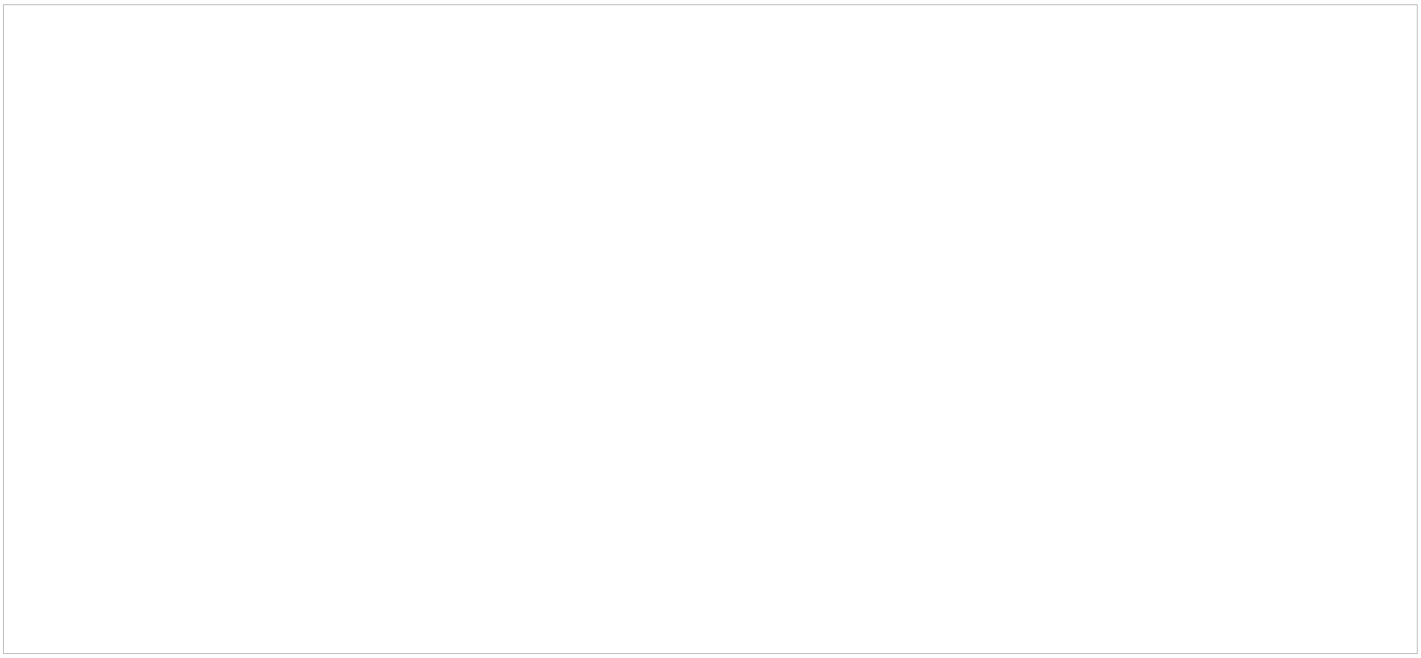
# Вкладка «Сетевые устройства»

На данной вкладке выполняется настройка и добавление в группу новых сетевых устройств.



По умолчанию в таблице отображаются 5 столбцов:

- **Идентификатор** — IP-адрес/MAC-адрес/диапазон (CIDR) сетевого устройства;
- **Описание** — описание сетевого устройства;
- **Группа** — группа, которой принадлежит сетевое устройство;
- **Тип** — профиль сетевого устройства;
- **Режим** — режим работы сетевого устройства.

## Управление таблицей

Набор отображаемых столбцов в таблице может быть изменен, для этого нажмите на иконку . В выпадающем списке нажмите на название столбца, отображение которого в таблице необходимо изменить.

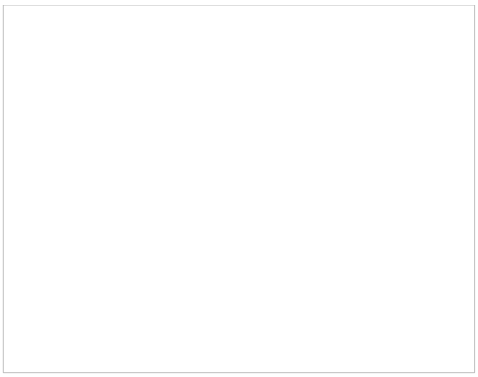
По умолчанию на странице отображается 25 записей, однако вы можете выбрать отображение 10, 50, 100, 200, 500 и 1000 записей на странице. Для этого нажмите на поле в правом верхнем углу списка и выберите в выпадающем списке необходимое количество для отображения.

Вы можете отсортировать таблицу по **Идентификатору**, **Описанию**, **Группе**, **Типу**, **Режиму** в порядке алфавитного возрастания или убывания с помощью иконки . По умолчанию все записи в таблице отображаются в порядке алфавитного возрастания по **Идентификатору**.

