

How to connect to olt.am

A guide for ISPs: from the application to a working OLT and instant TR-069 changes.

1. Quick start

Connecting one OLT takes 15–20 minutes and does not stop your network. The OLT stays in your network; the link to the platform runs through a WireGuard tunnel from your MikroTik. Everything is done in the ISP portal with the “Connect OLT” wizard.

1. **Portal.** After the request you receive the workspace `your-isp.olt.am` and an administrator login.
2. **Tunnel.** The wizard gives one line for the MikroTik terminal. In 10–20 seconds the tunnel is up.
3. **OLT access.** Telnet login and password; SNMP communities are optional. The “Check” button shows the OLT's response.
4. **TR-069.** The ACS profile is assigned automatically, and the “TR-069 script” on the MikroTik makes ONU changes instant.

A minute after adding, all ONUs with their signal appear in the workspace, and new ONUs on the “New ONUs” page.

2. What to prepare

MikroTik

- RouterOS 7 (WireGuard built in) and internet access. Outgoing UDP 51820 is needed to `vpn.olt.am` (217.113.16.35); no inbound ports need to be opened.
- The OLT management IP must be reachable from the MikroTik (usually a separate management VLAN or subnet).
- Access to the MikroTik terminal: WinBox or WebFig → New Terminal.
- RouterOS 6 — via OpenVPN, on request.

OLT

- ZTE C300 / C320, ZXAN V2.1.0 (V1.2.x is also supported with limitations). Cards: GTGO, GTGH, GTGHK, SMXA, SCXN.
- BDCOM P3xxx (EPON/GPON), V-SOL V1600: ONU monitoring and management; TR-069 depending on the ONU's capabilities.
- Telnet (port 23) and SNMP v2c (port 161) enabled on the OLT management interface.

- A telnet user with configuration rights (privilege 15 on ZTE).
- Read and write SNMP communities are optional: the platform takes them from the OLT config or creates its own.

Network for ONUs

- A Mgmt VLAN for ONUs with a DHCP pool on the MikroTik — for TR-069 and remote access to the ONU web interface.
- ONUs in the Mgmt VLAN must reach the ACS through the same MikroTik.

ONU

- Any GPON ONU the OLT registers. To manage Wi-Fi/ports via OMCI, an ONU type on the OLT with the right set of ports (the platform picks it by model and can create types).
- For TR-069: an ONU with a CWMP client; ZTE F6xx and Huawei HG8xxx work out of the box, on some OEM models TR-069 is enabled in the ONU web interface.

3. MikroTik tunnel

No public IP for the OLT and no port forwarding needed. Your MikroTik connects to the hub `vpn.olt.am` over WireGuard (UDP 51820).

How to get and run the script

1. In the portal: Settings → OLT → “+ Connect OLT”. Step 1 “MikroTik tunnel”: tunnel name and the OLT IP in your network (as the MikroTik sees it) → “Create tunnel”.
2. The platform shows one line for the terminal: `/tool fetch url="https://217.113.16.35/mt/...rsc" ... dst-path=evx-olt.rsc; :delay 1s; /import evx-olt.rsc` . “Copy” button.
3. Open WinBox or WebFig → New Terminal, paste the line and press Enter. At the end the terminal prints `EVX-OLT: done` .
4. In 10–20 seconds the wizard shows “● online”. Click “Next →”.

The link is one-time and valid for 5 minutes. If you missed it, get a new one: “Tunnels” menu → the tunnel's “Script” button.

What the script does

1. Creates the WireGuard interface `evx-olt` , the hub peer and the tunnel address `10.250.x.y/32` .

2. Forwards only two ports from the tunnel address to the OLT: telnet 23 and SNMP 161 (dst-nat and masquerade). Nothing else passes from the tunnel into the ISP network.
3. Adds masquerade towards the tunnel so the OLT and ONUs can reply to the hub (ACS, traps).
4. All objects are marked `comment="EVX-OLT ..."` : re-running is safe — the script first removes its previous objects.

Several OLTs behind one MikroTik

One tunnel per router, any number of OLTs behind it. For the next OLT: “Tunnels” menu → “+ OLT behind this router”. The platform gives an add-on script: it forwards ports only to the new OLT (2301/16101, 2302/16102 ...); the tunnel and existing OLTs are not interrupted.

Do not run a new tunnel's full script on a router where an olt.am tunnel already works: it replaces the old tunnel and disconnects its OLTs.

How to remove

All platform objects are removed from the MikroTik with one terminal command:

```
:foreach i in=[/ip firewall nat find comment~"EVX-OLT"] do={/ip firewall nat remove $i}; :foreach i in=[/ip firewall filter find comment~"EVX-OLT"] do={/ip firewall filter remove $i}; :foreach i in=[/ip address find comment~"EVX-OLT"] do={/ip address remove $i}; :foreach i in=[/interface wireguard peers find comment~"EVX-OLT"] do={/interface wireguard peers remove $i}; :foreach i in=[/interface wireguard find comment~"EVX-OLT"] do={/interface wireguard remove $i}
```

4. OLT access and basic settings

Wizard step 2: OLT access

- **OLT name** and vendor (can be “detect automatically”).
- **Telnet login and password** — a user with configuration rights. On ZTE: `username oltam password <password> privilege 15`.
- **SNMP community** for read and write can be left empty: the platform takes them from the OLT config, and if there are none, creates random ones and saves the config.

