Подключение MikroTik к WiFiVerify — пошаговая инструкция

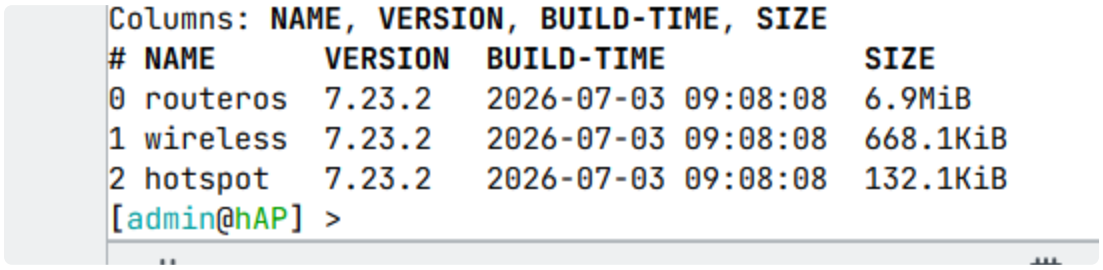
Настройка MikroTik через готовый скрипт из кабинета занимает 20–30 минут. Инструкция проверена 15.11.2026 на hAP lite (RB941-2nD, RouterOS 7.23.2) и 06.11.2026 на hAP ac lite (RouterOS 7.25.1).

Что понадобится

- **Роутер MikroTik с RouterOS 7.** Версия видна внизу окна Winbox или по команде `/system resource print`.
- **Компьютер с программой WinBox** — бесплатная программа MikroTik для настройки роутеров, все шаги инструкции делаются в ней. Скачайте с официальной страницы mikrotik.com/download/winbox: для Windows — архив ZIP, распакуйте и запустите `WinBox.exe`, устанавливать не нужно; есть версии для macOS и Linux. Нужна версия 4 (номер в заголовке окна, например WinBox 4.5). Роутер находится на вкладке **Neighbors** — подключайтесь по MAC-адресу, логин `admin`.
- **Аккаунт в кабинете WiFiVerify** (admin.wifiverify.ru) и добавленная точка с типом роутера MikroTik.
- **Два телефона** для проверки: так видно, что гости входят одновременно.
- **20–30 минут.** Если роутер уже раздаёт Wi-Fi гостям, выберите время без посетителей: во время настройки интернет на гостевой сети может пропадать.

Проверьте пакеты RouterOS. Winbox → New Terminal:

```
/system package print
```



В списке должны быть `wireless` (или `wifi-qcom` у моделей серии ax) и `hotspot`. На hAP lite, hAP ac lite и других моделях с процессором smips или mipsbe эти пакеты ставятся **отдельно**. Без `wireless` не будет Wi-Fi, без `hotspot` в меню IP не будет раздела Hotspot.

Как поставить недостающий пакет:

1. Посмотрите версию RouterOS и тип процессора внизу окна Winbox, например `smips / hAP lite / 7.23.2`.
2. На компьютере откройте mikrotik.com → Software → Download и скачайте для своей версии архив **Extra packages** под свой процессор.
3. Распакуйте архив и возьмите нужные файлы, например `wireless-7.23.2-smips.npk` и `hotspot-7.23.2-smips.npk`. Версия пакета должна **точно** совпадать с версией RouterOS.
4. Winbox → **Files** → перетащите файлы в корень списка (не в папку).
5. В терминале выполните `/system reboot`. При загрузке пакеты установятся сами, и `/system package print` покажет их в списке.

Кнопка System → Packages → Check For Updates делает то же самое, но у части провайдеров сервер обновлений MikroTik недоступен (ошибка `connection timed out`). Тогда ставьте пакеты способом выше. Сброс к заводским настройкам пакеты не удаляет.

Если MikroTik уже настроен под другие задачи (VLAN, несколько сетей, сложный файрвол), начните со **Способа вручную** в конце инструкции или напишите в поддержку.

У вас точка доступа cAP или wAP? Их заводские настройки другие, эта инструкция не подойдёт — идите по отдельной: `MikroTik cAP / wAP — отдельная точка WiFiVerify`.

Шаг 1. Подключите и сбросьте роутер

Кабель от вашего основного роутера или провайдера вставляется **только в порт Internet (ether1)**. Компьютер для настройки — в любой порт LAN или по Wi-Fi MikroTik.

1. Кабель интернета → порт **Internet** (в Winbox он называется `ether1`).
   - Порты **LAN 1, 2, 3…** в Winbox называются `ether2`, `ether3`, `ether4`… Если вставить кабель интернета в LAN, MikroTik начнёт раздавать адреса в вашу основную сеть и мешать ей.
2. Компьютер → кабелем в **LAN 1** или по Wi-Fi к сети `MikroTik-XXXXXX`.
3. Откройте Winbox → вкладка **Neighbors** → **Refresh**. Роутер появится в списке.
4. Нажмите на строку с адресом `192.168.88.1` (столбец Board's Port — `bridge`), логин `admin`, пароль: пустой (старые модели) или напечатанный на наклейке (новые) → **Connect**.

