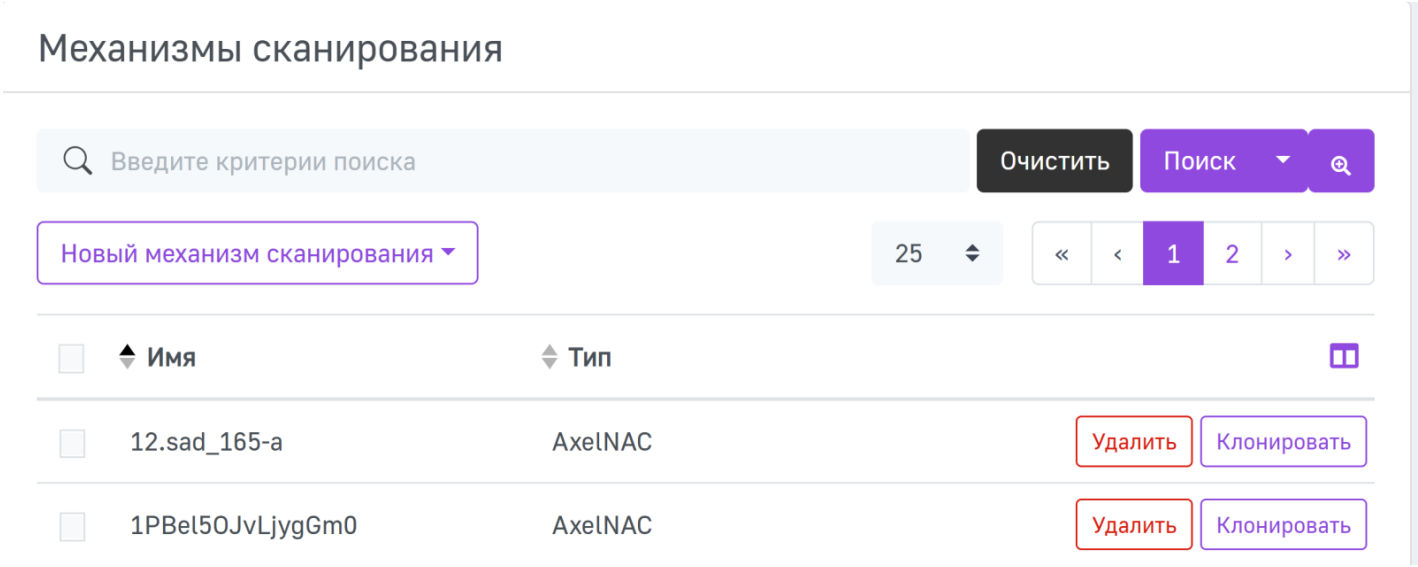
Вкладка «Механизмы сканирования»

Сканер **AxelNAC** является предустановленным в AxelNAC сканером соответствия и позволяет проводить проверку соответствия заданным политикам безопасности. Он проверяет устройства на базе Windows с помощью протокола подключения к сканируемому устройству WinRS и Linux с помощью протокола подключения к сканируемому устройству SSH. Конфигурация сканера может включать в себя как WinRS или SSH, так и оба протокола одновременно. AxelNAC выберет подходящий под ОС устройства протокол.

Вкладка «Механизмы сканирования»

На данной вкладке выполняется создание и настройка механизмов сканирования.



По умолчанию в таблице отображаются 5 столбцов:

- **Имя** — имя механизма сканирования;
- **Тип** — тип механизма сканирования.

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.

