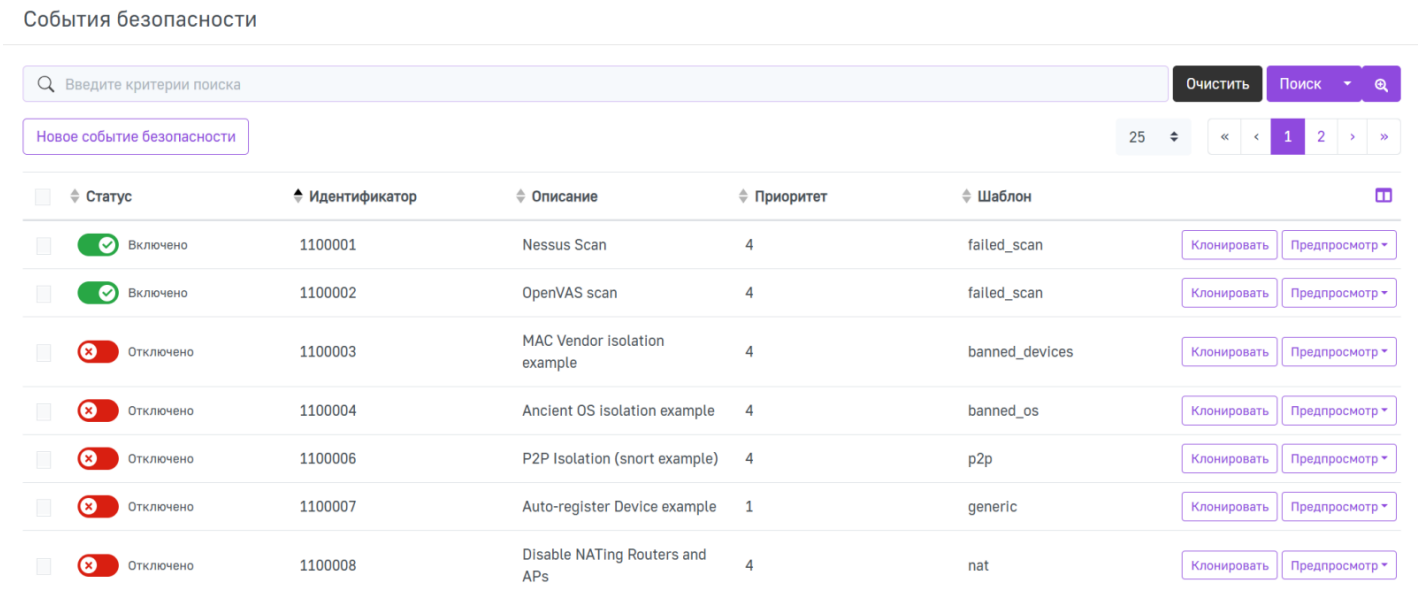
Страница «События безопасности»

События безопасности (Security Events) — это модуль, который позволяет реагировать на действия и состояния конечных устройств. AxelNAC позволяет реагировать на смену профиля устройства, на несоответствие политикам ИБ устройства, а также реагировать на превышение устройством порогового уровня потребляемого трафика. Функционал **событий безопасности** позволяет комбинировать уведомление администраторов ИБ и изолирование устройства, вызвавшего событие, от общей сети с последующим указанием инструкций и действий на портале администратора AxelNAC. Событие безопасности вызывается с помощью триггеров.

Страница «События безопасности»

На данной вкладке выполняется создание события безопасности, редактирование и смена статуса его работы.



По умолчанию в таблице отображаются 5 столбцов:

- **Статус** — активность события безопасности;
- **Идентификатор** — идентификатор события безопасности;
- **Описание** — описание, содержащее краткую информацию о событии безопасности;
- **Приоритет** — приоритет события безопасности;
- **Шаблон** — шаблон события безопасности.

Управление таблицей

Набор отображаемых столбцов в таблице может быть изменен, для этого нажмите на иконку. В выпадающем списке нажмите на название столбца, отображение которого в таблице необходимо изменить.

