Интеграция AxelNAC с точками доступа Eltex серии WEP/WOP-xL

В данной статье рассматривается процесс интеграции AxelNAC с точками доступа Eltex серии WOP/WEP в автономном режиме и режиме локальной коммутации.

Список точек поддерживаемых в профиле:

- WEP-2L;
- WOP-2L;
- WEP-3ax;
- WEP-200L;
- WOP-20L;
- WEP-30L, WEP-30L-Z;
- WOP-30L;
- WOP-30LI;
- WOP-30LS.

Настройка Eltex серии WOP/WEP в автономном режиме (на примере WOP-30L)

Настройки на точке доступа

В данном примере конфигурации используются следующие значения:

- **10.10.205.206** – IP-адрес AxelNAC (в данном контексте используется один адрес для портала и интерфейса обработки RADIUS-запросов);
- **10.10.205.159** – IP-адрес точки доступа;
- **PASSWORD** – пароль RADIUS;
- **1812** – порт аутентификации в AxelNAC;
- **1813** – порт аккаунтинга в AxelNAC;
- **3799** – порт disconnect в точке доступа;
- **PROD_SSID** – название SSID с авторизацией 802.1x;
- **GUEST_SSID** – название гостевой SSID с портальной авторизацией.

Настройка авторизации 802.1x

Шаг 1. Подключитесь к точке доступа по протоколу SSH.

Шаг 2. Войдите в конфигурацию интерфейса, на котором будет настроен SSID:

```
WOP-30L(root):/# configure
WOP-30L(config):/# interface
WOP-30L(config):/interface# wlan0-va0
```

Шаг 3. Войдите в конфигурацию VAP и укажите название SSID:

```
WOP-30L(config):/interface/wlan0-va1# vap
WOP-30L(config):/interface/wlan0-va1/vap# ssid PROD_SSID
```

Шаг 4. Укажите режим безопасности — 802.1x:

```
WOP-30L(config):/interface/wlan0-va1/vap# ap-security
WOP-30L(config):/interface/wlan0-va1/vap/ap-security# mode WPA2_1X
WOP-30L(config):/interface/wlan0-va1/vap/ap-security# exit
```

Шаг 5. Настройте параметры RADIUS-сервера AxelNAC:

```
WOP-30L(config):/interface/wlan0-va1/vap# radius
WOP-30L(config):/interface/wlan0-va1/vap/radius# auth-port 1812
WOP-30L(config):/interface/wlan0-va1/vap/radius# auth-address 10.10.205.206
WOP-30L(config):/interface/wlan0-va1/vap/radius# auth-password PASSWORD
WOP-30L(config):/interface/wlan0-va1/vap/radius# acct-port 1813
WOP-30L(config):/interface/wlan0-va1/vap/radius# acct-address 10.10.205.206
WOP-30L(config):/interface/wlan0-va1/vap/radius# acct-password PASSWORD
WOP-30L(config):/interface/wlan0-va1/vap/radius# acct-periodic true
WOP-30L(config):/interface/wlan0-va1/vap/radius# domain axeldemo.pro
WOP-30L(config):/interface/wlan0-va1/vap/radius# use-macaddr-as-password true
```

Шаг 6. Сохраните конфигурацию:

```
WOP-30L(config):/interface/wlan0-va1/vap/radius# save
```

Настройка портальной (гостевой) авторизации

Шаг 1. Подключитесь к точке по протоколу SSH.

Шаг 2. Войдите в конфигурацию интерфейса, на котором будет настроен SSID:

```
WOP-30L(root):/# configure
WOP-30L(config):/# interface
WOP-30L(config):/interface# wlan0-va1
```

Шаг 3. Войдите в конфигурацию VAP и укажите название SSID:

```
WOP-30L(config):/interface/wlan0-va1# vap
WOP-30L(config):/interface/wlan0-va1/vap# ssid GUEST_SSID
```

Шаг 4. Укажите режим безопасности – открытый доступ:

```
WOP-30L(config):/interface/wlan0-va1/vap# ap-security
WOP-30L(config):/interface/wlan0-va1/vap/ap-security# mode off
WOP-30L(config):/interface/wlan0-va1/vap/ap-security# exit
```

