

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** .

The screenshot shows the AxelNAC web interface. The top navigation bar includes 'Статус', 'Отчёты', 'Аудит', 'Узлы', 'Пользователи', and 'Конфигурация'. The main content area is titled 'События безопасности' and features a search bar with the placeholder 'Введите критерии поиска'. Below the search bar is a table with the following columns: 'Статус', 'Идентификатор', 'Описание', 'Приоритет', and 'Шаблон'. The table contains several rows of security events, each with a checkbox for status, a green checkmark or red X, an identifier, a description, a priority number, and a template name. Action buttons 'Клонировать' and 'Предпросмотр' are visible for each event. A sidebar on the left contains a 'Фильтр' section and a list of configuration options, with 'События безопасности' highlighted in purple.

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.

The diagram shows a portion of the 'События безопасности' table. It highlights the search bar and the first three columns: 'Статус', 'Идентификатор', and 'Описание'. Blue arrows point from the search bar to each of these columns, indicating that they are sortable. The first row of the table shows a status of 'Включено', an identifier of '1100001', and a description of 'Nessus Scan'.

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.

Статус	Идентификатор	Описание	Приоритет	Шаблон
Отключено	3000001	Block all mobile devices	10	banned_devices
Отключено	3000002	Block Apple iPod, iPhone or iPad	10	banned_devices
Отключено	3000003	Block BlackBerries	10	banned_devices
Отключено	3000004	Block PS3 and PSP	10	banned_devices
Отключено	3000005	Block Slingbox	10	banned_devices

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**.

Статус	Идентификатор	Описание	Приоритет
Включено	1100001	Nessus Scan	4
Включено	1100002	OpenVAS scan	4
Отключено	1100003	MAC Vendor isolation example	4
Отключено	1100004	Ancient OS isolation example	4

Клонирование событий безопасности

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

Шаблон
failed_scan
failed_scan
banned_devices

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.

Описание	Приоритет	Шаблон
Nessus Scan	4	failed_scan
OpenVAS scan	4	failed_scan
MAC Vendor isolation example	4	banned_devices
Ancient OS isolation example	4	banned_os
P2P Isolation (snort example)	4	p2p
Auto-register Device example	1	generic

Профиль подключения

- Conn_profile_multi
- Conn_profile_provisioning
- EAP_connect_test
- EAP_connect_test-copy
- EAP_connect_test_1
- Guest_access_locale_auth
- SMS-test_profile
- conn_AD_test
- default
- open_ssid_test
- secure_ssid_test
- stress_test_conn_profile
- test_connect_noEAP
- test_connect_noEAP-WLC
- test_connect_noEAP-copy1

Клонировать Предпросмотр

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/>