SAMM

Installation Manual

Install SAMM step by step — Windows, Ubuntu, MikroTik (RouterOS), or a ready server
then link your licence, pay, renew and connect your routers

Edition 2 · November 2026

samm.securytik.com

Contents

1. Which installation should I choose?
2. Before you start: IP addresses (never use one address twice)
3. Install on Windows (laptop or PC)
4. Turn on virtualization (Intel VT-x / AMD-V) in the BIOS
5. Install on Ubuntu Server (your own server or a VPS)
6. Install on a MikroTik router (container)
7. Get a ready server from us (automatic setup)
8. First login
9. Your licence: create an account, link SAMM, pay, renew
10. Connect your routers (NAS) — local or through the VPN
11. Turn on the extra features (Data Log, SAMM Fallback, Health, backups, updates)
12. Problems and solutions

> **How to read this manual**
> Do the steps in order. Copy commands exactly as written (the dark boxes). Do not skip a step. When a step says ✅ you may continue; when it says ❌ stop and fix it first.

1. Which installation should I choose?

Your situation	Choose	Section
I have a Windows 10/11 **Pro** PC or laptop that stays on all the time	Windows	3 + 4
I have a server, a virtual machine or a VPS (rented cloud server)	Ubuntu Server	5
I have a strong MikroTik (RB5009, CCR2004, CCR2116, CCR2216, hAP ax², L009, CHR) with a USB/microSD disk	MikroTik container	6
I do not want to install anything	Ready server from us	7

> **Our advice**
> For a real network with many users, use **Ubuntu Server** or a **ready server**. Windows is good for small networks and for testing. The MikroTik container is the newest and lightest option.

2. Before you start: IP addresses

Every device on the network needs **its own** IP address. Think of an IP like a phone number: if two devices have the same number, calls go to the wrong one and nothing works.

> ⚠️ **The golden rule**
> The router, your PC and SAMM are **three different addresses**. Never give SAMM the router's address or the PC's address. Never use an address another device already uses.

Pick one option (copy its numbers)

Option	MikroTik router	Windows PC	SAMM	Subnet
1 ⭐ best	`10.10.10.1`	`10.10.10.10`	`10.10.10.20`	`/24 = 255.255.255.0`
2	`10.20.30.1`	`10.20.30.10`	`10.20.30.20`	`/24`
3	`172.16.50.1`	`172.16.50.10`	`172.16.50.20`	`/24`

This manual uses **Option 1**. If you pick another option, only change the numbers.

Check that the addresses are free

1. Open **WinBox**, connect to the router, click **New Terminal**.
2. Paste:

   ```
   /ip address print
   ```

   ✅ No line starts with `10.10.10.` → Option 1 is free.
   ❌ A line starts with `10.10.10.` → use Option 2, then Option 3.
3. Paste:

   ```
   /ping 10.10.10.20 count=3
   ```

   ✅ `timeout` → nobody uses it. Good.
   ❌ You get replies → the address is taken. Choose another option.

Give the router its address (on a free port)

Example: the PC (or the SAMM server) is plugged into **ether5**, and nothing else is on ether5.

```
/interface bridge port remove [find interface=ether5]
/ip address add address=10.10.10.1/24 interface=ether5 comment=SAMM
/ip service set api disabled=no
```

> ⚠️ **Careful**
>
> The first line takes ether5 out of your LAN bridge. Only do it if ether5 is empty. The last line turns on the RouterOS API, which SAMM uses to manage the router.

3. Install on Windows

What you need

- Windows 10 or 11 **Pro**, Enterprise or Education, or Windows Server 2019+. **Windows Home does not work** (it has no Hyper-V).
- 8 GB RAM or more (SAMM uses 4 GB), and 40 GB free disk.
- A **network cable** from the PC to the router. Wi-Fi often does not work.
- Virtualization ON in the BIOS (section 4 shows how).

How do I know my Windows edition?

Press `Windows` + `R`, type `winver`, press `Enter`. If it says **Home**, you must upgrade to Pro first.

Step 1 — Give the PC a fixed IP

1. Press `Windows` + `R`, type `ncpa.cpl`, press `Enter`.
2. Right-click **Ethernet** → **Properties**.
3. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.
4. Choose **Use the following IP address** and type:

IP address	`10.10.10.10`
Subnet mask	`255.255.255.0`
Default gateway	`10.10.10.1`
Preferred DNS	`8.8.8.8`
Alternate DNS	`1.1.1.1`

5. Click **OK**, then **OK**.
6. Test: press `Windows` + `R`, type `cmd`, then:

```
ping 10.10.10.1
```

✅ `Reply from 10.10.10.1` → good.
❌ `Request timed out` → check the cable and that it is in ether5.

Step 2 — Run the installer

1. Right-click the **Start** button → **Terminal (Admin)** or **Windows PowerShell (Admin)** → **Yes**. (Not "Command Prompt".)
2. Paste this line and press `Enter`:

```
irm https://samm.securytik.com/install-windows.ps1 | iex
```

If that site cannot be reached, use the mirror:

```
irm https://dl.securytik.com/install-windows.ps1 | iex
```

Step 3 — Answer the questions

It asks	You answer
Which network adapter	The number of the **Ethernet** adapter (the cable to the router)
SAMM's IP address	**`10.10.10.20/24`** — never **`.10`** (the PC) or **`.1`** (the router)
Gateway — your MikroTik's address	**`10.10.10.1`**
DNS servers	Press Enter
CPU / RAM / disk	Press Enter for each
Continue? [y/N]	Type `y` and press Enter

> **If it says "already answers on the network"**
> That address is used by another device. Type a different one, for example **`10.10.10.30/24`**.

> **If it asks to restart Windows**
> This happens once, to switch on Hyper-V. Restart. After you sign in, it continues by itself; if it does not, open PowerShell (Admin) again and paste the same line.

The installation takes **10 to 20 minutes** and shows a progress bar. Do not close the window and do not turn off the PC.

Step 4 — Open SAMM

At the end, two shortcuts appear on the desktop: **SAMM Admin** and **SAMM Info**. Open **SAMM Admin**, or type in Chrome:

```
http://10.10.10.20/admin
```

Login	Username / password
SAMM panel	`admin` / `admin` (change it at once)
SSH into SAMM's machine	`samm` / `samm`
Root (console)	`root` / `samm`

> **Keep the PC awake**
>
> SAMM starts with Windows by itself. On a laptop keep the charger connected and set "When I close the lid" to **Do nothing** (Control Panel → Power Options).

To remove SAMM later: open **SAMM Info** on the desktop and type `uninstall-samm`.

4. Turn on virtualization (VT-x / AMD-V)

If the installer says **virtualization is off**, or **Intel VT-x**, or **Hyper-V cannot start**, do this section.

First: is it already on?

1. Press Ctrl + Shift + Esc (Task Manager).
2. Click **Performance** → **CPU**.
3. Under the graph look at **Virtualization**:
   ✅ **Enabled** → nothing to do.
   ❌ **Disabled** → turn it on in the BIOS (below).

Which processor do I have?

In Task Manager → **Performance** → **CPU**, the processor name is at the top right: it starts with **Intel** (for example Intel Core i5) or **AMD** (for example AMD Ryzen 5). Write it down: the BIOS option name depends on it.

Processor	Set to Enabled	Needed?
Intel	**Intel Virtualization Technology** (VT-x, Vanderpool)	Yes — required
	Execute Disable Bit (XD bit, No-Execute Memory Protection)	Yes — Hyper-V needs it (usually already on)
	Intel VT-d (Virtualization for Directed I/O)	Optional
AMD	**SVM Mode** (AMD-V, Secure Virtual Machine)	Yes — required
	NX Mode (No-Execute)	Yes — Hyper-V needs it (usually already on)
	IOMMU (AMD-Vi)	Optional

> **Nothing else changes**
> Do not change Secure Boot, the boot order, the disk mode (AHCI/RAID) or the clock. Change only the options in the table above.

