Общие сведения

События безопасности — это модуль, который позволяет реагировать на действия и состояния конечных устройств. AxelNAC позволяет реагировать на смену профиля устройства (тип устройства, MAC-вендора, отпечаток DHCP и т.д.), на несоответствие политикам ИБ устройства, а также реагировать на превышение устройством порогового уровня потребляемого трафика.

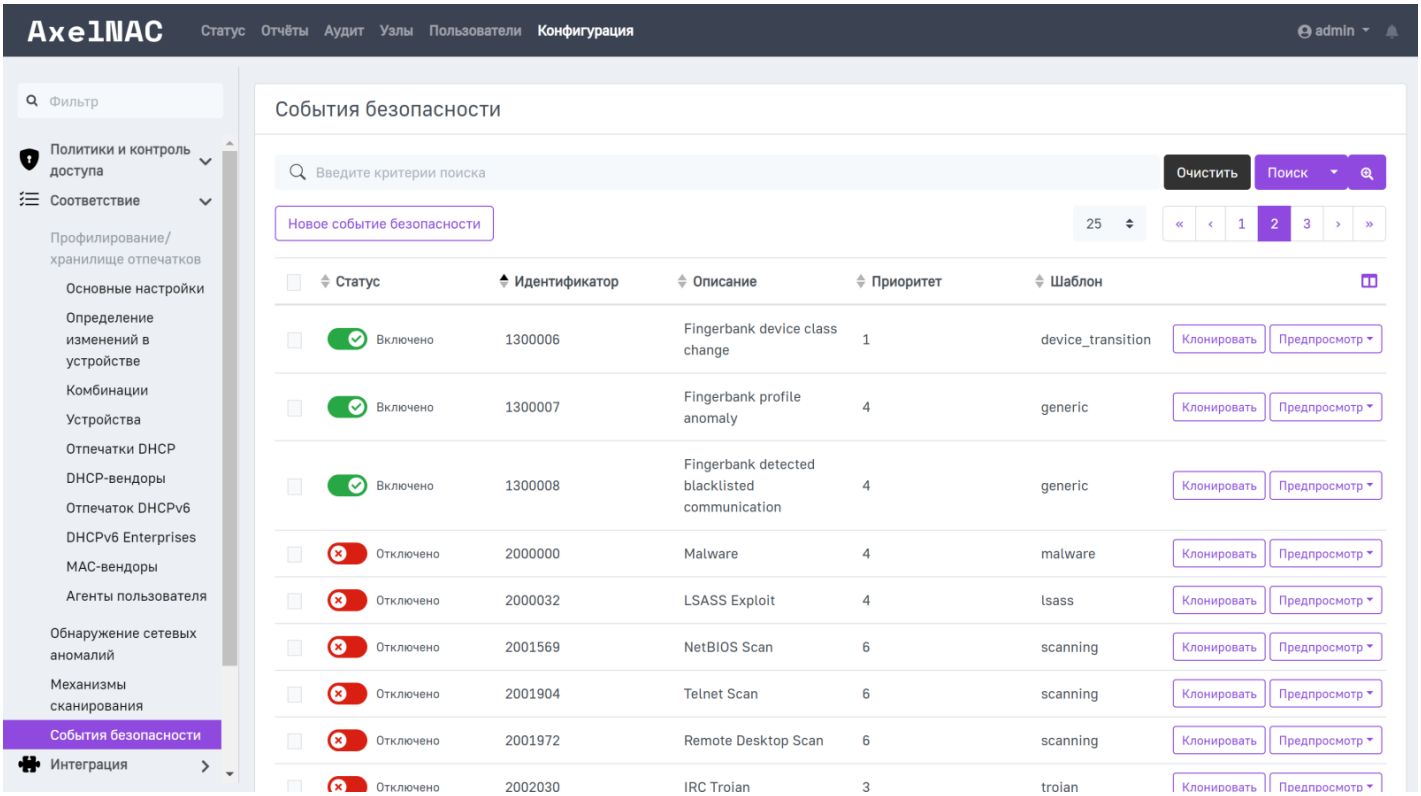
Функционал **событий безопасности** позволяет комбинировать уведомление администраторов ИБ и изолирование устройства, вызвавшего событие, от общей сети с последующим указанием инструкций и действий на портале администратора AxelNAC.

Глобально, события безопасности позволяют выполнять следующие действия с конечными устройствами, которые попали под настроенные условия:

- **Снять устройство с регистрации**;
- **Зарегистрировать устройство в сети**;
- **Изолировать устройство**;
- **Отправить уведомление на электронную почту Администратора сети** ;
- **Отправить уведомление на электронную почту владельца конечного устройства** ;
- **Отправить уведомление на определенную электронную почту** ;
- **Выполнить скрипт**;
- **Завершить активное событие безопасности**.

