MikroTik Router Connection Guide

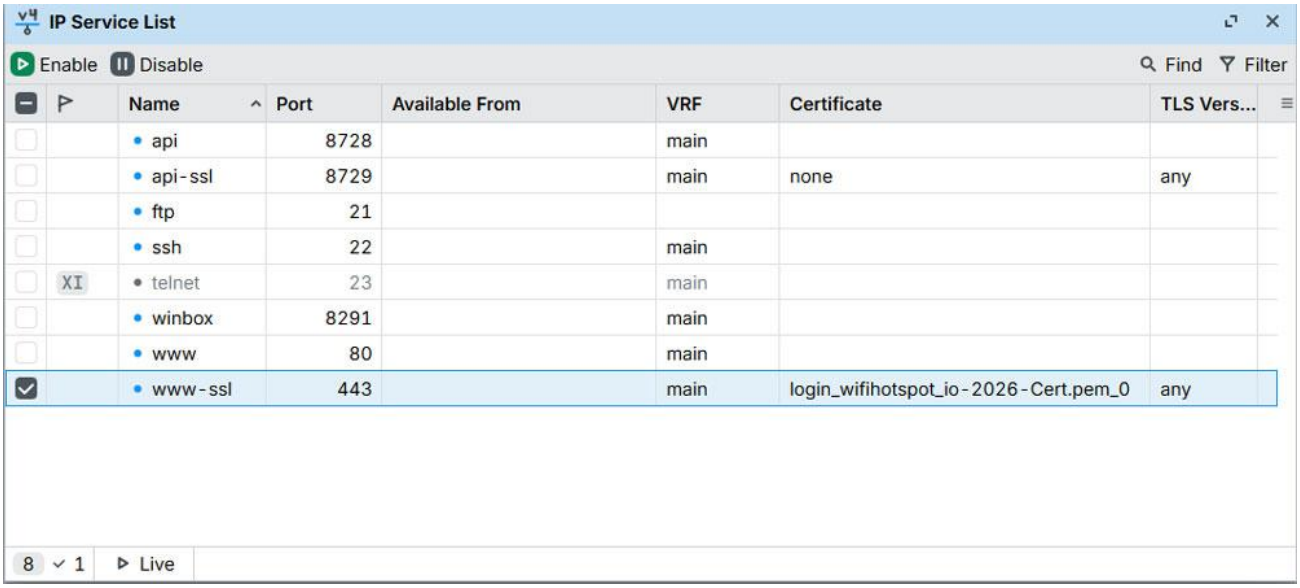
ONLINE SOLUTIONS | ISP BILLING

A practical, illustrated WinBox guide for connecting a MikroTik router to your ISP billing workspace.

Portal: ispbilling.onlinesolutions.co.ke
Support: support@onlinesolutions.co.ke | 0704 480 883

Before starting: Back up your RouterOS configuration. Use RouterOS v7 for the HTTPS REST API used by the billing form. Some screenshots supplied show older WinBox/RouterOS versions; menu appearance may differ.

Security: Use a dedicated account, a valid HTTPS certificate and restricted management access, preferably through a VPN. Do not expose management services openly to the internet.