Turn it on in the BIOS

1. Save your work and restart the PC.
2. As soon as the screen lights up, press the BIOS key again and again:

Brand	Key	Where the option usually is
Dell	F2	Virtualization Support → Enable Intel Virtualization Technology
HP	Esc, then F10	Advanced / System Configuration → Virtualization Technology (VTx)
Lenovo	F1 or F2 (or the Novo button)	Security or Configuration → Intel Virtualization Technology / AMD SVM
ASUS	F2 or Del	Advanced Mode (F7) → Advanced → CPU Configuration
Acer	F2	Advanced or Main → Intel Virtualization Technology
MSI	Del	OC → CPU Features
Gigabyte	Del	Tweaker → Advanced CPU Settings
Desktop PC (other)	Del	Advanced → CPU Configuration

3. Set the option to **Enabled**:
   - **Intel** processor: **Intel Virtualization Technology** (also called **VT-x**).
   - **AMD** processor: **SVM Mode** (also called **AMD-V**).
4. How to move in the BIOS: arrow keys `↑` `↓` `←` `→` to move, `Enter` to open an option, choose **Enabled**, `Enter` again. In a graphical BIOS you can use the mouse. If a menu is hidden, look for **Advanced Mode** (often `F7`).
5. Press `F10` → **Yes** (save and exit).
6. Check Task Manager again: it must say **Virtualization: Enabled**. After Hyper-V is on, Windows may instead show **"A hypervisor has been detected"** — that also means it is on.

> **No BIOS key works?**
> In Windows: Settings → System → Recovery → Advanced startup → **Restart now** → Troubleshoot → Advanced options → **UEFI Firmware Settings** → Restart.

Turn on Hyper-V (if the installer did not)

Open PowerShell (Admin) and paste:

```
Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -All
```

Type `Y` to restart. Then run the SAMM installer again.

Common problems

• No virtualization option in the BIOS → update the BIOS from the maker's site; very old PCs cannot run SAMM.

• "Feature name not found" → your Windows is Home; upgrade to Pro.

• Windows itself runs inside VMware / Proxmox / Hyper-V → turn on **nested virtualization** in that outer system (VMware: "Virtualize Intel VT-x/EPT", VM powered off).

5. Install on Ubuntu Server (own server or VPS)

What you need

- A **fresh** Ubuntu Server 22.04, 24.04 or 26.04 (or Debian 12 / 13). Server edition, not desktop.
- 2 CPU cores, 4 GB RAM, 40 GB disk at least. Internet access.
- The **root** password, or a user with `sudo`.

Step 1 — Connect to the server

From Windows open PowerShell (or use Termius / PuTTY) and type (use your server's address):

```
ssh root@10.10.10.20
```

Step 2 — A fixed IP (local servers only)

On a VPS the provider already gives a fixed IP — skip this step. On your own server in your network, edit the network file:

```
sudo nano /etc/netplan/50-cloud-init.yaml
```

Make it look like this (your card name may be `eth0`, `ens18`... see it with `ip a`):

```
network:
  version: 2
  ethernets:
    eth0:
      addresses: [10.10.10.20/24]
      routes:
        - to: default
          via: 10.10.10.1
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1]
```

Save (Ctrl+O, Enter, Ctrl+X) and apply:

```
sudo netplan apply
```

Step 3 — Install SAMM (one line)

```
curl -fsSL https://samm.securytik.com/install.sh | sudo bash
```

If GitHub or the site is blocked in your country, use the mirror:

```
curl -fsSL https://dl.securytik.com/install.sh | sudo bash
```

It asks	You answer
Cloudflare token	Press `Enter` (skip; you can add it later)
HTTP port (only if port 80 is busy)	Press `Enter` for 8080

After a few minutes it prints **SAMM is installed and running**. Open:

```
http://10.10.10.20/admin
```

Login `admin` / `admin`. On a VPS use the VPS public IP instead of 10.10.10.20.

> **VPS with a firewall?**
> In your provider's panel allow: TCP 80 and 443 (panel), UDP 51820 (WireGuard VPN for your routers). If you use L2TP: UDP 500, 4500, 1701. SSTP: the TCP port shown in SAMM's VPN page.

6. Install on a MikroTik router (container)

What you need

- RouterOS **7.23 or newer**.
- An arm64 or x86 router: RB5009, hAP ax², L009, CCR2004, CCR2116, CCR2216, x86 or CHR. **Not** hEX, RB750 or old models.
- A USB stick or microSD of **30 GB or more**, formatted **ext4**.

Step 1 — Turn on container mode

1. WinBox → **New Terminal**, paste:

   ```
   /system device-mode update container=yes
   ```

2. The router waits for you: within **5 minutes**, **unplug the power and plug it back** (or press the reset button once quickly, as the message says). A normal reboot is not enough.

Step 2 — Prepare the disk

```
/disk print
```

Find your USB/microSD (for example `usb1`), then format it (this erases it):

```
/disk format usb1 file-system=ext4 label=samm
```

Step 3 — One line installs everything

```
/tool fetch url="https://samm.securytik.com/install-routeros.rsc" dst-path=samm-instal
l.rsc; /import samm-install.rsc
```

It checks the router, installs the **container** package, finds the disk, downloads SAMM and starts it. When it asks you to (after a reboot or a power cycle), **paste the same line again** — it continues where it stopped.

Step 4 — Keep SAMM running after a reboot

```
/container set [find where name~"^app-samm"] start-on-boot=yes restart-policy=always
/system scheduler remove [find name=samm-watchdog]
/system scheduler add name=samm-watchdog start-time=startup interval=1m on-event=":for
each c in=[/container find where name~\"^app-samm\" and stopped] do={/container start
\$c}"
```

Open the panel: `http://<router IP>:8000/admin` — login `admin` / `admin`. The router talks to its own SAMM on **`127.0.0.1`**.

> **⚠️ Updating SAMM on MikroTik deletes its data**
> Before any update: SAMM → Tools → Backup → create a backup → **download it to your PC**. Then remove and re-add the app, and restore the backup.

> **"Could not download" / fetch refused?**
> The router's device-mode blocks downloads. Run `/system device-mode print`; if `fetch: no`, run `/system device-mode update fetch=yes` and power-cycle again.

7. Get a ready server from us

No installation at all: we rent the server, buy your **.com** domain, install SAMM with your company name and link your licence.

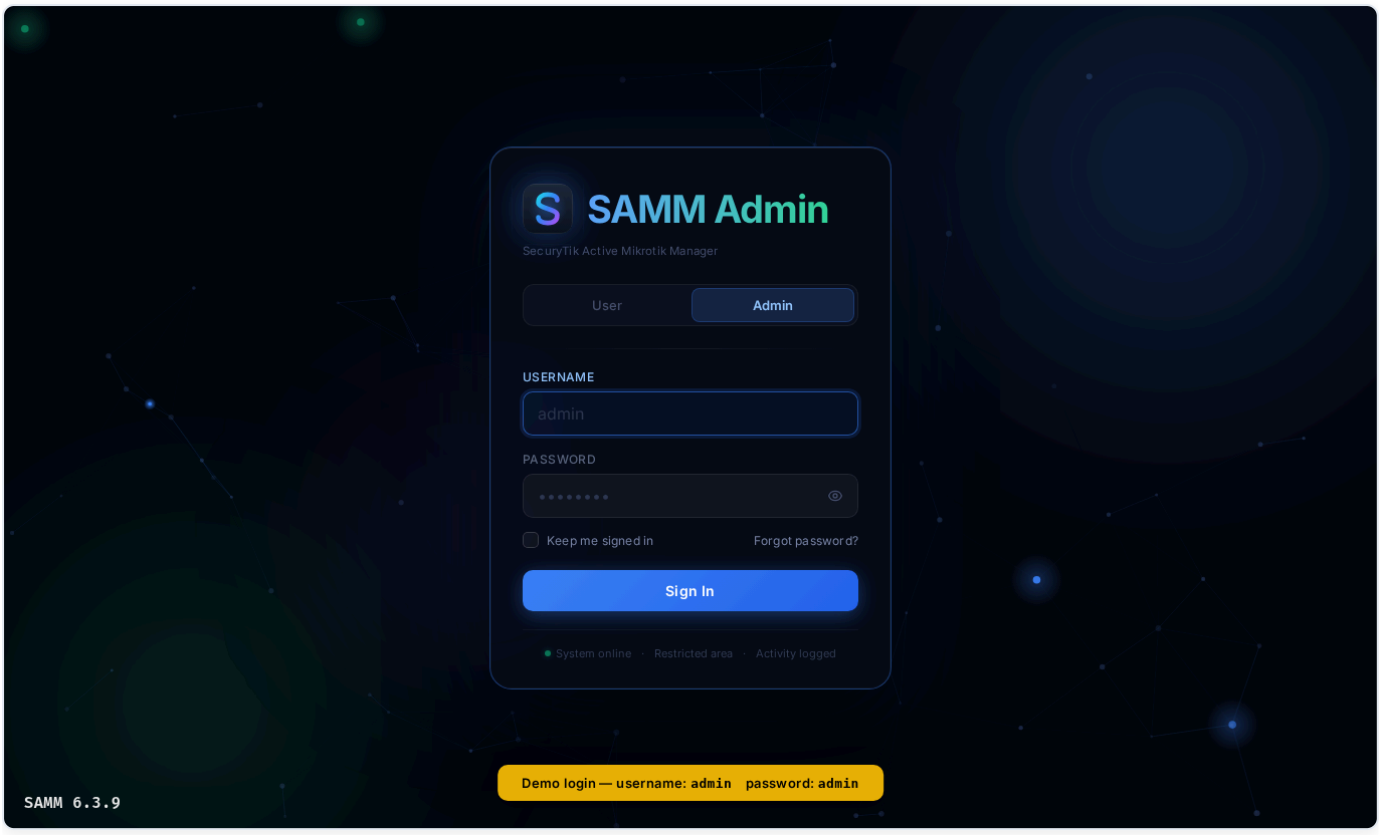
Size	Server	Price / year
Small	6 cores · 12 GB RAM · 200 GB SSD	$100
Medium	8 cores · 24 GB RAM · 300 GB SSD	$200
Large	12 cores · 48 GB RAM · 400 GB SSD	$300

