Конфигурация событий безопасности

В данной статье описан процесс конфигурации событий безопасности: как создать событие безопасности, задать роли, на которое оно будет распространяться, как задать условия срабатывания и т.д.

Создание события безопасности

Для того, чтобы создать событие безопасности, перейдите в раздел **Конфигурация → Соответствие → События безопасности** и нажмите **Новое событие безопасности**. После этого откроется окно конфигурации события безопасности. В данном окне вам будут доступны следующие параметры:

- **Активировать событие безопасности** — включение срабатывания данного события безопасности;
- **Идентификатор** — идентификатор события. Данный параметр назначается автоматически;
- **Описание** — описание события безопасности;
- **Приоритет** — приоритет события безопасности. При выявлении нескольких событий на одном конечном устройстве, будет выполняться событие с самым наименьшим значением;
- **Использование списка ролей** — данный переключатель позволяет выбрать для каких ролей будет применяться/не будет применяться событие безопасности:
  - **Игнорирование ролей** — при выбранном положении, событие безопасности будет применяться ко всем ролям, кроме перечисленных в поле ниже;
  - **Разрешенные роли** — при выбранном положении, событие безопасности будет применяться только к ролям, перечисленным в поле ниже.
- **Список ролей** — какие роли не должны быть затронуты данным событием в системе безопасности;

Для корректной работы события безопасности, при использовании списка разрешенных ролей, необходимо добавить в список целевые роли, которые указаны в действиях (например, роль для изоляции или регистрации).

- **Триггеры событий** — действия или параметры, которые вызывают событие безопасности (можно выбрать одно или несколько):
  - **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 (например, событие, поступившее от сканера соответствия).
- **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;
  - **Изолировать** — выдать роль изолированного устройства. Вы можете настроить страницу, которая будет отображаться на портале, кнопку, URL для переадресации, предоставление возможности хосту самостоятельно перезапустить регистрацию;
  - **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);
  - **Адресат сообщения** — отправить сообщение на электронную почту другого пользователя. Необходимо указать адрес электронной почты;
  - **Выполнить скрипт** — выполнить скрипт в AxelNAC. Необходимо указать путь к скрипту
  - **Остановить еще одно событие безопасности** — завершить действие другого события безопасности в системе.
- **Грейс-период** — период "остывания" события. Событие не сработает повторно в указанный период;
- **Окно** — период, по истечении которого событие автоматически закроется;
- **Задержка на** — задержка перед срабатыванием события безопасности.

Для сохранения события безопасности нажмите **Сохранить**. Для того, чтобы сбросить изменения, нажмите **Сбросить**.

Триггеры событий

Вы можете установить любое количество триггеров для срабатывания событий безопасности. Для этого нажмите **Добавить триггер**, выберите вид триггера и условие.

Конечное устройство

В данной вкладке вы можете настроить срабатывание события безопасности по параметрам конечного устройства:

- **MAC-адрес** — событие безопасности сработает при совпадении с указанным MAC-адресом;
- **Сетевое устройство** — событие безопасности сработает при совпадении с указанным IP-адресом;
- **Группа сетевых устройств** — событие безопасности сработает при совпадении с указанной группой сетевых устройств.

- Вводимые в поля значения чувствительны к регистру;
- При указании MAC-адреса необходимо использовать только строчные символы.

Для каждого параметра можно выбрать один из следующих операторов:

- **Содержит** — параметр содержит указанные значения;
- **Не равно** — параметр не содержит указанные значения.

Для более точной фильтрации вы можете использовать в качестве MAC-адреса или IP-адреса регулярные выражения.

Профилирование устройства

В данной вкладке вы можете настроить срабатывание события безопасности по совпадению с профилем в хранилище отпечатков:

- **Устройство** — событие безопасности сработает при совпадении с указанным типом устройства;
- **Отпечаток DHCP** — событие безопасности сработает при совпадении с указанным отпечатком DHCP;
- **DHCP-вендор** — событие безопасности сработает при совпадении с указанным DHCP вендора;
- **Отпечаток DHCPv6** — событие безопасности сработает при совпадении с указанным отпечатком DHCPv6;
- **DHCPv6 Enterprise** — событие безопасности сработает при совпадении с указанным значением DHCPv6 Enterprise;
- **MAC-вендор** — событие безопасности сработает при совпадении с указанным MAC OUI (MAC-идентификатором вендора).