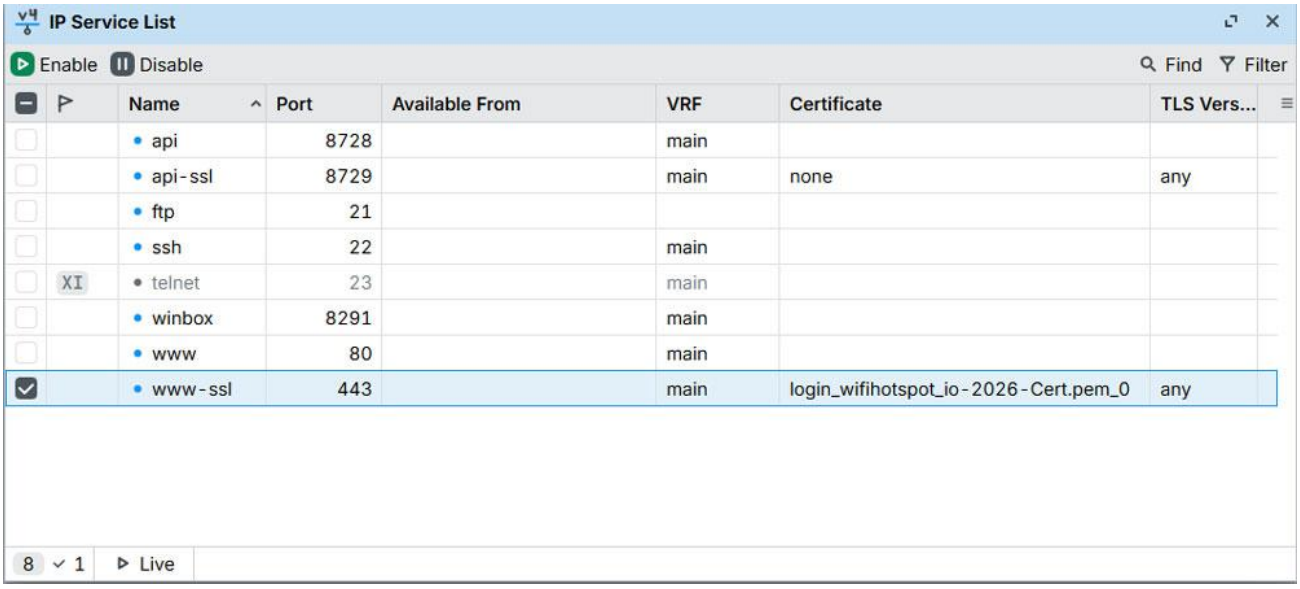


1. Confirm HTTPS service (www-ssl)

Open **WinBox** → **IP** → **Services**. Find **www-ssl** and verify it is enabled. Confirm its port (typically 443) and that a suitable TLS certificate is selected.

The billing form expects an HTTPS management URL such as **https://router.yourisp.co.ke:443** — do not append **/rest**. The cPanel server must be able to reach this URL.

A certificate for a private hostname or self-signed certificate may require trusted CA configuration on the server.



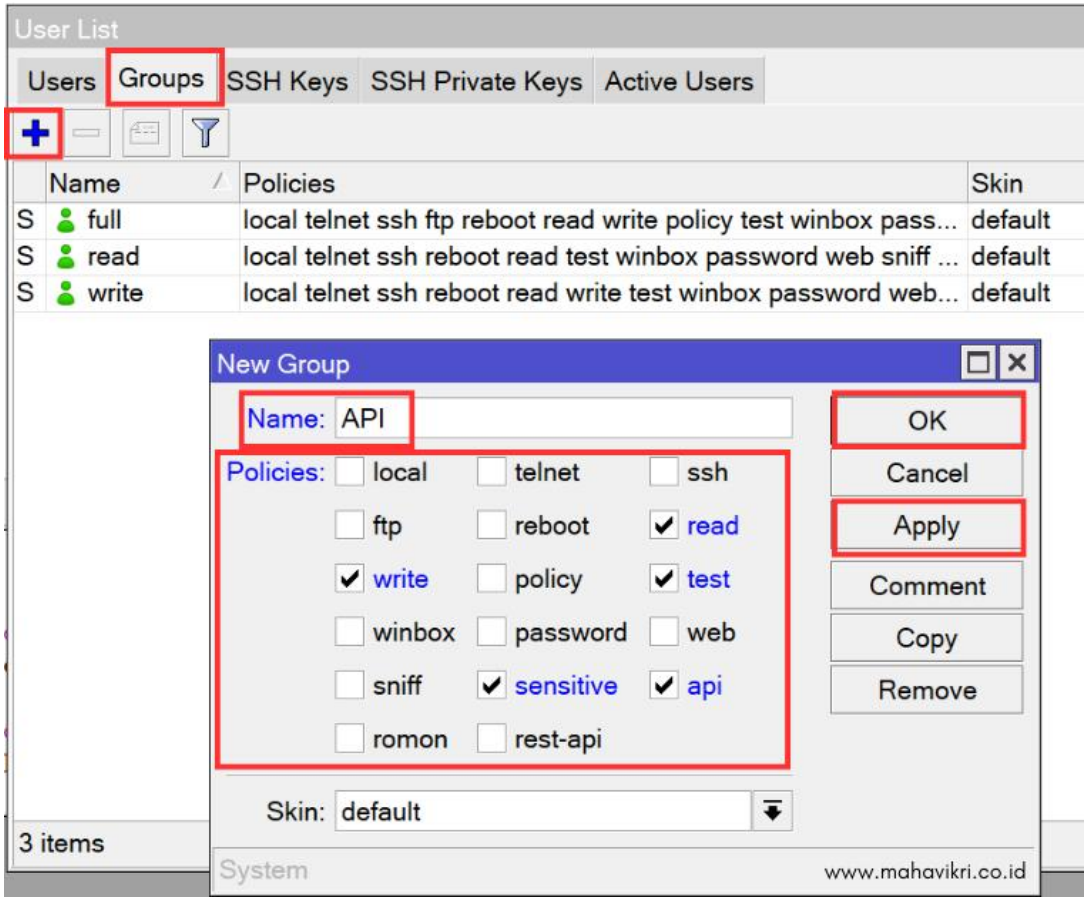
Do not enable plain HTTP (www) or open unrestricted access just to make the connection work.