По умолчанию на странице отображается 25 записей, однако вы можете выбрать отображение 10, 50, 100, 200, 500 и 1000 записей на странице. Для этого нажмите на поле в правом верхнем углу списка и выберите в выпадающем списке необходимое количество для отображения.

Вы можете отсортировать таблицу по **Статусу, Идентификатору**, **Описанию**, **Приоритету**, **Шаблону** в порядке алфавитного возрастания или убывания с помощью иконки. По умолчанию все записи в таблице отображаются в порядке алфавитного возрастания по **Идентификатору**.

Для переключения между страницами используйте блок в правом верхнем углу списка.

Создание нового события безопасности

Для того, чтобы создать новое событие безопасности, нажмите **Новое событие безопасности** в левом верхнем углу страницы.

В данном меню доступны следующие настройки:

1. **Активировать событие безопасности** — включение срабатывания данного события безопасности;
2. **Идентификатор** — идентификатор события, который будет отображаться в таблице со списком всех событий безопасности. Данный параметр назначается автоматически;
3. **Описание** — описание события безопасности, которое будет отображаться в таблице со списком всех событий безопасности;
4. **Приоритет** — приоритет события безопасности. При выявлении нескольких событий на одном конечном устройстве, будет выполняться событие с самым наименьшим значением;
5. **Игнорирование списка ролей** — при активации данного параметра событие не затрагивает роли, указанные в параметре **Список ролей.** При деактивации данного параметра событие затрагивает только роли, указанные в параметре **Список ролей**;
6. **Список ролей** — список игнорируемых/разрешенных ролей в событии безопасности;
7. **Триггеры событий** — действия или параметры, которые вызывают событие безопасности (можно выбрать одно или несколько). Нажмите кнопку **Добавить триггер**, чтобы добавить следующие параметры:
    - **Конечное устройство** — срабатывание произойдет, если параметр конечного устройства совпадает с указанным;
    - **Профилирование устройства** — срабатывание произойдет, если один из критериев профиля устройства совпадает с указанным;
    - **Использование данных** — срабатывание произойдет, если один из параметров использования данных совпадет с указанным;
    - **Событие** — срабатывание произойдет если случится указанное событие.

• Вводимые в поля значения чувствительны к регистру;
• В поле **MAC-вендор** необходимо указать префикс вендора (первые три октета) в формате xxaabb (например, 23ab17). Символы "-", ":" не обрабатываются;
• Поле **MAC-адрес** должно быть заполнено в формате aa:bb:cc:dd:ee:ff.

8. **Действия, связанные с событием:**
    - **Снять с регистрации** — снять регистрацию с устройства;
    - **Зарегистрировать** — зарегистрировать устройство в системе. Вы можете указать целевую роль и срок предоставления доступа. При активации данного параметра появляются следующие параметры:
        - **Целевая роль** — роль зарегистрированного устройства;
        - **Период доступа без реавторизации** — срок предоставления доступа зарегистрированному устройству.

