УТВЕРЖДАЮ
Президент ООО «УК «МАКС» —
управляющей организации ООО «СВЯЗЬ»

_____ М. А. Клевцов
«___» _____ 2026 г.

Wi-Fi.Click с модулем Radius

Инструкция по установке

Версия документа 1.0
Правообладатель — ООО «СВЯЗЬ»
Москва, 2026

1. Назначение документа

Документ содержит порядок установки и первичной настройки программного обеспечения «Wi-Fi.Click с модулем Radius» (далее — ПО) в инфраструктуре лицензиата. Документ предназначен для системного администратора лицензиата, имеющего опыт работы с операционными системами семейства Linux, средствами контейнеризации и оборудованием беспроводных сетей.

2. Состав программного обеспечения

Составная часть	Назначение и сетевые порты
Сервер аутентификации	Приём и обработка запросов на проверку права доступа от сетевого оборудования по протоколу RADIUS. Порты 1812/udp и 1814/udp
Сервер учёта сеансов	Приём сообщений о начале, продолжении и завершении сеансов, учёт объёма переданных данных. Порты 1813/udp и 1815/udp
Служба страницы авторизации	Формирование страницы входа в сеть, приём идентификационных данных пользователя, выдача разрешения на доступ. Внутренний порт 8080/tcp
Служба размещения материалов страницы авторизации	Выдача изображений, стилей и загруженных владельцем сети материалов. Внутренний порт 80/tcp
Личный кабинет и программный интерфейс	Управление объектами, сетевым оборудованием, способами идентификации и отчётами. Внутренний порт 3030/tcp
Служба авторизации по входящему звонку	Проверка номера телефона пользователя по факту входящего звонка на выделенный номер
Служба выдачи кодов по звонку	Сообщение пользователю кода доступа голосовым вызовом
Служба регламентных задач	Выполнение периодических операций: закрытие просроченных сеансов, формирование отчётов, обслуживание журналов
Служба обмена данными	Обмен сведениями с внешними системами владельца сети и поставщиками идентификации
Система управления базами данных	Хранение сведений об объектах, оборудовании, пользователях и сеансах. Внутренний порт 27017/tcp
Обратный прокси-сервер	Приём соединений по протоколу HTTPS, выдача сертификатов, распределение запросов между службами. Порты 80/tcp и 443/tcp

3. Требования к среде установки

Параметр	Значение
Операционная система	Ubuntu Server 22.04 LTS или 24.04 LTS, Astra Linux Special Edition 1.7, РЕД ОС 7.3 или иной дистрибутив Linux с ядром не ниже 5.15
Средства контейнеризации	Docker Engine 24.0 и выше, Docker Compose версии 2
Процессор	4 вычислительных ядра
Оперативная память	8 ГБ (из них не менее 2,5 ГБ отводится системе управления базами данных)

Дисковое пространство	100 ГБ; журнал сеансов за год при 1000 пользователях в сутки занимает около 20 ГБ
Сетевые адреса	Один общедоступный адрес протокола IP версии 4 для приёма запросов от сетевого оборудования и для страницы авторизации
Доменные имена	Два имени: для страницы авторизации и для личного кабинета; записи должны указывать на адрес сервера
Сетевые порты (входящие)	80/tcp, 443/tcp — страница авторизации и личный кабинет; 1812/udp, 1814/udp — аутентификация; 1813/udp, 1815/udp — учёт сеансов
Внешние услуги	Отправка SMS (поставщик по выбору лицензиата) и, при использовании авторизации по звонку, входящая телефонная линия

4. Порядок установки

4.1. Проверка целостности дистрибутива

```
tar -xzf wfc-radius-<версия>.tar.gz
cd wfc-radius-<версия>
sha256sum -c SHA256SUMS
```

Все строки должны завершаться словом `OK`.