Для переключения между страницами используйте блок в правом верхнем углу списка.

## Создание нового сетевого устройства

Для того чтобы создать новое сетевое устройство, нажмите**Новое сетевое устройство** в левом верхнем углу страницы и выберите из выпадающего списка группу, в которую его нужно добавить. Например, группа **default**. После этого откроется меню конфигурации сетевого устройства.

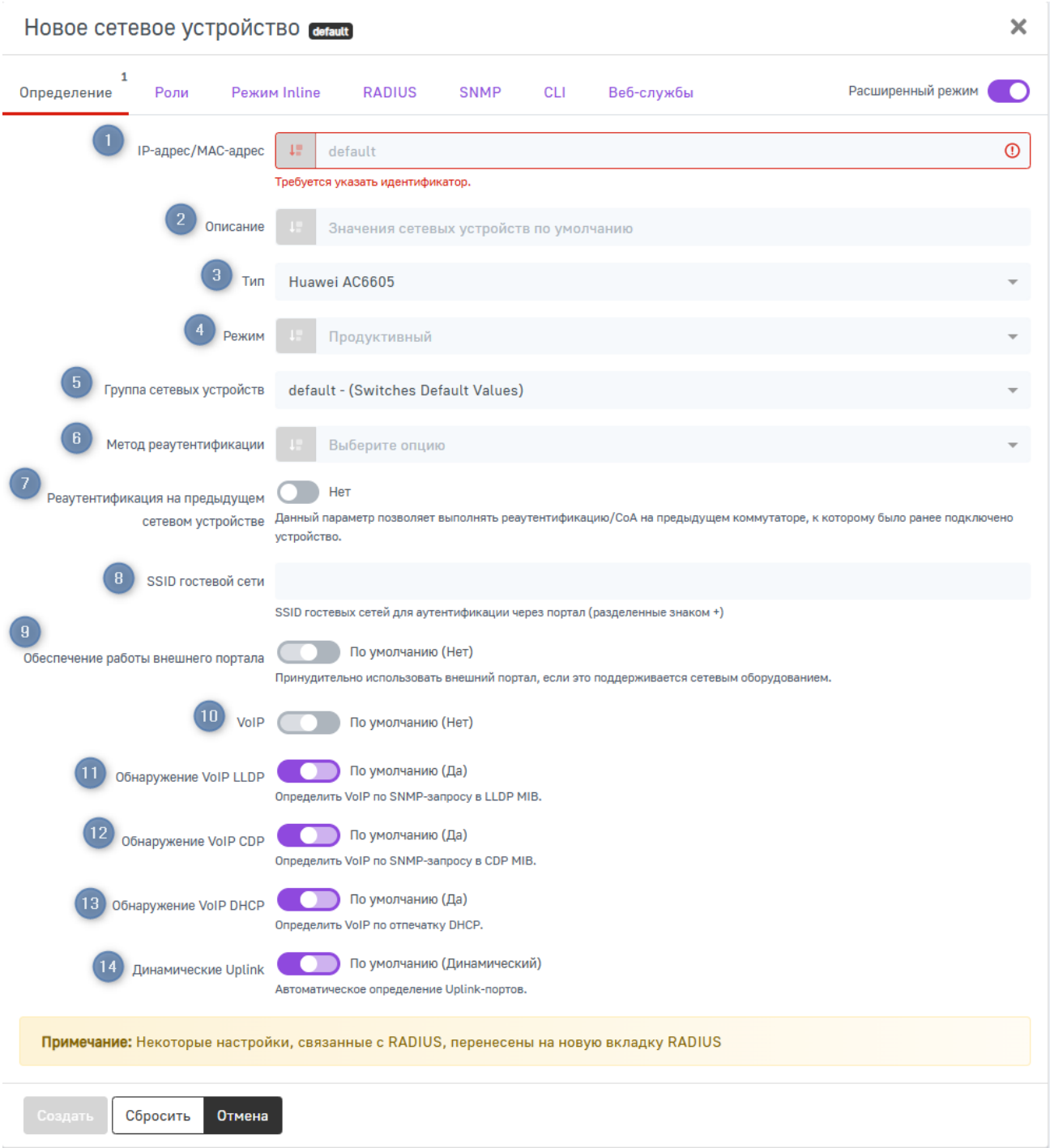


При выборе группы, устройству будут назначены настройки, указанные в группе. Чтобы их изменить, отредактируйте параметры сетевого устройства

## Определение

На данной вкладке можно задать глобальные параметры для сетевого оборудования.

В левом верхнем углу, справа от названия вкладки **Определение**, отображается количество оставшихся обязательных для заполнения полей.