Шаг 5. Настройте параметры RADIUS-сервера AxelNAC:

```
WOP-30L(config):/interface/wlan0-va1/vap# radius
WOP-30L(config):/interface/wlan0-va1/vap/radius# auth-port 1812
WOP-30L(config):/interface/wlan0-va1/vap/radius# auth-address 10.10.205.206
WOP-30L(config):/interface/wlan0-va1/vap/radius# auth-password PASSWORD
WOP-30L(config):/interface/wlan0-va1/vap/radius# acct-port 1813
WOP-30L(config):/interface/wlan0-va1/vap/radius# acct-address: 10.10.205.206
WOP-30L(config):/interface/wlan0-va1/vap/radius# acct-password PASSWORD
WOP-30L(config):/interface/wlan0-va1/vap/radius# acct-periodic true
WOP-30L(config):/interface/wlan0-va1/vap/radius# domain axeldemo.pro
WOP-30L(config):/interface/wlan0-va1/vap/radius# use-macaddr-as-password true
WOP-30L(config):/interface/wlan0-va1/vap/radius# exit
```

Шаг 6. Настройте параметры портала:

```
WOP-30L(config):/interface/wlan0-va1/vap# captive-portal
WOP-30L(config):/interface/wlan0-va1/vap/captive-portal# enabled true
WOP-30L(config):/interface/wlan0-va1/vap/captive-portal# verification-mode external-portal
WOP-30L(config):/interface/wlan0-va1/vap/captive-portal# client-mac-format xx:xx:xx:xx:xx:xx
WOP-30L(config):/interface/wlan0-va1/vap/captive-portal# nas-id-format XX-XX-XX-XX-XX-XX
WOP-30L(config):/interface/wlan0-va1/vap/captive-portal# disconnect-on-reject false
WOP-30L(config):/interface/wlan0-va1/vap/captive-portal# scenarios
WOP-30L(config):/interface/wlan0-va1/vap/captive-portal/scenarios# scenario-redirect
WOP-30L(config):/interface/wlan0-va1/vap/captive-portal/scenarios/scenario-redirect# redirect-url  http://10.31.10.206/Eltex::AP?switch_url=<SWITCH_URL>&ap_mac=<AP_MAC>&client_mac=<CLIENT_MAC>&wlan=<
```

Шаг 7. Сохраните конфигурацию:

```
WOP-30L(config):/interface/wlan0-va1/vap/captive-portal/scenarios/scenario-redirect# save
```

Особенности

Функционал Disconnect Message (DMs) и Change of Authorization (CoA)

На данных точках доступа за обработку сообщений Disconnect Message (DMs) и Change of Authorization (CoA) отвечает один компонент — DAS-сервер. По умолчанию используется единый 3799 порт (не рекомендуется менять).

Шаг 1. Подключитесь к точке по протоколу SSH.

Шаг 2. Настройте DAS-сервер:

```
WOP-30L(config):/# das-server
WOP-30L(config):/das-server# enabled true
WOP-30L(config):/das-server# auth-password PASSWORD
```

Шаг 3. Сохраните настройки:

```
WOP-30L(config):/das-server# save
```

Особенности настройки доступа администратора к точке доступа по SSH с авторизацией через RADIUS

Если на точке доступа нет локального пользователя с указанным именем, вход будет невозможен. Точка доступа будет отправлять RADIUS-запрос на AxelNAC, но с указанием в поле**password** некорректного значения, которое всегда приведет к ответу **Reject**. Если RADIUS-сервер недоступен, то точка доступа авторизует данного пользователя локально.

Настройка vWLC с точкой доступа (на примере WEP-2L)

В данном руководстве точки доступа управляются через vWLC, но коммутируют клиентский трафик в автономном режиме, без туннелирования на контроллер.

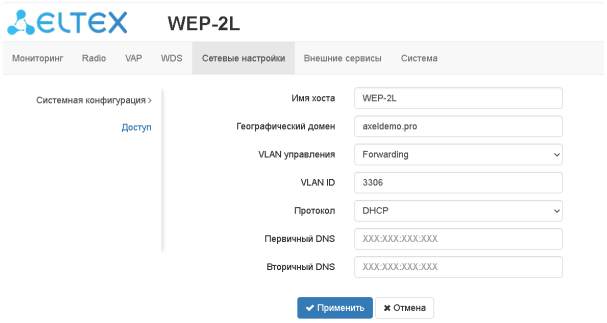
Настройка DHCP

Шаг 1. Настройте DHCP-сервер с учетом режима локальной коммутации.

