

Captive Portal

Router setup guide

Guest WiFi · MikroTik HotSpot · WinBox / Terminal

GUEST LOGIN PAGE

<https://captive-portal.firozmahmud.dev/login>

CAPTIVE KICK

<https://captive-portal.firozmahmud.dev/connect>

 HTTPS

 MikroTik HotSpot

 Verified POC

TYPE

Implementation guide

AUDIENCE

Network & DevOps

STATUS

Proof of concept

Configure the router so guests reach the login page and receive internet after submit.

 Live web version at </setup-guide> · PDF rebuilt with `make router-pdf`

Firoz Mahmud

Captive Portal · captive-portal.firozmahmud.dev

Contents

Contents

- 1 Before you start. 2
- 2 How it works 2
- 3 Rules for every router. 3
 - 3.1 What the router must send 3
- 4 MikroTik Hotspot configuration 4
 - 4.1 Copy-paste values 4
 - 4.2 Step-by-step 4
 - 4.2.1  1. Enable Hotspot 4
 - 4.2.2  2. External login page 5
 - 4.2.3  3. Walled garden 5
 - 4.2.4  4. Shared HotSpot user 6
 - 4.2.5  5. Test end-to-end 6
- 5 After the guest submits 7
- 6 Presence heartbeat (verified on POC) 7
- 7 Troubleshooting 8
- 8 Security recommendations 9
- 9 Final validation checklist. 9

1 Before you start

This guide configures a **MikroTik RouterOS HotSpot** so guests on your guest WiFi are redirected to an already-deployed captive portal, fill name/age/gender (**Male / Female / Other**), and **submit** (submit = consent; there is no separate checkbox), then receive full internet access. You only configure the router — the portal (already live) handles the login page and guest records.

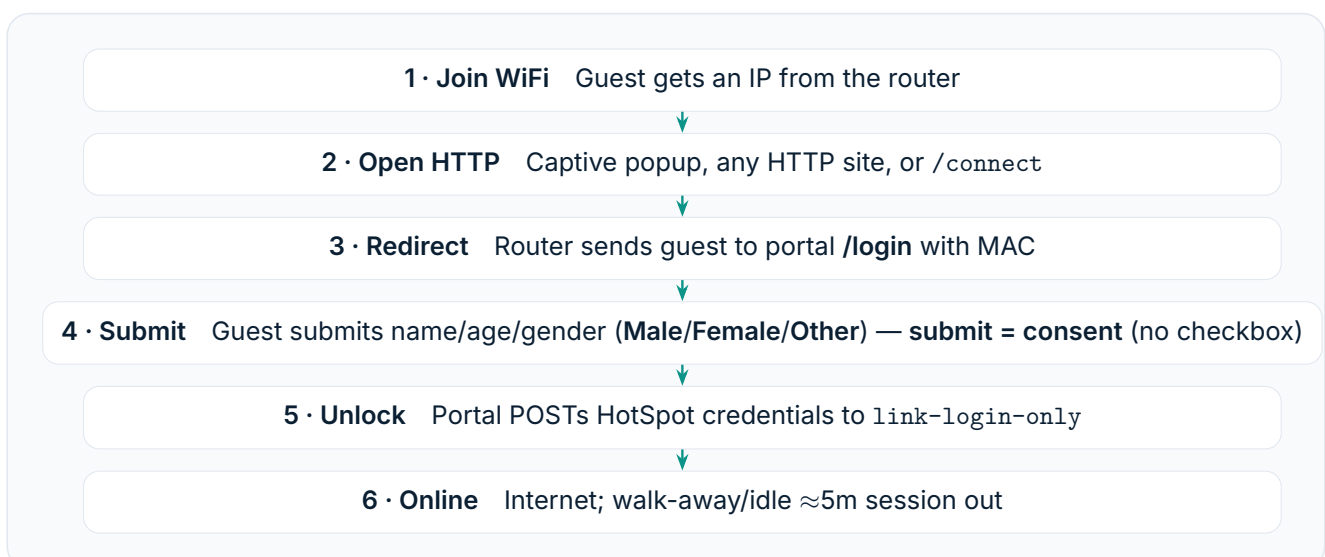
Note

The guest login page is already live at <https://captive-portal.firozmahmud.dev/login>. Open it in a browser first to confirm the form loads before touching the router. Portal home: <https://captive-portal.firozmahmud.dev>.

