

# Гостевой доступ с согласованием пользователем-спонсором запроса от пользователя-гостя

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.

## Настройка источника аутентификации

Для того чтобы добавить источник аутентификации, выполните следующие действия:

**Шаг 1.** Перейдите в раздел **Конфигурация → Политики и контроль доступа → Источники аутентификации** и в блоке **Внешние источники** нажмите кнопку **Новый внешний источник**. В выпадающем списке выберите значение **Sponsor**.

**Шаг 2.** На открывшейся странице заполните поля следующим образом:

- **Имя** — Sponsor (данное имя будет отображаться в списке источников аутентификации);
- **Описание** — введите описание источника аутентификации (данное описание будет отображаться в списке источников аутентификации);
- **Связанные источники аутентификации** — выберите домен, для которого будет работать этот источник аутентификации (вы можете оставить это поле пустым, чтобы разрешить работу источника с любыми соединениями);
- **Запрещённые домены** — в данном поле вы можете указать домены, для которых будет запрещена работа данного источника аутентификации (blacklist);
- **Разрешенные домены** — в данном поле вы можете указать домены, для которых будет разрешена работа данного источника аутентификации (whitelist);
- **Таймаут ссылки активации** — 30 минут (данное значение определяет, в течение какого срока после запроса пользователь-гость может быть активирован пользователем-спонсором);
- **Разрешить локальный домен** — Да (данное значение разрешает автоматическую регистрацию пользователей-гостей, которые находятся в локальном домене);
- **Заменить хост в ссылке активации** — оставьте пустым (данное значение может быть задано для перенаправления пользователя-гостя на внешний ресурс для регистрации, например, если AxelNAC не настроен на внешнюю сеть, из которой приходит пользователь-гость);
- **Зарегистрировать при активации** — Активировано (данное значение определяет, должен ли оставаться пользователь-гость на портале регистрации до ее окончания);
- **Обязательная аутентификация спонсора** — Да (данное значение определяет, должен ли пользователь-спонсор вводить свои учетные данные для подтверждения регистрации пользователя);
- **Язык** — По умолчанию (данное значение будет выбирать язык портала по локали браузера);
- **Создать локальную учетную запись** — Да (данное значение определяет, создавать ли учетную запись пользователя в AxelNAC. В случае, когда запись создана, пользователю не нужно будет повторно проходить спонсорскую регистрацию);
- **Метод хэширования паролей базы данных** — NTLM (для того, чтобы пользователь мог аутентифицироваться необходимо выбирать значения NTLM или Plaintext);
- **Длина пароля** — 8 (данное значение определяет размер автоматически сгенерированного пароля, который будет отправлен пользователю-гостю);
- **Количество входов в систему для локальной учетной записи** — 0 (данное значение определяет, сколько раз гостевая учетная запись может подключиться к сети. При указании 0, ограничение отсутствует);
- **Истечение срока действия локальной учетной записи** — 0 (данное значение определяет срок действия учетной записи. При указании 0, будет применяться срок предоставления доступа, указанный в правилах аутентификации для пользователя-гостя).

**Шаг 3.** Настройте правила аутентификации. Для того чтобы добавить правило, нажмите **Добавить правило** и введите имя правила аутентификации. В нашем случае мы будем пропускать всех пользователей, поэтому правило может быть названо **catchall**.

**Шаг 4.** Нажмите **Добавить действие**, чтобы добавить действия при срабатывании данного правил и из выпадающего списка выберите параметр **Роль** и значение **guest**.

**Шаг 5.** Нажмите на знак плюса справа от первого действия и из выпадающего списка выберите параметр **Срок предоставления доступа** и значение **1 час**, затем нажмите **Создать**.

## Настройка профиля подключения

Для того чтобы добавить созданный источник аутентификации в профиль подключения, выполните следующие действия:

**Шаг 1.** Перейдите в раздел **Конфигурация → Политики и контроль доступа → Профили подключения** и откройте профиль подключения, который вы хотите связать с данным источником аутентификации.

**Шаг 2.** На открывшейся странице заполните все необходимые поля и активируйте переключатель в строке **Перераспределение ролей MAC-аутентификации с портала**. Таким образом, даже для устройств, которые уже были зарегистрированы в AxelNAC, будет использоваться выбранный источник аутентификации.

**Шаг 3.** В строке **Фильтр** выберите тип подключения и укажите SSID (если подключение беспроводное).

**Шаг 4.** В строке **Источники** укажите источник, который вы создали на предыдущем этапе и нажмите **Сохранить**.

Для того, чтобы письмо с запросом на регистрацию или с учетными данными было отправлено спонсору/гостю, необходимо также настроить интеграцию с почтовым сервером. Настройка выполняется в разделе **Конфигурация → Настройки системы → Основные настройки → Уведомления**.

## Настройка Captive-портала

Также необходимо настроить работу Captive-портала в самом AxelNAC:

**Шаг 1.** Перейдите в раздел **Конфигурация → Сетевое взаимодействие → Интерфейсы** и выберите интерфейс, который будет использоваться для предоставления доступа к сети.

**Шаг 2.** В строке **Дополнительный демон(ы) прослушивания** добавьте значение **portal** из выпадающего списка, затем нажмите **Сохранить**.

**Шаг 3.** Перейдите в раздел **Статус → Службы** и перезапустите следующие службы:

- haproxy-portal;
- httpd.portal;
- iptables.

## Создание пользователя-спонсора

После того как источник аутентификации создан и настроен, необходимо создать пользователя-спонсора. Для этого выполните следующие действия:

**Шаг 1.** Перейдите в раздел **Пользователи → Создать** и заполните поля **Имя пользователя (PID)**, **Пароль** и **E-mail**. Данные значения будут использоваться пользователем-спонсором для входа в подтверждения запросов на регистрацию.

**Шаг 2.** В строке **Окно регистрации** укажите желаемый срок действия учетной записи администратора.

**Шаг 3.** В строке **Действия** из выпадающего списка выберите параметр **Назначить роль спонсора**, затем нажмите **Создать**.

## Гостевой доступ

Пользователь-гость создается следующим образом:

**Шаг 1.** Пользователь-гость подключается к сети, после чего в браузере у него открывается страница аутентификации.

**Шаг 2.** Пользователь-гость принимает условия и вводит свою электронную почту и электронную почту спонсора. Электронная почта спонсора вводится для того, чтобы избежать внешних запросов. Если почта не совпадает с существующей, клиенту будет отказано в регистрации.

**Шаг 3.** Пользователю-спонсору на почту приходит запрос на регистрацию с кнопкой активации.

**Шаг 4.** При нажатии на кнопку пользователь-спонсор перенаправляется на страницу аутентификации, где он должен ввести свои учетные данные для активации пользователя-гостя.

**Шаг 5.** У пользователя-гостя на портале отображаются выданные ему учетные данные. Эти же данные будут автоматически направлены ему на электронную почту.

## Повторный вход гостя без участия спонсора.

После регистрации гостя возможен вход по полученной учетной записи, без согласования запроса со спонсором. Для этого необходимо выполнить следующие шаги:

**Шаг 1.** Перейдите в раздел **Конфигурация → Политики и контроль доступа → Профили подключения** и откройте профиль подключения, который был создан для предоставления гостевого доступа.

**Шаг 2.** В строке **Источники** нажмите на знак плюса справа от вашего источника и выберите источник **local** из выпадающего списка, затем нажмите **Сохранить**.

Теперь пользователю при подключении будет предоставляться выбор способа аутентификации на портале. Таким образом, пользователь сможет запросить регистрацию у спонсора, либо сможет самостоятельно подключиться, используя ранее полученные учетные данные.