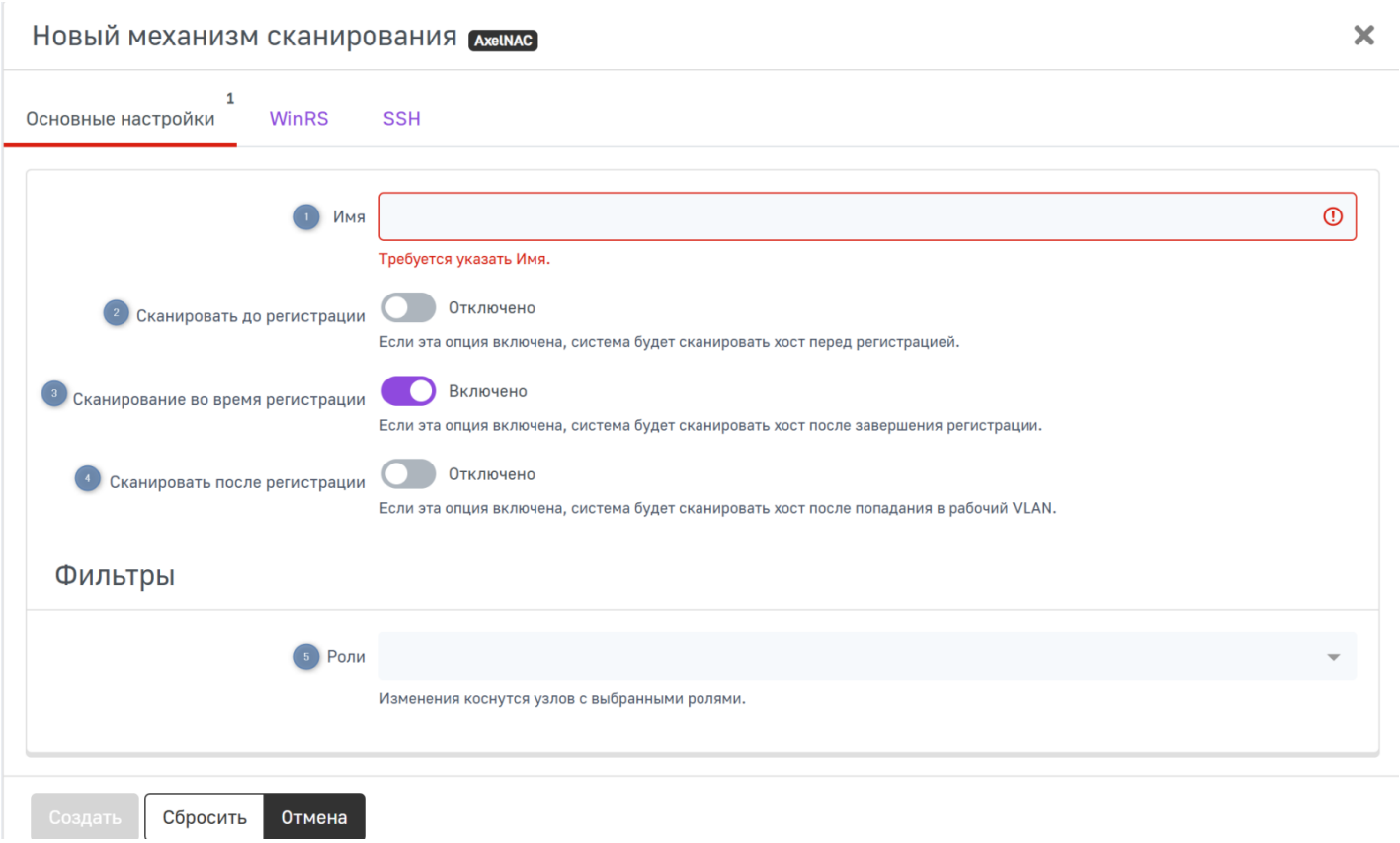
Вы можете отсортировать таблицу по **Имени, Типу** в порядке алфавитного возрастания или убывания с помощью иконки . По умолчанию все записи в таблице отображаются в порядке алфавитного возрастания по **Имени**.

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

Создание нового механизма сканирования

Для создания нового механизма сканирования нажмите **Новый механизм сканирования** и выберите из выпадающего списка AxelNAC.

Вкладка «Основные настройки»



