

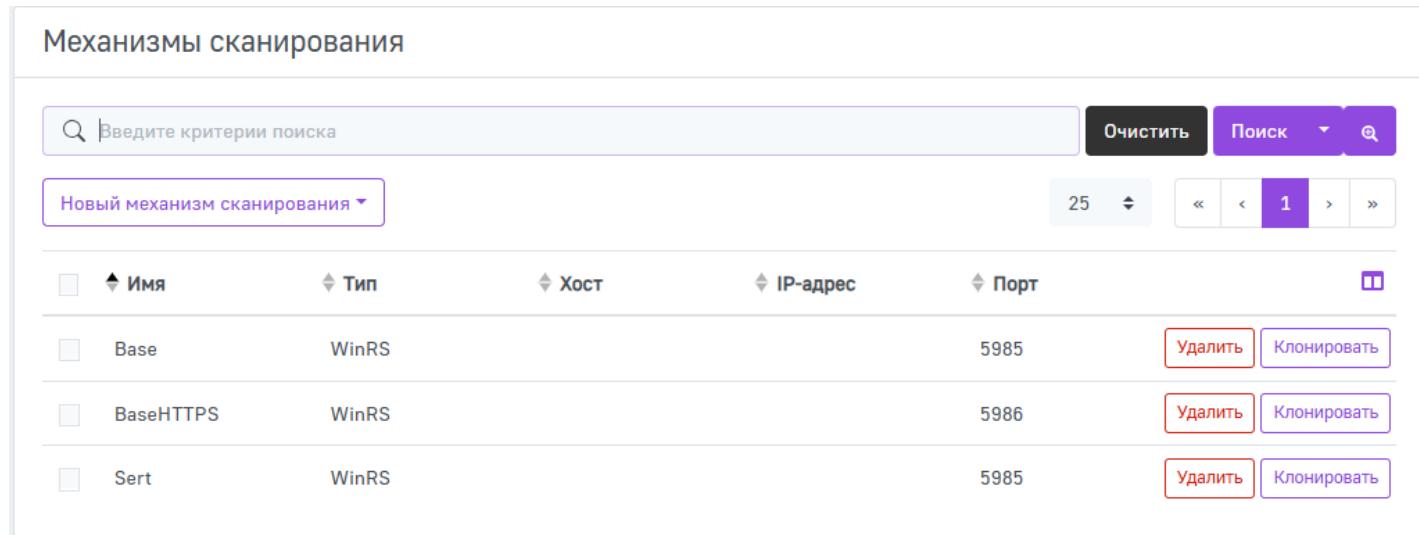
Страница «Механизмы сканирования»

Механизмы сканирования — AxelNAC может использовать сканеры уязвимостей для активного сканирования конечных устройств на соответствие политикам информационной безопасности, или использовать встроенный сканер соответствия. В качестве основного механизма сканирования используется WinRS, который взаимодействует со встроенным протоколом в ОС Windows. В случаях, когда клиентское устройство не соответствует установленным политикам, оно будет изолироваться с ограничением доступа к сети для устранения несоответствий.

Вкладка «Механизмы сканирования»

На данной вкладке выполняется создание и настройка механизмов сканирования.

Механизмы сканирования



Новый механизм сканирования					25	1
Имя	Тип	Хост	IP-адрес	Порт	Иконка	
Base	WinRS			5985	Удалить Клонировать	
BaseHTTPS	WinRS			5986	Удалить Клонировать	
Sert	WinRS			5985	Удалить Клонировать	

По умолчанию в таблице отображаются 5 столбцов:

- **Имя** — имя механизма сканирования;
- **Тип** — тип механизма сканирования;
- **Хост** — неприменимо к текущему сканеру;
- **IP-адрес** — неприменимо к текущему сканеру;
- **Порт** — порт для подключения.