Сбросьте роутер к заводским настройкам, если его уже настраивали и непонятно, что в нём сейчас: System → Reset Configuration, все галочки сняты («No Default Configuration» **не ставить**) → Reset Configuration. Через 1–2 минуты снова войдите через Neighbors.

Сброс **не стирает файлы**. В Files могут остаться старый `wifiverify.rsc`, `hotspot/login.html` от прошлой настройки и `auto-before-reset.backup` — копия прежней конфигурации с секретными ключами. В шаге 7 мы их удалим.

Пароль. Новый Winbox просит сменить пароль не окном, а строкой в терминале: `Change your password (Ctrl-C to skip)`. Задать пароль обязательно — не позже шага 4, когда сеть станет открытой. Сохраните его в менеджер паролей.

Проверка. Winbox → **New Terminal**:

```
/ip dhcp-client print
```

В строке `ether1` должен быть статус `bound` и адрес. Значит, MikroTik получил интернет.

Safe Mode (кнопка вверху окна Winbox, в терминале — Ctrl+X) откатывает изменения, если связь с роутером оборвётся. Включайте его, когда меняете сетевые настройки вручную. Но учтите:

- **мастер Hotspot Setup с включённым Safe Mode ничего не создаёт** — перед шагом 3 его нужно выключить;
- выключите его перед перезагрузкой и в конце настройки, иначе часть изменений откатится. Если роутер перезагрузился в Safe Mode, повторите шаг 5 (запуск скрипта): он вернёт наши настройки.

Шаг 2. Скачайте файлы в кабинете

Скачайте файлы **сейчас, до создания хотспота**: после шага 3 компьютер, подключённый к MikroTik, тоже окажется за страницей входа и потеряет интернет. В кабинете уже собраны два файла с данными именно вашей точки: адрес сервера, идентификатор точки (NAS ID) и её секретный ключ.

1. Войдите в кабинет: admin.wifiverify.ru.
2. Раздел **Точки (роутеры)**. Если точки ещё нет, нажмите «Добавить» и выберите тип **MikroTik**.
3. У нужной точки нажмите **«Конфиг»**.
4. В блоке **«Способ 1. Скриптом»** нажмите обе кнопки:
    - **Скачать wifiverify.rsc** — скрипт настройки;

- **Скачать login.html** — страница, которая перенаправляет гостя на вход.

5. Перед запуском можно раскрыть **«Показать текст скрипта»** и прочитать его целиком.

Оба файла содержат секретный ключ вашей точки. Не пересылайте их посторонним и не публикуйте скриншоты текста скрипта.

Шаг 3. Создайте хотспот

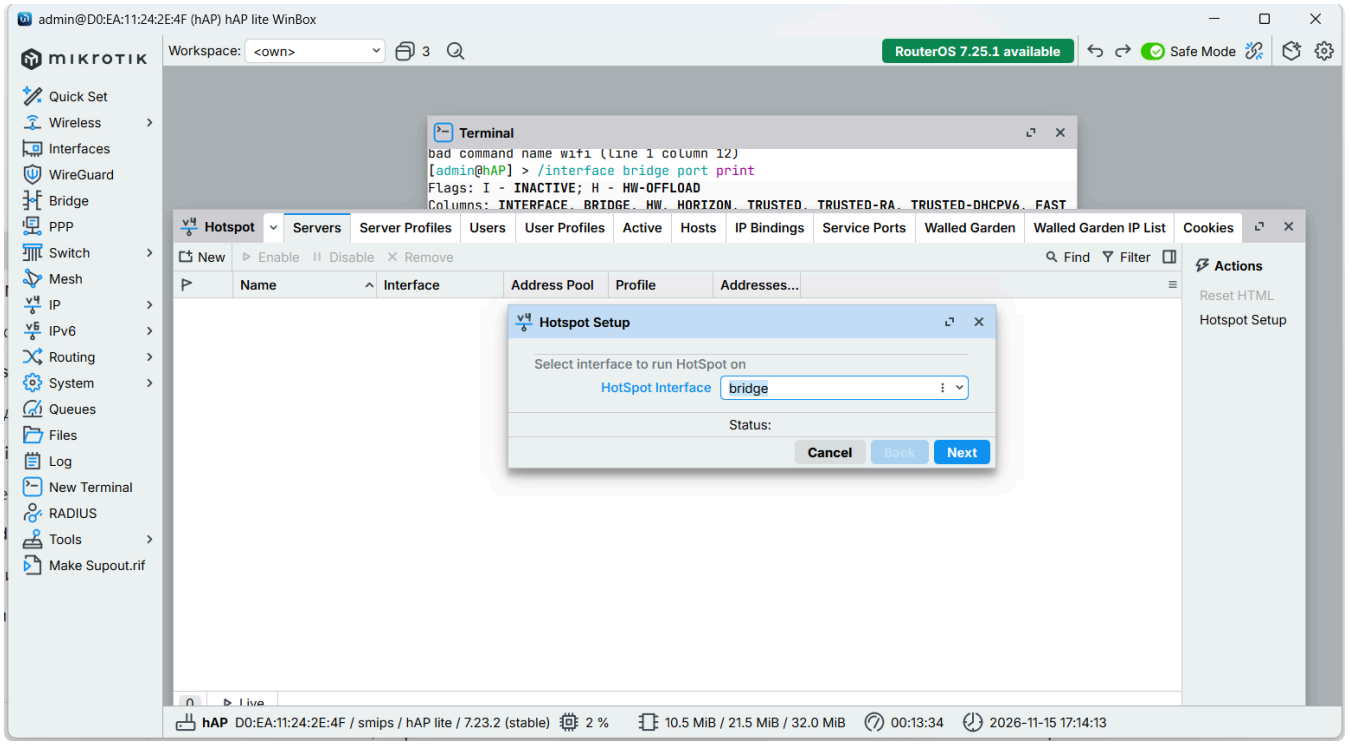
Хотспот — встроенная в MikroTik функция, которая не пускает гостя в интернет, пока он не пройдёт вход. Создаётся мастером за пару минут.