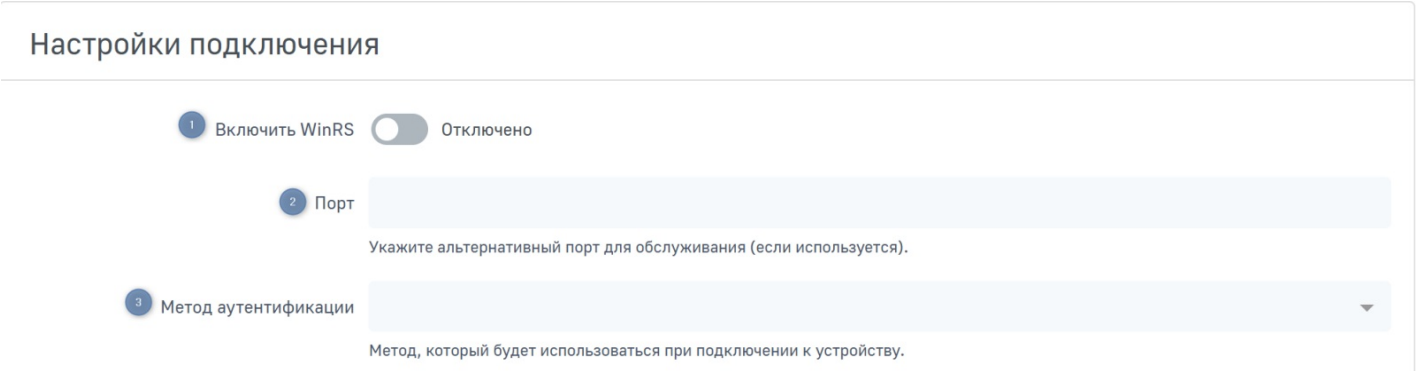
1. **Имя** — имя механизма сканирования;
2. **Сканировать до регистрации** — запуск сканирования при появлении устройства в регистрационной VLAN;
3. **Сканирование во время регистрации** — запуск сканирования сразу после регистрации на Captive-портале;
4. **Сканирование после регистрации** — запуск сканирования в продуктивной сети (**pfdhcplistener** должен принимать продуктивный dhcp-трафик);
5. **Роли** — список ролей узлов, для которых будет применен механизм сканирования.

- Для успешного подключения к сканируемому устройству, необходимо создать на нем локальную учетную запись с правами администратора.
- По умолчанию время ожидания ответа на каждый из запросов, отправляемых сканером AxelNAC при сканировании, имеет значение в 300 секунд.

Вкладка «WinRS»

На вкладке **WinRS** находятся блоки **Настройки подключения**, **Фильтры** и **Проверки**. Заполните параметры в них, чтобы настроить использование транспорта WinRS.

Блок «Настройки подключения»



В данном блоке доступны следующие параметры:

1. **Включить WinRS** — при активации данного параметра включается использование протокола WinRS;

   Если не активировать данный параметр, сканирование по данному протоколу проводиться не будет.

Если параметры **Включить WinRS** и **Включить SSH** активированы — происходит параллельное подключение по обоим включенным протоколам. В этом случае проверка проводится в зависимости от типа ОС. В случае, если событие безопасности 1300006 настроено так, что при смене MAC-адреса устройство переводится в изоляцию, то для использования функционала автоматического определения ОС для одного и того же супликанта эту опцию необходимо отключить. Если при изоляции устройство переводится в подсеть, отличную от той, в которой оно находилось во время сканирования, сканирование завершается неуспешно.

2. **Порт** — порт для подключения (по умолчанию создается порт 5985 — для базовой аутентификации, порт 5986 — для аутентификации по сертификату и HTTPS);
3. **Метод аутентификации** — метод аутентификации, который будет использоваться при подключении к устройству:
   - **По сертификату** — аутентификация на основе сертификата. По умолчанию будет выбран данный метод аутентификации. При выборе этого метода появляются следующие параметры:
     - **Имя пользователя** — имя учетной записи на конечном хосте, к которому будет подключаться сканер;
     - **Файл сертификата** — сертификат для подключения к сканируемому хосту;

       Сертификат должен начинаться с:
       ------BEGIN CERTIFICATE-----
       И заканчиваться:
       -----END CERTIFICATE-----
     - **Цепочка сертификатов УЦ** — файл с цепочкой сертификатов;

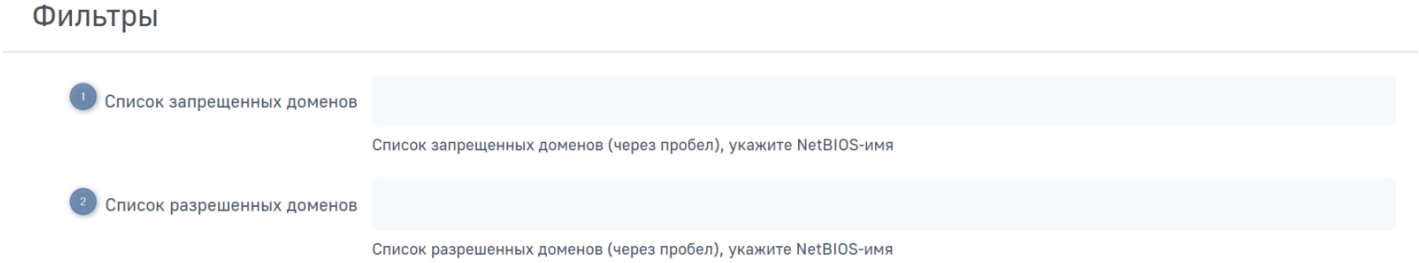
       Сертификат должен начинаться с:
       ------BEGIN CERTIFICATE-----
       И заканчиваться:
       -----END CERTIFICATE-----
     - **Закрытый ключ** — закрытый ключ, соответствующий серверному сертификату сканирования. Ключ должен быть в формате PEM;

