

В данной статье описано, как настроить источник аутентификации eDirectory для аутентификации и авторизации пользователей. Этот метод аутентификации использует каталог LDAP для хранения учетных данных пользователей.

Создание нового источника аутентификации Edirectory

Для того чтобы создать новый источник аутентификации Edirectory, нажмите **Новый внутренний источник** в левом верхнем углу таблицы. После этого откроется меню конфигурации нового источника.

Новый источник аутентификации **Edirectory** ✕

1

Имя

Требуется указать имя.

2

Описание

3

Хост

389

Нет

4

Таймер недоступности

60

Данный параметр определяет, сколько секунд сервер должен быть отмечен как недоступный перед повторным обращением к нему. При указании нескольких LDAP-серверов или DNS-имени, указывающего на несколько IP-адресов, этот параметр может быть использован для обеспечения более последовательного обхода отказа. Значение 0 отключает эту функцию.

5

Таймаут подключения

1

Таймаут LDAP-подключения.

6

Таймаут запроса

5

Таймаут LDAP-запроса.

7

Таймаут отклика

10

Таймаут LDAP-отклика.

8

Базовое DN

9

Область применения

Subtree

10

Атрибут имени пользователя

Основной SAML-атрибут, содержащий имя пользователя.

11

Прочие атрибуты

Прочие атрибуты, которые могут быть использованы как имя пользователя (для применения изменений необходимо перезапустить службу radiusd).

12

Имя атрибута электронной почты

mail

Имя атрибута LDAP, содержащего адрес электронной почты, по которому будет производиться фильтрация.

13

Привязать DN

Оставьте это поле пустым, если вы хотите выполнить анонимную привязку.

14

Пароль

Тест

15

Кэшировать соответствия правилу

☐

При активации данного параметра AxelNAC кэширует результаты, где есть соответствие правилу.

16

Отслеживать

☒

Хотите ли вы отслеживать этот источник

17

Случайное подключение

☐

Выбрать LDAP-сервер для запроса случайным образом.

18

Связанные области

Области, которые будут связаны с данным источником.

19

Правила аутентификации

Добавить правило

20

Правила администрирования

Добавить правило

Создать

Сбросить

Отмена

В данном меню доступны следующие настройки:

1. **Имя** — имя источника аутентификации, которое будет отображаться в таблице со списком всех источников аутентификации. Задается при создании источника и не может быть изменено в дальнейшем;
2. **Описание** — описание источника аутентификации, которое будет отображаться в таблице со списком всех источников аутентификации;
3. **Хост** — адрес сервера, на котором развернута служба **eDirectory**. В полях справа можно указать порт, по которому происходит взаимодействие AxelNAC и Active Directory, который можно посмотреть [здесь](#). Также можно указать метод шифрования соединения, если он требуется. При выборе метода шифрования необходимо настроить соответствующие

поля на вкладке **Сертификаты**;