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 **Имени**, **Типу**, **Хосту**, **IP-адресу**, **Порту** в порядке алфавитного возрастания или убывания с помощью иконки . По умолчанию все записи в таблице отображаются в порядке алфавитного возрастания по **Имени**.

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



Создание нового механизма сканирования

Для того чтобы создать новый механизм сканирования, нажмите **Новый механизм сканирования** в левом верхнем углу страницы и выберите **WinRS** в выпадающем списке.

Новый механизм сканирования WnRIS

1 Имя Требуется указать Имя.

2 Метод аутентификации По сертификату
Метод, который будет использоваться при подключении к устройству.

3 Имя пользователя

4 Порт 5985
Укажите альтернативный порт для обслуживания (если используется).

5 Файл сертификата Сертификат для подключения к сканируемому хосту. Только .pem файл

6 Цепочка сертификатов УЦ Только .pem файл. Добавьте файл с цепочкой сертификатов

7 Закрытый ключ Только .pem файл

8 Пароль для закрытого ключа Только при необходимости.

9 Скрипт установки Убедитесь, что вы сохранили все настройки, нажав кнопку "Сохранить".

10 Роли Изменение коснется узлов с выбранными ролями.

11 Список запрещенных доменов Список запрещенных доменов (через пробел), укажите NetBIOS-имя

12 Список разрешенных доменов Список разрешенных доменов (через пробел), укажите NetBIOS-имя

13 Обновление ОС Включено
30 Допустимое количество дней с момента последнего обновления

14 Проверка антивируса Включено

15 Проверка обновлений баз антивируса Отключено

16 Допустимое количество дней с момента последнего обновления баз антивируса 14

17 Принадлежность пользователя к домену Отключено

18 Дополнительная проверка имени пользователя Отключено
Дополнительная проверка имени пользователя из данных radius и хоста

19 Проверка обновлений безопасности ОС Отключено

20 Запущенные службы Отключено
Перечислите требуемые пакеты обновлений безопасности ОС (через пробел)

21 Проверка автозапуска служб Отключено
Если данный параметр активирован, сканер будет проверять, включена ли автозагрузка у перечисленных выше служб.

22 Сканировать до регистрации Отключено
Если данная функция активирована, система будет сканировать хост перед регистрацией.

23 Сканирование во время регистрации Включено
Если данная функция активирована, система сканирует каждый хост после завершения регистрации.

24 Сканировать после регистрации Отключено
Если данная функция активирована, система будет сканировать хост после попадания в продуктивный VLAN.

В данном меню доступны следующие настройки:

1. **Имя** — имя механизма сканирования, который будет отображаться в таблице со списком всех механизмов сканирования;
2. **Метод аутентификации** — метод, который будет использоваться при подключении к устройству. Существуют следующие методы:
 - **По сертификату** — аутентификация на основе сертификата;
 - **Базовый** — аутентификация на основе учетных данных (имя пользователя/пароль);
 - **Базовый через HTTPS** — защищенная аутентификация на основе учетных данных (имя пользователя/пароль) с использованием SSL-сертификата.
3. **Имя пользователя** — имя учетной записи на конечном хосте, к которому будет подключаться сканер;
4. **Порт** — порт для подключения (по умолчанию 5985);
5. **Файл сертификата** — сертификат для подключения к сканируемому хосту;
6. **Цепочка сертификатов УЦ** — файл с цепочкой сертификатов;
7. **Закрытый ключ** — закрытый ключ для расшифровки цепочки сертификатов;
8. **Пароль для закрытого ключа** — пароль для доступа к закрытой части сертификата;
9. **Скрипт установки** — скрипт установки для автоматической конфигурации конечного сканируемого узла;
10. **Роли** — список ролей узлов, для которых будет срабатывать механизм фильтрации;
11. **Список запрещенных доменов** — список доменов, для которых запрещено подключение к сети с данным механизмом фильтрации, укажите NetBIOS-имя;
12. **Список разрешенных доменов** — список доменов, для которых разрешено подключение к сети с данным механизмом фильтрации, укажите NetBIOS-имя;
13. **Обновление ОС** — при активации данного параметра производится проверка обновлений ОС. Укажите допустимое количество дней с момента последнего обновления в поле ниже;