В данном меню доступны следующие настройки:

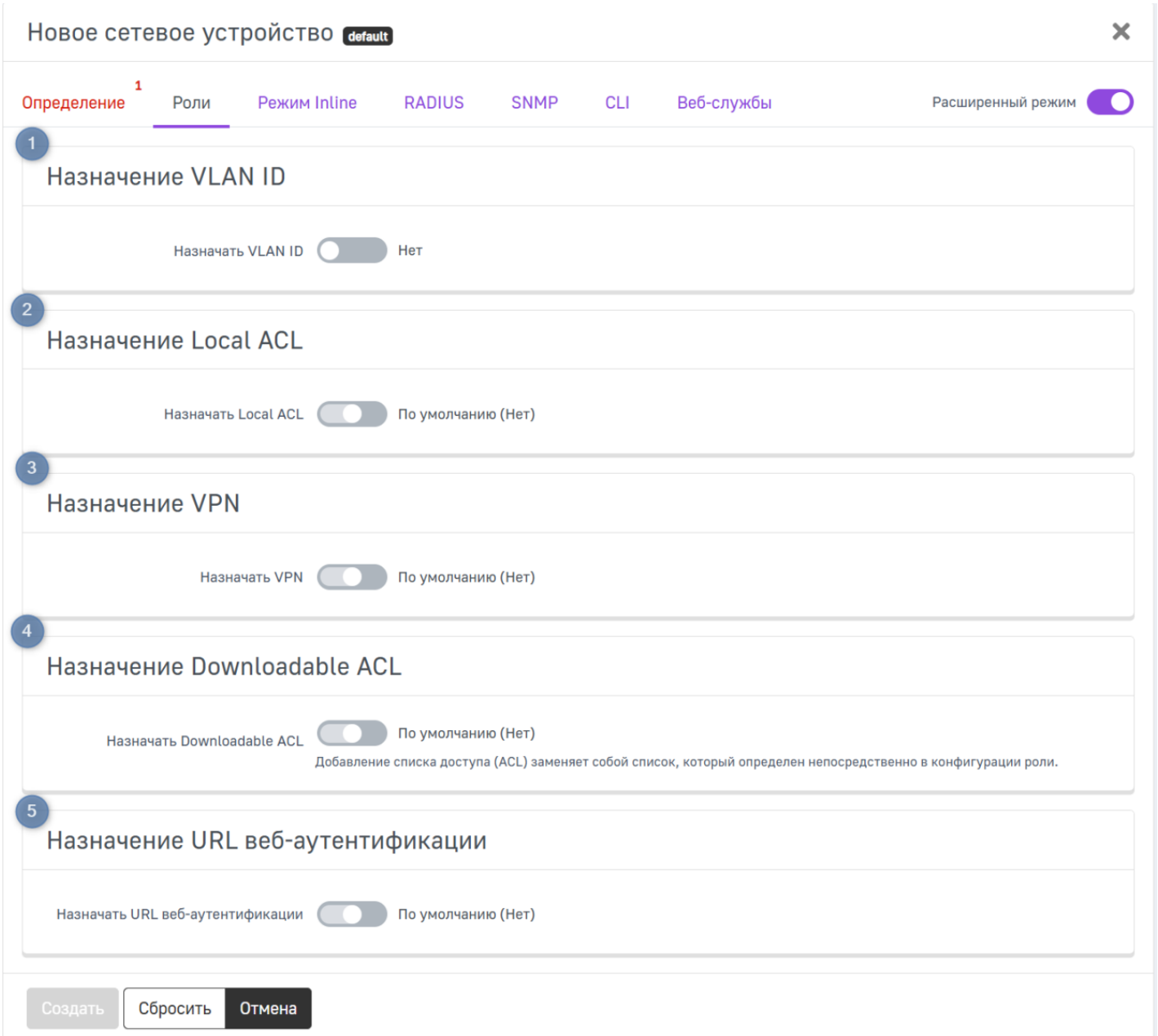
1. **IP-адрес/MAC-адрес** — идентификатор сетевого устройства, который будет отображаться в таблице со списком сетевых устройств;
2. **Описание** — описание сетевого устройства, которое будет отображаться в таблице со списком сетевых устройств;
3. **Тип** — профили сетевого оборудования. Подробнее о профилях вы можете прочитать здесь. Для некоторых типов устройств доступна возможность **Просмотреть шаблон сетевого устройства**. При нажатии на кнопку [ ] открывается страница, где можно просмотреть и изменить настройки уже существующего шаблона сетевого устройства. Подробнее о профилях вы можете прочитать здесь;
4. **Режим** — режим работы сетевого устройства. Возможные значения:
   - **Тестирование** — режим работы позволяет убедиться в корректности выполнения правил аутентификации, но клиентская сессия не будет настроена в соответствии с ними;
   - **Регистрация** — режим работы позволяет убедиться в корректности выполнения правил аутентификации, но клиентская сессия не будет настроена в соответствии с ними (за исключением VoIP-устройств, управляемых через SNMP-trap);
   - **Продуктивный** — режим работы позволяет выполнять настройку клиентских сессий и является полнофункциональным режимом работы.
5. **Группа сетевых устройств** — группа, в которое будет входить сетевое устройство;
6. **Метод реаутентификации** — метод, с помощью которого происходит реаутентификация. Возможные значения:
   - **Telnet** — команда на реаутентификацию передается по протоколу **Telnet**;
   - **SSH** — команда на реаутентификацию передается по протоколу **SSH**;
   - **SNMP** — команда на реаутентификацию передается по протоколу **SNMP** ;
   - **RADUIS** — команда на реаутентификацию передается по протоколу **RADUIS**;
   - **HTTP** — команда на реаутентификацию передается по протоколу **HTTP**;

- **HTTPS** — команда на реаутентификацию передается по протоколу **HTTPS**.