1. Go to **samm.securytik.com** and sign in (or create an account).
2. Open **Dashboard → Get a server**.
3. Choose the size, a server name and the number of users.
4. Search for your **.com** domain, or pick a suggestion.
5. Click pay and choose a payment method. **Pay within 2 hours**, or the order is cancelled.
6. Wait. Everything is automatic. You receive an **e-mail** with your panel address (`https://your-domain/admin`) and a strong password.

> **Renewal**
> Renewal opens 7 days before the year ends. Renew at least **1 day before** the end, or the server, the domain and the data are deleted. Keep your own backups too.

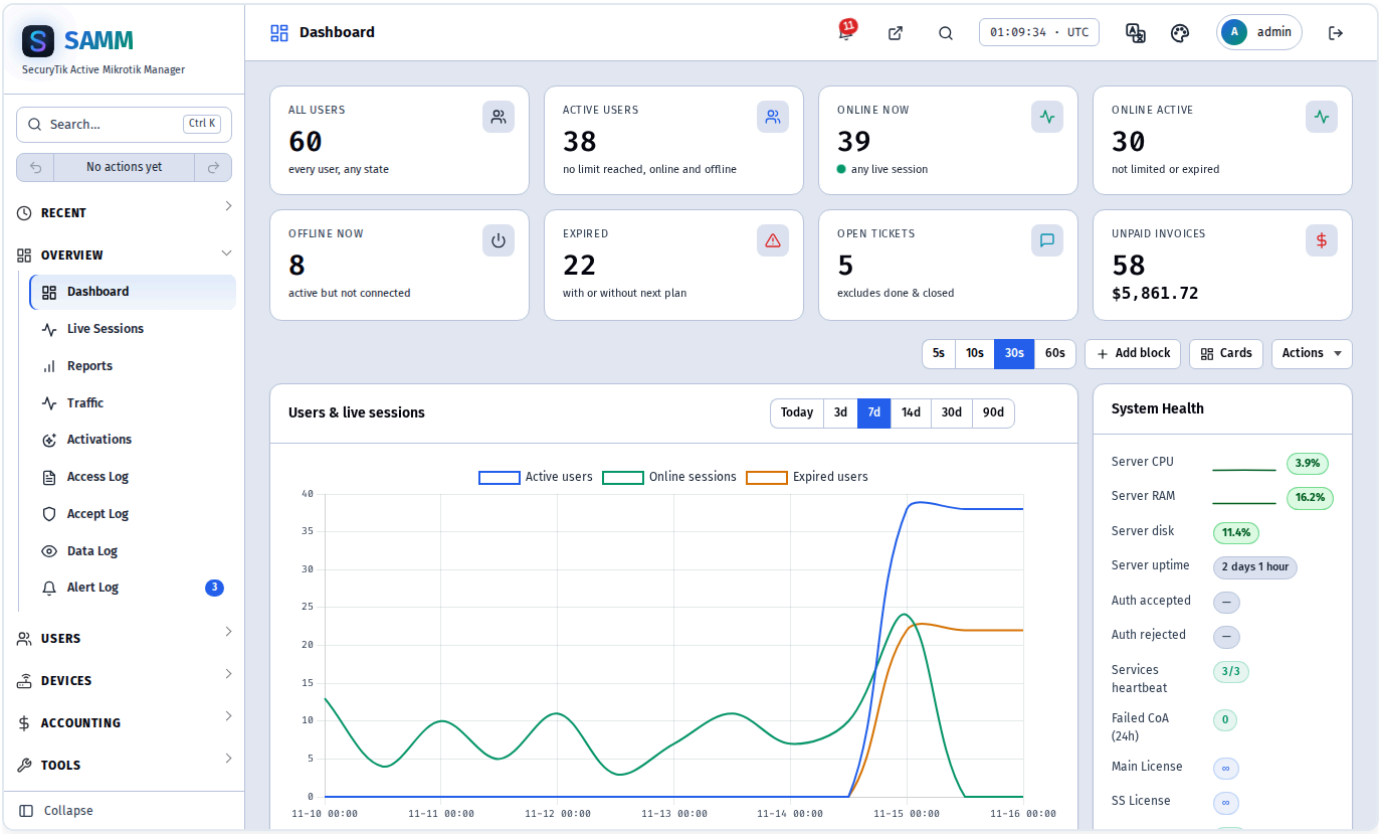
SSH access: **Dashboard → Servers** lets you create your own SSH login.

8. First login



The SAMM login page

1. Open `http://<SAMM IP>/admin` (example `http://10.10.10.20/admin`).
2. Sign in with `admin` / `admin`.
3. Change the password at once: top-right profile menu → **Profile**, or **System → Admins**.



The dashboard after login

9. Your licence: account, link, pay, renew

A new SAMM works **without a licence** with small limits (25 users, 1 router). To get more, link it to your SecuryTik account and choose a plan.

Plan	Users	Hotspot cards	Routers
Unregistered	25	25	1
Free	100	50	2
Lite	500	1,500	4
Plus	1,000	3,000	6
Pro	2,000	6,000	12
Mega	5,000	15,000	24
Max	10,000	30,000	unlimited
Unlimited	unlimited	unlimited	unlimited

