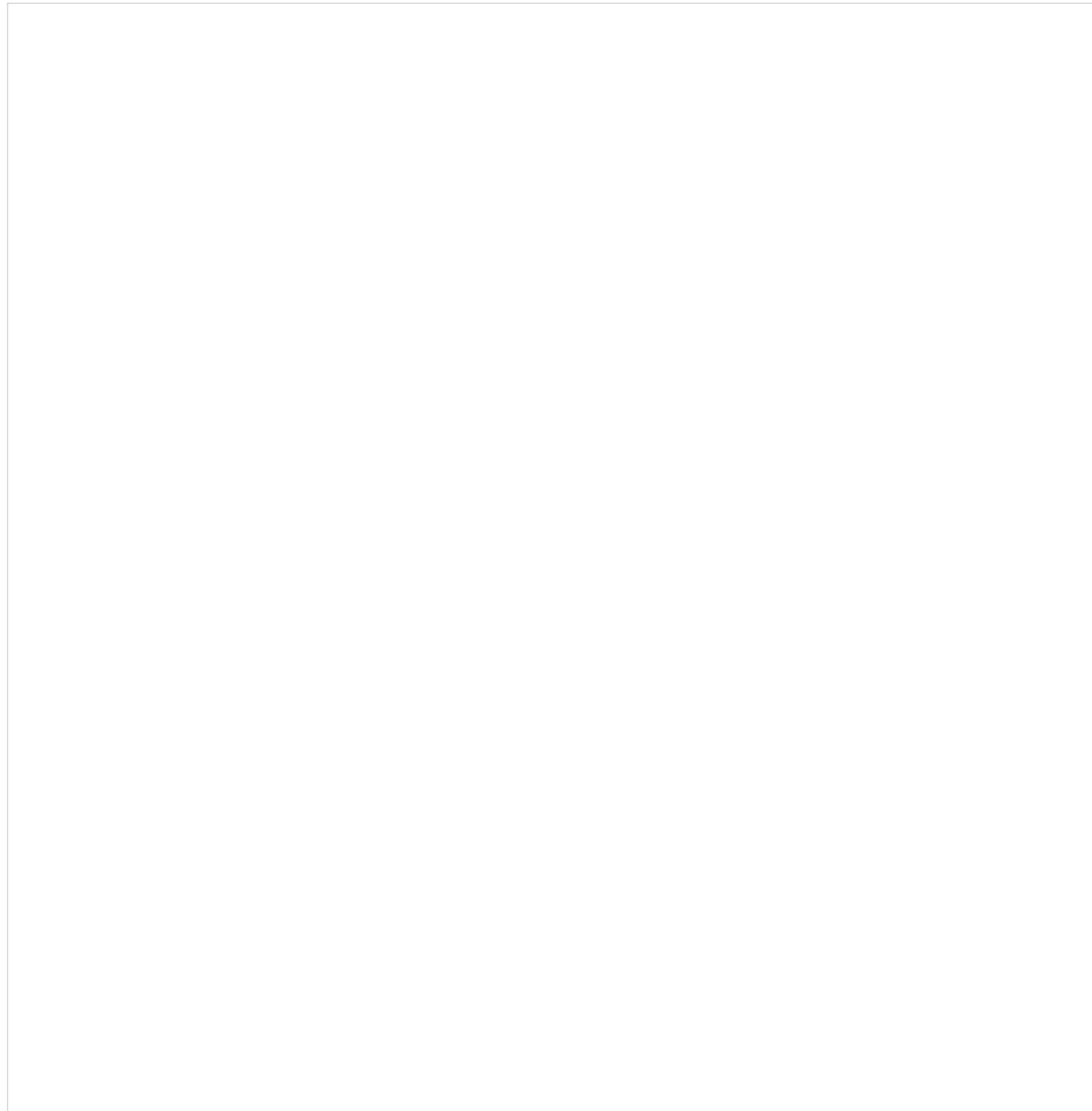


Sponsor

В данной статье описано, как разрешить пользователям-гостям регистрировать свои устройства с помощью запроса доступа у пользователя-спонсора. При таком методе аутентификации пользователь-гость получит доступ к сети после согласования запроса пользователем-спонсором.

Создание нового источника аутентификации Sponsor

Для того чтобы создать новый источник аутентификации Sponsor 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. **Связанные источники аутентификации** — источники, которые будут связаны с этим источником (для реализации спонсорского доступа). Выбирать можно только источники, способные работать с адресом электронной почты;
4. **Запрещенные домены** — домены, запрещенные для регистрации электронной почты. Допускается использование подстановочных знаков (*axelhac.org). Запрещенные домены проверяются перед разрешенными;

5. **Разрешенные домены** — домены, разрешенные для регистрации электронной почты. Допускается использование подстановочных знаков (*axelnac.org). Разрешенные домены проверяются после запрещенных;
6. **Таймаут ссылки активации** — данный параметр определяет промежуток времени, предоставляемый спонсору на вход в почту и переход по ссылке активации;
7. **Разрешить локальный домен** — при активации данного параметра разрешается самостоятельная регистрация из локального домена с указанием адреса электронной почты;
8. **Заменить хост в ссылке активации** — данное значение устанавливается для изменения имени хоста в ссылке валидации. Для применения изменений необходимо перезапустить службу **haproxy**;
9. **Спонсорский BCC** — адреса для отправки скрытой копии писем с запросом и подтверждением доступа. Список адресов разделяется запятой;
10. **Зарегистрировать при активации** — при отключении данного параметра пользователь-гость должен оставаться на портале, ожидая, пока спонсор подтвердит доступ;
11. **Обязательная аутентификация спонсора** — если параметр активен, спонсору необходимо аутентифицироваться на портале для валидации запроса пользователя-гостя;
12. **Язык** — язык, на котором будет отправлено письмо спонсору;
13. **Создать локальную учетную запись** — при активации данного параметра в системе AxeINAC будет создана локальная учетная запись на основании указанного имени пользователя;

Данная учетная запись, в случае, если при первичной регистрации данного источника аутентификации в качестве метода хэширования паролей базы данных были выбраны методы **Plaintext** или **NTLM**, позволяет пользователю аутентифицироваться через предустановленный источник local.

14. **Метод хэширования паролей базы данных** — алгоритм, используемый для хэширования паролей в базе данных. Влияет только на вновь созданные и сброшенные пароли;
15. **Длина пароля** — длина генерируемого пароля;
16. **Количество входов в систему для локальной учетной записи** — число раз, сколько локальная учетная запись может быть использована после ее создания. Значение 0 отключает ограничение;
17. **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;
18. **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 порталенную 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: 719

Последнее обновление: 8 июл., 2025

Обновлено от: Ильина В.

Ревизия: 1

База знаний AxeINAC -> Документация -> Система контроля доступа к сети «AxeINAC». Версия 2.0.1 -> AxeINAC. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Политики и контроль доступа» -> Страница «Источники аутентификации» -> Вкладка «Внешние источники» -> Sponsor

<https://docs.axel.pro/entry/719/>