7. **Реаутентификация на предыдущем сетевом устройстве** — данный параметр позволяет отправлять команду на реаутентификацию сессии устройства или пользователя на данном сетевом устройстве, если MAC-адрес был ранее определен на другом сетевом устройстве, контролируемом AxelNAC;
8. **SSID гостевой сети** (появляется только при выборе типа устройства **Huawei AC6605**) — имена гостевых сетей, для которых будет работать механизм перенаправления на портал с использованием протокола China Portal Protocol (должны быть разделены знаком **+**);
9. **Обеспечение работы внешнего портала** — принудительно использовать внешний портал регистрации, если это поддерживается сетевым оборудованием;
10. **VoIP** — задает отправку особых RADIUS-атрибутов для назначения Voice VLAN для устройств, для которых активирован параметр VoIP;
11. **Обнаружение VoIP LLDP** — автоматическое задание атрибута VoIP для сетевых устройств на основе SNMP-запросов в LLDP MIB;
12. **Обнаружение VoIP CDP** — автоматическое задание атрибута VoIP для сетевых устройств на основе SNMP-запросов в CDP MIB;
13. **Обнаружение VoIP DHCP** — автоматическое задание атрибута VoIP для сетевых устройств на основе отпечатка DHCP;
14. **Динамические Uplink** — автоматическое определение Uplink-портов. При включении отправляет информацию о поднявшемся порте используя SNMP-trap.

## Роли

На данной вкладке можно задать и переопределить параметры ранее созданных ролей для данного сетевого устройства.



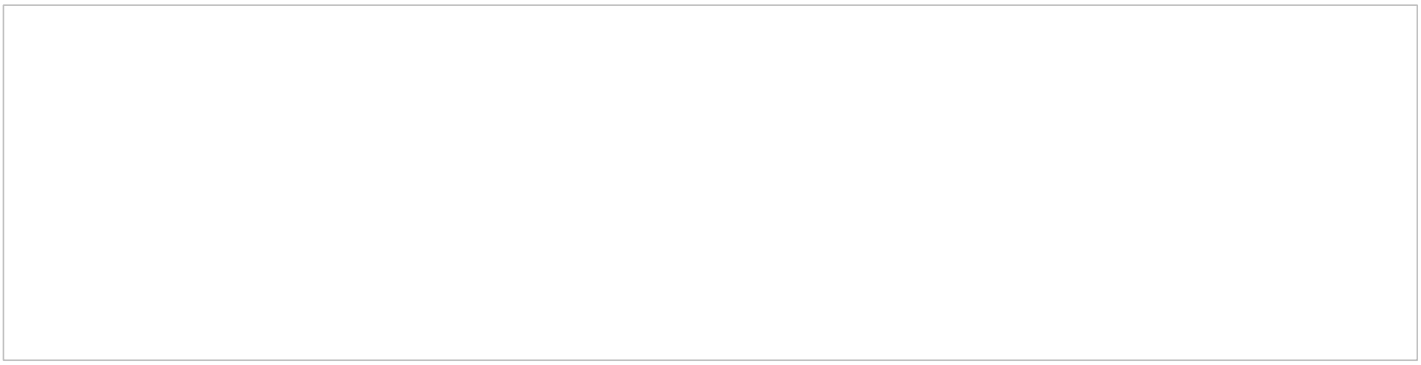

В данном меню доступны следующие настройки:

1. **Назначать VLAN ID** — должно ли при применении ролей к сессиям пользователей или устройств происходить назначение VLAN. При активации данного параметра появляется возможность задать VLAN для ранее созданных ролей. Отсутствие значения VLAN ID у роли при ее назначении означает, что значение VLAN не будет отправлено на сетевое устройство и большинство сетевых устройств применит к сессии пользователя VLAN по умолчанию, указанный в