4.2. Параметры установки

```
cp .env.example .env
chmod 600 .env
nano .env
```

Параметр	Назначение
`PUBLIC_IP`	Общедоступный адрес сервера, на который сетевое оборудование направляет запросы аутентификации и учёта
`AUTH_DOMAIN`	Доменное имя страницы авторизации
`API_DOMAIN`	Доменное имя личного кабинета и программного интерфейса
`MONGO_PASS`	Пароль учётной записи системы управления базами данных
`JWT_SECRET`	Секретное значение для подписания сеансовых признаков личного кабинета
`ADMIN_EMAIL, ADMIN_PASS`	Первая учётная запись администратора личного кабинета
`LICENSE_KEY`	Лицензионный ключ, выданный правообладателем
`SMS_PROVIDER, SMS_LOGIN, SMS_PASS, SMS_SENDER`	Параметры подключения к поставщику услуг отправки SMS

Параметры способов идентификации (Единая система идентификации и аутентификации, Сбер ID, Альфа ID, Mobile ID) задаются в каталоге `config` отдельными файлами настройки и заполняются после получения доступа у соответствующего поставщика. Их заполнение не требуется для начала работы: по умолчанию доступны идентификация по коду из SMS и по входящему звонку.

4.3. Запуск установки

```
sudo ./install.sh
```

Сценарий выполняет: проверку средств контейнеризации, свободного места и занятости портов; сверку контрольных сумм; загрузку образов; создание тома базы данных и инициализацию набора реплик; запуск составных частей; получение сертификата для указанных доменных имён; создание первой учётной записи администратора.

Продолжительность установки — от 10 до 20 минут, из них до 5 минут занимает инициализация базы данных. Признак успешного завершения — сообщение `Установка завершена` и перечень запущенных составных частей.

4.4. Проверка работоспособности

```
docker compose ps
curl -I https://<AUTH_DOMAIN>/
curl -I https://<API_DOMAIN>/
echo "User-Name=test,User-Password=test" | radclient -x <PUBLIC_IP>:1812 auth <общий секрет>
```

Ожидаемый результат: все составные части в состоянии `running`; страница авторизации и личный кабинет отвечают кодом 200; сервер аутентификации отвечает на проверочный запрос (для несуществующего пользователя — отказом, что подтверждает приём и обработку запросов).

4.5. Подключение сетевого оборудования

В личном кабинете создаётся объект (обслуживаемый адрес), после чего для него добавляется сетевое оборудование: наименование, сетевой адрес устройства и общий секрет. Те же значения указываются на оборудовании в настройках серверов аутентификации и учёта: адрес сервера — `PUBLIC_IP`, порт аутентификации — 1812, порт учёта — 1813, общий секрет — заданный при добавлении. В настройках гостевой сети оборудования включается перенаправление неавторизованных пользователей на адрес страницы авторизации, а доменные имена страницы авторизации и платёжных служб вносятся в перечень разрешённых до авторизации.

Проверенные модели оборудования: точки доступа и контроллеры MikroTik (RouterOS 6.49 и 7.x), Comfast, KingsIoT, Tenda, а также любое оборудование с поддержкой аутентификации по протоколу RADIUS и перенаправления на внешнюю страницу авторизации.

5. Обновление и удаление

Обновление: получить новый дистрибутив, создать копию базы данных, выполнить `docker compose down`, сохранить `.env` и каталог `config`, распаковать новый дистрибутив в тот же каталог, выполнить `sudo ./install.sh`. Обновление не затрагивает данные: том базы данных и каталог загруженных материалов сохраняются.

Удаление: `docker compose down -v` и удаление каталога установки.

6. Типовые ошибки установки

Проявление	Причина и устранение
Сетевое оборудование сообщает об отсутствии ответа сервера аутентификации	Порты 1812/udp и 1813/udp закрыты межсетевым экраном либо на оборудовании указан неверный общий секрет. Проверить правила межсетевого экрана и значение секрета в личном кабинете
Страница авторизации не открывается у пользователя	Доменное имя страницы авторизации не внесено в перечень разрешённых до авторизации на сетевом оборудовании

Сертификат для доменных имён не получен	Записи доменных имён не указывают на адрес сервера либо закрыт порт 80/tcp, необходимый для проверки владения именем
Не приходит код из SMS	Не заданы или неверны параметры поставщика услуг отправки SMS; проверить журнал службы страницы авторизации
Составная часть базы данных не запускается	Недостаточно оперативной памяти для заданного размера кэша либо отсутствуют права на каталог тома данных

7. Техническая поддержка

Адрес электронной почты: support@wi-fi.click. Телефон: 8 (495) 181-66-61. Приём обращений — круглосуточно.