14. **Проверка антивируса** — при активации данного параметра производится проверка нахождения антивируса в активном состоянии;
15. **Проверка обновлений баз антивируса** — при активации данного параметра производится проверка обновлений антивируса. Укажите допустимое количество дней с момента последнего обновления баз антивируса в поле ниже;
16. **Принадлежность пользователя к домену** — при активации данного параметра производится проверка принадлежности пользователя по его SID к домену, указанному в источнике аутентификации, который ассоциирован с профилем подключения с работающим механизмом сканирования;
17. **Дополнительная проверка имени пользователя** — данный параметр позволяет включить дополнительную проверку соответствия атрибута User-Name RADIUS-запроса подключающегося пользователя и АРМ при проверке на принадлежность пользователя к домену;
18. **Проверка обновлений безопасности ОС** — при активации данного параметра производится проверка обновлений безопасности ОС. Перечислите требуемые пакеты обновлений безопасности ОС в поле ниже;
19. **Запущенные службы** — при активации данного параметра производится проверка обновлений безопасности ОС. Перечислите требуемые пакеты обновлений безопасности ОС в поле ниже;
20. **Проверка автозапуска служб** — при активации данного параметра сканер будет проверять, включена ли автозагрузка у перечисленных выше служб;
21. **Сканировать до регистрации** — при активации данного параметра система будет сканировать хост перед регистрацией;
22. **Сканирование во время регистрации** — при активации данного параметра система сканирует каждый хост после завершения регистрации;
23. **Сканировать после регистрации** — при активации данного параметра система будет сканировать хост после попадания в продуктивный VLAN.

Для того чтобы создать механизм сканирования, 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 механизма сканирования

Для того чтобы найти определенный механизм сканирования, можно выполнить поиск по критериям: **Имя**, **Тип**, **IP-адрес** и **Порт**. 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:

- **Имя** — поиск по имени механизма сканирования;;
- **IP-адрес** — поиск по IP-адресу, указанном в механизме сканирования;
- **Порт** — порт для подключения;
- **Тип** — поиск по типу механизма сканирования.

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 экспорттировать существующий запрос, чтобы воспользоваться им позднее или импортировать уже существующий запрос. Все эти действия можно выбрать из выпадающего списка после нажатия на иконку .

Редактирование настроек механизма сканирования

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

Клонирование механизма сканирования

Для того чтобы создать копию определенного механизма сканирования, нажмите **Клонировать**. После этого вам будет предложено отредактировать скопированный механизм сканирования.

Имя	Тип	Хост	IP-адрес	Порт	
Base	WinRS			5985	Удалить Клонировать

Также в режиме редактирования механизма сканирования вы можете в конце страницы нажать кнопку **Клонировать**.



Удаление механизма сканирования

Для того чтобы удалить механизм сканирования, нажмите **Удалить**. После этого подтвердите удаление.

Имя	Тип	Хост	IP-адрес	Порт	
Base	WinRS			5985	Удалить Клонировать

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



Групповые действия

Для того чтобы выполнить действия с несколькими механизмами сканирования, отметьте необходимые события безопасности. Чтобы выполнить действия со всеми событиями безопасности в списке, нажмите на селектор в шапке таблицы.

Имя

- Base
- BaseHTTPS
- Sert

3 выбрано

Экспорт в CSV

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: 760

Последнее обновление: 8 июл., 2025

Обновлено от: Ильина В.

Ревизия: 1

База знаний AxeINAC -> Документация -> Система контроля доступа к сети «AxeINAC». Версия 2.0.1 -> AxeINAC. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Соответствие» -> Страница «Механизмы сканирования» -> Страница «Механизмы сканирования»

<https://docs.axel.pro/entry/760/>