- **Изолировать** — выдать роль изолированного устройства. Вы можете выбрать шаблон страницы, которая будет отображаться на портале, добавить текст кнопки, URL для переадресации, разрешить хосту самостоятельно перезапустить регистрацию. При активации данного параметра появляются следующие параметры:
  - **Роль во время изоляции** — роль, выдающаяся изолированному устройству;
  - **Использовать шаблон** — страница, отображающаяся на Captive-портале в случае срабатывания события безопасности. Шаблон такой страницы может быть создан или изменен в директории **/usr/local/pf/html/captive-portal/templates/**;
  - **Текст кнопки** — текст, отображаемый на кнопке события в форме события безопасности для хостов;
  - **URL для переадресации** — целевой URL-адрес, на который AxelNAC будет перенаправлять устройство. По умолчанию используется URL переадресации из конфигурации профиля подключения;
  - **Активировать автоматически** — данный параметр определяет, может ли хост самостоятельно устранить причину события безопасности (кнопка **Активировать сеть**). Если параметр выключен, пользователю необходимо обратиться в службу поддержки;
  - **Максимальное количество попыток** — число попыток самостоятельного исправления причин смены роли. После использования всех попыток хост будет заблокирован и потребуется обратиться в службу поддержки. Данная функция нужна для ограничения пользователей, специально вызывающих события безопасности.
- **Отправить уведомление на электронную почту Администратора** — отправить уведомление на электронную почту администратора AxelNAC;
- **Отправить уведомление на электронную почту владельца конечного устройства** — отправить сообщение на электронную почту устройства, вызвавшего событие (если почта указана). При активации данного параметра появляются следующий параметр:
  - **Дополнительное сообщение** — сообщение, отправляемое вместе с уведомлением о срабатывании события безопасности.
- **Адресат сообщения** — отправить сообщение на электронную почту другого пользователя. При активации данного параметра появляются следующие параметры:
  - **Адрес электронной почты** — адрес электронной почты, на который будет отправлено сообщение;
  - **Дополнительное сообщение** — сообщение, отправляемое вместе с уведомлением о срабатывании события безопасности;
  - **Использовать шаблон** — шаблон сообщения, которое будет присылаться в случае срабатывания события безопасности.
- **Выполнить скрипт** — выполнить скрипт в AxelNAC. Необходимо указать путь к скрипту. При активации данного параметра появляются следующий параметр:
  - **Путь к скрипту** — путь к скрипту, выполняющемуся в AxelNAC.

    В команде запуска скрипта можно использовать следующие переменные:
    • $mac: MAC-адрес конечного устройства;
    • $ip: IP-адрес конечного устройства;
    • $vid: Идентификатор события безопасности.
- **Остановить еще одно событие безопасности** — завершить действие другого события безопасности в системе. При активации данного параметра появляются следующие параметры:
  - **Событие безопасности, которое будет завершено** — событие безопасности, которое будет завершено при активации данного события безопасности.

9. **Динамическое окно** — работает только для событий безопасности аккаунтинга. Такое событие будет открыто в соответствии со временем, заданным при создании события безопасности аккаунтинга (например, у вас есть событие безопасности при использовании трафика более 10 ГБ/месяц. Если вы превысите лимит через 3 дня, то сработает событие безопасности, а дата его окончания будет установлена на последний день текущего месяца);
10. **Грейс-период** — количество времени, по истечении которого событие безопасности может снова сработать. Это может быть использовано для того, чтобы дать хостам время (например, 2 минуты) на загрузку инструментов для устранения проблемы или отключения P2P-приложения;
11. **Окно** — количество времени, по истечении которого событие безопасности закрывается автоматически. Вместо того чтобы предоставлять людям возможность повторно включать сеть, можно на определенный период времени открыть событие безопасности;
12. **Задержка на** — задержка перед срабатыванием события безопасности.

Для того чтобы создать событие безопасности, 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**.

Поиск события безопасности

Для того чтобы найти определенного агента пользователя, можно выполнить поиск по критериям: **Идентификатор**, **Описание**, **Шаблон**. Введите интересующий критерий в поле поиска и нажмите **Поиск**. Нажмите **Очистить**, чтобы сбросить критерии поиска.

Также можно выполнять поиск по нескольким критериям. Для этого нажмите на иконку лупы  справа от кнопки **Поиск**.

В меню расширенного поиска вы можете выбрать операторы **И** и **ИЛИ** и указать несколько критериев для поиска. Поиск можно вести по критериям:

- **Идентификатор** — поиск по идентификатору события безопасности;
- **Описание** — поиск по описанию события безопасности;

- **Шаблон** — поиск по шаблону события безопасности.

Также вам доступны следующие операторы:

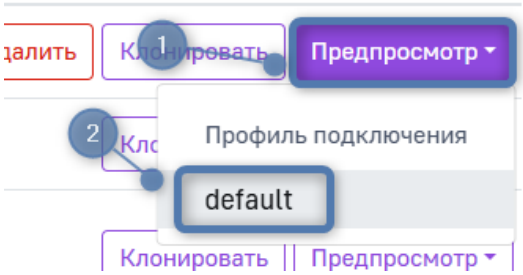
- **равно**;
- **не равно**;
- **начинается с**;
- **заканчивается на**;
- **содержит.**

Для того чтобы изменить порядок выражений, нажмите и удерживайте иконку и перетащите выражение. Для того чтобы удалить выражение, нажмите на иконку .