2. Create a dedicated user group

Go to **System** → **Users** → **Groups** and click **+**. Name the group, for example **isp-billing**.

For RouterOS v7 REST operations, the group must include the permissions actually needed by the integration, including **read**, **write** and **rest-api** where applicable. Use **api** only if the integration requires the classic API.

The pictured example selects **sensitive** and **api** but not **rest-api**; do not copy it blindly. Avoid granting sensitive/policy permissions unless proven necessary.

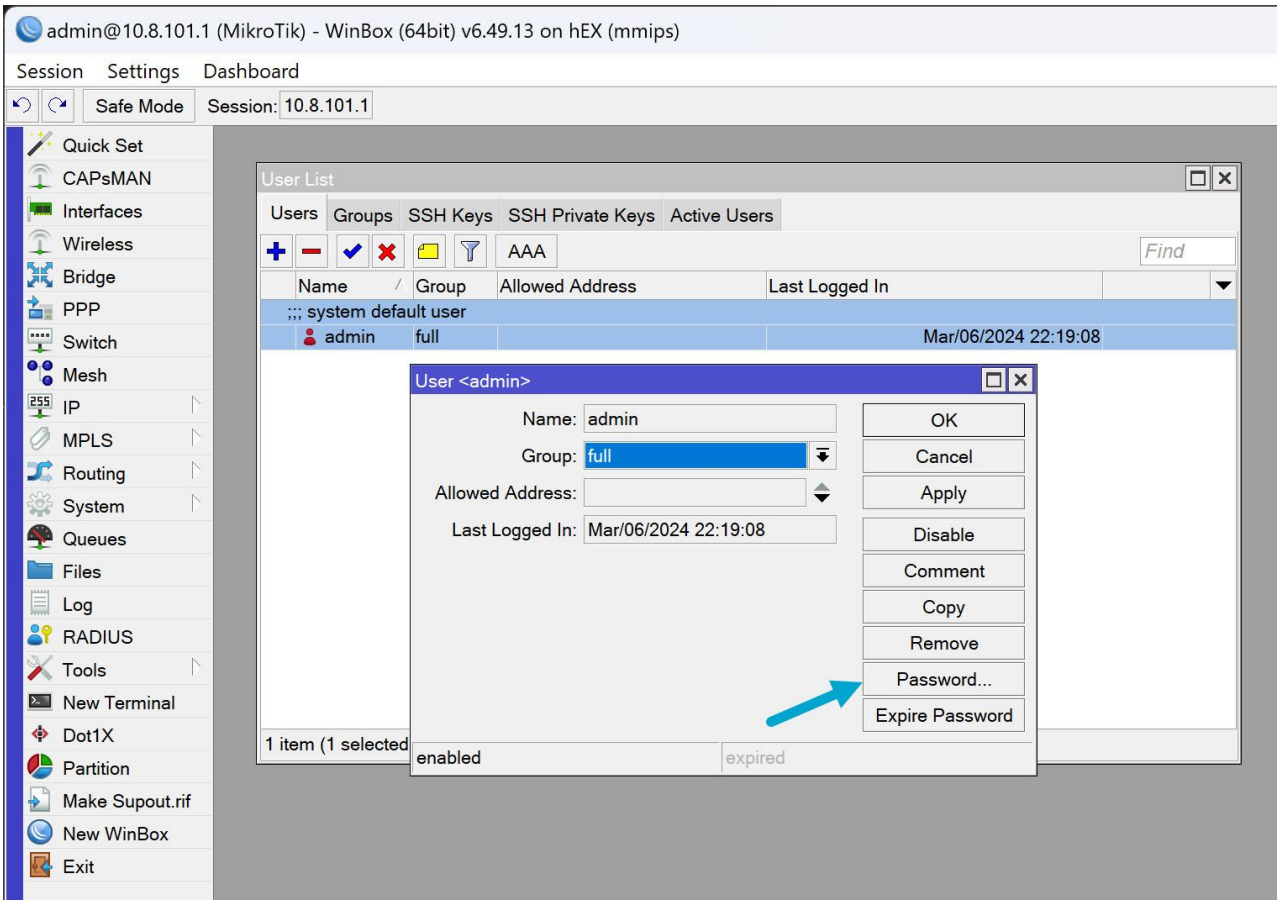


3. Create the router integration account

Open **System** → **Users** → **Users**, click **+**, and create a separate user such as **ispbilling**. Assign the dedicated group created in Step 2.