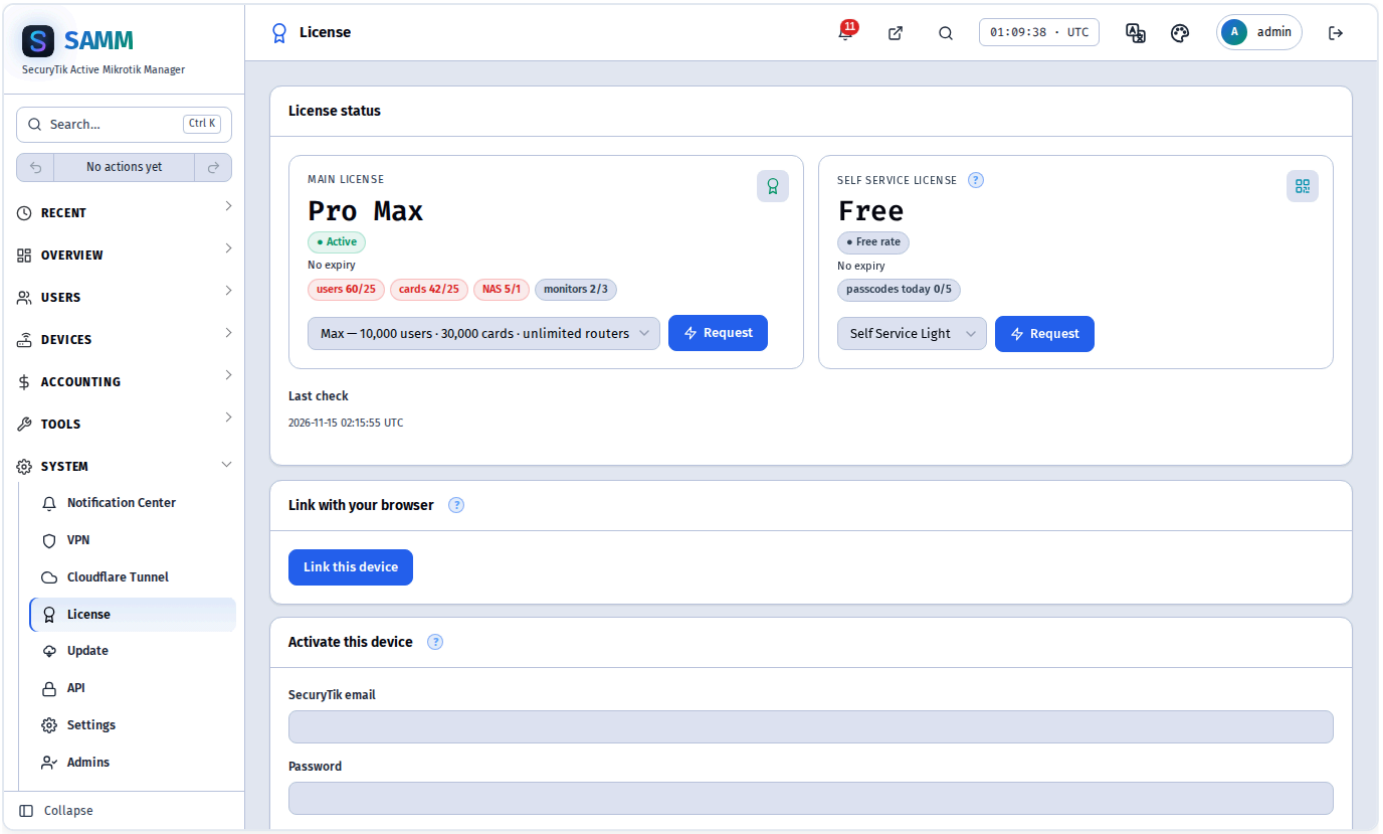
Prices: see **samm.securytik.com/pricing**. Every plan has every feature; the plan only sets the limits.

Step 1 — Create your account

Go to **samm.securytik.com** → **Sign up**. Use your real e-mail; confirm it.

Step 2 — Link your SAMM to your account

1. In SAMM open **System → License**.
2. Click **Link this device**. SAMM shows a **code**.
3. On your phone or PC open **samm.securytik.com**, sign in, and approve the code (Dashboard → **Link a device**).
4. SAMM becomes **Free** automatically.



System → License

Step 3 — Buy a plan and pay

1. On samm.securytik.com open **Dashboard → Devices** and pick your SAMM (or choose a plan from SAMM's License page).
2. Choose the plan and how long (for example 1 year).
3. Click **Continue to payment** and choose a payment method shown on the page.
4. Pay. The licence becomes active by itself within minutes. In SAMM, the License page shows the new plan (click re-check if needed).

> **Card payment**
> To pay by bank card, message us on WhatsApp **+961 81 507 933** with your licence ID; we send you a payment link.

Step 4 — Renew

- **Dashboard → Devices** → your device → **Renew**. Pay the same way.
- Switch on **Auto-renew** if you do not want to remember.
- You get reminders before the end date.

If you forget to renew

Stage	What happens
Warning	A red banner. Everything still works.
Grace	A short time to renew. Users stay online.
Soft lockdown	Changes stop; users can still log in for about 7 days.
Hard lockdown	Only the renewal page works.

Your data is never deleted. Renew at any stage and everything starts again by itself.

10. Connect your routers (NAS)

A **NAS** is the MikroTik your subscribers connect to (PPPoE / Hotspot). SAMM must reach it, and it must reach SAMM.

Where is SAMM?	Where is the router?	Use
Same network (Windows / local server / MikroTik)	Same network	Case A — add by IP
VPS / ready server (on the internet)	Anywhere	Case B — VPN one-line link
Local	Another city / behind NAT	Case B (SAMM's VPN port must be forwarded to SAMM on your main router)

Case A — Router on the same network

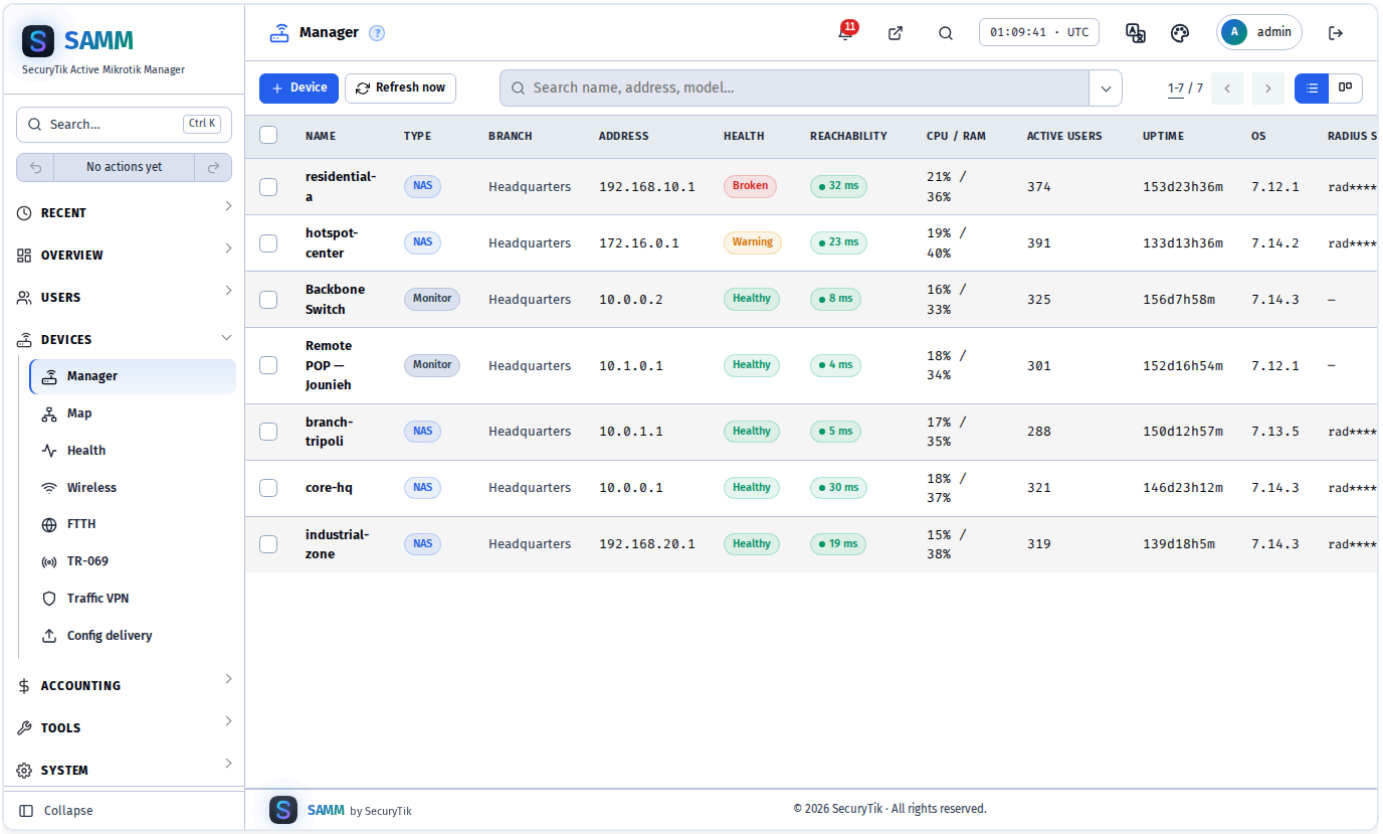
1. On the router make sure the API is on:

```
/ip service set api disabled=no
```

