

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** ✕

1

Имя

Требуется указать имя.

2

Описание

3

SMS-шлюз

4

Таймаут активации по SMS

10

минут

Данный параметр определяет промежуток времени, предоставляемый гостю, который зарегистрировался с использованием SMS-подтверждения, на ввод PIN-кода.

5

SMS-сообщение (\$pin будет заменен на PIN-код)

PIN: \$pin

6

Длина PID

6

Количество цифр в PIN-коде.

7

Создать локальную учетную запись

☐

Нет

Создайте локальную учетную запись в системе AxelNAC на основании указанного имени пользователя.

8

Метод хэширования паролей базы данных

NTLM

Алгоритм, используемый для хэширования паролей в базе данных. Влияет только на вновь созданные и сброшенные пароли.

9

Длина пароля

8

Длина генерируемого пароля.

10

Количество входов в систему для локальной учетной записи

0

Число раз, сколько локальная учетная запись может быть использована после ее создания. Значение 0 устанавливает бесконечное число раз.

11

Истечение срока действия локальной учетной записи

0

секунд

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

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. **SMS-шлюз** — шлюз, с помощью которого AxelNAC отправляет SMS-сообщение;
4. **Таймаут активации по SMS** — данный параметр определяет промежуток времени, предоставляемый гостю, который зарегистрировался с использованием SMS-подтверждения, на ввод PIN-кода;
5. **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 AxelINAC 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 — **Bcrypt**;
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: 1923

Последнее обновление: 29 сент., 2025

Обновлено от: Ильина В.

Ревизия: 4

База знаний AxelINAC -> Документация -> Система контроля доступа к сети «AxelINAC». Версия 2.2.0 -> AxelINAC. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Политики и контроль доступа» -> Страница «Источники аутентификации» -> Вкладка «Внешние источники» -> SMS

<https://docs.axel.pro/entry/1923/>