настройках данного порта (точное поведение вашего сетевого устройства уточняйте в документации производителя вашего сетевого устройства). Значение **-1** для VLAN ID какой-либо роли означает, что вместо сообщения **Access-Accept** при применении данной роли сетевое устройство получит сообщение **Access-Reject** и сессия будет заблокирована. У некоторых предустановленных ролей есть значения по умолчанию;
2. **Назначать Local ACL** — должно ли при применении ролей к сессиям пользователей или устройств происходить назначение локального ACL. При активации данного параметра в поле для ролей необходимо задать имя ACL, которое создано на сетевом оборудовании. Данное имя будет прислано сетевому оборудованию для применения к клиентской сессии RADIUS по итогу авторизации. Если ACL с указанным именем не создан на сетевом устройстве, большинство сетевых устройств будут игнорировать все параметры, переданные в RADIUS-ответе, такие как VLAN ID или URL-redirect;
3. **Назначать VPN** — нужно ли назначать роли VPN. При активации данного параметра в поля вписываются RADIUS-атрибут. Он будет прислан сетевому оборудованию для клиентской сессии RADIUS по итогу авторизации.
4. **Назначать Downloadable ACL** — нужно ли назначать Downloadable ACL указанной роли. Добавление списка доступа (ACL) заменяет собой список, который определен непосредственно в конфигурации роли. Он будет прислан сетевому оборудованию для клиентской сессии RADIUS по итогу авторизации;
5. **Назначать URL веб-аутентификации** — нужно ли назначать роли URL веб-аутентификации. При активации данного параметра в поля вписывается адрес в формате RADIUS-атрибута, на который пользователь будет перенаправлен при веб-аутентификации. Ссылка указывается в зависимости от оборудования (Пример: **http://10.10.0.205/Cisco::ASA**). Оно будет прислано сетевому оборудованию для клиентской сессии RADIUS по итогу авторизации.

## Режим Inline

Режим Inline в AxelNAC позволяет контролировать сессии пользователей и устройств на сетевом оборудовании, не поддерживающем протокол 802.1x и другие методы интеграции с сетевым оборудованием. Для работы данного режима VLAN пользователей/устройств должны терминироваться на AxelNAC, который будет обеспечивать маршрутизацию и применение ограничений к пользовательскому трафику (трафику устройств).



В данном меню доступны следующие настройки:

1. **Условия для режима Inline** — установить режим Inline, если выполняется любое из условий. Количество условий может быть неограниченно. Возможные условия:
   - **Всегда** — режим будет применяться для любого подключаемого устройства;
   - **Порт** — режим будет применяться только на определенных портах. В данном условии необходимо также выбрать номер порта;
   - **MAC-адрес** — режим будет применяться только для определенных MAC-адресов. В данном условии необходимо также указать MAC-адрес;
   - **SSID сети Wi-Fi** — режим будет применяться только для определенных SSID. В данном условии также необходимо указать SSID сети Wi-Fi.

## RADIUS

На данной вкладке можно настроить интеграцию RADIUS.

В данном меню доступны следующие настройки:

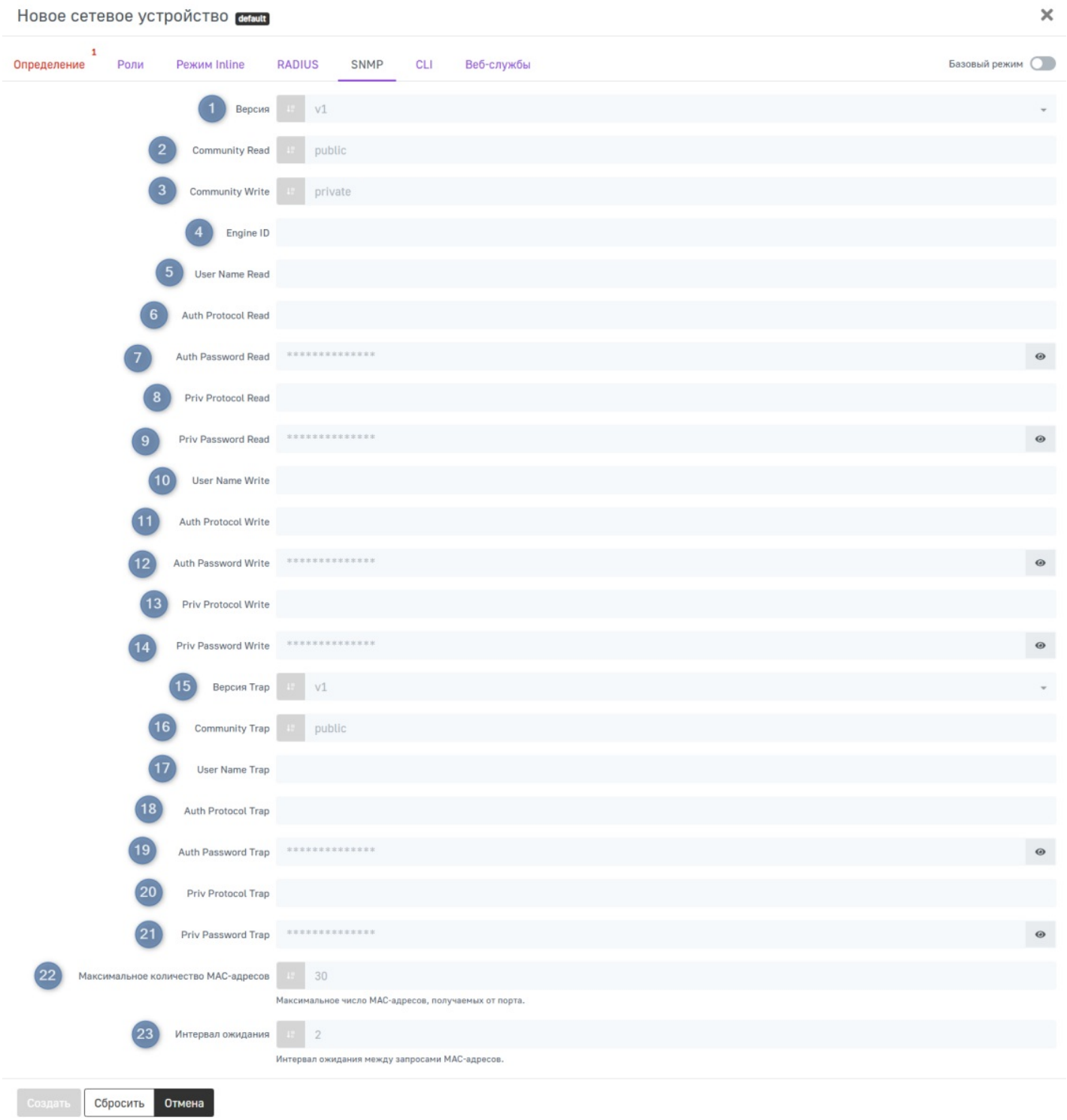
1. **Секретная фраза** — укажите секретную фразу, которую вы настроили на коммутаторе;
2. **Использовать CoA** — использовать CoA, если он доступен, для реаутентификации пользователя. При отключении данного параметра будет использоваться RADIUS Disconnect, если он доступен;

