

Active Directory

В данной статье описано, как настроить источник аутентификации с использованием каталога **Active Directory (AD)**. Это позволяет аутентифицировать пользователей через централизованный каталог, предоставляемый службой Microsoft Active Directory, обеспечивая гибкость и безопасность при управлении доступом к сети.

Создание нового источника аутентификации Active Directory

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

Основное

На данной вкладке указываются основные настройки источника аутентификации.

В правом верхнем углу названия вкладки **Основное** отображается количество оставшихся обязательных для заполнения полей.

Новый источник аутентификации **Active Directory**

Основное 1 Сертификаты

1. Имя Требуется указать имя.

2. Описание

3. Хост 399 Нет

4. Режим верификации SSL: **Нет**
Режим проверки SSL при подключении через LDAP. Применяется только при использовании Start TLS или LDAPS.

5. Таймер недоступности: **0**
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.

6. Таймаут подключения: **1**
Таймаут LDAP-подключения.

7. Таймаут запроса: **5**
Таймаут LDAP-запроса.

8. Таймаут отклика: **10**
Таймаут LDAP-отклика.

9. Базовое DN:

10. Область применения: **Subtree**

11. Атрибут имени пользователя: **sAMAccountName**
Основной SAML-атрибут, содержащий имя пользователя.

12. Прочие атрибуты:
Прочие атрибуты, которые могут быть использованы как имя пользователя (для применения изменений необходимо переместить службу таблиц).

13. Добавление поисковых атрибутов LDAP-фильтра:
Данные атрибуты будут добавлены к сгенерированному LDAP-фильтру, созданному для атрибутов поиска.

14. Имя атрибута электронной почты: **mail**
Имя атрибута LDAP, содержащего адрес электронной почты, по которому будет производиться факторинг.

15. Принимать DN: ☐
Оставьте это поле пустым, если вы хотите выполнять асинхронную проверку.

16. Пароль: **Тест**

17. Калибровка соответствия прав: ☐
При нахождении данного параметра Active Directory возвращает результаты, где есть соответствие праву.

18. Отключать: ☐
Включить или выключить этот источник.

19. Случайное подключение: ☐
Выбор LDAP-сервера для запроса случайным образом.

20. Секционная область:
Область, которая будет связана с данным источником.

21. Правила аутентификации:

22. Правила администрирования:

В данном меню доступны следующие настройки:

- 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;
- Описание** — описание источника аутентификации, которое будет отображаться в таблице со списком всех источников аутентификации;
- Хост** — доменное имя или IP-адрес контроллера домена Active Directory, используемого для аутентификации. Поддерживает указание нескольких серверов для отказоустойчивости. В полях справа можно указать порт, по которому происходит взаимодействие AxelNAC и Active Directory, который можно посмотреть [в данном разделе](#). Также можно указать метод шифрования соединения, если он требуется. При выборе метода шифрования необходимо настроить соответствующие поля на вкладке **Сертификаты**;
- Режим верификации SSL** — режим проверки SSL при подключении через LDAP. Применяется только при использовании Start TLS или LDAPS. Возможные варианты:
 - нет** — верификация не требуется;
 - optional** — в случае, если верификация не пройдена, соединение устанавливается, а в журналах выводится соответствующее сообщение;
 - require** — в случае, если верификация не пройдена, соединение не устанавливается.
- 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;
- Таймаут подключения** — максимальное время ожидания установления LDAP-соединения перед его разрывом. Используется для предотвращения зависания процессов при недоступности сервера;
- Таймаут запроса** — максимальное время ожидания выполнения LDAP-запроса перед его прерыванием. Позволяет ограничить время обработки сложных или неэффективных запросов;
- Таймаут отклика** — период, в течение которого система ожидает LDAP-отклика после отправки запроса. Применяется для предотвращения зависания соединений в случае задержек со стороны сервера;
- Базовое DN** — начальная точка (Distinguished Name) в дереве Active Directory, с которой начинается поиск учетных записей. Определяет область видимости поиска пользователей;
- Область применения** — определяет, какие группы или подразделения AD будут использовать этот источник аутентификации. Может применяться к отдельным подразделениям или ко всему каталогу. 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.
- Атрибут имени пользователя** — основной SAML-атрибут, содержащий имя пользователя. Используется для идентификации учетной записи при входе;
- Прочие атрибуты** — прочие атрибуты, которые могут быть использованы как имя пользователя (для применения

изменений необходимо перезапустить службу **radiusd-auth.service**);

13. **Добавление поисковых атрибутов LDAP-фильтра** — данные атрибуты будут добавлены к сгенерированному LDAP-фильтру, созданному для атрибутов поиска;
14. **Имя атрибута электронной почты** — имя атрибута LDAP, содержащего адрес электронной почты, по которому будет производиться фильтрация;
15. **Привязать DN** — учетная запись (**Distinguished Name**), используемая для аутентификации в службе AD при поиске пользователей. Оставьте это поле пустым, если вы хотите выполнить анонимную привязку;
16. **Пароль** — пароль учетной записи, указанной в поле **Привязать DN**, для выполнения запросов к AD;
17. **Кэшировать соответствия правилу** — при активации данного параметра программа кэширует результаты, где есть соответствие правилу. Это снижает нагрузку на сервер и ускоряет повторные проверки;
18. **Отслеживать** — включает логирование событий аутентификации и диагностику работы источника;
19. **Случайное подключение** — выбирает LDAP-сервер для запроса случайным образом при наличии нескольких серверов, что позволяет распределять нагрузку;
20. **Связанные области** — области, которые будут связаны с данным источником;
21. **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**;
 - **Задать роль по *не найдено***.
 - **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**.

22. **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**.

Сертификаты

На данной вкладке указываются необходимые для работы данного источника сертификаты.

В данном меню доступны следующие настройки:

1. **Файл сертификата клиента** — файл, содержащий путь к сертификату клиента (если требуется сертификат клиента).
2. **Файл ключа клиента** — файл, содержащий путь к ключу клиента (если требуется сертификат клиента).
3. **Файл СА** — файл, содержащий путь к файлу с дополнительными центрами сертификации.

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: 1905

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» -> Active Directory

<https://docs.axel.pro/entry/1905/>