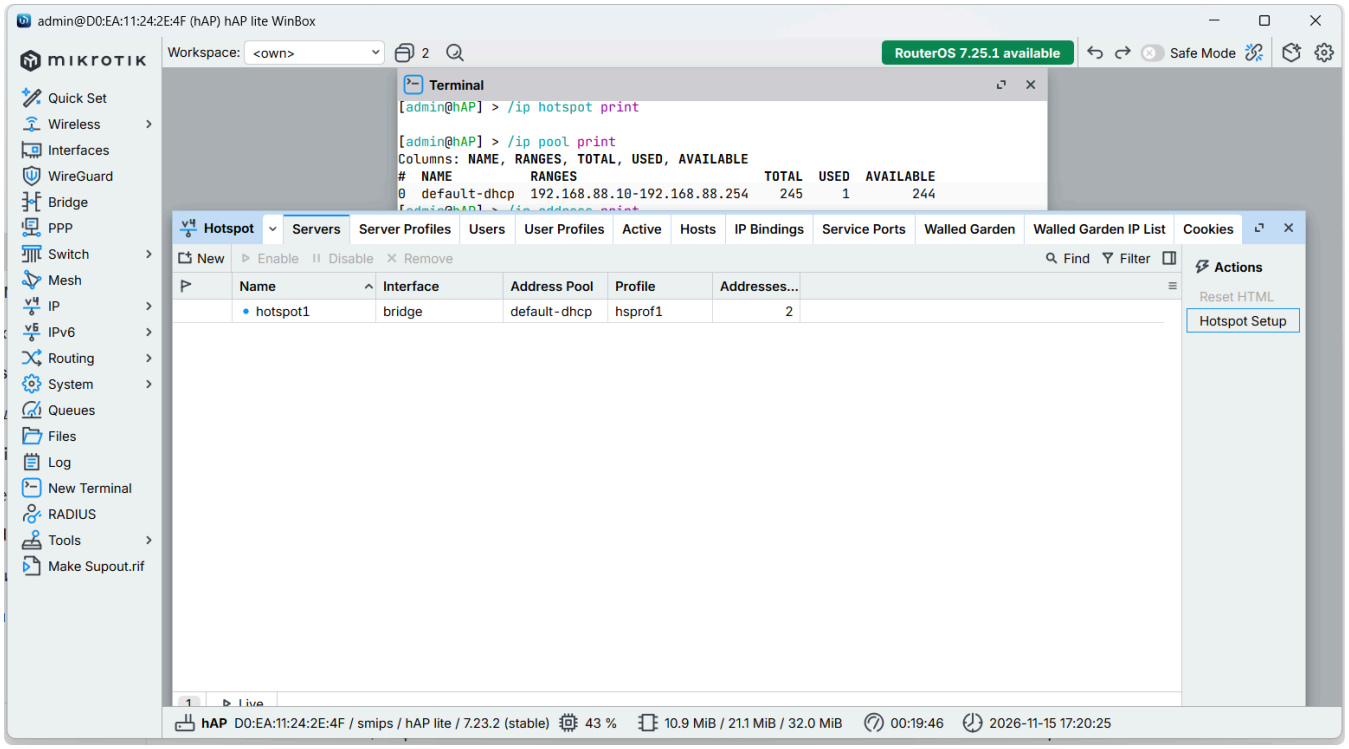
Сначала выключите Safe Mode. С включённым Safe Mode мастер доходит до конца, но ничего не создаёт, а в строке Status пишет `safe mode already held by somebody`.

Проверьте, куда подключён MikroTik. Если на шаге Local Address мастер предлагает адрес **вашей основной сети** (например `192.168.0.96/24` — тот же диапазон, что у основного роутера), нажмите **Cancel** и настройте гостевую сеть по разделу «Если MikroTik стоит за другим роутером» ниже.