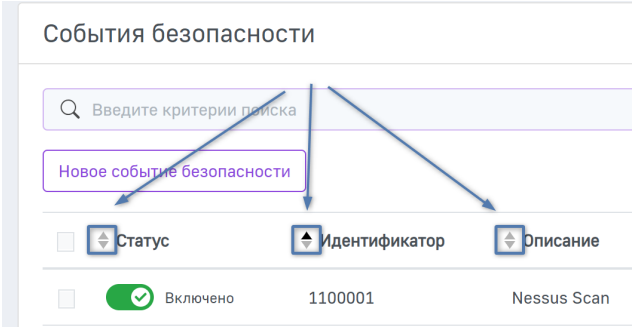
Список событий безопасности

Все события безопасности доступны в разделе **Конфигурация → Соответствие → События безопасности** .



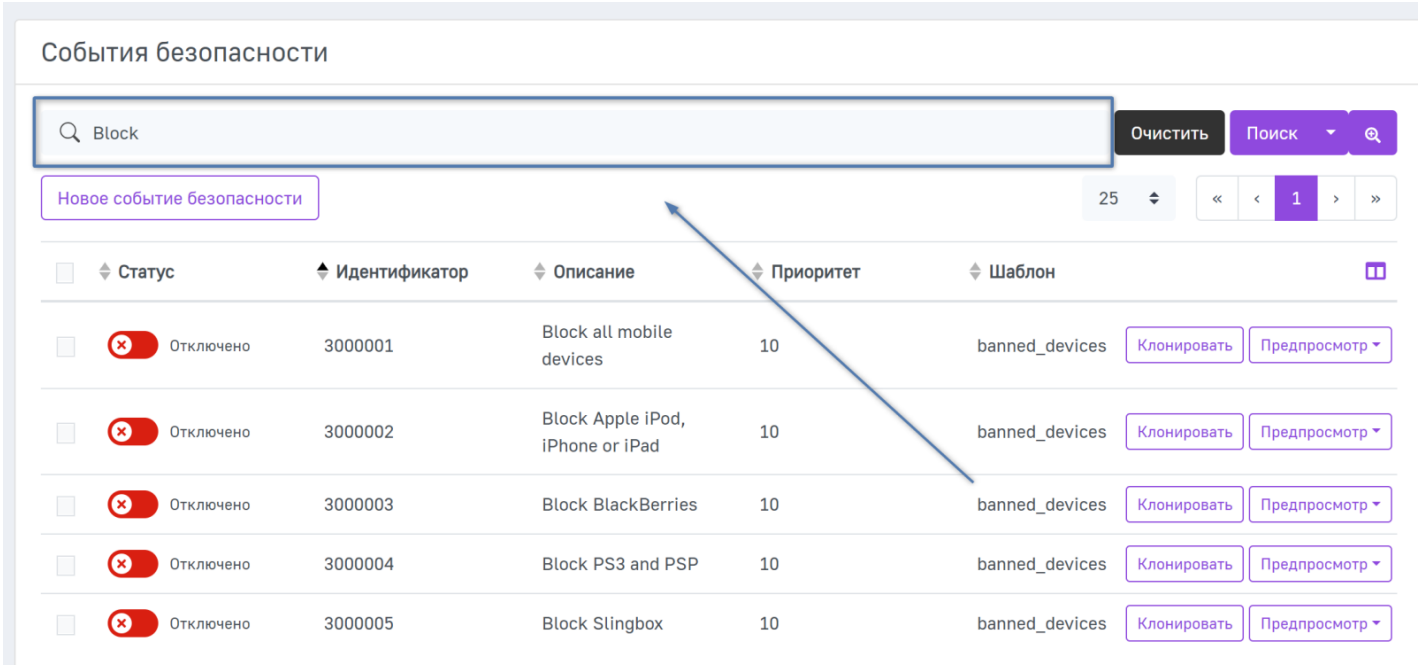
На данной странице вы можете просмотреть список всех созданных событий безопасности, задать параметры поиска, активировать работу, клонировать, выполнить предпросмотр отображаемой HTML-страницы и экспортировать список.

Вы также можете отсортировать список по любой из колонок. Для этого нажмите на иконку сортировки слева от имени колонки.