“Check” — the platform logs in to the OLT over telnet and SNMP through the tunnel and shows the response.

“Add OLT” saves the OLT; within a minute boards, PON ports and all ONUs with signal appear.

What the platform reads from the OLT

Cards and versions, PON ports, uplinks and VLANs, ONU types, speed profiles (tcont/traffic), VLAN profiles, SIP profiles, all ONUs with configuration and signal, alarm and command logs. Nothing changes until your first action.

Wizard step 4: basic settings

- **Internet VLAN** : the default for authorizing new ONUs.
- **Management VLAN** (Mgmt / VoIP / TR-069) and **Mgmt IP pool** with gateway — the DHCP network for ONUs on the MikroTik.
- **Remote ACL** : the network allowed to reach the ONU web interface (usually the Mgmt network).
- **TR-069 interface** : via Mgmt IP (recommended) or via WAN.
- The “Apply to all ONUs” checkbox connects already working ONUs to TR-069 and Mgmt.

All of this can be changed later on the OLT tabs: VLAN, ONU IP pools, Remote ACL.

Traps

On the OLT page, the “Enable SNMP traps” button turns on sending traps to `10.250.0.1` through the tunnel — OLT alarms reach events within seconds.

5. TR-069 and instant changes

The platform has a built-in ACS. Each OLT gets an ACS profile: through the tunnel — `http://10.250.0.1:7547` (OLTs added with the wizard use this) or public — `http://217.113.16.35:7547` . ONUs get it at authorization, with the “Connect to ACS” button or the step 4 checkbox; auto-connect finds ONUs missing from the ACS every 10 minutes.

Instant changes: the “TR-069 script”

Without it an ONU applies TR-069 changes (Wi-Fi, ports, passwords) only at its scheduled check-in — up to 5 minutes. For the ACS to reach the ONU immediately (connection request), the MikroTik must allow access from the tunnel to the ONU Mgmt network.

1. Set the ONU Mgmt pools for the OLT: OLT tab “ONU IP pools” (or wizard step 4). There can be several pools.
2. “Tunnels” menu → the tunnel's “TR-069 script” button → one line → into the MikroTik terminal, as when creating the tunnel.
3. The script allows on the MikroTik access from `evx-olt` to the Mgmt pools on TCP 58000 and 7547 and adds masquerade so ONU replies return into the tunnel. The tunnel and OLT access are not interrupted.
4. As soon as the MikroTik fetches the script, the hub routes this OLT's Mgmt pools into the tunnel itself. Changes from the ONU card apply within seconds.

If the ONU Mgmt network is already reachable from the hub directly, this script is not needed.

Model specifics

- ZTE F6xx, Huawei HG8xxx: TR-069 comes up automatically via OMCI from the OLT.
- Some OEM models (CTC/ITMS firmware) need a WAN connection with the TR069 service inside the ONU, created in its web interface or via OMCI (`wan-ip ... / wan ... service tr069`).

What the platform stores

Wi-Fi and passwords set by the provider are remembered: after the subscriber resets the router they are restored on the first Inform.

6. Checks and common problems

Checks

- Tunnel: “Tunnels” menu — “● online”; the “Check” button shows the tunnel, telnet and SNMP to the OLT separately. On the MikroTik: `/interface wireguard peers print` — the hub peer has a last-handshake.
- OLT: the OLT page shows boards, PON ports and the ONU count; “Poll OLT” refreshes the data immediately.
- TR-069: the ONU card shows the ACS as “online”; after the “TR-069 script” changes from the card apply within seconds.

The tunnel does not come up

- Outgoing UDP 51820 is blocked — check the firewall of the MikroTik and the upstream network.
- Wrong time on the MikroTik — WireGuard is sensitive to the clock; enable the NTP client.
- The add-on script or the “TR-069 script” stopped with “This router has another EVX-OLT tunnel” — the script belongs to another tunnel. Take the script of the tunnel that runs on this router.

OLT not responding

- Wrong OLT IP — you need the OLT management address as the MikroTik sees it (check with ping from the MikroTik).
- Telnet or SNMP is disabled on the OLT, or an ACL on the OLT blocks the MikroTik address.
- Wrong telnet login or password, or the user lacks rights.

The ONU does not reach TR-069

- There is no Mgmt VLAN with DHCP for ONUs, or the pool is not set in the OLT settings.
- There is no route from the ONU Mgmt network to the ACS via the MikroTik.
- Changes apply only after a few minutes — run the “TR-069 script”.

Security

- Nothing is opened to the outside on the MikroTik: the router connects to the hub itself.
- Only telnet 23 and SNMP 161 to the OLT pass from the tunnel into the ISP network, and after the “TR-069 script” — TCP 58000 and 7547 to the ONU Mgmt pools.
- OLT passwords are stored encrypted; every command on the OLT is in the portal log.
- On the OLT page you can restrict OLT access (ACL) to the MikroTik address — the platform checks the login and rolls back the change if access is lost.

Contact

Write to us via the [form on olt.am](#) or your manager — we will connect together.