Гостевой доступ с использованием SMS-аутентификации

В данной статье описано, как разрешить пользователям-гостям регистрировать свои устройства, используя номер своего сотового телефона. При таком методе аутентификации на указанный номер сотового телефона будет отправлено SMS с PIN-кодом для доступа к сети. Данное SMS-сообщение будет отправлено AxelNAC с помощью различных VoIP GSM-шлюзов (SMS-шлюзов).

Интеграция с SMS-шлюзом

Для создания интеграции с SMS-шлюзами пользователь должен иметь роль **Администратор** или обладать правами **SMS_GATEWAY_CREATE**, **SMS_GATEWAY_READ**, **SMS_GATEWAY_UPDATE**, **SMS_GATEWAY_DELETE**, **SMS_SEND_METHOD_AVAILABLE**, **DEFAULT_SEND_METHOD_SMS** и **System - Create**.

Для настройки интеграции с SMS-шлюзами с типом **SMSC** понадобится активный аккаунт в системе **SMSC.ru**.

Для того чтобы выполнить интеграцию AxelNAC с SMS-шлюзом, выполните следующие действия:

Шаг 1. Перейдите в раздел **Конфигурация → Интеграция → SMS-шлюзы** и нажмите **Новый SMS-шлюз**.

Шаг 2. В открывшемся окне конфигурации заполните следующие поля:

- **Имя** — укажите имя SMS-шлюза, которое будет отображаться в системе;
- **Тип** — выберите тип SMS-шлюза:
  - **SMSC** — при выборе данного значения может быть настроена интеграция с SMTP-to-SMS-службой SMSC.ru;
  - **Yeastar TG** — при выборе данного значения может быть настроена интеграция с SMS-шлюзами Yeastar TG, а также будут предзаполнены стандартные значения **типа**, **адреса** и **шаблона запроса к API** шлюзов, произведенных компанией Yeastar;
  - **Пользовательское** — при выборе данного значения может быть настроена интеграция с SMS-шлюзами, не проверенными в системе.
- **Тип API** — укажите метод API-запроса:
  - **Email2sms** — при выборе данного значения все запросы будут отправляться с помощью метода Email2SMS API;
  - **GET** — при выборе данного значения все запросы будут отправляться с помощью метода GET.
- **Имя пользователя** — укажите логин для доступа к выбранному SMS-шлюзу/провайдеру;
- **Пароль** — укажите пароль для доступа к выбранному SMS-шлюзу/провайдеру;
- **Параметры, специфичные для метода Email2sms:**
  - **Шаблон Email-адреса API** — укажите шаблон, в который будут подставляться значения для доступа к API;
  - **Шаблон темы письма** — укажите шаблон, в который будут подставляться значения для заполнения темы письма;
  - **Шаблон содержимого письма** — укажите шаблон, в который будут подставляться значения для заполнения содержимого письма.
- **Параметры, специфичные для метода GET:**
  - **Адрес API** — укажите адрес, по которому будет осуществляться доступ к API;
  - **Шаблон запроса к API** — укажите шаблон API-запроса, в который будут подставляться значения перед отправкой;
  - **Отправка учетных данных** — данный параметр определяет, будет ли данный SMS-шлюз использоваться для отправки учетных данных и PIN-кодов.

Сохраните новую интеграцию, нажав **Создать**.

Гостевой доступ с самостоятельной регистрацией пользователей

Функционал AxelNAC позволяет позволяет предоставить пользователям гостевой доступ к сети с их самостоятельной регистрацией. Для того чтобы настроить вашу системы для работы с таким сценарием, выполните действия, описанные ниже.

Добавление источника SMS-аутентификации

Для того чтобы добавить источник аутентификации, выполните следующие действия:

Шаг 1. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Источники аутентификации** и нажмите **Новый внешний источник**, после чего в выпадающем списке выберите **SMS**.

