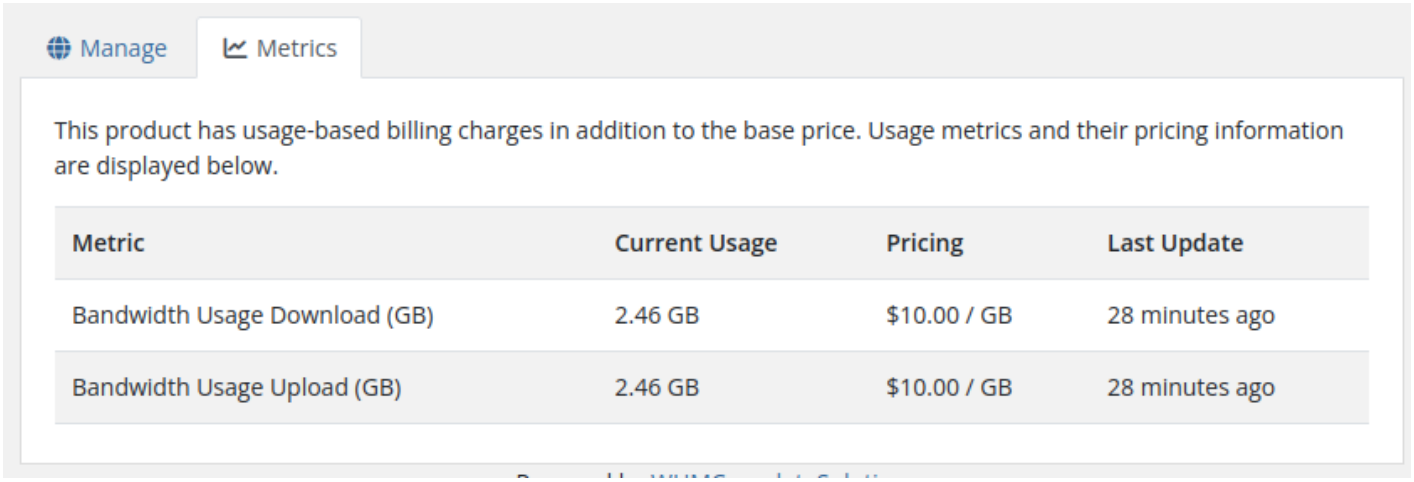
When WHMCS Metric Billing is enabled for the product, clients can track their current traffic consumption and billing rates under the **Metrics** tab on their service management page.

Metrics Tab Overview

The tab presents:

- **Bandwidth Usage Download (GB)** — cumulative downloaded data counted towards usage-based billing.
- **Bandwidth Usage Upload (GB)** — cumulative uploaded data counted towards usage-based billing.
- **Pricing** — unit price charged per gigabyte (e.g. `$10.00 / GB`).
- **Last Update** — relative time when metrics were last synchronized from the Mikrotik router by the WHMCS cron job.

Screenshot



client-area-metrics.png