1. Winbox → **IP → Hotspot** → справа в панели **Actions** кнопка **Hotspot Setup**.
2. Пройдите мастер, следя за строкой Status внизу окна:

Шаг мастера	Что указать
HotSpot Interface	**`bridge`** — выберите из списка. По умолчанию мастер подставляет `wlan1`, с ним хотспот не заработает
Local Address of Network	`192.168.88.1/24`, галочка Masquerade Network стоит. Если тут `10.5.50.1/24`, вы выбрали не `bridge` — нажмите Back
Address Pool of Network	по умолчанию (`192.168.88.10-192.168.88.254`)
Select Certificate	`none`
IP Address of SMTP Server	`0.0.0.0`
DNS Servers	по умолчанию
DNS Name	**оставить пустым**
Name of Local HotSpot User	оставить как есть, ниже мы его удалим





3. Проверьте: в IP → Hotspot → Servers должен появиться `hotspot1` на `bridge` с профилем `hsprof1`.
4. **Удалите локального пользователя хотспота**, которого создал мастер. Иначе гость, знающий его логин, сможет войти без проверки номера. В New Terminal:

```
/ip hotspot user remove [find where name!="default-trial"]
/ip hotspot user print
```

В списке должна остаться только служебная запись `default-trial` со звёздочкой: её удалить нельзя, и она никого не пускает. Команда `remove [find]` без условия не подходит: она спотыкается об эту запись и не удаляет остальных.

Интернет на компьютере пропал — это нормально. Хотспот закрывает весь `bridge`: все порты LAN и Wi-Fi MikroTik теперь гостевые. Если к этому роутеру подключены касса или компьютеры сотрудников, они тоже окажутся за страницей входа — подключите их к основному роутеру. Winbox по MAC-адресу продолжает работать.

Если интернет на компьютере нужен до конца настройки, пропустите его временно. MAC-адрес берите из списка на роутере, а не из Windows: у ноутбука несколько адаптеров, и легко ошибиться.

```
/ip hotspot host print
/ip hotspot ip-binding add mac-address=XX:XX:XX:XX:XX:XX type=bypassed
comment="setup PC - remove"
```

Вместо `XX:XX:XX:XX:XX:XX` подставьте MAC компьютера из первой команды (строка с его IP-адресом). В шаге 7 этот обход обязательно удалим.

Если мастер дошёл до конца, а хотспот не появился (в IP → Hotspot → Servers пусто), создайте его командами. Для заводской конфигурации с сетью `192.168.88.1/24` на `bridge`:

```
/ip pool print
/ip hotspot profile add name=hsprof1 hotspot-address=192.168.88.1 dns-name=""
login-by=http-pap use-radius=yes
/ip hotspot add name=hotspot1 interface=bridge address-pool=default-dhcp
profile=hsprof1 disabled=no
/ip hotspot reset-html hotspot1
/ip hotspot print
```

В `address-pool` укажите имя пула из первой команды (в заводской конфигурации — `default-dhcp`). На вопрос `reset-html` ответьте `y`. В выводе последней команды должен быть `hotspot1` на `bridge` без флагов `X` и `I`.

Хотспот с флагом `I` и надписью `inactivated, not allowed by device-mode`. На RouterOS 7.17 и новее заводской режим устройства может запрещать хотспот. Выполните `/system device-mode update hotspot=yes` и **в течение 5 минут выдерните питание роутера** на 10 секунд (кнопку reset не зажимать — сбросится конфиг). После включения `/system device-mode print` покажет `hotspot: yes`, а флаг `I` у хотспота пропадёт. Удалённо это не сделать: MikroTik требует физического подтверждения.

Шаг 4. Откройте гостевую сеть

После сброса Wi-Fi MikroTik закрыт паролем (WPA2) и называется `MikroTik-XXXXXX`. Гостевую сеть обычно делают открытой: гостя проверяет страница входа, а пароль только мешает. Если вы хотите оставить пароль, этот шаг можно пропустить: пароль можно посмотреть командой `/interface wireless security-profiles export show-sensitive`.

1. **Сначала задайте пароль роутера**, если не сделали это в шаге 1: System → Users → admin → Password. В открытой сети любой человек рядом может подключиться к роутеру через Winbox, и без пароля он сможет его перенастроить. После смены пароля Winbox отключится — войдите с новым паролем.
2. Откройте сеть и дайте ей понятное имя. В New Terminal:

```
/interface wireless security-profiles set [find default=yes] mode=none
/interface wireless set [find default-name=wlan1] ssid=Guest hide-ssid=no
```

Имя `Guest` можно заменить на своё, например `Hotel_Guest`. У двухдиапазонных моделей повторите вторую команду для `wlan2` (например `ssid=Guest-5G`). Сеть не должна быть скрытой — иначе гости её не увидят. Телефоны, подключённые к старой сети, отключатся: подключите их к новой.

Если MikroTik стоит за другим роутером

Так бывает, когда MikroTik ставят внутри уже работающей сети заведения: кабель от основного роутера воткнут не в ether1 или ether1 входит в общий бридж, и MikroTik получает адрес вашей сети. Хотспот на таком бридже ставить нельзя: он перехватит весь трафик и поднимет второй DHCP-сервер в вашей сети.

