

Hotspot Radius Manager

The RADIUS server and admin portal behind campus and enterprise Wi-Fi — logins, speed and data limits, vouchers and guests, and the records that prove who used which IP address.

Version 1.0 · October 2026

When a complaint arrives with only an IP address and a time, the question is never whether the Wi-Fi was busy — it is *who* had that address. Hotspot Radius Manager logs every user in through your existing routers, gives each one their own speed, device and data limit, and keeps every login and session with the user, IP, MAC and access point. It runs on one Linux server inside your network. **Your users and their records never leave your premises.**

1,50,000

user accounts, tested on one server

6,000

users online at the same time

One command

installs FreeRADIUS, database, HTTPS and portal

15-day trial

full features, created by the installer

How a login works

Less than a second from joining the Wi-Fi to the line in the log.

1

Joins the Wi-Fi

The router shows your branded login page.

2

Router asks RADIUS

Username, password and MAC go to the server.

3

Rules checked

Validity, devices, time, data quota, site.

4

Own speed

Accepted with the user's own speed limit.

5

On the record

User, IP, MAC, access point, time, data.

Getting people online

Every method runs on the same accounts, groups and limits, so a voucher visitor and a directory user get the same rules and the same logging.

Accounts

Created by an admin, the username generator, a bulk upload of up to 1,50,000 rows, or the API. PAP, CHAP and MS-CHAPv2.

LDAP / Active Directory

Users log in with the password they already have. Directory groups map to plans; a scheduled sync disables leavers. Several servers with failover.

Vouchers

Batches of up to 10,000 codes with time, data, validity and device limits, printed as cards with a QR code that logs the visitor in.

OTP and guest approval

A one-time code by SMS or email, or a registration form approved by the person being visited — the login is sent to the visitor.

Click-through

Accept the terms and connect, for a few minutes per session and per day, with the consent recorded against the device.

MAC devices

Printers, smart TVs and IoT log in by their MAC address without a login page, bound to that MAC alone.

Speed, limits and fair use

A group is a plan. Every member gets its limits for themselves — not a share of one connection.

Speed per user

Upload and download with burst, per group or for one user. Changing a group changes the speed of its users who are already online.

Limits

Devices at once, session and idle timeout, online time per day and per month, and a monthly data quota.

