

Вкладка «Группы сетевых устройств»

На данной вкладке создаются группы сетевых устройств, содержащие настройки для сетевых устройств этой группы.

По умолчанию в таблице отображаются 4 столбца:

- **Идентификатор** — имя группы сетевых устройств;
- **Описание** — описание группы сетевых устройств;
- **Тип** — профиль сетевых устройств в группе;
- **Режим** — режим работы сетевых устройств в группе.

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**, **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 новой группы сетевых устройств

Для того чтобы создать новое сетевое устройство, нажмите **Новая группа сетевых устройств** в левом верхнем углу страницы. После этого откроется меню конфигурации группы сетевых устройств.

Определение

На данной вкладке можно указать глобальные настройки коммутатора для сетевого оборудования.

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

1. **Идентификатор** — идентификатор группы сетевых устройств, который будет отображаться в таблице со списком всех групп сетевых устройств;
2. **Описание** — описание группы сетевых устройств, которое будет отображаться в таблице со списком всех групп 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 сетевых устройств в группе. 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. **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 ;
 - **RADIUS** — команда на реаутентификацию передается по протоколу RADIUS;
 - **HTTP** — команда на реаутентификацию передается по протоколу HTTP;

- **HTTPS** — команда на реаутентификацию передается по протоколу HTTPS.
- 6. **Реоутентификация на предыдущем сетевом устройстве** — данный параметр позволяет отправлять команду на реаутентификацию сессии устройства или пользователя на сетевых устройствах данной группы, если MAC-адрес был ранее определен на другом сетевом устройстве, контролируемом AxelNAC;
- 7. **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 +);
- 8. **Обеспечение работы внешнего портала** — принудительно использовать внешний портал для регистрации, если это поддерживается сетевым оборудованием;
- 9. **VoIP** — задает отправку особых RADIUS-атрибутов для назначения Voice VLAN для устройств, для которых активирован параметр VoIP;
- 10. **Обнаружение VoIP LLDP** — автоматическое задание атрибута VoIP для сетевых устройств на основе SNMP-запросов в LLDP MIB;
- 11. **Обнаружение VoIP CDP** — автоматическое задание атрибута VoIP для сетевых устройств на основе SNMP-запросов в CDP MIB;
- 12. **Обнаружение VoIP DHCP** — автоматическое задание атрибута VoIP для сетевых устройств на основе отпечатка DHCP;
- 13. **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 данной группы сетевых устройств.

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 роли из Downloadable ACL. 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 вписываются 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.

Определение
2
Роли
Режим Inline
RADIUS
SNMP
CLI
Веб-службы
Базовый режим

1

Версия

v1

2

Community Read

public

3

Community Write

private

4

Engine ID

5

User Name Read

6

Auth Protocol Read

7

Auth Password Read

8

Priv Protocol Read

9

Priv Password Read

10

User Name Write

11

Auth Protocol Write

12

Auth Password Write

13

Priv Protocol Write

14

Priv Password Write

15

Версия Trap

v1

16

Community Trap

public

17

User Name Trap

18

Auth Protocol Trap

19

Auth Password Trap

20

Priv Protocol Trap

21

Priv Password Trap

22

Максимальное количество MAC-адресов

30

Максимальное число MAC-адресов, получаемых от порта.

23

Интервал ожидания

2

Интервал ожидания между запросами MAC-адресов.

Создать

Сбросить

Отмена

В данном меню доступны следующие настройки:

- Версия** — версия протокола SNMP (v1, v2c, v3), используемая для обмена данными;
- Community Read** — строка сообщества SNMP, которая предоставляет доступ для чтения к данным устройства в SNMPv1 и SNMPv2;
- Community Write** — строка сообщества SNMP, которая предоставляет доступ для записи данных устройства в SNMPv1 и SNMPv2;
- Engine ID** — идентификатор механизма аутентификации в SNMPv3;
- User Name Read** — имя пользователя для чтения данных в SNMPv3;
- Auth Protocol Read** — используемый протокол аутентификации (MD5, SHA) для чтения в SNMPv3;
- Auth Password Read** — пароль аутентификации для чтения в SNMPv3;
- Priv Protocol Read** — используемый протокол шифрования (DES, AES) для чтения SNMPv3;
- Priv Password Read** — пароль шифрования для чтения в SNMPv3;
- User Name Write** — имя пользователя для записи данных в SNMPv3;
- Auth Protocol Write** — используемый протокол аутентификации для записи в SNMPv3;
- Auth Password Write** — пароль аутентификации для записи в SNMPv3;
- Priv Protocol Write** — используемый протокол шифрования для записи в SNMPv3;
- Priv Password Write** — пароль шифрования для записи в SNMPv3;
- Версия Trap** — версия протокола SNMP (v1, v2c, v3), используемая для SNMP Trap-сообщений;
- Community Trap** — строка сообщества для приема SNMP Trap-сообщений в SNMP v1/v2c;
- 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 подключения к устройствам группы 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 подключения к устройствам группы 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 безопасной передачи данных между веб-браузером и сервером.
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**. Для того чтобы сбросить введенные параметры на стандартные значения, нажмите **Сбросить**. Для того чтобы вернуться на предыдущую страницу без сохранения выполненных на странице действий, нажмите **Отменить**.

Элементы

На данной вкладке можно увидеть сетевые устройства, входящие в эту группу. Данная вкладка появляется при просмотре

уже существующей группы.

Текущие элементы

Список сетевых устройств, находящихся в этой группе. На них распространяются настройки, которые указаны в группе. В таблице отображаются следующие поля:

- **Идентификатор** — имя группы сетевых устройств;
- **Описание** — описание группы сетевых устройств;
- **Тип** — профиль сетевых устройств в группе.

Новый элемент

Поле добавления устройства, принадлежащего другой группе. Для добавления устройства в эту группу введите его название или выберите его из выпадающего списка, после чего нажмите кнопку Добавить новый элемент. Устройство удаляется из предыдущей группы и переносится в таблицу **Текущие элементы**.

При добавлении в новую группу настройки новой группы применяются к устройству и полностью перезаписывают все настройки устройства.

Поиск группы сетевых устройств

Для того чтобы найти определенную группу сетевых устройств, можно выполнить поиск по критериям: **Идентификатор**, **Описание**, **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 группы сетевых устройств;
- **Описание** — поиск по описанию группы сетевых устройств;
- **Режим** — поиск по режиму, выбранному для группы сетевых устройств;
- **Тип** — поиск по типу, выбранному для группы сетевых устройств.

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 группы сетевых устройств

Для того чтобы отредактировать группу сетевых устройств, нажмите на строку в таблице с названием нужной группы сетевых устройств. На открывшейся странице можно изменить все параметры группы сетевых устройств.

Клонирование группы сетевых устройств

Для того чтобы создать копию определенной группы сетевых устройств, нажмите **Клонировать**. После этого вам будет предложено отредактировать скопированную группу сетевых устройств.

Также в режиме редактирования группы сетевых устройств вы можете в конце страницы нажать кнопку **Клонировать**.

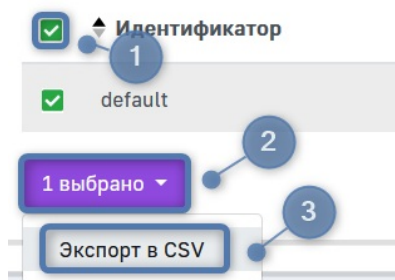
Удаление группы сетевых устройств

Для того чтобы удалить группы сетевых устройств, нажмите **Удалить**. После этого подтвердите удаление.

Также в режиме редактирования группы сетевых устройств вы можете в конце страницы нажать кнопку **Удалить**. После этого подтвердите удаление.

Групповые действия

Для того чтобы выполнить действия с несколькими группами сетевых устройств, отметьте необходимые группы сетевых устройств. Чтобы выполнить действия со всеми группами сетевых устройств 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.

Импортировать групп сетевых устройств

Подробнее об импорте вы можете прочитать [здесь](#).

ID статьи: 1931

Последнее обновление: 15 янв., 2026

Обновлено от: Ильина В.

Ревизия: 5

База знаний AxelNAS -> Документация -> Система контроля доступа к сети «AxelNAS». Версия 2.2.0 -> AxelNAS. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Политики и контроль доступа» -> Страница «Сетевые устройства» -> Вкладка «Группы сетевых устройств»

<https://docs.axel.pro/entry/1931/>