Set a unique strong password. Restrict the account to the billing server or VPN source IP when possible.

The screenshot shows an existing **admin** account for reference. **Do not use or change the main administrator account for this integration.**

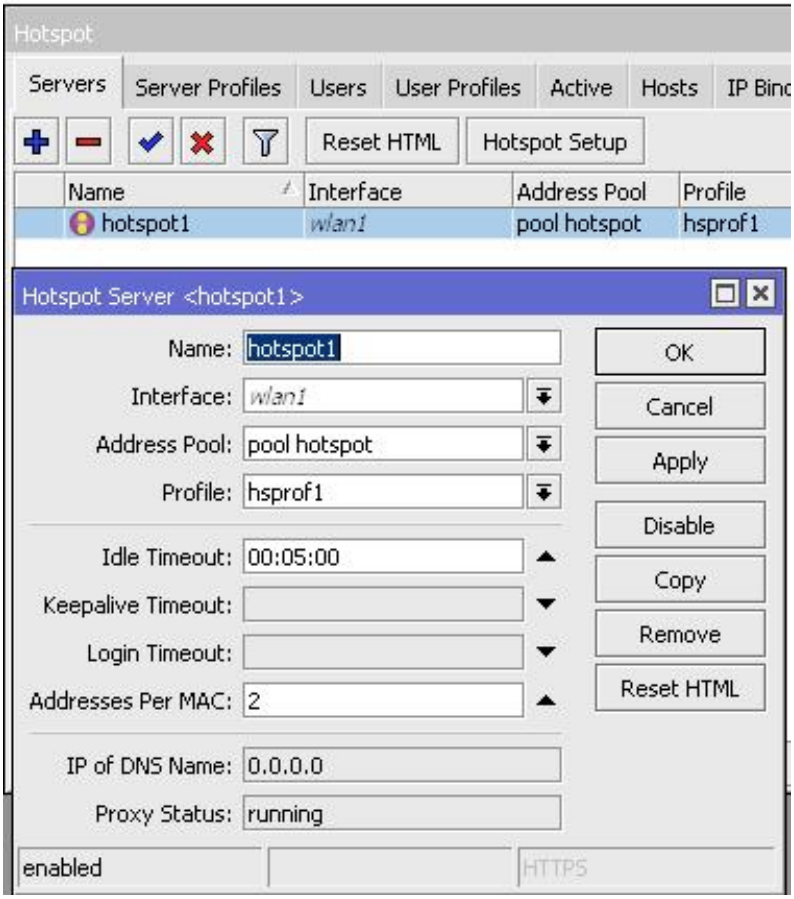


4. Find the Hotspot server name

If you sell Wi-Fi Hotspot packages, go to **IP** → **Hotspot** → **Servers**.

Copy the value under **Name**, such as **hotspot1**. Enter that exact name into **Existing hotspot server name** in the billing portal.

The screenshot also shows the interface and address pool; these are not substitutes for the Hotspot server name.