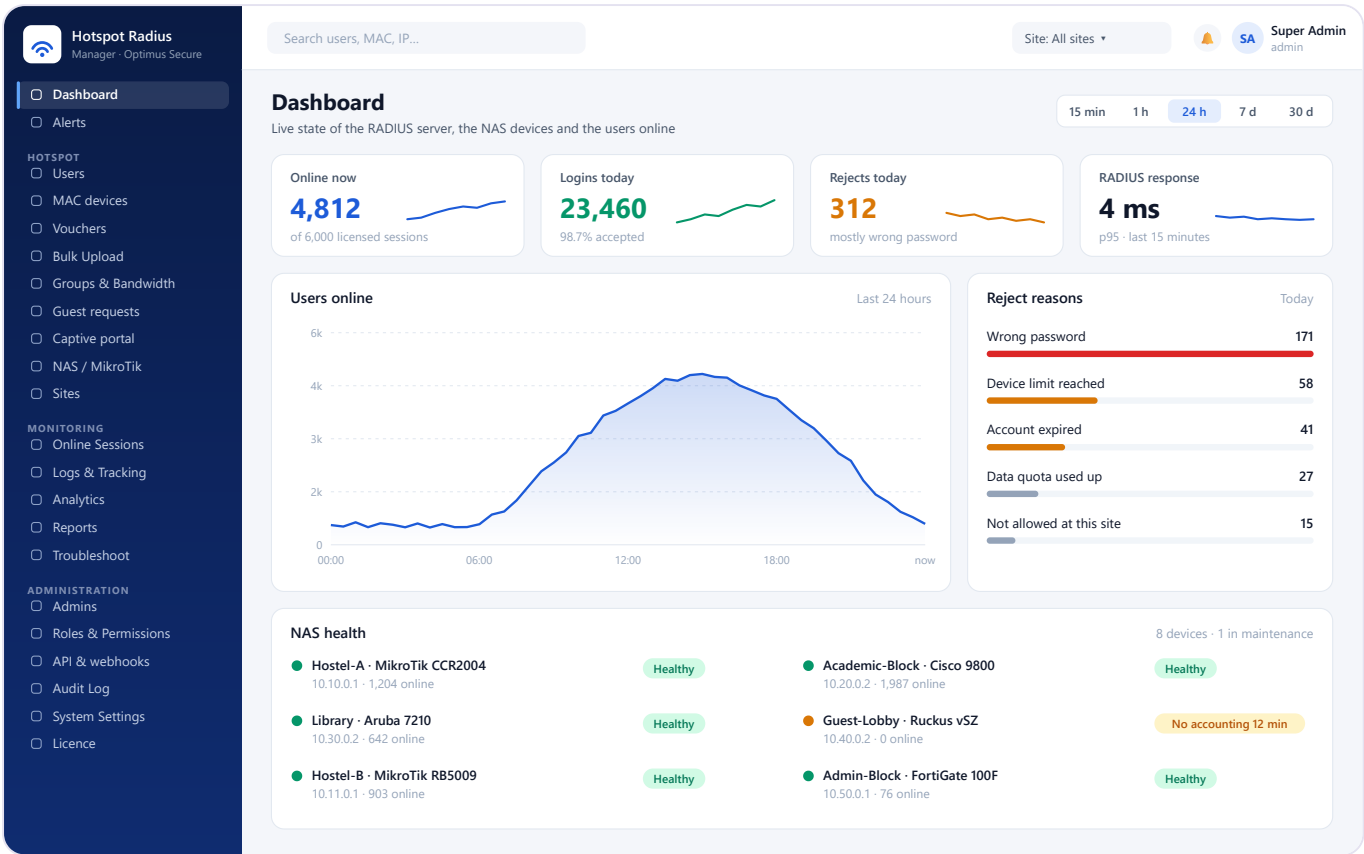
Fair usage

After a set amount of data in a day or a month the speed drops automatically — also during a session that is already running.

Time rules and network

Access only on certain days and hours, a different speed at night, and VLAN, MikroTik address list and IP pool per group.

The admin portal



The dashboard: users online, logins and rejects with their reasons, RADIUS response time and the health of every router. Example data.

Users

A 360° page per user: devices, data used, sessions, login history and every change. Own fields, saved views and bulk actions.

Online sessions

Who is online where, live speed and data. Disconnect one or many — the router confirms it.

Troubleshooter

Type a username or MAC and see why a login fails, with the fix. Test a login and watch a live feed.

The login page

Designed in the portal, put on the router as a ready package.

Designer with live preview

Logo, colours, background, texts and terms, previewed on a phone and a laptop. Several portals, such as students and guests.

Three languages

English, हिन्दी and বাংলা, chosen from the phone's language and switchable by the visitor.

Any mix of login methods

Account, voucher, mobile OTP, guest registration and free Wi-Fi as tabs on one page.

Consent you can show

Every change to the terms is a version; who accepted which version, from which device and when is recorded.

Routers and controllers

Ready configuration for each vendor, with speed limits sent in that vendor's own format.

VENDOR	PRODUCTS	STATUS
MikroTik	RouterOS hotspot (v6 and v7)	Tested in production
Cisco	IOS-XE, Catalyst 9800 WLC	Configuration provided
HPE Aruba	ArubaOS controller / gateway	Configuration provided
Ruckus	SmartZone, Unleashed	Configuration provided
Fortinet	FortiGate captive portal	Configuration provided
Cambium	cnMaestro, cnPilot	Configuration provided
Ubiquiti	UniFi hotspot	Configuration provided
Others	Any device that speaks standard RADIUS	Generic settings

Onboarding check

After adding a router, a live test shows reachability, firewall, unknown client, wrong secret, first login and first accounting.

Health and maintenance

Last login and accounting per router, availability, peak online. Maintenance mode so planned work raises no alarm; secret rotation without dropped logins.

Knowing what happened

Login and session records

Every attempt with its reason, IP, MAC and router; every session with times and data. "Who had this IP at this time" in one search, exported as CSV.

Retention you choose

Keep records as long as your policy or CERT-In requires; older records are archived, not lost.

18 reports

Users, usage, logins per router, peak online, outages, vouchers, SMS, admin activity and sites, as PDF, Excel or CSV — on demand or emailed on a schedule.

Analytics and forecast

Trends of peak online, active users, data and logins, a weekday-by-hour heatmap, and when the licence, capacity or disk will run out.

Alerts

RADIUS or database down, a router offline, a reject spike, CPU, memory or disk, licence, certificate and backup problems.

Handled, not just sent

Email, Slack, Teams, Google Chat or a webhook. Acknowledge with a note, reminders, escalation, and a resolved message.

Administration and security

Each admin sees and changes only what their role and sites allow, and every action is recorded.

