Техническая документация

Спецификации, требования к оборудованию и порядок настройки

Дата обновления: 04.09.2026

ТЕХНИЧЕСКАЯ ДОКУМЕНТАЦИЯ WiFiAuth

1. СИСТЕМНЫЕ ТРЕБОВАНИЯ

1.1. Для гостевых устройств

- Любое устройство с Wi-Fi модулем;
- Современный веб-браузер с поддержкой JavaScript.

1.2. Для точек доступа

- MikroTik, RouterOS версии 7.x или новее — на сегодня единственная платформа с полной автоматической настройкой (DHCP, hotspot, RADIUS, walled garden, VPN-канал управления) прямо из личного кабинета;
- При добавлении роутера можно указать другой тип оборудования (Cisco, Ubiquiti, иное), но автонастройка и управление функциями (например, смена Wi-Fi SSID из личного кабинета) для них пока не реализованы.

2. НАСТРОЙКА ТОЧКИ ДОСТУПА (MikroTik)

Настройка выполняется одной командой, а не вручную. После добавления роутера в личном кабинете (раздел «Оборудование → Роутеры») на странице роутера, вкладка «Первоначальная настройка MikroTik», доступна готовая команда для вставки в New Terminal (Winbox) или SSH-сессию.

Команда скачивает и применяет .rsc-скрипт, который настраивает:

- DHCP-сервер для гостевой сети (собственный адресный пул на каждый роутер);
- hotspot-профиль с авторизацией через RADIUS и учётом сессий;
- walled garden — разрешённые до авторизации адреса (домен страницы входа и стандартные проверки подключения ОС);
- кастомную страницу входа, которая передаёт гостя на внешний портал авторизации;
- VPN-туннель (OpenVPN) до сервера биллинга — канал управления роутером, работает независимо от баланса клиента.

Скрипт идемпотентен — повторный запуск безопасен, старые одноимённые объекты конфигурации пересоздаются. Конфигурация привязывается к MAC-адресу устройства при первом успешном запуске; при замене оборудования привязку нужно снять в личном кабинете кнопкой «Отвязать оборудование».

3. АВТОРИЗАЦИЯ ГОСТЕЙ

Параметр	Значение
Протокол	HTTP/HTTPS
Метод авторизации	Подтверждение номера телефона исходящим звонком: гость сам звонит на показанный номер, отвечать не требуется

Длительность сессии	Согласно параметрам объекта (точки) и подключённой услуге

4. VPN-КАНАЛ УПРАВЛЕНИЯ

Каждый роутер получает выделенный адрес и отдельную учётную запись для VPN (OpenVPN, авторизация по логину и паролю через RADIUS, без клиентского сертификата). Этот канал предназначен только для связи роутера с биллингом (управление конфигурацией, мониторинг) и не зависит от баланса или статуса подписки клиента.

5. БЕЗОПАСНОСТЬ

- Шифрование трафика личного кабинета и API: TLS;
- Хеширование паролей учётных записей: bcrypt;
- Внутренний API биллинга не публикуется в открытый интернет — доступен только серверу личного кабинета по служебному каналу;
- Защита конфигурации роутера от копирования на другое устройство — привязка к MAC-адресу.