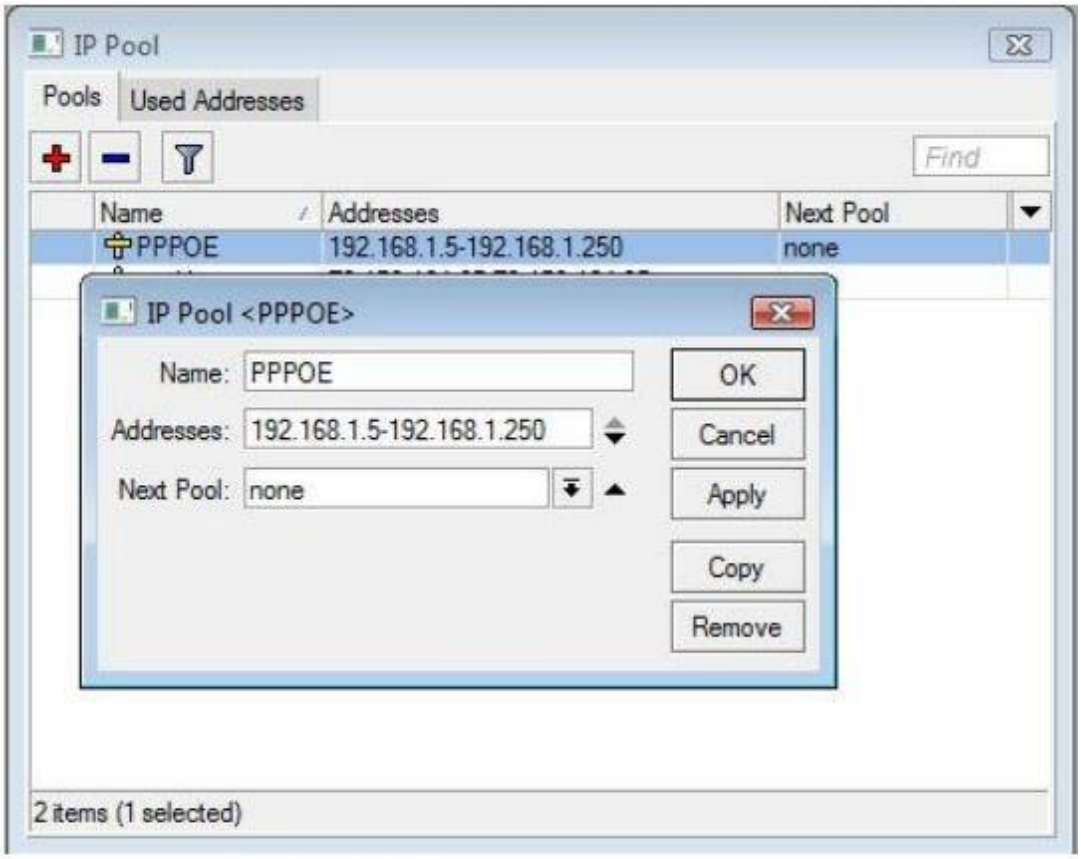


5. Find the PPPoE IP pool

If you provide PPPoE home/office connections, open **IP** → **Pool**.

Identify the pool assigned to your PPPoE service and copy its **Name** exactly. For example, the screenshots show **pool1** and **PPPOE** on different routers.

Use the actual pool on your router. Do not create a duplicate pool merely to match these examples.



if pppoe setup over other ethernet port like LOCAL

6. Enter the details in Online Solutions

Sign in to your ISP portal and open **Add MikroTik router**. Fill the fields as follows:

Router name: Any recognizable label (required).
Management HTTPS URL: Secure address reachable from the billing server (required).
API username/password: Dedicated RouterOS account (required for new connection).
Trusted CA certificate path: Optional; only if the server needs a private CA certificate.
Hotspot HTTPS login URL: Optional; used for the captive portal when configured.
PPPoE gateway IPv4: Only if your PPPoE setup needs it.
Existing PPPoE IP pool: For existing PPPoE pool provisioning.
Existing hotspot server: For Hotspot provisioning.

Leave **Enable provisioning and package sales** unchecked until connection and package mapping have been tested.

7. Test before activating sales

Save the router. Confirm the billing server can establish a TLS-verified connection and authenticate using the dedicated account.

Test read-only access first, then carefully test creating and disabling a **test** subscriber on the correct Hotspot or PPPoE service. Verify that no live customers are affected.

Only after the tests pass should you enable provisioning and package sales. Verify renewals, expiry handling and reconnect behavior separately.

If connection fails: Check RouterOS version, certificate hostname, www-ssl status, source-IP firewall rules, VPN/routing, REST permissions and server outbound connectivity.