Нужен отдельный **гостевой бридж** со своей сетью, в который входит только Wi-Fi для гостей. Команды ниже — для Wi-Fi на пакете `wireless` (`wlan1`, `wlan2`); они переводят **весь** Wi-Fi роутера в гостевую сеть и делают её открытой. Перед ними задайте пароль роутера (шаг 4, пункт 1). Если у вас `/interface wifi` (модели серии ax) или Wi-Fi роутера нужен и сотрудникам, напишите в поддержку: настроим под ваш случай.

```
/interface bridge add name=bridge_guest comment="WiFiVerify guest"
/interface bridge port remove [find where interface~"wlan"]
:foreach i in=[/interface wireless find] do={/interface bridge port add
bridge=bridge_guest interface=$i}
/interface wireless security-profiles set [find default=yes] mode=none
/interface wireless set [find default-name=wlan1] mode=ap-bridge ssid=Guest
hide-ssid=no disabled=no
/interface wireless set [find default-name=wlan2] mode=ap-bridge ssid=Guest-
5G hide-ssid=no disabled=no
/ip address add address=10.0.1.1/24 interface=bridge_guest
comment="WiFiVerify guest"
/ip pool add name=pool_guest ranges=10.0.1.2-10.0.1.254
/ip dhcp-server add name=dhcp_guest interface=bridge_guest address-
pool=pool_guest lease-time=1h disabled=no
/ip dhcp-server network add address=10.0.1.0/24 gateway=10.0.1.1 dns-
server=10.0.1.1
/ip dns set servers=77.88.8.8,8.8.8.8 allow-remote-requests=yes
/ip hotspot profile add name=hsprof_guest hotspot-address=10.0.1.1 dns-
name="" login-by=http-pap use-radius=yes
/ip hotspot add name=hotspot1 interface=bridge_guest address-pool=pool_guest
profile=hsprof_guest disabled=no
/ip hotspot reset-html hotspot1
/ip firewall nat add chain=srcnat src-address=10.0.1.0/24 action=masquerade
comment="WiFiVerify guest"
```

Имя сети `Guest` можно заменить на своё. Если ваша основная сеть сама использует адреса `10.0.1.x`, возьмите другой диапазон, например `10.0.7.x`.

Проверьте, что у роутера **один** выход в интернет:

```
/ip route print where dst-address=0.0.0.0/0
```

Должна быть одна активная строка (флаг `A`). Если строк две, например вы прописали адрес вручную, а DHCP-клиент остался, удалите лишнее: при ручном адресе — `/ip dhcp-client remove [find]`. Иначе часть пакетов теряется и вход гостей обрывается. Адрес, прописанный вручную, исключите из раздачи DHCP на основном роутере.

Дальше — шаги 5–7 как обычно: скрипт сам найдёт хотспот на `bridge_guest`. Папка для login.html будет та, которую назовёт скрипт.

Шаг 5. Запустите скрипт

1. Winbox → **Files** (меню слева).

2. Если в корне уже лежит `wifiverify.rsc` от прошлой настройки, удалите его (выделить → Remove).
3. Перетащите мышью в это окно файлы **wifiverify.rsc** и **login.html** из папки «Загрузки». У них должна быть сегодняшняя дата.
4. Winbox → **New Terminal** и выполните одну команду:

```
/import file-name=wifiverify.rsc
```

Вывод выглядит примерно так:

```
[admin@Hotel1] > /import file-name=wifiverify.rsc
WiFiVerify: start
WiFiVerify: profile hsprof1, put login.html into folder: hotspot
WiFiVerify: hotspot user profiles: shared-users=unlimited
WiFiVerify: DNS OK
WiFiVerify: check that the guest Wi-Fi network is not hidden
WiFiVerify: now put login.html into the folder shown above (replace the old
one)
WiFiVerify: job wifiverify-dns installed (hourly: RADIUS and walled garden
follow server DNS names)
WiFiVerify: done
Script file loaded and executed successfully
```

Имя роутера в приглашении сменится на NAS ID вашей точки. **Запомните папку** из строки со словами `put login.html` — она стоит в самом конце, после `into folder:` (в примере `hotspot`, на некоторых моделях `flash/hotspot`). `hsprof1` — название профиля, для следующего шага оно не нужно. Если хотспотов несколько, строк будет несколько.

Если вместо этого появилось `WiFiVerify: hotspot server not found`, хотспот не создан: вернитесь к шагу 3 и запустите команду ещё раз. Повторный запуск безопасен.