Before you begin, make sure:

- The guest WiFi interface/bridge already has working DHCP, NAT, and internet access.
- You have WinBox/WebFig/SSH admin access to the router.
- You have a phone or laptop that can join guest WiFi with mobile data off, for testing.
- You have exported a RouterOS backup (`/export file=pre-hotspot-backup`) in case you need to undo a change.

2 How it works



This guide covers **MikroTik HotSpot**. RADIUS stays unchecked in the HotSpot wizard — authentication here is HotSpot local users plus the portal's return-login POST, not an external RADIUS server.

Note

Session timers (verified POC): user profile default idle **5m**, keepalive **2m**, mac-cookie **3d**; HotSpot

profile `hsprof4` must include **http-pap**; portal splash/CSRF and auth TTL default **60 minutes**.

3 Rules for every router

1. **Splash / login.html must pass the guest MAC** — without `mac=` the form cannot unlock internet.
2. **Guests need a router intercept (or captive kick)** — typing bare HTTPS /login skips `$(mac)`. Use the captive popup, any HTTP site, or portal /connect.
3. **Walled garden must allow the portal domain only** — add `captive-portal.firozmahmud.dev`. Do not add the kick host (default `neverssl.com`).
4. **HTTP PAP on the active server profile** — POC: `hotspot1` → `hsprof4` (not only profile default). Missing `http-pap` causes login-page loops.
5. **Saving guests on the portal is not enough** — the router must also receive the unlock signal.

What the router must send

Parameter	MikroTik	Purpose
Device MAC	<code>\$(mac)</code>	Guest identity (required)
Unlock endpoint	<code>\$(link-login-only)</code>	Portal POST target (required)
Router / bridge MAC	<code>static router_mac</code> in <code>login.html</code>	AP identity (no <code>\$(router-mac)</code>)
Original site	<code>\$(link-orig)</code>	Post-login redirect
Guest IP	<code>\$(ip)</code>	Records (optional)
Identity / server	<code>\$(identity), \$(server-name)</code>	Site / HotSpot name

⚠ Warning

If MAC is missing: *Could Not Identify This Device*. On guest WiFi open /connect or `http://neverssl.com` — do not type the portal HTTPS URL expecting a redirect.

These must line up with the portal's own settings: `PORTAL_PUBLIC_URL` is the domain used above and in the walled garden; `MIKROTIK_HOTSPOT_USER` / `MIKROTIK_HOTSPOT_PASSWORD` must match the HotSpot user you create in Section 4.

4 MikroTik Hotspot configuration

Copy-paste values

Splash URL (reference)

preferred: `hotspot/login.html`

URL

```
https://captive-portal.firozmahmud.dev/login?mac=$(mac)&ip=$(ip)&host-ip=$(host-ip)&hostname=$(hostname)&link-login-only=$(link-login-only)&link-orig=$(link-orig)&server-name=$(server-name)&identity=$(identity)&server-address=$(server-address)&interface-name=$(interface-name)
```

Open live login: <https://captive-portal.firozmahmud.dev/login> · kick: <https://captive-portal.firozmahmud.dev/connection>
· host: captive-portal.firozmahmud.dev

Walled garden

RouterOS

```
/ip hotspot walled-garden add dst-host=captive-portal.firozmahmud.dev
```