Вы можете сохранить и экспортировать существующий запрос, чтобы воспользоваться им позднее или импортировать уже существующий запрос. Все эти действия можно выбрать из выпадающего списка после нажатия на иконку .

Предпросмотр события безопасности

Профили подключения включают файлы, в том числе шаблоны, используемые в событиях безопасности. При нажатии на Предпросмотр отображается список доступных профилей. При выборе профиля откроется связанный шаблон, если он был использован в событии. В случае изменения шаблона в профиле, событие отобразится с учетом внесенных изменений.

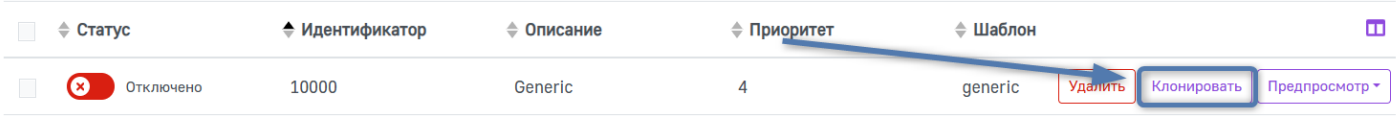


Редактирование настроек события безопасности

Для того чтобы отредактировать события безопасности, нажмите на строку в таблице с названием нужного события безопасности. На открывшейся странице можно изменить все параметры события безопасности.

Клонирование события безопасности

Для того чтобы создать копию определенного события безопасности, нажмите **Клонировать**. После этого вам будет предложено отредактировать скопированное событие безопасности.



Также в режиме редактирования события безопасности вы можете в конце страницы нажать кнопку **Клонировать**.

Удаление события безопасности

Для того чтобы удалить событие безопасности, нажмите **Удалить**. После этого подтвердите удаление.

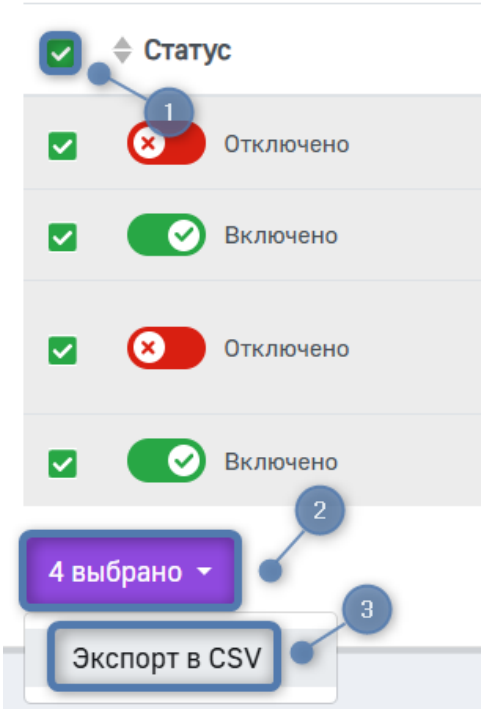
Предустановленные события безопасности невозможно удалить.

Также в режиме редактирования события безопасности вы можете в конце страницы нажать кнопку **Удалить**. После этого подтвердите удаление.

Групповые действия

Для того чтобы выполнить действия с несколькими событиями безопасности, отметьте необходимые события безопасности.

Чтобы выполнить действия со всеми событиями безопасности в списке, нажмите на селектор в шапке таблицы.



На данный момент единственное доступное групповое действие в системе — **Экспорт в CSV**. При его выборе, файл в формате **.csv**, содержащий записи таблицы, попадает в менеджер загрузки вашего браузера.

ID статьи: 418
Последнее обновление: 29 мая, 2025
Обновлено от: Ильина В.
Ревизия: 22
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 1.0.0 -> AxelNAC. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Соответствие» -> Страница «События безопасности» -> Страница «События безопасности»
https://docs.axel.pro/entry/418/