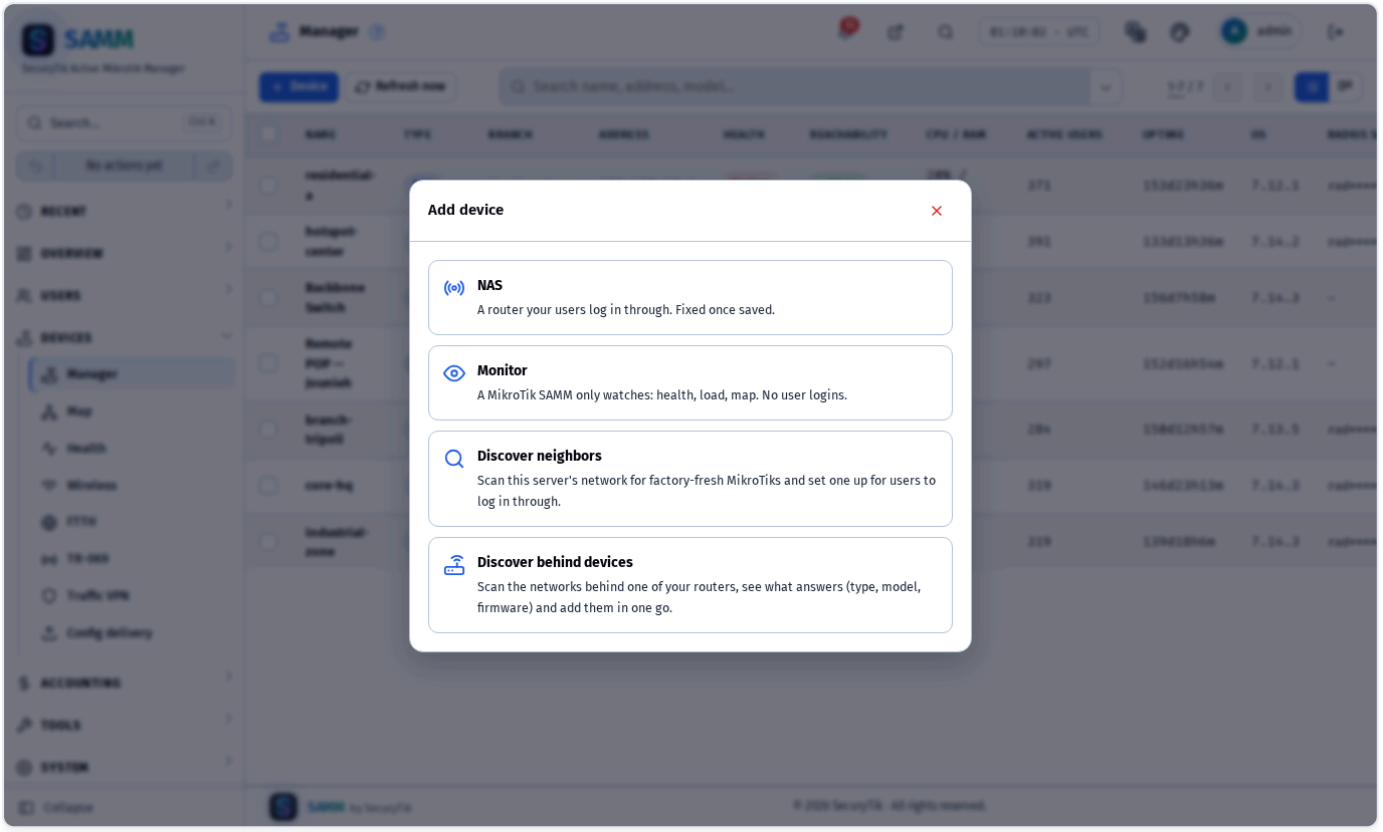
2. In SAMM open **Devices → Manager**, click **+ Device**, then choose **NAS**.
3. Fill in the **New Router** form:

NAS IP or hostname	**`10.10.10.1`**
Shortname	any name, e.g. `Main`
Type	MikroTik
RADIUS shared secret	a password you invent (letters and numbers, no spaces)
CoA port / API port	leave as they are
API user / API password	the WinBox login of the router

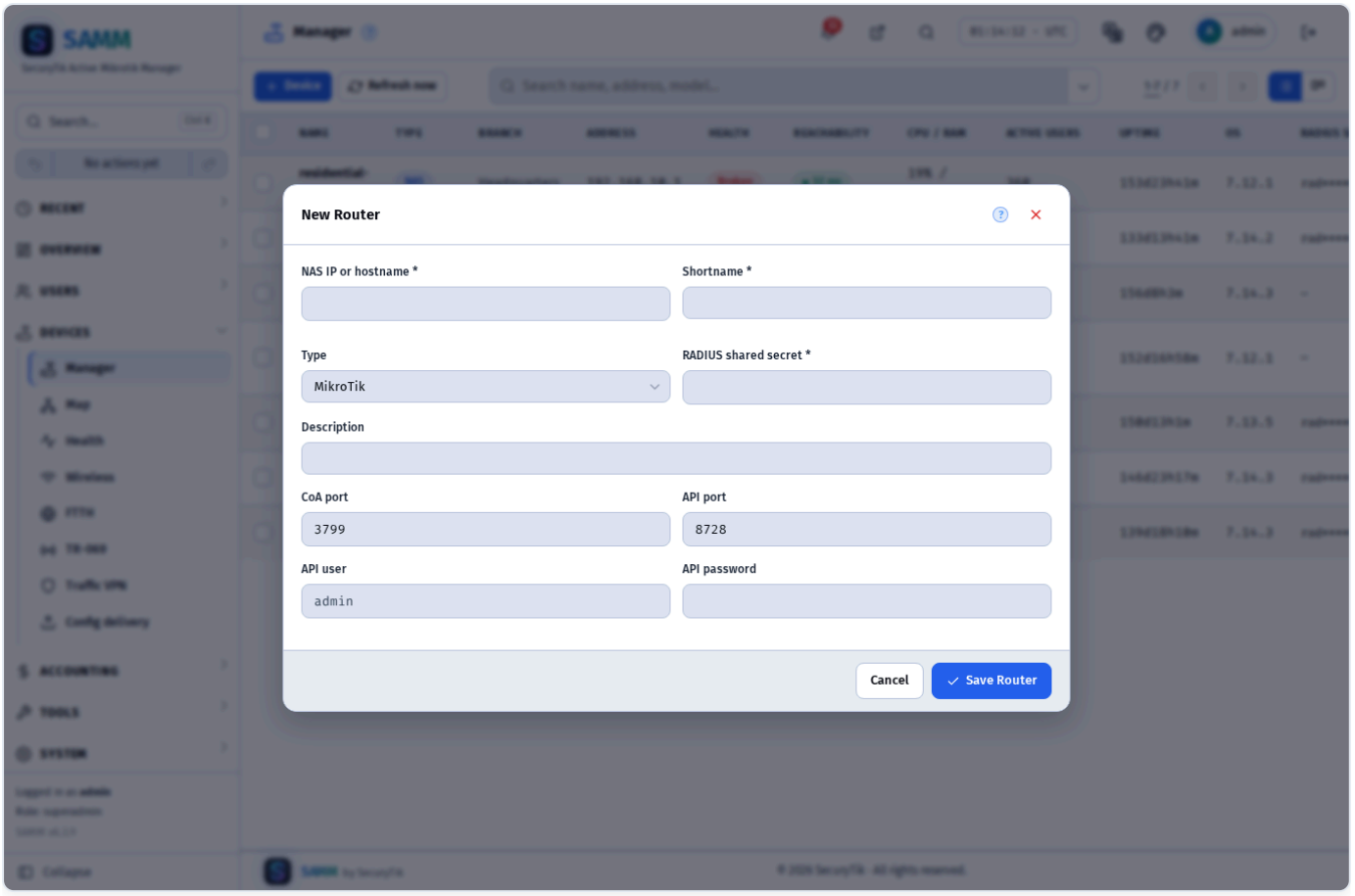
4. Click **Save Router**.
5. Tick the router in the list → **Actions → Push RADIUS**. SAMM writes the RADIUS settings into the router for you (you can also use the router's ⋮ menu).
6. Wait until the router shows **Healthy**.



Devices → Manager — every router with its health



+ Device → choose NAS



The New Router form

Case B — Router far away or SAMM on a VPS: the VPN link

SAMM has its own VPN. The router opens a tunnel to SAMM, so it works behind NAT, on 4G, anywhere.

Which VPN type?