Do **not** add `neverssl.com`. Portal host: captive-portal.firozmahmud.dev

HotSpot user

password must match the portal

RouterOS

```
/ip hotspot user add name=portal-guest password=<portal-password> profile=default
/ip hotspot user profile set [find default] shared-users=100
```

 Login method: HTTP PAP on active profile (e.g. `hsprof4`)

Step-by-step

1. Enable Hotspot

- **Where:** IP → Hotspot → run the setup wizard, or configure manually
- Select the guest WiFi interface or bridge — never the WAN or management LAN
- Leave RADIUS unchecked — authentication is local HotSpot users plus the portal POST

Verify

`/ip hotspot print` lists a hotspot server bound to the guest interface. Note `profile=` (POC: `hsprof4`).

2. External login page

Set **Login By** to **HTTP PAP** on the **active** server profile (e.g. hsprof4), then replace hotspot/login.html under WinBox **Files** → **hotspot** (path must be hotspot/login.html, not Files root):

HTML

```
<html><head><title>Redirect</title></head><body>
<form name="redirect" action="https://captive-portal.firozmahmud.dev/login" method="get">
  <input type="hidden" name="mac" value="$(mac)">
  <input type="hidden" name="ip" value="$(ip)">
  <input type="hidden" name="host-ip" value="$(host-ip)">
  <input type="hidden" name="hostname" value="$(hostname)">
  <input type="hidden" name="link-login-only" value="$(link-login-only)">
  <input type="hidden" name="link-orig" value="$(link-orig)">
  <input type="hidden" name="server-name" value="$(server-name)">
  <input type="hidden" name="identity" value="$(identity)">
  <input type="hidden" name="server-address" value="$(server-address)">
  <input type="hidden" name="interface-name" value="$(interface-name)">
  <!-- Per-router bridge MAC (no $(router-mac)). POC: e4:8d:8c:36:45:db -->
  <input type="hidden" name="router_mac" value="e4:8d:8c:36:45:db">
  <input type="hidden" name="ssid" value="captive-portal-open-wifi">
</form>
<script>document.redirect.submit();</script>
</body></html>
```

RouterOS substitutes \$(mac), \$(link-login-only), etc. with real values when it serves this page to the guest. Confirm with `/file print` where name "login.html" → hotspot/login.html.

RouterOS

```
/ip hotspot print detail
/ip hotspot profile set hsprof4 login-by=http-pap,http-chap,cookie
/ip hotspot user profile set [find name=default] idle-timeout=5m keepalive-timeout=2m mac-cookie-timeout=3d
```

Warning

Login By must be **HTTP PAP** on the active profile from `/ip hotspot print detail` (e.g. hsprof4), not only profile default.

3. Walled garden

A guest has no internet at all before logging in — the walled garden is the one exception that lets them still reach the portal to see the login page.

RouterOS

```
/ip hotspot walled-garden add dst-host=captive-portal.firozmahmud.dev
```

 Warning

Do **not** add `neverssl.com` (default `CAPTIVE_KICK_URL`) to the walled garden — HotSpot must intercept that HTTP URL.

 Verify

`/ip hotspot walled-garden print` shows the rule. From a guest device that has *not* logged in yet, `captive-portal.firozmahmud.dev` still loads over HTTPS while other sites do not.

 4. Shared HotSpot user

After the guest submits the form, the portal authenticates to *this* HotSpot user on your router — not the guest's own credentials — to open internet for that guest's MAC.

Portal	MikroTik
<code>portal-guest</code> (env <code>MIKROTIK_HOTSPOT_USER</code>)	<code>/ip hotspot user name</code>
<code>MIKROTIK_HOTSPOT_PASSWORD</code>	same password on the router

RouterOS

```
/ip hotspot user add name=portal-guest password=<portal-password> profile=default
/ip hotspot user profile set [find default] shared-users=100
```

 Security

Use a strong, unique password here — it is a shared secret between router and portal, not something a guest ever sees. Never reuse the router's admin password.