Поиск событий безопасности

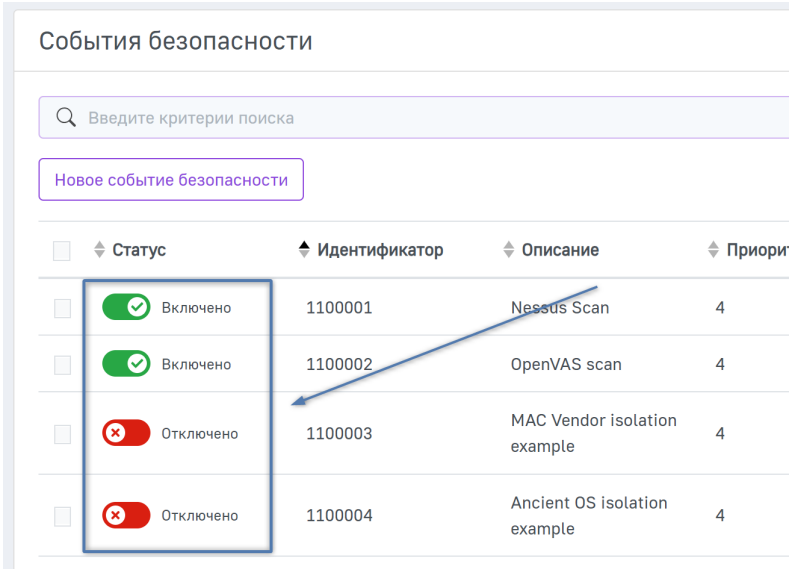
Для того чтобы выполнить поиск событий безопасности, нажмите на строку поиска в верхней части списка, введите ключевое слово для поиска и нажмите **Поиск**. В качестве ключевого слова может использоваться идентификатор или описание события безопасности, а также имя шаблона HTML-страницы, который будет использоваться при срабатывании события.



Для того чтобы сбросить условия поиска, нажмите **Очистить**.

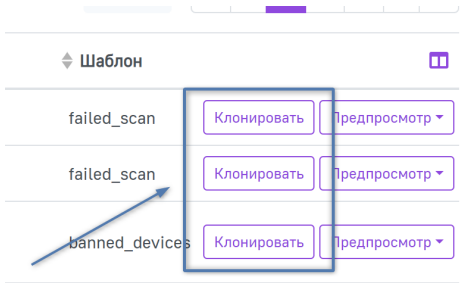
Быстрая активация событий безопасности

Для того чтобы активировать/деактивировать работу события безопасности, нажмите на переключатель в колонке **Статус**.



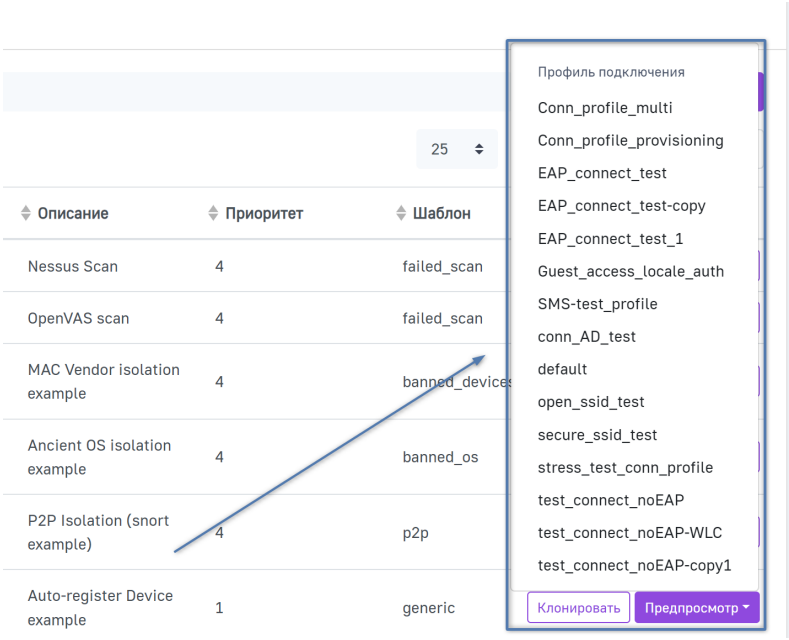
Клонирование событий безопасности

Для того чтобы клонировать событие безопасности, нажмите **Клонировать** в правой части таблицы. После этого откроется окно конфигурации нового события безопасности.



Предпросмотр HTML-страницы

Для того чтобы выполнить предпросмотр HTML-страницы, отображаемой при срабатывании события безопасности, нажмите **Предпросмотр** в правой части таблицы. При нажатии вам будет предложено выбрать профиль подключения, для которого вы хотите выполнить предпросмотр. После выбора профиля подключения будет отображена HTML-страница.



ID статьи: 977
Последнее обновление: 8 окт., 2024
Обновлено от: Михалева А.
Ревизия: 4
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.1.0 -> AxelNAC. Руководство администратора -> События безопасности -> Общие сведения
https://docs.axel.pro/entry/977/