Your router	Choose
RouterOS 7	**WireGuard** (fastest, simplest) ⭐
RouterOS 6	**L2TP/IPsec** (RouterOS 6 has no WireGuard)
Two or more routers behind the same public IP	**SSTP**

Step 1 — Turn on the VPN servers (once)

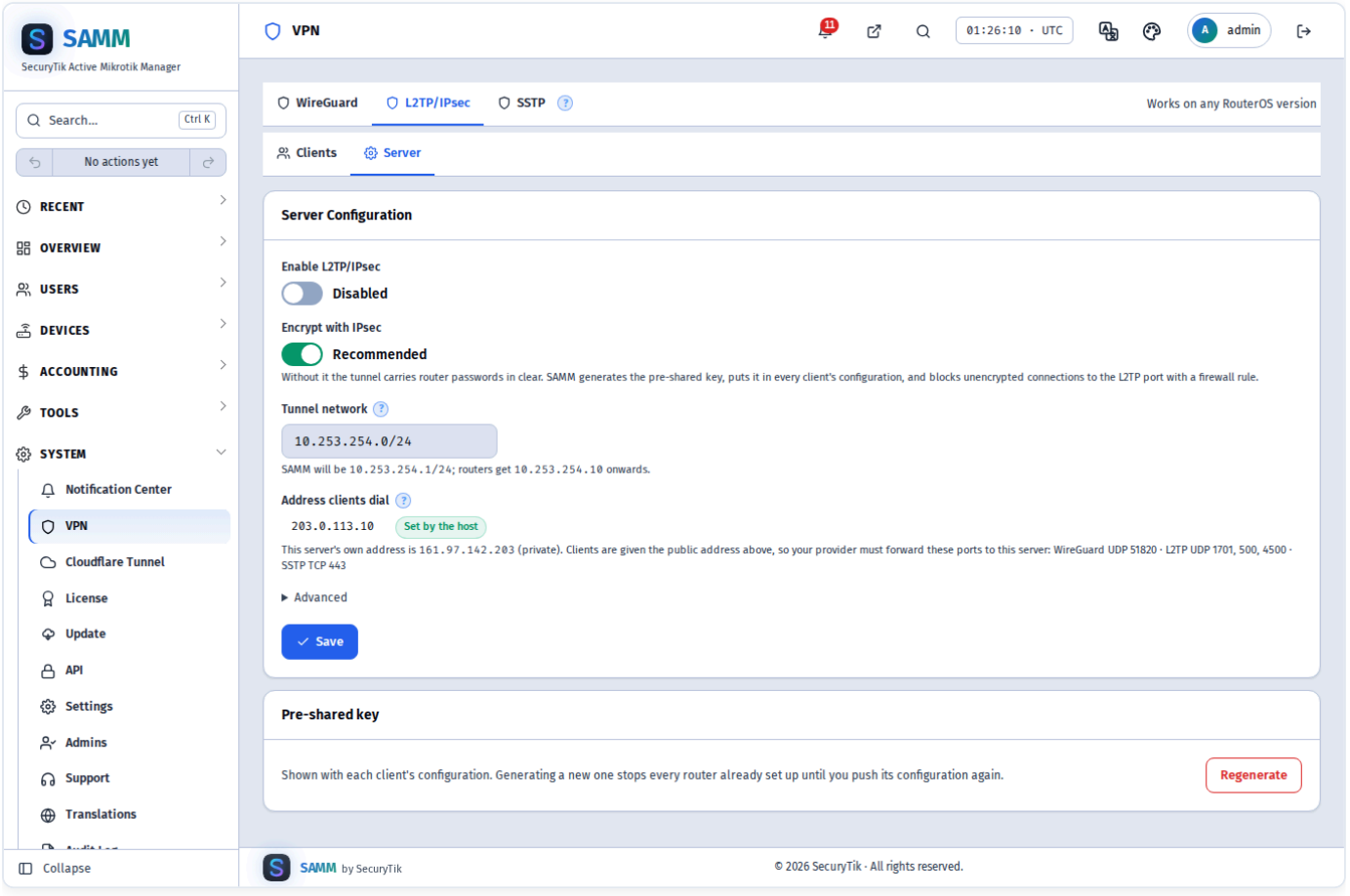
> ⚠️ **All three VPN servers are OFF on a new SAMM**
> WireGuard, L2TP/IPsec and SSTP come ready but switched off. A router cannot connect until you switch on its server. Switch on the ones your routers need — we recommend all three.

WireGuard (RouterOS 7)

1. SAMM → **System → VPN** → tab **WireGuard → Server**.
2. Click **Generate Keys** (only the first time; creates the server keys).
3. Keep the port `51820` and the addresses as they are.
4. Switch the server **On**, click **Save**, confirm.

L2TP/IPsec (RouterOS 6 and 7)

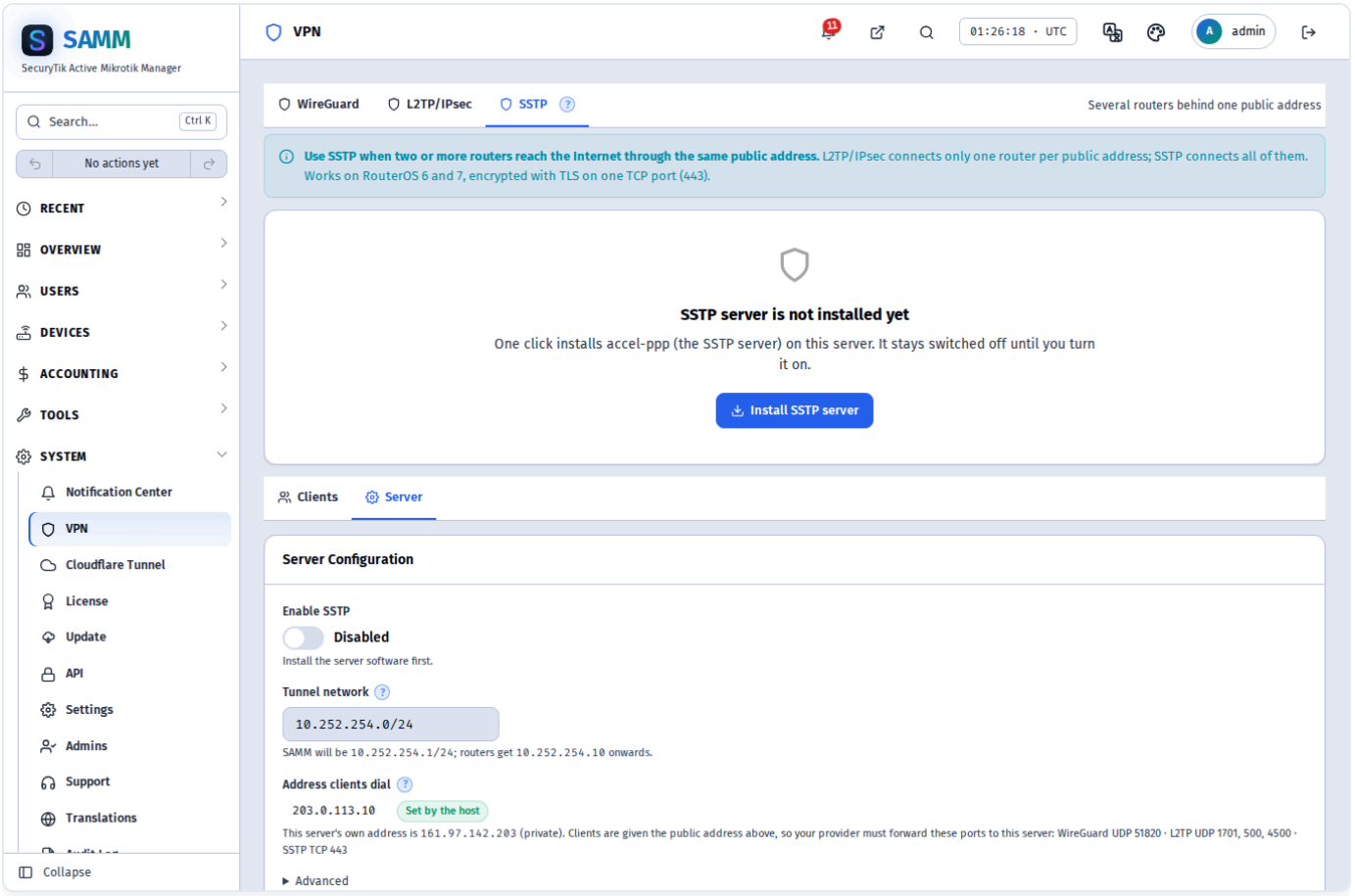
1. **System → VPN** → tab **L2TP/IPsec → Server**.
2. Switch **Enable L2TP/IPsec** on (it shows *Disabled* until you do).
3. Keep **Encrypt with IPsec** ON (recommended: without it router passwords travel in clear). SAMM creates the pre-shared key and gives it to every router.
4. Keep the tunnel network as it is, click **Save**.