Шаг 2. В открывшемся окне конфигурации заполните следующие поля:

- **Имя** — укажите имя источника аутентификации, которое будет отображаться в системе;
- **Описание** — укажите описание для источника аутентификации, которое будет отображаться в системе;
- **SMS-шлюз** — выберите SMS-шлюз, интеграцию с которым вы настроили в предыдущем разделе;
- **Таймаут активации по SMS** — укажите время, которое предоставляется пользователю на ввод PIN-кода, полученного по SMS;
- **SMS-сообщение** — укажите текст SMS-сообщения, которое будет отправлено пользователю. Значение **$pin** будет заменено на сгенерированный PIN-код в отправленном сообщении;
- **Длина PID** — укажите количество цифр в PIN-коде;

- **Создать локальную учетную запись** — данный параметр определяет, будет ли создана локальная учетная запись в AxelNAC для пользователя-гостя;
- **Метод хэширования паролей базы данных** — укажите алгоритм, который будет использоваться для хэширования паролей в базе данных. Рекомендуемое значение — **Bcrypt**;
- **Длина пароля** — укажите количество символов в генерируемом пароле для учетной записи;
- **Количество входов в систему для локальной учетной записи** — укажите число разрешенных входов в систему для созданной локальной учетной записи до ее деактивации;
- **Истечение срока действия локальной учетной записи** — укажите промежуток времени, по истечении которого созданная локальная учетная запись будет деактивирована.

Шаг 3. Нажмите **Добавить правило** в строке **Правила аутентификации** и назовите его **catchall**. В качестве действий установите следующие параметры:

- **Роль** — укажите роль, которая будет выдаваться пользователю;
- **Срок предоставления доступа** — укажите срок, на который пользователю будет предоставлен доступ.

Сохраните новый источник аутентификации, нажав **Создать**.

Настройка профиля подключения

После того, как вы создали источник аутентификации, необходимо добавить его в профиль подключения. Выполните следующие действия:

Шаг 1. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Профили подключения** и кликните по профилю, который вы хотите использовать, либо создайте новый нажав **Новый профиль подключения**.

Шаг 2. Настройте профиль подключения под свои предпочтения и политики сетевой безопасности.

Шаг 3. В строке Источники нажмите **Добавить источник** и выберите источник, созданный в предыдущем разделе, из выпадающего списка.

Шаг 4. Сохраните профиль подключения.

Captive-портал, связанный с профилем подключения, можно просмотреть в любой момент. Для этого нажмите **Предпросмотр** рядом с названием подключения.

Проверка работы подключения

Для того чтобы проверить работу подключения, выполните следующие действия:

Шаг 1. Отключите и снимите с регистрации клиентское устройство.

Шаг 2. Снова подключите клиентское устройство к сети. При правильной конфигурации, должен появиться Captive-портал с новой опцией регистрации по SMS.

Шаг 3. Пройдите регистрацию с помощью номера телефона и убедитесь, что на указанный номер пришло SMS с PIN-кодом.

Шаг 4. Введите полученный PIN-код на Captive-портале и убедитесь, что вы получили доступ к сети.

Отправка учетных данных в SMS-сообщении с помощью API в ручном режиме описана здесь.

Гостевой доступ с предварительной регистрацией пользователей

Также AxelNAC предоставляет возможность предварительно зарегистрировать гостевую учетную запись для доступа к сети и отправить учетные данные по SMS. Для этого выполните следующие действия:

Шаг 1. Перейдите в раздел **Пользователи → Создать**.

Шаг 2. В открывшемся окне заполните все необходимые данные для пользователя (имя пользователя, пароль, номер телефона, политика доступа).

Шаг 3. Активируйте параметр **Отправить учетные данные по SMS** .

Шаг 4. В появившемся поле SMS-шлюз выберите SMS-шлюз, через который вы хотите выполнить отправку учетных данных.

После этого нажмите **Создать**, чтобы сохранить изменения и отправить учетные данные на номер телефона, указанный в профиле пользователя.

ID статьи: 932
Последнее обновление: 23 янв., 2026
Обновлено от: Михалева А.
Ревизия: 12