Раздел «Политики и контроль доступа»

При подключении конечного устройства к сети AxelNAC необходимо иметь возможность назначить ему или его пользователю роль. Затем эта роль может транслироваться во VLAN, набор ACL, идентификатор политики производителя коммутатора или в комбинацию всего этого.

В данном разделе доступны следующие страницы:

1. **Роли**: сущность, которую можно присвоить сессии пользователя или устройства по результатам правил аутентификации или назначить явно пользователю или узлу. Внутри себя может содержать назначаемые VLAN, ACL и т.д. Настройки ролей могут быть уточнены или переопределены на уровне сетевых устройств или групп сетевых устройств, поэтому рекомендуется создавать глобальные роли, например **Телефоны**, **Администраторы**, **Пользователи**, **Принтеры** и т.д.
2. **Домены**: если вы хотите аутентифицировать пользователей или компьютеры по доменному логину и паролю, используя протоколы **PEAP** и **EAP-MSCHAPv2**, необходимо настроить интеграцию сервера AxelNAC с контроллерами домена. Каждый сервер AxelNAC должен быть введен в домен индивидуально.
3. **Источники аутентификации**: источники аутентификации содержат в себе настройки по взаимодействию с внешними хранилищами учетных данных пользователей. Каждый источник содержит в себе правила авторизации, задающие критерии, и результирующие действия, применяемые к сессии подключаемого устройства/пользователя.
4. **Сетевые устройства**: для работы AxelNAC к нему необходимо подключить конечные сетевые устройства: коммутаторы, WiFi-контроллеры или точки доступа, VPN-шлюзы, на которых будут контролироваться подключение пользователей и/или устройств. В данном разделе вы можете настроить интеграцию с этими устройствами и настроить/переопределить назначение VLAN, ACL или политик по ролям.
5. **Профили подключения**: профили подключения позволяют задать параметры для управления подключениями, включая выбор протокола (например, **TCP/IP** или **VPN**) и коммутатора. Они также определяют список источников аутентификации, где происходит поиск пользователей или устройств для проверки их прав доступа. Также можно задать другие настройки, такие как: работа сканера, логика работы Captive-портала и т.д.

Для правильной работы AxelNAC рекомендуется выполнять настройки в следующем порядке:
1. Источники аутентификации.
2. Области.
3. Роли.
4. Домены Active Directory.
5. Сетевые устройства.
6. Профили подключения.

ID статьи: 237
Последнее обновление: 13 мая, 2025
Обновлено от: Егоров В.
Ревизия: 7
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 1.0.0 -> AxelNAC. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Политики и контроль доступа» -> Раздел «Политики и контроль доступа»
https://docs.axel.pro/entry/237/