

Страница «Журналы аудита DNS»

На странице **Журналы аудита DNS** отображается список записей, содержащих DNS-запросы, обработанные встроенным DNS-сервером. Этот журнал позволяет отслеживать, какие доменные имена запрашивали устройства и анализировать, каким образом они были обработаны.

Журналы аудита DNS

Очистить

Поиск

25

<< < 1 2 > >>

<input type="checkbox"/>	Создано	IP-адрес	MAC-адрес	Qname	Qtype	Область применения	Ответ	<input type="checkbox"/>
<input type="checkbox"/>	05-12-2025 07:43	192.168.49.91	a3:00:5a:27:fa:88 ↗	facebook.com	AAAA	blocked		
<input type="checkbox"/>	05-12-2025 04:59	192.168.151.71	10:1e:ad:f9:af:c9 ↗	youtube.com	PTR	allowed	192.168.236.242	

По умолчанию в таблице отображаются 7 столбцов:

- **Создано** — дата и время регистрации события в журнале аудита DNS;
- **IP-адрес** — IP-адрес устройства;
- **MAC-адрес** — MAC-адрес устройства;
- **Qname** — запрашиваемое доменное имя;
- **Qtype** — тип запрашиваемой записи;
- **Область применения** — результат обработки запроса;
- **Ответ** — ответ DNS-сервера на запрос.

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 в порядке возрастания или убывания с помощью иконки ☐. По умолчанию все записи в таблице отображаются в порядке алфавитного возрастания по **MAC-адресу**.

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

Поиск записи в журналах

Для того чтобы найти определенную запись в журнале, можно выполнить поиск по критериям: **MAC-адрес**. 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 журнала** — поиск по уникальному номеру для каждой записи в журнале;
- **Создано** — поиск по дате и времени регистрации события в журнале аудита DNS;
- **IP-адрес** — поиск по IP-адресу устройства;
- **MAC-адрес** — поиск по MAC-адресу устройства;
- **Qname** — поиск по запрашиваемому доменному имени;
- **Qtype** — поиск по типу запрашиваемой записи DNS;
- **Область применения** — поиск по результату обработки запроса;
- **Ответ** — поиск по ответу DNS-сервера на запрос.

Также вам доступны следующие операторы:

- **равно**;
- **не равно**;
- **начинается с**;
- **заканчивается на**;
- **содержит**;
- **больше чем** (доступно для критерия **Создано**);
- **меньше чем** (доступно для критерия **Создано**);
- **больше или равно** (доступно для критерия **Создано**);
- **меньше или равно** (доступно для критерия **Создано**).

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

Просмотр информации о записи в журнале

Для того чтобы посмотреть информацию о записи в журналах, нажмите на строку в таблице с названием нужной записи. После этого откроется вкладка **Запись в журнале аудита DNS**, на которой можно посмотреть все параметры выбранной записи.

Запись в журнале DNS 145




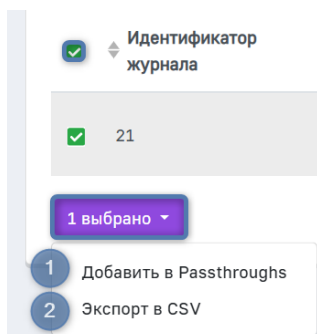
- 1 Создано 2025-12-05 04:59:26
- 2 IP-адрес 192.168.151.71
- 3 MAC-адрес 10:1e:ad:f9:af:c9
- 4 Qname youtube.com
- 5 Qtype PTR
- 6 Ответ 192.168.236.242
- 7 Область применения allowed

На данной вкладке доступны следующие параметры:

1. **Создано** — дата и время регистрации события в журнале аудита DNS;
2. **IP-адрес** — IP-адрес устройства;
3. **MAC-адрес** — MAC-адрес устройства;
4. **Qname** — запрашиваемое доменное имя;
5. **Qtype** — тип запрашиваемой записи;
6. **Ответ** — ответ DNS-сервера на запрос;
7. **Область применения** — результат обработки запроса.

Групповые действия

Для того чтобы выполнить действия с несколькими записями в журнале, отметьте необходимые записи. Чтобы выполнить действия со всеми записями в списке, нажмите на селектор  в шапке таблицы.



Список доступных групповых действий:

1. **Экспорт в Passthroughs** — создает на основе выбранных DNS-записей правила исключения и записывает их в

- конфигурационный файл **config/base/fencing**. Passthrough позволяет пользователям, находящимся внутри сети, доступ к определенным внешним ресурсам снаружи без прохождения обычных проверок;
2. **Экспорт в CSV** — файл в формате **.csv**, содержащий записи таблицы, попадает в менеджер загрузки вашего браузера.

ID статьи: 1430

Последнее обновление: 10 дек., 2025

Обновлено от: Михалева А.

Ревизия: 5

База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.0.1 -> AxelNAC. Руководство по использованию веб-интерфейса -> Меню «Аудит» -> Страница «Журналы аудита DNS» -> Страница «Журналы аудита DNS»
<https://docs.axel.pro/entry/1430/>