   Данное значение будет использоваться системой в случае, если на вкладке **Определение** в поле **Метод реаутентификации** выбрано значение **RADIUS**. В ином случае заданное в этом поле значение не будет применено.

3. **IP-адрес контроллера** — данный IP-адрес будет использоваться для запросов на реаутентификацию. Обычно применяется только для Wi-Fi-соединений;
4. **Disconnect-порт** — укажите порт для переадресации запроса Disconnect;
5. **CoA-порт** — укажите порт для переадресации CoA-запроса;
6. **Валидация после MFA** — добавить дополнительную проверку в поток RADIUS, чтобы определить, успешно ли пользователь подтвердил MFA;
7. **Доступ к CLI/VPN разрешен** — разрешить данному сетевому оборудованию использовать AxelNAC в качестве RADIUS-сервера для доступа к CLI или VPN.

## SNMP

На данной вкладке находятся настройки интеграции с сетевым оборудованием.



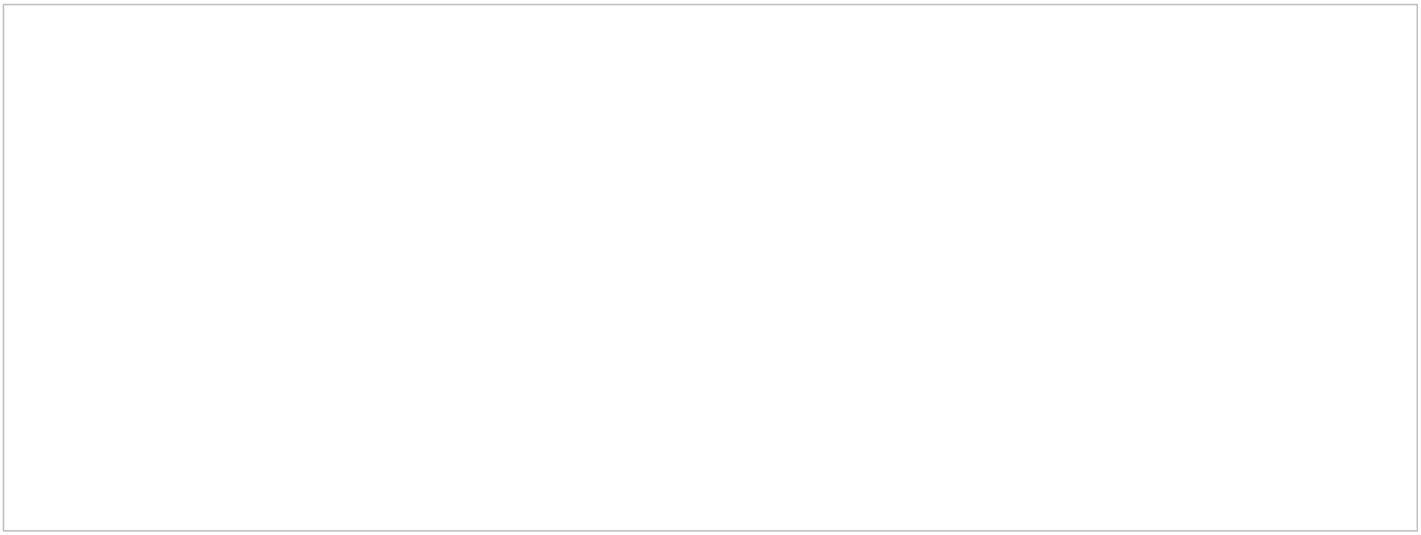

В данном меню доступны следующие настройки:

