RadiusForge

Getting Started

Your first organisation, plan, subscriber and router

RadiusForge for ISPs & WISPs · Version 2026.10.17 · radiusforge.co.uk

> **Who this guide is for**
>
> This guide assumes you know little or nothing about RADIUS, MySQL or Linux servers. If you're already comfortable with those, skip ahead to the **User Guide**. If you haven't installed RadiusForge yet, start with the **Install Guide** or **Quick Start**.

What RadiusForge actually does

Every time someone connects to your network — a home broadband customer whose router dials in, a Wi-Fi hotspot user, a VPN user — something has to answer three questions instantly:

1. **Is this person allowed to connect?** (checking a username and password)
2. **If yes, how fast should their connection be, and what settings do they get?**
3. **How long were they connected, and how much data did they use?**

The system that answers those questions is called **RADIUS**. Think of it as a doorman who also sets the rules: every router or access point asks RADIUS "*can this person in?*", RADIUS checks its records and says yes or no, and if yes, tells the router exactly what that person may do — their speed limit, for example.

RadiusForge is the control panel for that doorman. The actual RADIUS software — a program called **FreeRADIUS** — is powerful but was built for network engineers, and configuring it normally means editing text files full of jargon. RadiusForge gives you web pages instead: add a customer, pick their speed plan from a dropdown, done.

The words you'll see everywhere

- **Subscriber** — one of your customers. Has a login name and password that their router or device uses to connect.
- **Plan** — a service tier, like "Home 50/10" or "Business 200/50". Sets the speed limit (and other settings) a subscriber receives.
- **Router (NAS)** — any router, access point or firewall that sends login requests to RadiusForge on your customers' behalf. In RADIUS jargon this is a "NAS" (Network Access Server) — nothing to do with a file-storage box. RadiusForge just calls them routers. Every one your customers connect through must be registered.
- **Session** — one continuous connection, from when a subscriber connects to when they disconnect. RadiusForge keeps a history.
- **Voucher** — a one-off code (for a Wi-Fi hotspot) that grants access for a set time or amount of data, then stops working. Great for campsites, hotels and cafés.
- **Organisation** — a self-contained network inside RadiusForge, with its own subscribers, plans, routers and staff. Run several and they stay completely separate. Most people need just one.
- **Staff** — the people who log into RadiusForge itself to manage things (not the same as subscribers). Staff have roles: **Owner** (full control, including who else has access), **Administrator** (full day-to-day control), and **Support** (can see everything, can't change anything).

Your first login: create your organisation

The first time you sign in with the admin account you made during install, RadiusForge shows a **welcome banner**: "*Create your first Organisation to start adding subscribers, plans and routers.*"

1. Sign in with that admin account.
2. Click **Create your first Organisation** in the welcome banner.
3. Give it a name — your ISP or company name, e.g. `My ISP` — and click **Create Organisation**.
4. You land back on the Dashboard as the **Owner** of your new organisation. Subscribers, Plans, Routers and Staff are all ready to use.

Name it for real

The organisation name appears around the console and on hotspot voucher sheets. Use the name you'd be happy for staff — and voucher users — to see.

A sensible first setup, in order

Set things up in this order and each step has what it needs from the one before.

1. Create a plan

Plans → Add plan. A plan is a speed tier. For a MikroTik network, pick **MikroTik** as the router platform and enter the download and upload speeds in plain Mbps (e.g. 50 and 10). Save. That's a complete plan.

2. Register a router

Routers → Add router. Enter:

- the **IP address** the router sends its requests from,
- a **shared secret** (a password-like value you set identically here and on the router), and
- the **platform** (e.g. MikroTik).

This tells RadiusForge to trust that router.

The shared secret must match exactly

The shared secret has to be typed identically here and in the router's own RADIUS settings. If it doesn't match, the router's requests are silently ignored — this is the single most common cause of "it isn't working."

3. Add a subscriber

Subscribers → Add subscriber. Give them a **username** and **password** (what their router/device will use to connect) and choose the **plan** you just made. Save. The subscriber can now authenticate.

4. Test the login

On the **Subscribers** page, use **Check a login** — type the username and password and RadiusForge tells you whether they'd be accepted, and why, without touching a router. A quick way to confirm everything lines up before real traffic arrives.

Your licence and trial

A new install starts on a **30-day trial** — you'll see a banner counting down. Your subscribers are authenticated the whole time regardless. The licence only controls whether staff can make **changes** in the console. When you have a licence file, upload it under **Licence** in the top menu. If a licence ever lapses, the console becomes read-only until you add a valid one — **logins are never interrupted**.

Where to go next

- **User Guide** — every screen explained in full, including **hotspot vouchers**.
- **Deployment Guide** — HTTPS, production hardening and safe upgrades.

Questions? **info@radiusforge.co.uk**