4. **Таймер недоступности** — данный параметр определяет, сколько секунд сервер должен быть отмечен как недоступный перед повторным обращением к нему. При указании нескольких LDAP-серверов или DNS-имени, указывающего на несколько IP-адресов, этот параметр может быть использован для обеспечения более последовательного обхода отказа. Значение 0 отключает эту функцию;
5. **Таймаут подключения** — максимальное время ожидания установления LDAP-соединения перед его разрывом. Используется для предотвращения зависания процессов при недоступности сервера;
6. **Таймаут запроса** — максимальное время ожидания выполнения LDAP-запроса перед его прерыванием. Позволяет ограничить время обработки сложных или неэффективных запросов;
7. **Таймаут отклика** — период, в течение которого система ожидает LDAP-отклика после отправки запроса. Применяется для предотвращения зависания соединений в случае задержек со стороны сервера;
8. **Базовое DN** — начальная точка в дереве каталога eDirectory, с которой начинается поиск учетных записей. Определяет область видимости поиска пользователей;
9. **Область применения** — определяет, какие группы или подразделения каталога eDirectory будут использоваться для аутентификации. Возможные варианты:
 - **Base object** ; — базовый объект, без учета дочерних объектов;
 - **One-level** — ближайшие дочерние объекты указанного объекта;
 - **Subtree** — все дочерние объекты **Базового DN**, включая вложенные;
 - **Children** — домен, который находится в дереве пространства имен под другим доменом (родительским), и в своем названии содержит имя родителя.
10. **Атрибут имени пользователя** — основной SAML-атрибут, содержащий имя пользователя;
11. **Прочие атрибуты** — прочие атрибуты, которые могут быть использованы как имя пользователя (для применения изменений необходимо перезапустить службу **radius-auth.service**);
12. **Имя атрибута электронной почты** — имя атрибута LDAP, содержащего адрес электронной почты, по которому будет производиться фильтрация;
13. **Привязать DN** — учетная запись (**Distinguished Name**), используемая для аутентификации в службе каталога при поиске пользователей. Оставьте это поле пустым, если вы хотите выполнить анонимную привязку;
14. **Пароль** — учетные данные, необходимые для доступа к серверу eDirectory;
15. **Кэшировать соответствия правилу** — при активации данного параметра AxelNAC кэширует результаты, где есть соответствие правилу;
16. **Отслеживать** — включает логирование событий аутентификации и диагностику работы источника;
17. **Случайное подключение** — выбирает LDAP-сервер для запроса случайным образом при наличии нескольких серверов, что позволяет распределять нагрузку;
18. **Связанные области** — области, которые будут связаны с данным источником;
19. **Правила аутентификации** — набор условий, определяющих, каким образом клиент или устройство должно быть проверено перед предоставлением доступа к сети. Нажмите **Добавить правило**, чтобы добавить правило аутентификации. Заполните следующие поля:
 - **Статус** — активно ли правило;
 - **Имя** — имя правила;
 - **Описание** — описание правила;
 - **Оператор** — принцип проверки условий. Значение **ALL** указывает, что должны быть выполнены все перечисленные условия. Значение **ANY** указывает, что должно быть выполнено хотя бы одно правило;
 - **Условия** — набор критериев, используемых для проверки клиента. Количество условий неограниченно и может изменяться с помощью нажатия на иконки ➕ ➖. Каждое условие состоит из следующих элементов:
 - **Атрибут** — параметр, который будет проверяться;
 - **Оператор** — тип сравнения или проверки;
 - **Значение** — ожидаемое значение атрибута для выполнения условия.
 - **Действия** — определяют, что произойдет после успешного выполнения условия правила. Количество действий неограниченно и может изменяться с помощью нажатия на иконки ➕ ➖. Каждое действие состоит из следующих элементов:
 - **Тип** — вид результата. Возможные значения:
 - **Роль**;
 - **Период доступа без реавторизации**;
 - **Дата снятия с регистрации**;
 - **Баланс времени**;
 - **Баланс трафика**;
 - **Роль из источника**;
 - **Инициировать RADIUS MFA**;
 - **Инициировать порталную MFA**.
 - **Значение** — значение, соответствующее указанному типу.

При аутентификации пользователя в сети его имя будет проверяться на наличие в каталоге Active Directory на основе Атрибута имени пользователя или Прочих атрибутов.

20. **Правила администрирования** — набор условий, использующиеся для управления доступом администратора к системе на основе различных критериев. Позволяют настроить уровни доступа пользователей в зависимости от ролей, источников аутентификации и других параметров. Нажмите **Добавить правило**, чтобы добавить правило администрирования. Заполните следующие поля:
 - **Статус** — активно ли правило;
 - **Имя** — имя правила;
 - **Описание** — описание правила;
 - **Оператор** — принцип проверки условий. Значение **ALL** указывает, что должны быть выполнены все перечисленные условия. Значение **ANY** указывает, что должно быть выполнено хотя бы одно правило;
 - **Условия** — набор критериев, используемых для проверки клиента. Количество условий неограниченно и может изменяться с помощью нажатия на иконки ➕ ➖. Каждое условие состоит из следующих элементов:
 - **Атрибут** — параметр, который будет проверяться;
 - **Оператор** — тип сравнения или проверки;
 - **Значение** — ожидаемое значение атрибута для выполнения условия.

- **Действия** — определяют, что произойдет после успешного выполнения условия правила. Количество действий неограниченно и может изменяться с помощью нажатия на иконки ➖ ➕. Каждое действие состоит из следующих элементов:
 - **Тип** — вид результата. Возможные значения:
 - **Уровень доступа;**
 - **Срок предоставления спонсорского доступа;**
 - **Назначить роль спонсора.**
 - **Значение** — значение, соответствующее указанному типу.

При аутентификации пользователя в сети его имя будет проверяться на наличие в каталоге Active Directory на основе Атрибута имени пользователя или Прочих атрибутов.

Для того чтобы создать новый источник, 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**.

ID статьи: 1909

Последнее обновление: 8 июл., 2025

Обновлено от: Михалева А.

Ревизия: 1

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 «Источники аутентификации» -> Вкладка «Внутренние источники» -> Edirectory

<https://docs.axel.pro/entry/1909/>