Connecting a MikroTik Router

After adding the router in SAS Radius (Adding and Editing a NAS), configure the MikroTik to use SAS Radius for PPPoE (and/or Hotspot). The commands below are for the RouterOS terminal. Replace `SAS_IP` with your SAS Radius server address and `SECRET` with the Shared Secret.

1. Add the RADIUS server

```
/radius add service=ppp,hotspot address=SAS_IP secret=SECRET timeout=3000ms
```

If the router has several IP addresses, set `src-address=` to the IP address you entered in the NAS form (1700 by default in SAS Radius).

> Use only **one** RADIUS server entry. Two RADIUS servers cause wrong online counts and duplicate sessions.

2. Allow disconnect and CoA requests

```
/radius incoming set accept=yes port=1700
```

The port must be the same as **Incoming (COA) Port** in the NAS form.

3. Use RADIUS for PPPoE

```
/ppp aaa set use-radius=yes accounting=yes interim-update=5m
```

On the PPPoE server, allow PAP and/or CHAP authentication and disable MS-CHAP v1/v2:

```
/interface pppoe-server server set [find] authentication=pap,chap
```

4. Hotspot (optional)

```
/ip hotspot profile set [find] use-radius=yes radius-interim-update=5m
```

5. Interim update and idle timeout

The router sends an **interim update** for each online user at the interval you set. SAS Radius closes sessions that send no update for longer than **User Idle Timeout** (*Settings → Advanced*). Keep the idle timeout at least 2 times the interim interval (for example interim 2 minutes, idle timeout 4 minutes); otherwise online users disappear from the online list.

6. Optional features

Feature in SAS Radius	Router setting
Live Traffic (Online Users)	`/snmp set enabled=yes` and the same community as **SNMP Community** in the NAS form.
Ping a user (Online Users)	SSH service enabled, and a router user entered in the NAS form's SSH fields.
IP Accounting / Free Zone	IP Accounting enabled on the router, and IP Accounting ON in the NAS form.

7. Expired users

To give expired users limited access (for example a renewal page) instead of rejecting them, create the expired IP pool on the router and an expired profile in SAS Radius. See the Profiles chapter.

Router behind NAT or far away

If the router reaches SAS Radius through NAT or over the internet, connect it with a VPN tunnel (for example L2TP or SSTP) and add the NAS with its **tunnel IP**. NAT between SAS Radius and the router breaks disconnect requests. See Disconnect and CoA.

Revision #6
Created 2026-11-05 11:36:09 UTC by Admin

Updated 2026-11-07 21:22:41 UTC by Admin