- Вводимые в поля значения чувствительны к регистру;
- При указании **MAC-вендора** необходимо использовать префикс вендора (первые три октета) в формате xxaabb (например, 23ab17). Символы "-", ":" не обрабатываются.

Для каждого параметра можно выбрать один из следующих операторов:

- **Содержит** — параметр содержит указанные значения;
- **Не равно** — параметр не содержит указанные значения.

Для более точной фильтрации вы можете использовать в качестве MAC- или DHCP-параметров регулярные выражения.

Использование данных

В данной вкладке вы можете настроить срабатывание события безопасности по использованию сетевого трафика:

- **Пропускная способность канала** — событие безопасности сработает при использовании определенного количества трафика. Данное условие содержит следующие дополнительные параметры:
  - **Направление** — направление трафика. Может принимать значения: **Всего**, **Входящее** и **Исходящее**;
  - **Лимит** — лимит трафика. В правой части поля вы можете выбрать одну из единиц измерения: **B (байты)**, **kB (килобайты)**, **MB (мегабайты)**, **GB (гигабайты)**, **TB (терабайты)**, **PB (петабайты)** и **XB (эксабайты)**;
  - **Интервал** — интервал отсчета трафика. Может принимать значения: **День**, **Неделя**, **Месяц** и **Год**.
- **Трафик исчерпан** — событие безопасности сработает при превышении количества трафика, выделенного конечному устройству;
- **Баланс времени исчерпан** — событие безопасности сработает при превышении времени доступа к сети, выделенного конечному устройству.

Событие

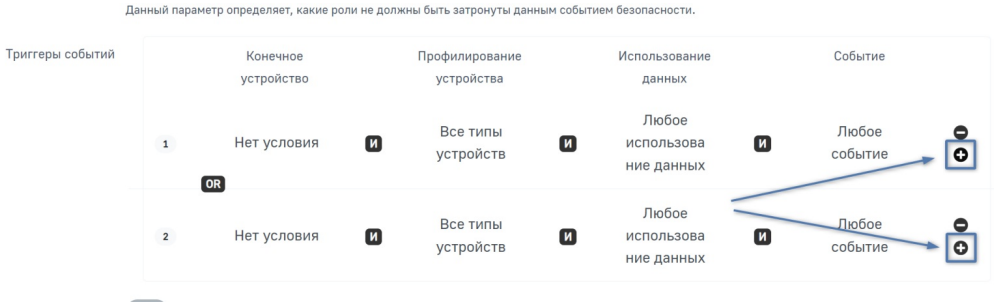
В данной вкладке вы можете настроить срабатывание события безопасности по идентификаторам событий, зарегистрированным в сети:

- **Пользовательское** — событие безопасности сработает при получении AxelNAC пользовательского идентификатора;
- **Определить** — событие безопасности сработает при получении AxelNAC идентификатора от детектора;
- **Внутреннее** — событие безопасности сработает при срабатывании другого события безопасности;
- **WinRS** — событие безопасности сработает при получении AxelNAC идентификатора от сканера WinRS;
- **Провайдер инициализации** — событие безопасности сработает при получении AxelNAC идентификатора от провайдера инициализации;
- **Событие Suricata** — событие безопасности сработает при получении AxelNAC идентификатора от системы обнаружения вторжений Suricata;
- **Suricata MD5** — событие безопасности сработает при получении AxelNAC MD5-хэша от системы обнаружения вторжений Suricata.

Вводимые в поля значения чувствительны к регистру.

Создание расширенных триггеров

При необходимости, вы можете добавить более сложные условия для срабатывания событий безопасности. Для этого нажмите на иконку **+** справа от заданного списка условий. После этого добавится еще одна строка условий с оператором **или**.



ID статьи: 587
Последнее обновление: 19 мая, 2025
Обновлено от: Егоров В.
Ревизия: 4
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.0.1 -> AxelNAC. Руководство администратора -> События безопасности -> Конфигурация событий безопасности
https://docs.axel.pro/entry/587/