OpenID

В данной статье описано, как настроить источник аутентификации с использованием протокола **OpenID Connect (OIDC)**. Этот метод позволяет пользователям входить в систему, используя учетные записи внешнего OpenID-провайдера.

Создание нового источника аутентификации OpenID

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

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. **ID приложения** — уникальный идентификатор OAuth 2.0-клиента, используемый для взаимодействия с OpenID-провайдером;
4. **Секретная фраза приложения** — секретный ключ, необходимый для безопасного обмена данными между AxelNAC и OpenID API;
5. **Адрес API** — базовый URL-адрес OpenID API, используемый для выполнения запросов аутентификации;

6. **Путь авторизации API** — URL-адрес конечной точки OpenID, на который отправляется запрос для аутентификации пользователя;
7. **Путь к токену API** — URL-адрес конечной точки, по которому приложение запрашивает токен доступа после успешной аутентификации;
8. **Область применения** — запрашиваемые приложением разрешения;
9. **API URL зарегистрированного пользователя** — URL-адрес API, по которому можно получить информацию о пользователе после успешной аутентификации;
10. **URL портала** — адрес веб-портала, где будет использоваться данный источник аутентификации. Имя хоста должно совпадать с именем вашего Captive-портала;
11. **Авторизованные домены** — список разрешенных доменов, разделенный запятыми;
12. **Создать локальную учетную запись** — при активации данного параметра в системе AxelNAC будет создана локальная учетная запись на основании указанного имени пользователя;
13. **Метод хэширования паролей базы данных** — алгоритм, используемый для хэширования паролей в базе данных. Влияет только на вновь созданные и сброшенные пароли;
14. **Длина пароля** — длина генерируемого пароля;
15. **Количество входов в систему для локальной учетной записи** — число раз, сколько локальная учетная запись может быть использована после ее создания. Значение 0 отключает ограничение;
16. **Истечение срока действия локальной учетной записи** — время прекращения действия локальной учетной записи. При значении 0 будет применяться период доступа без реавторизации, указанный в правилах аутентификации для данного пользователя;
17. **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 портальную MFA**.
        - **Значение** — значение, соответствующее указанному типу.
18. **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.**
        - **Значение** — значение, соответствующее указанному типу.
19. **Сопоставления пользователей** — механизм, позволяющий связать учетные записи OpenID с локальными учетными записями в системе. Нажмите **Добавить сопоставление**, чтобы добавить правило администрирования. Заполните поля, чтобы создать сопоставление.
20. **Атрибут имени пользователя** — основной SAML-атрибут, содержащий имя пользователя.

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: 1076
Последнее обновление: 8 июл., 2025
Обновлено от: Ильина В.
Ревизия: 1

https://docs.axel.pro/entry/1076/