

Add server (Mikrotik router)

Mikrotik VPN module **WHMCS**

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

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).

Name	<input type="text" value="vpn-██████.pl"/>
Hostname	<input type="text" value="vpn-██████.pl"/>
IP Address	<input type="text"/>
Assigned IP Addresses (One per line)	<input type="text" value="192.168.222.14"/> <input type="text" value="192.168.222.15"/> <input type="text" value="192.168.222.16"/> <input type="text" value="192.168.222.17"/> <input type="text" value="192.168.222.18"/> <input type="text" value="192.168.222.19"/> <input type="text" value="192.168.222.20"/> <input type="text" value="192.168.222.21"/>
Monthly Cost	<input type="text" value="0.00"/>
Datacenter/NOC	<input type="text"/>
Maximum No. of Accounts	<input type="text" value="200"/>
Server Status Address	<input type="text"/> To display this server on the server status page, enter the full path to the server status folder (required to be uploaded to each server you want to monitor) - eg. https://www.example.com/status/
Enable/Disable	<input type="checkbox"/> Tick to disable this server

04-add-server-1.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.

Server Details

The screenshot shows a configuration form for the 'PUQ Mikrotik VPN' module. The 'Module' dropdown is set to 'PUQ Mikrotik VPN' and a 'Test Connection' button is highlighted. A green notification bar states '✓ Connection successful. Some values have been auto-filled.' The 'Username' field contains 'admin' and the 'Password' field is masked with dots. The 'Access Hash' field is empty. The 'Secure' checkbox is checked with the label 'Tick to use SSL Mode for Connections'. The 'Port' field is set to '443' and the 'Override with Custom Port' checkbox is unchecked. At the bottom, there are 'Save Changes' and 'Cancel Changes' buttons.

05-add-server-2.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.

Revision #6

Created 20 April 2026 06:38:53 by Ruslan

Updated 2 June 2026 17:07:02 by Ruslan