System → VPN → L2TP/IPsec → Server: switch on "Enable L2TP/IPsec", then Save

SSTP (several routers behind one public IP)

1. **System → VPN** → tab **SSTP → Server**.
2. Switch **Enable SSTP** on, keep the port, click **Save**.

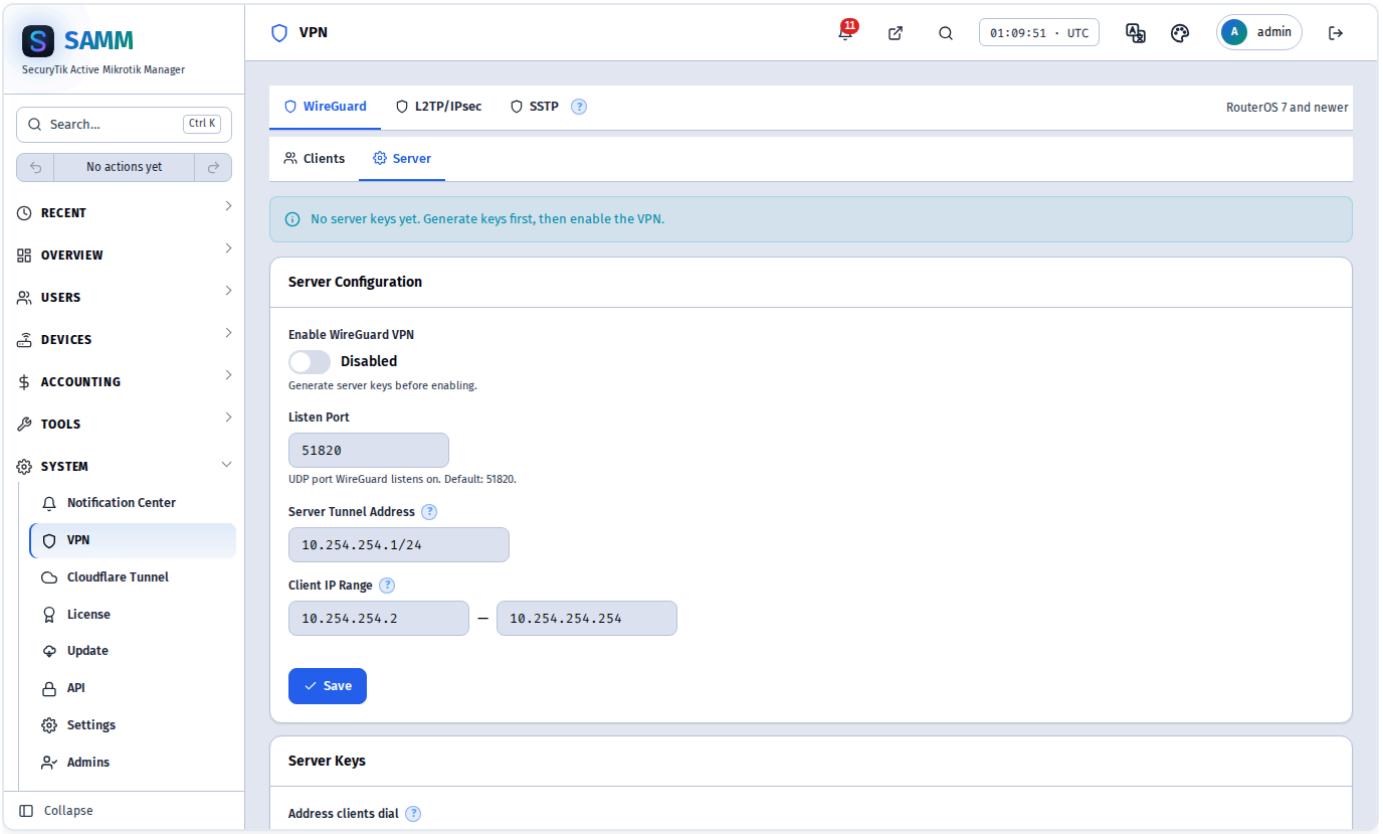


System → VPN → SSTP → Server

Open or forward the ports

VPN	Port
WireGuard	UDP 51820
L2TP/IPsec	UDP 1701, 500, 4500
SSTP	TCP 443

On a VPS: allow these ports in the provider's firewall. SAMM at home or in the office (behind NAT): forward these ports from your main router to SAMM's IP. The Server tab shows the exact ports and the public address it gives to routers.

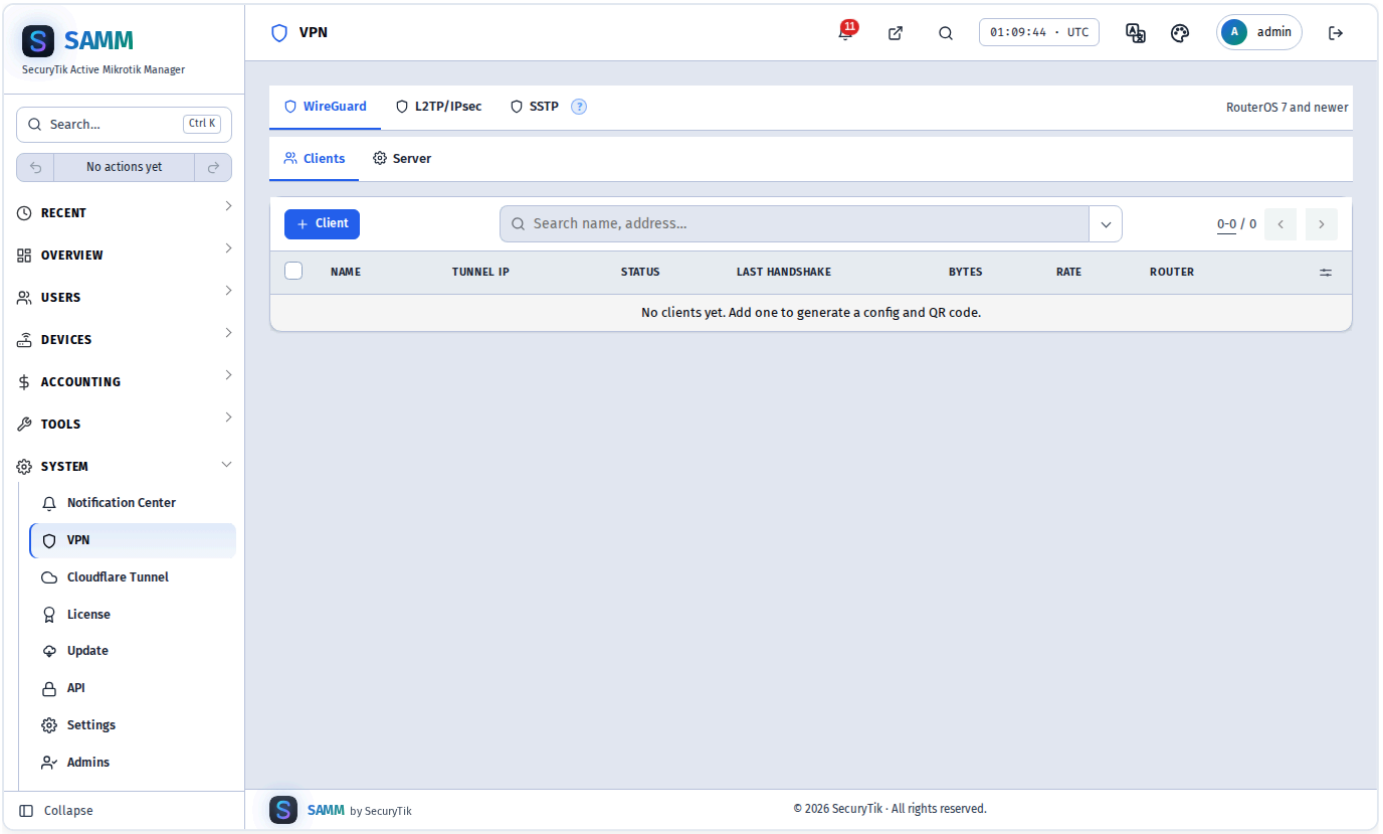


System → VPN → Server

> ⚠️ **Never press "Regenerate Keys" later**
> It disconnects every router already connected. Generate keys only the first time.