       Закрытый ключ должен начинаться с:
       -----BEGIN PRIVATE KEY-----
       И заканчиваться:
       -----END PRIVATE KEY-----
     - **Пароль для закрытого ключа** — пароль для доступа к закрытой части сертификата;
     - **Установочный скрипт** — скрипт установки для автоматической конфигурации конечного сканируемого узла.
   - **Базовый** — аутентификация на основе учетных данных (имя пользователя/пароль). При выборе данного метода появляются следующие параметры:
     - **Имя пользователя** — имя учетной записи на конечном хосте, к которому будет подключаться сканер;
     - **Пароль** — пароль локальной учетной записи для подключения к сканеру.
   - **Базовый через HTTPS** — защищенная аутентификация на основе учетных данных (имя пользователя/пароль) с использованием SSL-сертификата. При выборе данного метода появляются следующие параметры:
     - **Имя пользователя** — имя учетной записи на конечном хосте, к которому будет подключаться сканер;
     - **Пароль** — пароль локальной учетной записи для подключения к сканеру;
     - **Цепочка сертификатов УЦ** — файл с цепочкой сертификатов;
     - **Установочный скрипт** — скрипт установки для автоматической конфигурации конечного сканируемого узла.

Подробная информация о каждом из методов аутентификации находится в разделе **Методы аутентификации сканера AxelNAC по протоколу WinRS**.

Блок «Фильтры»

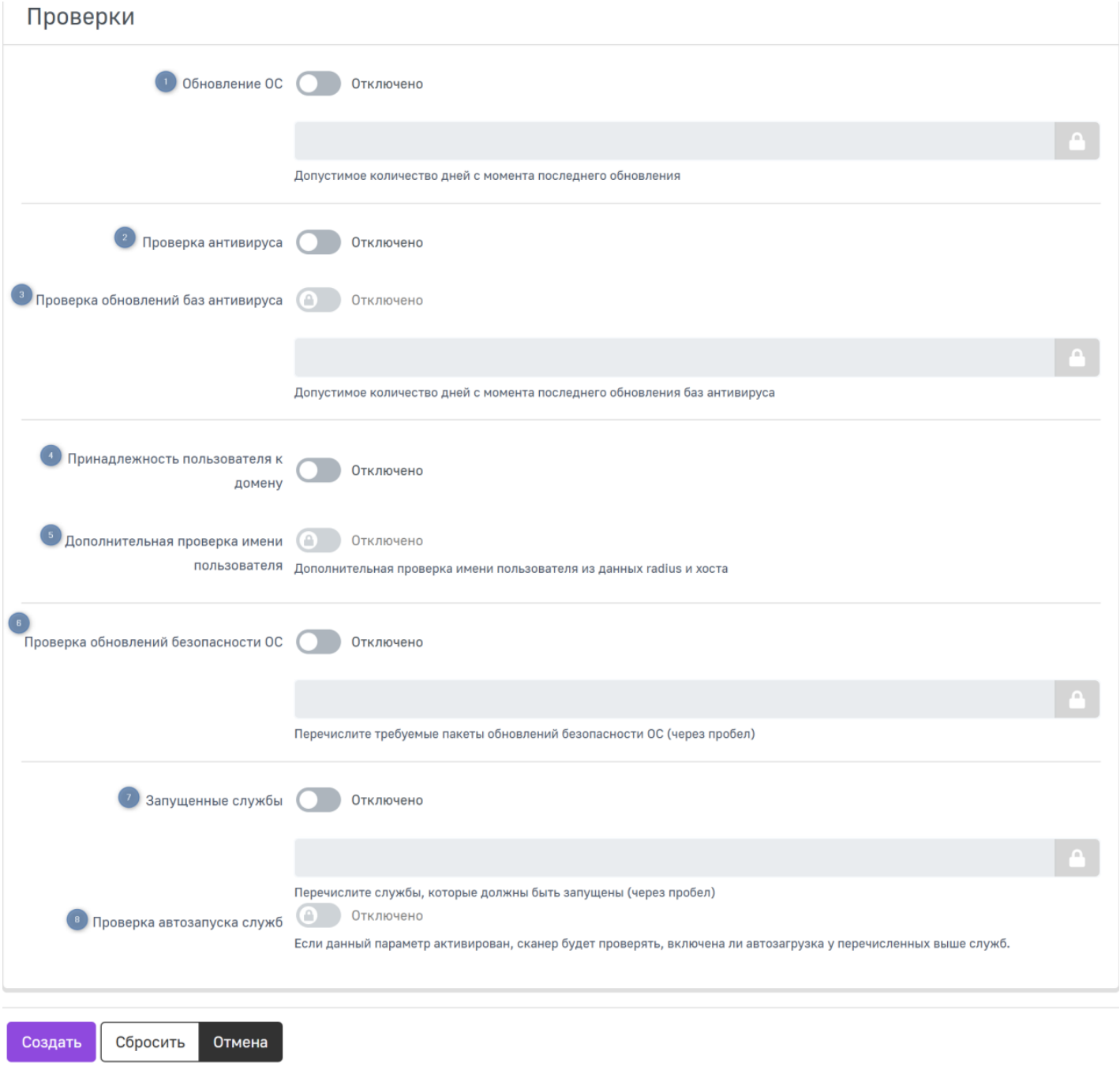
В случае, если в имени домена указано WORKGROUP, проверки из данного блока не выполняются. Это связано с тем, что данное имя присваивается для устройств, не введенных в домен.