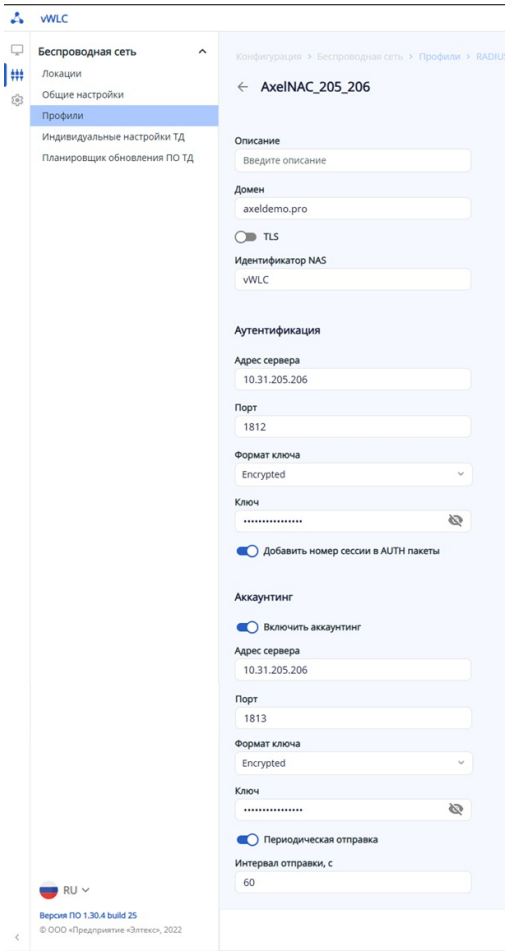
При настройке DHCP-сервера, чтобы точка работала полностью в режиме локальной коммутации, не указывается опция: **suboption 12 ascii-text "192.168.1.1"** — адрес терминирования SoftGRE-туннелей.

Настройка управляющего интерфейса

Шаг 1. Зайдите на точку доступа, используя веб-интерфейс, после получения IP-адреса по DHCP и укажите режим его работы как показано на скриншоте:

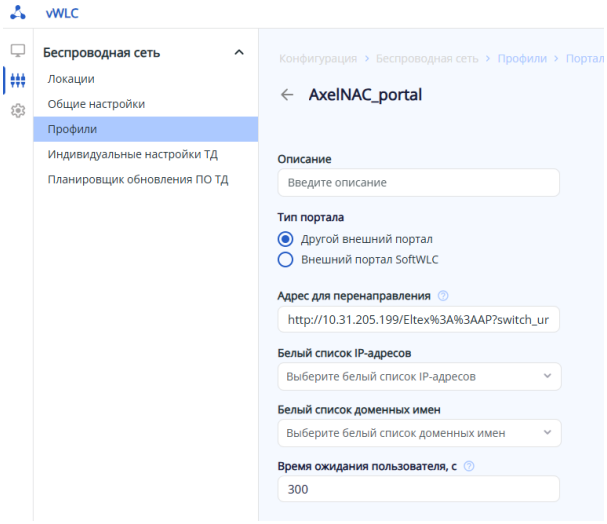


Шаг 2. Настройте профиль RADIUS-сервера как показано на скриншоте:

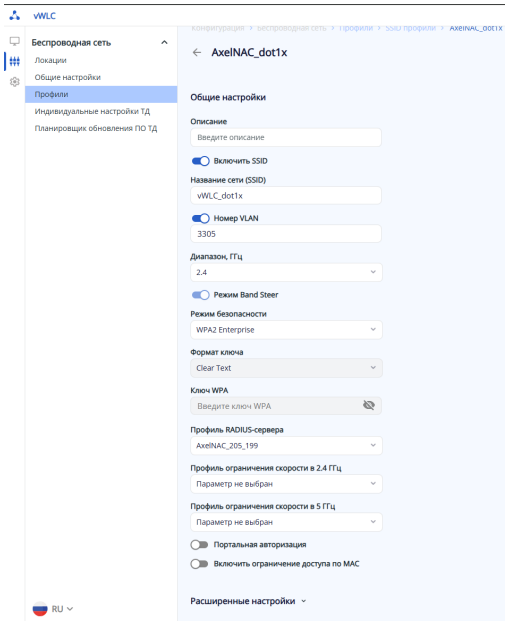


Шаг 3. Настройте профиль портала как показано на скриншоте:

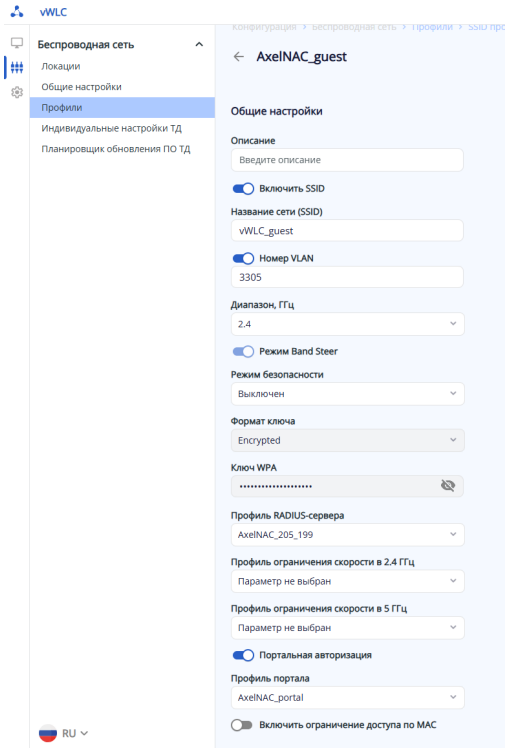
Адрес портала указывается с экранированием спецсимволов: **http(s)://10.31.205.199/Eltex%3A%3AAP?switch_url=<SWITCH_URL>&ap_mac=<AP_MAC>&client_mac=<CLIENT_MAC>&wlan=<SSID>&redirect_url=<ORIGINAL_URL>&nas-ip=<NAS_IP>**



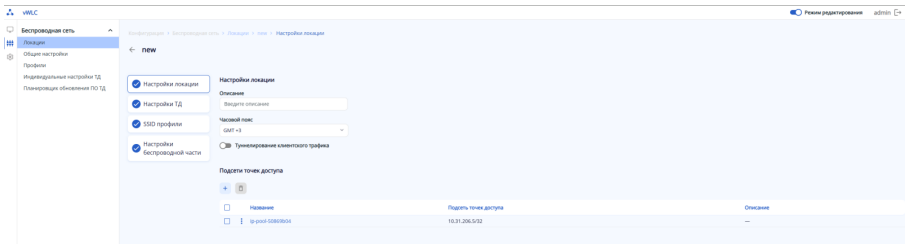
Шаг 4. Настройте профиль SSID для dot1x и укажите профиль RADIUS-сервера как показано на скриншоте:



Шаг 5. Настройте профиль MAB и укажите профиль RADIUS-сервера и профиль портала как показано на скриншоте:

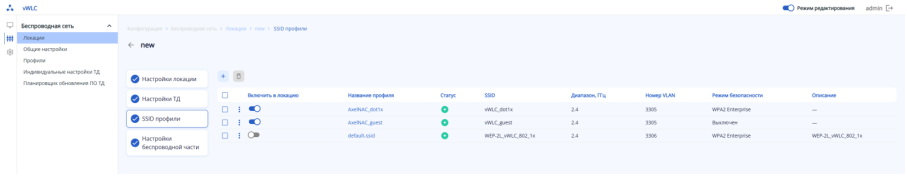


Шаг 6. Настройте локацию как показано на скриншоте:



В данном примере указана маска 32 (для одной точки доступа).

Шаг 7. Включите в локации необходимые SSID как показано на скриншоте:



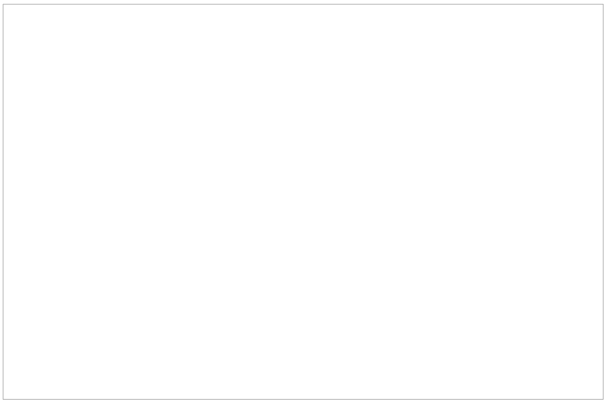
Особенности

В данном режиме (без предоставления по DHCP опции 12) точка доступа использует свой интерфейс как **bridge** и не отправляет весь клиентский трафик через туннель на контроллер. Соответственно, точка доступа должна получать на своем интерфейсе трафик от нужных VLAN через **trunk** коммутатора.