 5. Test end-to-end

1. Connect a phone to **guest WiFi** with mobile data **off**.
2. Open any **HTTP** site (e.g. `http://neverssl.com`) — do **not** type the portal HTTPS URL expecting HotSpot to inject `mac=`.
3. If you dismissed the captive popup: open `https://captive-portal.firozmahmud.dev/connect` (kick → intercept → `/login?mac=...`).
4. Confirm the address bar has `mac=`, `link-login-only=`, and `router_mac=`.
5. Fill name, age, gender (**Male / Female / Other**) and submit — **submit = consent** (no checkbox); ordinary browsing should work immediately.

 Warning

HTTPS-only browsing (e.g. `https://google.com`) cannot be redirected by HotSpot. Use HTTP, the captive popup, or `/connect`.

 Verify

On the router: `/ip hotspot active print` lists the guest's MAC as active.

On the portal: the guest appears on `/list` immediately after submit. Connection status starts **Offline** until presence reports that MAC (Section 6). Admin `/list` updates live via SSE.

5 After the guest submits

Submitting the login form is `consent` (hidden `consent=1`; no separate tick). The portal saves the guest record, then auto-POSTs the HotSpot username and password to `link-login-only` (the router's own login endpoint) so the browser — not a server-to-server call — performs the unlock.

 Security

By default the portal only sends the HotSpot password to a **private, loopback, or link-local** IP (the normal case for a router's LAN login URL, e.g. `192.168.190.1`). A non-private `link-login-only` host is refused unless added to `MIKROTIK_UNLOCK_HOSTS` — this stops the HotSpot password from ever reaching an unexpected or spoofed host.

Operator pages: Guests `/list`; API call history `/api-call-history` (counts by date — does not change unlock).

6 Presence heartbeat (verified on POC)

Near-realtime **Online / Offline** on portal `/list`. Does **not** change guest login or unlock.

 Verify

Verified POC (Sep 2026): `script portal-presence; profile default On Login + On Logout (portal-guest); idle-timeout=5m; schedulers portal-presence-startup + portal-presence-5m; walled garden allows captive-portal.firozmahmud.dev`. Steps below are for a new router or reinstall.

 Note

Verified: HotSpot **On Login** and **On Logout** + scheduler `portal-presence-5m + startup`. Profile `idle-timeout=5m` for walk-away → Offline $\approx$ 5m.

1. Set the same secret in portal `.env` / GitHub `MIKROTIK_PRESENCE_SECRET` and the MikroTik script. Compose must pass it into the portal container; redeploy. Empty secret → API 503.
2. **System** → **Scripts** → **New** — name exactly `portal-presence`; check **Don't Require Permissions**; paste `setup/mikrotik/presence-report.rsc` (or `presence-report.local.rsc` with secret filled).
3. POC CONFIG defaults: SSID `captive-portal-open-wifi`, bridge `bridge-hotspot`, server `hotspot1`, URL `https://captive-portal.firozmahmud.dev/mikrotik/presence`. Edit secret if using the placeholder file.

- On the guest HotSpot **user profile**: **On Login + On Logout** = `/system script run portal-presence`.
- Run Script once; check Log (`portal-presence: OK`), Files `portal-presence-last.json`, and `/list Status`.

RouterOS

```
/ip hotspot user profile set [find name=default] \
  on-login="/system script run portal-presence" \
  on-logout="/system script run portal-presence"
```

If guests use another profile, set On Login / On Logout on that profile. Full WebFig steps: [docs/mikrotik/presence-script-](https://docs.mikrotik.com/presence-script-...)