1. **Версия** — версия протокола SNMP (v1, v2c, v3), используемая для обмена данными;
2. **Community Read** — строка сообщества SNMP, которая предоставляет доступ для чтения к данным устройства в SNMPv1 и SNMPv2;
3. **Community Write** — строка сообщества SNMP, которая предоставляет доступ для записи данных устройства в SNMPv1 и SNMPv2;
4. **Engine ID** — идентификатор механизма аутентификации в SNMPv3;
5. **User Name Read** — имя пользователя для чтения данных в SNMPv3;
6. **Auth Protocol Read** — используемый протокол аутентификации (MD5, SHA) для чтения в SNMPv3;
7. **Auth Password Read** — пароль аутентификации для чтения в SNMPv3;
8. **Priv Protocol Read** — используемый протокол шифрования (DES, AES) для чтения SNMPv3;
9. **Priv Password Read** — пароль шифрования для чтения в SNMPv3;
10. **User Name Write** — имя пользователя для записи данных в SNMPv3;
11. **Auth Protocol Write** — используемый протокол аутентификации для записи в SNMPv3;
12. **Auth Password Write** — пароль аутентификации для записи в SNMPv3;
13. **Priv Protocol Write** — используемый протокол шифрования для записи в SNMPv3;
14. **Priv Password Write** — пароль шифрования для записи в SNMPv3;
15. **Версия Trap** — версия протокола SNMP (v1, v2c, v3), используемая для SNMP Trap-сообщений;
16. **Community Trap** — строка сообщества для приема SNMP Trap-сообщений в SNMP v1/v2c;
17. **User Name Trap** — имя пользователя для приема Trap-сообщений в SNMPv3;

18. **Auth Protocol Trap** — используемый протокол аутентификации для Trap-сообщений в SNMPv3;
19. **Auth Password Trap** — пароль аутентификации для Trap-сообщений в SNMPv3;
20. **Priv Protocol Trap** — используемый протокол шифрования для Trap-сообщений в SNMPv3;
21. **Priv Password Trap** — пароль шифрования для Trap-сообщений в SNMPv3;
22. **Максимальное количество MAC-адресов** — максимальное число MAC-адресов, получаемых от порта;
23. **Интервал ожидания** — интервал ожидания между запросами MAC-адресов.

## CLI

На данной вкладке можно настроить подключение через командную строку.

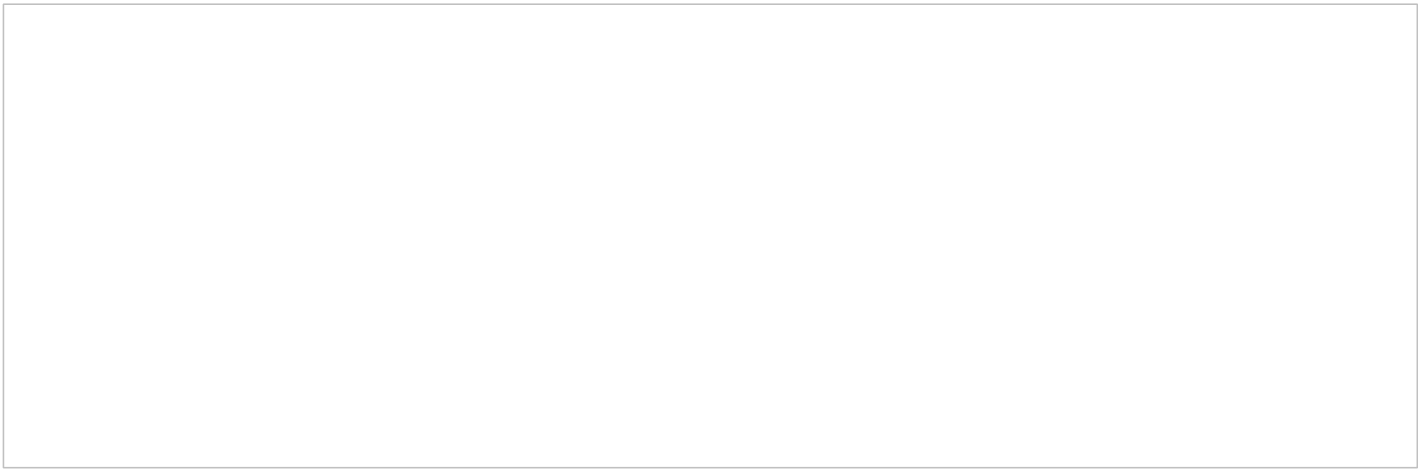


В данном меню доступны следующие настройки:

1. **Транспортный протокол** — протокол для управления подключением через командную строку. Возможные варианты:
   - **Telnet** — передает данные в виде текста;
   - **SSH** — передает данные в зашифрованном формате по защищенному каналу.
2. **Имя пользователя** — имя пользователя;
3. **Пароль** — пароль пользователя;
4. **Пароль Enable** — пароль для получения большего количества прав, вводится при подключении на коммутаторе.