Roles	Super Admin, Admin, Site Admin, Operator and Viewer, plus custom roles from 38 separate permissions
Sites	Campuses or buildings own their users, routers, groups and voucher batches; a site admin sees only theirs. Per-site roaming rules
Admin sign-in	Two-step codes with recovery codes, Microsoft Entra ID single sign-on, logout, idle timeout and account expiry for temporary staff
Portal access	The admin portal can be limited to trusted networks; the users' own pages stay reachable
Sensitive actions	The password is asked again before showing passwords, exporting secrets, restoring backups or changing admins
Audit trail	Every admin action with who, when and from where — hash-chained, so a changed or deleted record is detected
Secrets	Router secrets behind their own permission; SMTP, SMS, API and webhook secrets encrypted at rest
HTTPS	Built-in certificate authority or your own certificate (PEM / PFX), with expiry alerts
The server	Root actions only through one checked helper; the firewall allows RADIUS only from known networks

Integrations

REST API Users, devices, groups, routers, sessions and disconnect, logs, vouchers, guests, reports and alerts, described in OpenAPI 3.1. Keys with scopes, IP allowlist, expiry and rate limits.	Webhooks Events for users, sessions, rejects, vouchers, guests and alerts, HMAC-signed and retried with a delivery history.
SIEM and syslog JSON, CEF or LEEF over syslog UDP / TCP / TLS, or Splunk HEC — nothing lost while the SIEM is down. Plain syslog to up to 10 servers.	SMS and email Generic HTTP, MSG91 (DLT) and 2Factor with automatic fallback and a cost log; any SMTP server for alerts, reports and codes.

Availability, backup and performance

Tested with 1,50,000 accounts: a burst of 500 simultaneous logins answered in 10.4 seconds and 6,000 logins in 10.9 seconds, with no login lost and portal pages answering in under 0.1 second.

Nightly backups
With retention, download, upload, optional AES-256 encryption and one-click restore.

Off-site and tested
An encrypted copy to another server after every backup, and scheduled test restores.

Safe upgrades
A backup before every upgrade and a one-command rollback. Optional standby server.

What it needs

Operating system	Ubuntu 22.04 / 24.04 / 26.04 LTS or Debian 12, 64-bit
Hardware	2 GB RAM and 5 GB disk for a small site; more cores, memory and disk for large user counts and long log retention
Components	FreeRADIUS 3.2, MariaDB, Node.js, nginx (HTTPS) and chrony — installed automatically
Browsers	Current Chrome, Edge, Firefox and Safari; the portals work on phones
Internet	For installation and the licence. Servers without internet are licensed with a signed file

PORT	DIRECTION	USED FOR
UDP 1812 / 1813	router → server	RADIUS authentication and accounting
UDP 3799	server → router	Disconnect and speed change (CoA); vendor default port
TCP 443	browsers → server	Admin portal, My Wi-Fi Account and API
TCP 80	Wi-Fi clients → server	Login-page helpers: password change, consent
UDP 123	router → server	Time sync (optional)

Licensing

Sized to the installation

By user accounts, routers, admins and users online at once. Archived users do not count.

A trial that is a full trial

Fifteen days with every feature, created by the installer the first time it runs.

Online or offline

Activate with a key, or with a signed licence file for a server without internet. Licences are bound to the server.

The Wi-Fi never stops

If a licence lapses only changes in the portal stop. Users keep logging in; logs, exports and backups keep working.

White-label option

Your own product name, company name, logo, colour, footer and support contact across the portals, emails, PDF reports, voucher cards and new login pages.

Installing and updating

```
$ curl -fsSL https://licence.opsec.co.in/downloads/hotspot-radius-manager/get.sh | sudo bash
# checks the download against its published SHA-256, sets up FreeRADIUS, MariaDB,
# HTTPS, time sync, the firewall and the portal, and prints the first admin login
```

- **Upgrades the same way.** Running the command again upgrades in place; users, settings and secrets are kept.
- **Reversible.** The database is backed up first and `hotspot-radius-manager rollback` restores the previous version.
- **Without internet.** Copy the bundle to the server and run `sudo ./install.sh`.

Available on request: PPPoE subscribers, VPN users, 802.1X / WPA2-Enterprise, paid hotspot with online payment and GST invoices, and a reseller portal.

Try it

One command on a spare Ubuntu server and a fifteen-day trial starts itself.

opsec.co.in/products/radius-manager.html

Talk to us

Pricing, a walkthrough on your network, or a question about your routers.

info@opsec.co.in · +91 95901 37009