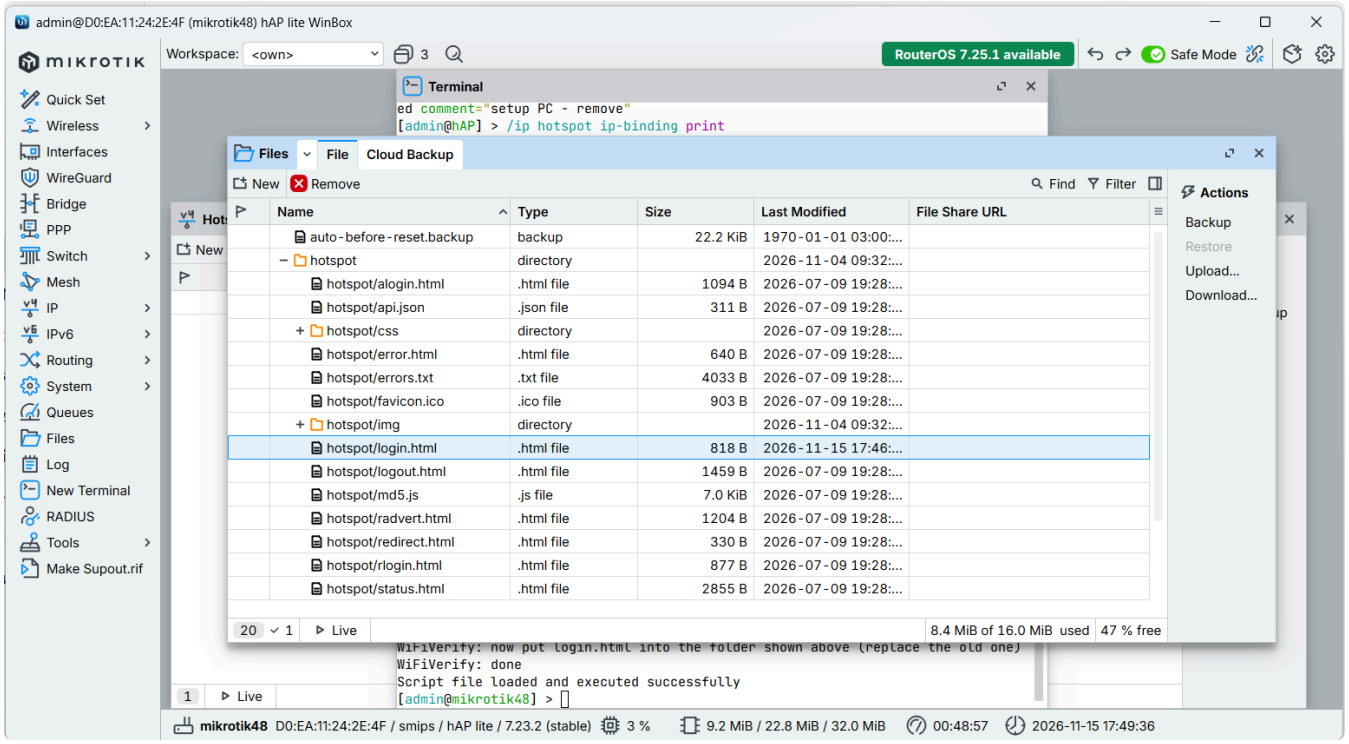
Если в выводе есть строки `WiFiVerify: WARNING …`, скрипт нашёл проблему: нет Wi-Fi (см. «Что понадобится»), хотспот стоит на бридже с адресом вашей основной сети (см. «Если MikroTik стоит за другим роутером») или у роутера два маршрута в интернет. Исправьте и запустите команду ещё раз. Строка `WARNING - removed … walled garden rule(s)` значит, что скрипт удалил опасное правило: ничего делать не нужно.

Строки `WiFiVerify: WARNING hotspot is blocked by device-mode` означают, что хотспот запрещён режимом устройства — см. конец шага 3 (команда и отключение питания). Повторять скрипт после этого не нужно.

Шаг 6. Положите login.html в папку хотспота

Файл `login.html` должен лежать в папке, которую назвал скрипт, и заменить стандартную страницу MikroTik. Winbox не заменяет файл при перетаскивании (пишет, что файл уже есть), поэтому старый сначала нужно удалить.

1. Winbox → **Files**. Раскройте папку из шага 5 (обычно `hotspot`) плюсиком или двойным щелчком.
2. Выделите в ней `login.html` → **Remove**.
3. Перетащите скачанный **login.html** с компьютера в эту папку.
4. Убедитесь, что у `hotspot/login.html` сегодняшняя дата и время (размер около 820 B).
5. Удалите из **корня** Files оба загруженных файла: они больше не нужны, а в `wifiverify.rsc` секретный ключ точки.




```
/file remove wifiverify.rsc
/file remove login.html
/file print where name~"login.html"
```

В выводе последней команды должен быть `hotspot/login.html` с сегодняшней датой (остальные строки — служебные `alogin.html`, `rlogin.html` и папка `xml`, их не трогаем).

Шаг 7. Проверьте вход и уберите лишнее

Проверять нужно **с телефона через Wi-Fi MikroTik**: на компьютере файл login.html напрямую не работает.