Настройка точки доступа в AxelNAC

Настройка авторизации 802.1x

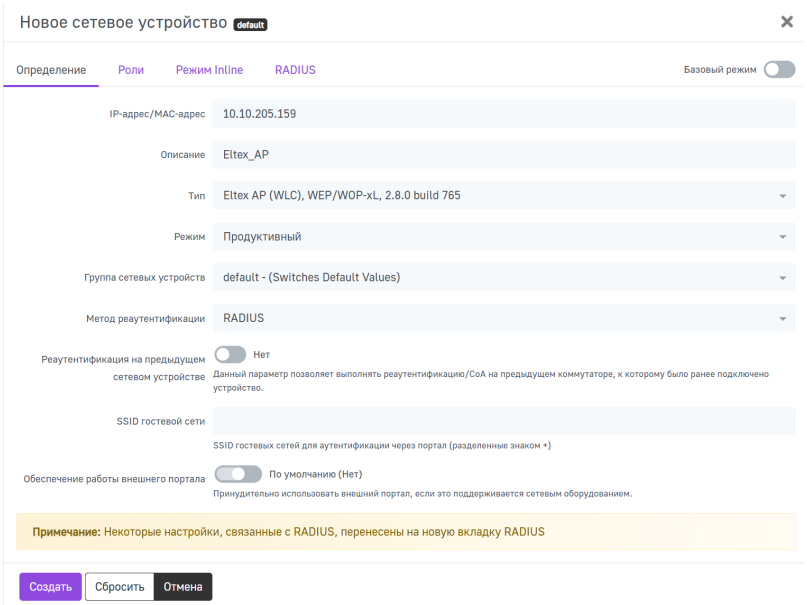
Шаг 1. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Сетевые устройства** , нажмите кнопку **Новое сетевое устройство** и в выпадающем списке выберите к какой группе должно принадлежать устройство (по умолчанию создана группа **default**).



Шаг 2. На открывшейся странице заполните поля следующим образом:

- **IP-адрес/MAC-адрес**: укажите IP-адрес точки доступа;
- **Тип**: Eltex AP (WLC), WEP/WOP-xL, 2.8.0 build 765;
- **Режим**: Продуктивный;
- **Метод реаутентификации**: RADIUS.

Остальные параметры остаются по умолчанию.



Шаг 3. Переключитесь на вкладку **Роли**. В разделе **Назначение VLAN ID** укажите номера VLAN для нужных ролей.

Шаг 4. Перейдите на вкладку **RADIUS** и выполните следующие настройки:

- **Секретная фраза:** укажите RADIUS-ключ указанный при настройке;
- **Disconnect-порт и CoA-порт**: оставьте пустыми (по умолчанию используется UDP порт 3799). Если вы указали иной порт в настройке das-server, укажите его в обоих полях;
- **Доступ к CLI/VPN:** [опционально] если требуется организовать доступ администраторов в CLI данной точки доступа по протоколу RADIUS – активируйте параметр.

На текущий момент точки доступа Eltex не поддерживают функционал передачи VLAN ID в рамках отправки CoA.

Остальные параметры остаются по умолчанию.

Шаг 5. Нажмите **Создать** в левом нижнем углу окна.

Настройка портальной (гостевой) авторизации

Шаг 1. Для настройки портальной (гостевой) авторизации в том же разделе выберите устройство, которое создали ранее.

Шаг 2. Активируйте параметр **Расширенный режим** в правом верхнем углу окна.

Шаг 3. На вкладке **Определение** укажите **SSID гостевой сети – GUEST_SSID**. Если гостевых SSID несколько, укажите их разделяя знаком +.

Шаг 4. Нажмите **Сохранить** в левом нижнем углу окна.

ID статьи: 1419
Последнее обновление: 9 апр., 2026
Обновлено от: Егоров В.
Ревизия: 9
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.1.0 -> AxelNAC. Руководство по интеграции с сетевым оборудованием -> Интеграция AxelNAC с точками доступа Eltex серии WEP/WOP-xL
https://docs.axel.pro/entry/1419/