

# SMS

В данной статье описано, как настроить источник аутентификации для гостевой аутентификации с использованием SMS-сообщений. При таком методе аутентификации на указанный номер будет отправлено сообщение с PIN-кодом для завершения регистрации пользователя и получения доступа к сети.

## Создание нового источника аутентификации SMS





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

### Новый источник аутентификации SMS ✕

- Имя**  !  
Требуется указать имя.
- Описание**
- SMS-шлюз**
- Таймаут активации по SMS**  минут  
Данный параметр определяет промежуток времени, предоставляемый гостю, который зарегистрировался с использованием SMS-подтверждения, на ввод PIN-кода.
- SMS-сообщение (\$pin будет заменен на PIN-код)**
- Длина PID**   
Количество цифр в PIN-коде.
- Создать локальную учетную запись**  Нет  
Создайте локальную учетную запись в системе AxelNAC на основании указанного имени пользователя.
- Метод хэширования паролей базы данных**   
Алгоритм, используемый для хэширования паролей в базе данных. Влияет только на вновь созданные и сброшенные пароли.
- Длина пароля**   
Длина генерируемого пароля.
- Количество входов в систему для локальной учетной записи**   
Число раз, сколько локальная учетная запись может быть использована после ее создания. Значение 0 устанавливает бесконечное число раз.
- Истечение срока действия локальной учетной записи**  секунд  
Время прекращения действия локальной учетной записи. При значении 0 будет применяться период доступа без реавторизации, указанный в правилах аутентификации для данного пользователя.
- Правила аутентификации**

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;
- SMS-шлюз** — шлюз, с помощью которого AxelNAC отправляет SMS-сообщение;
- Таймаут активации по SMS** — данный параметр определяет промежуток времени, предоставляемый гостю, который зарегистрировался с использованием SMS-подтверждения, на ввод PIN-кода;
- SMS-сообщение** — укажите текст SMS-сообщения, которое будет отправлено пользователю. Значение **\$pin** будет заменено на сгенерированный PIN-код в отправленном сообщении;

6. **Длина PID** — укажите количество цифр в PIN-коде;
7. **Создать локальную учетную запись** — данный параметр определяет, будет ли создана локальная учетная запись в AxelNAC для пользователя-гостя;
8. **Метод хэширования паролей базы данных** — алгоритм, используемый для хэширования паролей в базе данных. Влияет только на вновь созданные и сброшенные пароли. Рекомендуемое значение — **Vcrypt**;
9. **Длина пароля** — укажите количество символов в генерируемом пароле для учетной записи;
10. **Количество входов в систему для локальной учетной записи** — число раз, сколько локальная учетная запись может быть использована после ее создания. Значение 0 отключает ограничение;
11. **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;
12. **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.

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: 1077

Последнее обновление: 29 сент., 2025

Обновлено от: Ильина В.

Ревизия: 3

База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.1.0 -> AxelNAC. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Политики и контроль доступа» -> Страница «Источники аутентификации» -> Вкладка «Внешние источники» -> SMS

<https://docs.axel.pro/entry/1077/>