1. Сбросьте текущие сессии хотспота, чтобы проверка шла с чистого листа (подключённые гости войдут заново). В New Terminal:

```
/ip hotspot active remove [find]
/ip hotspot cookie remove [find]
```

2. На телефоне выключите мобильный интернет и подключитесь к гостевой сети. Страница входа обычно открывается сама; если нет, откройте в браузере **http://neverssl.com** (именно http, без s).
3. Откроется страница входа WiFiVerify. Введите номер и пройдите звонок.
4. После подтверждения номера открывается интернет, а если в кабинете задан «Переход после подключения», — сайт заведения. На Android окно входа закрывается само, как только появился интернет.
5. **Пока первый телефон в сети, войдите со второго.** Оба должны получить интернет одновременно.

Проверка на роутере:

```
/ip hotspot active print
/radius monitor 0 once
```

- В `/ip hotspot active print` — оба телефона (пользователь `guest`, флаг `R`), в столбце `SESSION-TIME-LEFT` — время сессии из кабинета.
- В `/radius monitor` — `accepts` больше нуля, `timeouts` и `bad-replies` равны нулю.

Уборка. Удалите временный обход для компьютера (если делали его в шаге 3) и копию старой конфигурации, которую роутер сделал при сбросе:

```
/ip hotspot ip-binding remove [find where comment="setup PC - remove"]
/file remove [find where name~"before-reset"]
/ip hotspot ip-binding print
```

В `ip-binding` не должно остаться записей с типом `bypassed`: такое устройство ходит в интернет без входа. Выключите Safe Mode, если он включён.

Готово: точка работает. В кабинете в разделе «Отчёты» появятся ваши сессии.

Что делает скрипт и чего не делает

Скрипт `wifiverify.rsc` — обычный текстовый файл с командами RouterOS, которые вы иначе ввели бы руками. Его можно открыть Блокнотом и прочитать до запуска.

Что меняет	Зачем
Имя роутера (System Identity) = NAS ID точки	По имени сервер узнаёт, какая это точка
Добавляет RADIUS-сервер WiFiVerify (и резервный, если он на другом адресе)	Через него роутер спрашивает сервер, можно ли пустить гостя
Разрешает гостям до входа открывать портал WiFiVerify (Walled Garden)	Иначе гость не увидит страницу входа
В профиле хотспота включает вход через RADIUS	Чтобы доступ давал сервер WiFiVerify, а не локальные пользователи
Снимает ограничение «один логин — одно устройство» (`shared-users=unlimited`)	Иначе в интернет попадает только один гость одновременно
Проверяет DNS, Wi-Fi, маршруты и пишет предупреждения `WARNING`	Чтобы частые ошибки было видно сразу
Удаляет правила Walled Garden без адреса и порта	Такое правило пускает гостей в интернет без входа
Ставит задание `wifiverify-dns` (при включении и раз в час)	Сверяет адрес сервера WiFiVerify по его имени и сам обновляет его в RADIUS и Walled Garden, если сервер переедет. Если имя не находится, ничего не меняет

Чего скрипт не делает:

- ничего не скачивает из интернета и не ставит пакетов;
- не трогает пароли, пользователей роутера, Wi-Fi, подключение к интернету и файрвол;
- не создаёт удалённого доступа к роутеру: у WiFiVerify нет возможности зайти в ваш MikroTik. Задание `wifiverify-dns` только спрашивает DNS адрес нашего сервера и правит наши же записи.

Все записи скрипт помечает комментарием `WiFiVerify` и при повторном запуске заменяет только их. Поэтому его можно безопасно запустить ещё раз — например, чтобы получить новую версию из кабинета. Задание можно увидеть в System → Scheduler и System → Scripts под именем `wifiverify-dns`, а его сообщения — в Log (строки `WiFiVerify:`).

Второй роутер для расширения зоны Wi-Fi

Если одного MikroTik не хватает на всё заведение, есть два варианта.

- **Точка доступа (рекомендуем).** Второй роутер только раздаёт гостевой Wi-Fi первого, без своего хотспота. В кабинете ничего добавлять не нужно, вторая подписка не нужна, гость проходит вход один раз. Подключается кабелем в порт гостевой сети первого роутера. Попросите в поддержке инструкцию «Второй MikroTik для гостевой сети» и скрипты к ней.
- **Отдельная точка.** Второй роутер со своим хотспотом, добавленный в кабинете как ещё одна точка со своим NAS ID. Подходит, если у второго роутера свой интернет, например в другом здании. Это **отдельная подписка**, и гостю при переходе между роутерами придётся входить заново. Настраивается по этой инструкции целиком, а если стоит внутри вашей сети — по разделу «Если MikroTik стоит за другим роутером».

Не подключайте второй роутер в режиме точки доступа в обычный порт сети заведения: гости получат вашу основную сеть в обход проверки номера.