Step 2 — Get the router's installation link

1. Open the **Clients** tab → **+ Client**.
2. Give it the router's name, choose **Managed NAS** (users log in through it) — or **Monitor only** for access points.
3. Save. SAMM shows a **one-line install link**. Click copy.



System → VPN → Clients

Step 3 — Paste it in the router

1. WinBox → the router → **New Terminal**.
2. Paste the line and press Enter. It creates the tunnel, SAMM's login on the router, the RADIUS settings and the expired-users page — all at once.
3. In SAMM the client turns green, and the router appears in **Devices → Manager**.

Last check on the router

PPPoE / Hotspot must use RADIUS. SAMM's push does it; to check by hand:

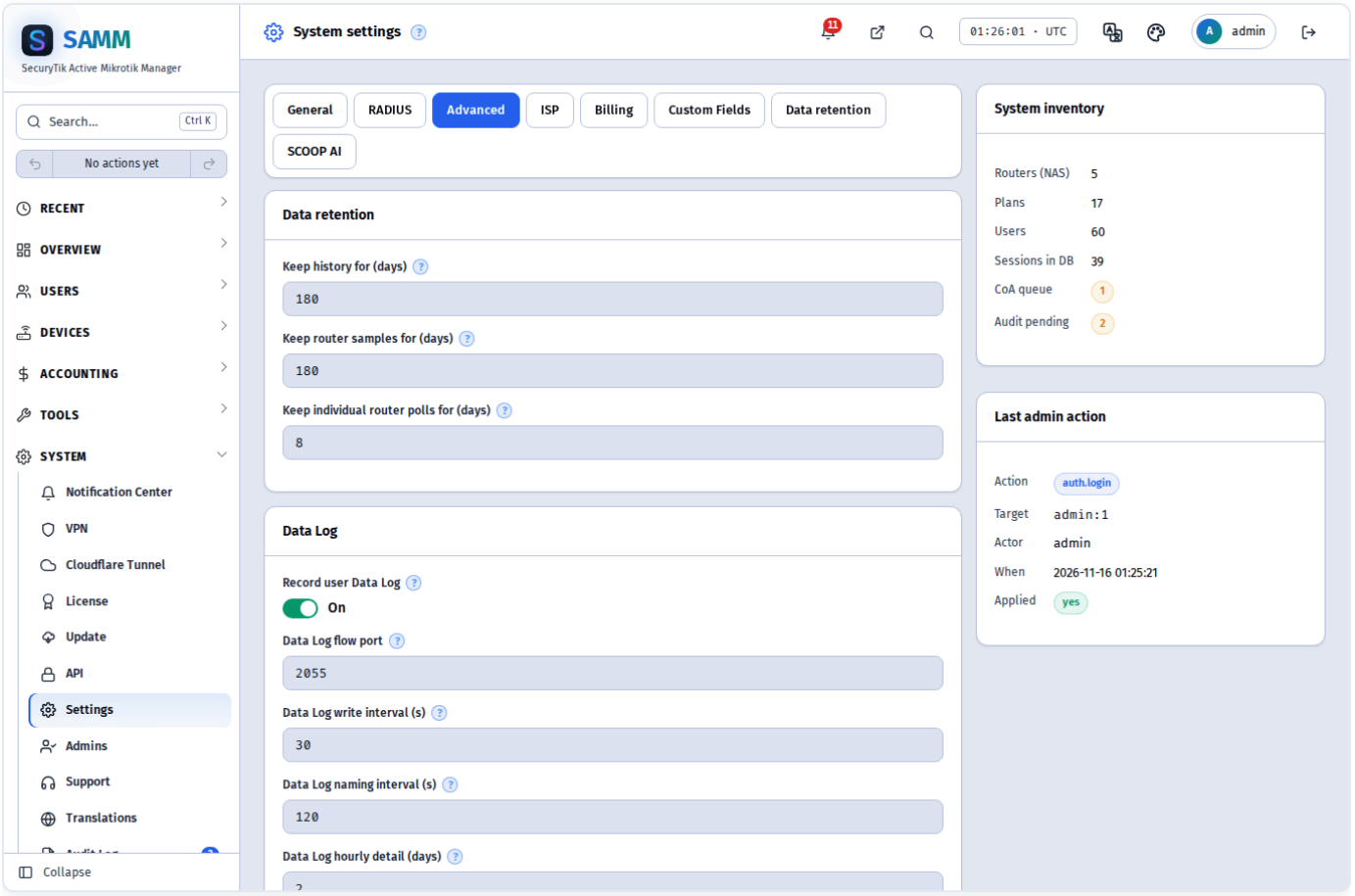
```
/radius print
/ppp aaa print
```

`/radius` must show SAMM's address with service `ppp,hotspot`, and `use-radius: yes`.

Next: create plans (**Users → Plans**) and subscribers (**Users → New customer**).

11. Turn on the extra features

Some features are off on a new SAMM, because they use disk space or change the router. Turn on what you need. Most are in **System → Settings → Advanced**.



System → Settings → Advanced

Data Log (where each user's traffic goes)

1. **System → Settings → Advanced → Data Log**.
2. Switch **Record user Data Log** ON.
3. Set how many days of hourly detail to keep, and the retention. Keep the other values as they are.
4. Save. Then open any user → **Data Log**: top sites and apps (YouTube, Facebook, WhatsApp...) with upload and download.

> **Good to know**
>
> The Data Log reads the router's own flow export; SAMM never sits in the traffic path. The figures are indicative; billing always uses RADIUS accounting. It needs the router to be managed by SAMM (API).

SAMM Fallback (users keep logging in if SAMM stops)

1. **System → Settings → Advanced → SAMM Fallback**.
2. Switch it ON for each router you want to protect.
3. Set the delay (how long SAMM may be unreachable before the router takes over).
4. Save. SAMM keeps a disabled copy of every active user on that router. If SAMM stops answering, the router logs users in by itself; when SAMM is back, everyone goes through SAMM again.

The status table on the same page shows each router's sync state and any user that failed to sync.

Network Health

System → Settings → Advanced → Network Health: checks your routers for common mistakes (dead backup lines, DNS open to the Internet, overlapping pools…) and alerts you. It is ON on new installs; keep it ON.

Data retention (legal records)

System → Settings → Data retention: keeps connection records (two years by default) and gives you the **Lookup** page "who used this address at this time?". Off until you switch it on.

Backups

Tools → Backup: create a backup and **download it to your PC** regularly (and always before an update on MikroTik).

Updates

System → Update: SAMM checks for a new signed version every day. Choose **notify** (a banner with an **Apply now** button, the default) or **auto** (applied by itself).

Publish the panel online (Cloudflare Tunnel)

System → Cloudflare Tunnel: paste a Cloudflare Zero Trust token to open SAMM from anywhere with HTTPS, without opening ports.

Per user: Parental control and VPN through SAMM

Open a user → **Edit**: switch on **Parental control** (families block categories and apps from the user portal) and/or **VPN through SAMM** (the user's traffic leaves through SAMM's server; needs a working VPN tunnel to the router). Many users at once: Users list → tick → bulk actions.

12. Problems and solutions

Problem	Solution
Windows: "virtualization is off" / VT-x	Section 4.
Windows Home	Upgrade to Pro, or use Ubuntu / a ready server.
"already answers on the network"	The IP is used by another device. Pick another free IP (section 2).
Panel does not open	Ping SAMM's IP; check the cable; on Windows open SAMM Info → check status; on a VPS check the firewall (TCP 80/443).
Router stays offline in SAMM	API on? (`/ip service print`); correct user/password; Case B: is the VPN server switched ON in System → VPN? Are its ports open/forwarded (UDP 51820 / UDP 1701, 500, 4500 / TCP 443)?
Users cannot log in	Check `/radius print` and that the RADIUS secret in SAMM and on the router are identical. Then Overview → Accept log in SAMM shows the reason.
Licence still "Unregistered"	System → License → Link this device, approve the code on samm.securytik.com.
Wi-Fi laptop: router cannot reach SAMM	Use a network cable. Many Wi-Fi cards cannot bridge a virtual machine.

> **Need help?**
> Open SAMM → System → Support, or write to us from samm.securytik.com.