## Веб-службы

На данной вкладке можно настроить подключение через API.



В данном меню доступны следующие настройки:

1. **Транспортный протокол** — протокол для управления подключением через API. Возможные варианты:
   - **HTTP** — протокол передачи данных между веб-браузером и сервером;
   - **HTTPS** — протокол передачи данных между веб-браузером и сервером с использованием **TLS/SSL**.
2. **Имя пользователя** — имя пользователя для подключения к API;
3. **Пароль** — пароль пользователя для подключения к API.

Для того чтобы создать новое сетевое устройство, заполните параметры конфигурации и нажмите **Создать**. Чтобы сбросить введенные параметры на стандартные значения, нажмите **Сбросить**. Для возвращения на предыдущую страницу без сохранения выполненных на странице действий, нажмите **Отменить**.

## Поиск сетевого устройства

Для того чтобы найти определенное сетевое устройство, можно выполнить поиск по критериям: **Идентификатор**, **Описание**, **Группа, Тип** или **Режим**. Введите интересующий критерий в поле поиска и нажмите **Поиск**. Нажмите **Очистить**, чтобы сбросить критерии поиска.

Также можно выполнять поиск по нескольким критериям. Для этого нажмите на иконку лупы справа от кнопки **Поиск**.

В меню расширенного поиска вы можете выбрать операторы **И** и **ИЛИ** и указать несколько критериев для поиска. Поиск можно вести по критериям:

- **Идентификатор** — поиск по идентификатору сетевого устройства;
- **Описание** — поиск по описанию сетевого устройства;
- **Режим** — поиск по режиму, выбранному для сетевого устройства;
- **Тип** — поиск по типу, выбранному для сетевого устройства.

Также вам доступны следующие операторы:

- **равно**;
- **не равно**;
- **начинается с** (недоступно для критерия **Тип**);
- **заканчивается на** (недоступно для критерия **Тип**);
- **содержит** (недоступно для критерия **Тип**).

Для того чтобы изменить порядок выражений, нажмите и удерживайте иконку и перетащите выражение. Для того чтобы удалить выражение, нажмите на иконку .

Вы можете сохранить и экспортировать существующий запрос, чтобы воспользоваться им позднее или импортировать уже существующий запрос. Все эти действия можно выбрать из выпадающего списка после нажатия на иконку .

## Редактирование настроек сетевого устройства

Для того чтобы отредактировать сетевое устройство, нажмите на строку в таблице с названием нужного сетевого устройства. На открывшейся странице можно изменить все параметры сетевого устройства.

## Клонирование сетевого устройства

Для того чтобы создать копию определенного сетевого устройства, нажмите **Клонировать**. После этого вам будет предложено отредактировать скопированное сетевое устройство.

Также в режиме редактирования сетевого устройства вы можете в конце страницы нажать кнопку **Клонировать**.

## Удаление сетевого устройства

Для того чтобы удалить сетевое устройство, нажмите **Удалить**. После этого подтвердите удаление.

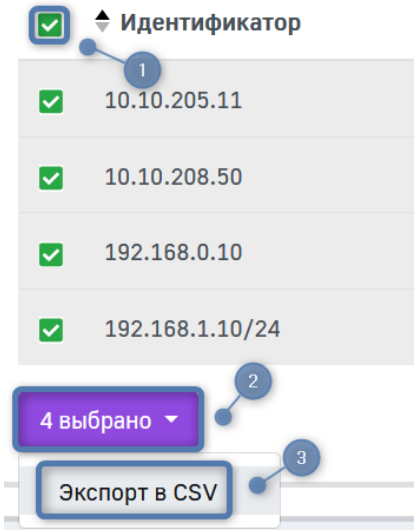
Также в режиме редактирования сетевого устройства вы можете в конце страницы нажать кнопку **Удалить**. После этого подтвердите удаление.

## Очистка кэша

Для того чтобы удалить временный кэш, хранящий в себе полученную по SNMP информацию, нажмите кнопку .

## Групповые действия

Для того чтобы выполнить действия с несколькими сетевыми устройствами, отметьте необходимые сетевые устройства. Чтобы выполнить действия со всеми сетевыми устройствами в списке, нажмите на селектор в шапке таблицы.




На данный момент единственное доступное групповое действие в системе — **Экспорт в CSV**. При его выборе, файл в формате **.csv**, содержащий записи таблицы, попадает в менеджер загрузки вашего браузера.

## Импорт сетевых устройств

Подробнее об импорте сетевых устройств вы можете прочитать здесь.

---

ID статьи: 1930
Последнее обновление: 15 янв., 2026
Обновлено от: Ильина В.
Ревизия: 8
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.2.0 -> AxelNAC. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Политики и контроль доступа» -> Страница «Сетевые устройства» -> Вкладка «Сетевые устройства»
https://docs.axel.pro/entry/1930/