Если что-то не так

Что видно	Причина	Что сделать
В меню IP нет раздела Hotspot	Не установлен пакет `hotspot`	«Что понадобится»: поставить пакет из Extra packages
Хотспот с флагом I: inactivated, not allowed by device-mode	RouterOS 7.17+: заводской режим устройства запрещает хотспот	/system device-mode update hotspot=yes, затем в течение 5 минут отключить питание (конец шага 3)

Что видно	Причина	Что сделать
Нет ни одной Wi-Fi сети; `/interface wireless print` отвечает `bad command`	Не установлен пакет `wireless`	«Что понадобится»: поставить пакет
Check For Updates: `connection timed out`	Сервер обновлений MikroTik недоступен у вашего провайдера	Скачать пакет на компьютере и загрузить в Files
Основной роутер «забит» адресами от MikroTik	Кабель интернета не в ether1 или ether1 входит в bridge	Кабель в Internet/ether1; если не помогло — сброс (шаг 1)
Winbox не подключается по MAC: `syn timeout`	Компьютер подключён со стороны интернета или выбрана не та строка в Neighbors	Кабелем в LAN или по Wi-Fi MikroTik; попробовать другую строку роутера или его IP-адрес
`username or password wrong`	Пароль задавали раньше и он неизвестен	Сброс кнопкой Reset: зажать при включении, отпустить, когда индикатор замигает (~5 с)
Мастер Hotspot Setup прошёл, а хотспота нет; в Status `safe mode already held by somebody`	Включён Safe Mode	Выключить Safe Mode и пройти мастер снова или создать хотспот командами (шаг 3)
Мастер предлагает адрес `10.5.50.1/24`	В первом окне остался `wlan1` вместо `bridge`	Back → выбрать `bridge`
Мастер предлагает адрес вашей основной сети (192.168.0.x и т.п.)	MikroTik стоит внутри сети заведения	Cancel; раздел «Если MikroTik стоит за другим роутером»
После создания хотспота на компьютере нет интернета, открывается страница MikroTik	Все порты LAN теперь гостевые	Нормально; временный обход — шаг 3
`/import` остановился с ошибкой на строке	Старая версия RouterOS или нестандартная конфигурация	Скриншот терминала — в поддержку

Что видно	Причина	Что сделать
Winbox пишет «файл существует» при перетаскивании login.html	В папке уже есть старый файл	Удалить старый, затем перетащить (шаг 6)
Гость сразу получает интернет без страницы входа	Хотспот не на той сети, устройство в `ip-binding` как `bypassed` или пустое правило Walled Garden	Проверить `/ip hotspot print` и `/ip hotspot ip-binding print`; запустить скрипт ещё раз — он удалит пустое правило
Страница входа не открывается, белый экран	login.html не в той папке	Шаг 6: положить в папку, которую назвал скрипт
Первый гость вошёл, а второй после звонка бесконечно видит «Подключаем к интернету»; в Log `no more sessions are allowed for user`	Ограничение «один логин — одно устройство»	`/ip hotspot user profile set [find] shared-users=unlimited` или запустить свежий скрипт из кабинета
Номер подтверждён, а «Подключаем к интернету» крутится у всех	Роутер не получает ответ RADIUS или NAS ID не совпадает	`/radius monitor 0 once`: если растут `timeouts` — `/radius print detail`; при `Network unreachable` — `/radius disable 0` и `/radius enable 0`; один маршрут 0.0.0.0/0; имя роутера = NAS ID
Гость был в сети, сессия закончилась, сайты не открываются и страницы входа нет	Сайты работают по HTTPS, роутер не может подменить их страницей входа	Переподключиться к Wi-Fi или открыть http://neverssl.com
Роутер перезагрузился или оборвалась связь в Safe Mode, часть настроек пропала	Safe Mode откатил изменения	Запустить скрипт ещё раз (шаг 5) и проверить шаг 3

Поддержка: info@wifiverify.ru, +7 995 986-04-22. Пришлите скриншот терминала после `/import` и NAS ID точки. Сам файл wifiverify.rsc пересылать не нужно.

Способ вручную, без скрипта

Если не хотите запускать скрипт, те же настройки вводятся руками. Шаги 1–4 (подключение, файлы, хотспот, гостевая сеть) остаются такими же. Все команды с данными вашей точки — в кабинете, «Конфиг» → **«Способ 2. Вручную»**:

1. **Имя роутера** = NAS ID точки.
2. **RADIUS:** IP → RADIUS → **+**. Service `hotspot`, Address — IP-адрес из кабинета (MikroTik не принимает имя сервера), Secret — из кабинета, Timeout `3s`, Comment `WiFiVerify 1`. Секрет лучше вставлять в это окно, а не в терминал: при вставке в терминал длинные строки иногда портятся.
3. **Хотспот:** вход только `HTTP PAP` через RADIUS, DNS Name пусто, `shared-users=unlimited`, локальные пользователи удалены — три команды из кабинета.
4. **Walled Garden:** две записи на IP портала (tcp 443 и 80), команды в кабинете уже с нужным адресом. Правил без адреса и порта быть не должно.
5. **DNS:** `:put [:resolve portal.wifiverify.ru]` должен вывести IP-адрес.
6. **login.html** — как в шаге 6.

Проверка и уборка — как в шаге 7.

При ручной настройке адрес сервера WiFiVerify записан цифрами и **сам не обновляется**. Если адрес сервера изменится, повторите пункты 2 и 4 — или настройте точку скриптом: он ставит задание, которое следит за адресом само.