7 Troubleshooting

Problem	Likely cause	Fix
Login page never appears	Walled garden missing	Add captive-portal.firozmahmud.dev to the walled garden
Login page never appears	No valid HTTPS certificate on captive-portal.firozmahmud.dev	Fix TLS on the Nginx side — guests will not bypass a certificate error
Login page loops after submit	http-pap on wrong profile	Fix active profile from <code>/ip hotspot print detail</code> (e.g. <code>hsprof4</code>), not only default
<i>Could Not Identify This Device</i>	Typed HTTPS URL / dismissed popup	Open <code>/connect</code> or <code>http://neverssl.com</code> ; do not walled-garden the kick host
Redirect never fires	HTTPS-only browse / no HTTP PAP	Use HTTP or <code>/connect</code> ; set HTTP PAP on active profile
Form submits, no internet	Wrong HotSpot password	Match <code>MIKROTIK_HOTSPOT_PASSWORD</code> with <code>/ip hotspot user</code> on the router
Form submits, no internet	Missing/malformed <code>link-login-only</code>	Fix <code>login.html</code> / splash redirect
Form submits, no internet	Unlock host not in the allowlist	Add the router's login host to <code>MIKROTIK_UNLOCK_HOSTS</code>
"Unlock not configured"	Missing <code>MIKROTIK_HOTSPOT_*</code>	Set <code>portal .env</code> / GitHub secrets and redeploy
Works in a browser, not on guest WiFi	Router not redirecting	Recheck HotSpot profile, interface, and <code>hotspot/login.html</code> path
Presence 503 / <code>/list</code> stuck Offline	Secret missing or not in compose	Set <code>MIKROTIK_PRESENCE_SECRET</code> ; redeploy; On Login/On Logout on correct profile

8 Security recommendations

POC / development	Before production
Keep the HotSpot password only in <code>.env</code> , never in source control.	Restrict WinBox/WebFig/SSH to a management subnet or VPN; disable unused services (telnet, ftp, www, api) you do not manage with.
Leave <code>MIKROTIK_UNLOCK_HOSTS</code> unset — the default already trusts only private/loopback IPs.	If the router's login URL is not a private IP (e.g. behind a load balancer), set <code>MIKROTIK_UNLOCK_HOSTS</code> explicitly rather than disabling the check.
Change the router's admin password from any default before exposing HotSpot to real guests.	Use a strong unique HotSpot password and router admin password; rotate both if either is suspected compromised. Keep RouterOS updated and back up configuration regularly.
Guest history is kept across portal deploys by default (<code>DEPLOY_RESET_DB=false</code>).	Only set GitHub variable <code>DEPLOY_RESET_DB=true</code> when you intentionally wipe the guest database (e.g. breaking schema change).

To undo this integration: remove the walled-garden rule and HotSpot user (`/ip hotspot walled-garden remove [find dst-host=...], /ip hotspot user remove [find name=...]`), and restore the default `login.html`. Keep a RouterOS export from before you started in case you need a full restore.

9 Final validation checklist

- ☐ <https://captive-portal.firozmahmud.dev/login> loads in a browser
- ☐ Guest WiFi already has working DHCP and internet before HotSpot is enabled
- ☐ HotSpot active profile **Login By** includes HTTP PAP (e.g. `hsprof4`)
- ☐ `hotspot/login.html` includes `$(mac)`, `$(link-login-only)`, and `bridge router_mac`
- ☐ Walled garden allows captive-portal.firozmahmud.dev (kick host *not* listed)
- ☐ HotSpot user password matches `MIKROTIK_HOTSPOT_PASSWORD` on the portal
- ☐ Guest arrives with `mac=` (popup, HTTP site, or `/connect`)
- ☐ After submit: internet works and the guest appears on `/list`
- ☐ (Optional / verified on POC) Presence: `MIKROTIK_PRESENCE_SECRET`; script `portal-presence`; On Login + On Logout on profile default; `idle-timeout=5m`; scheduler `portal-presence-5m`; `/list` Status updates
- ☐ Portal deploy keeps guest history (`DEPLOY_RESET_DB=false` in GitHub Actions variables / `server.env`)
- ☐ Router admin password changed from any default; configuration backup taken