В данном блоке доступны следующие параметры:

1. **Список запрещенных доменов** — список доменов, для которых запрещено подключение к сети с данным механизмом фильтрации, укажите NetBIOS-имя;
2. **Список разрешенных доменов** — список доменов, для которых разрешено подключение к сети с данным механизмом фильтрации, укажите NetBIOS-имя.

Блок «Проверки»



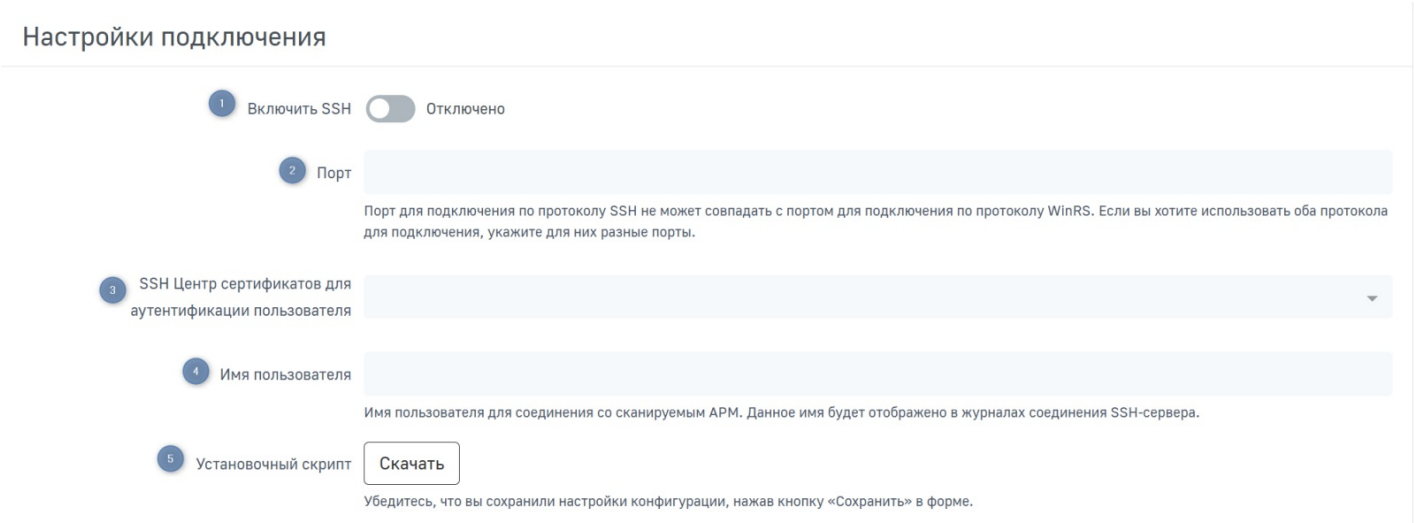
В данном блоке доступны следующие параметры:

1. **Обновление ОС** — данный параметр позволяет включить проверку наличия обновлений ОС. Также в поле ниже вы можете указать конкретное количество дней с момента последнего обновления (значение по умолчанию — 30 дней);
2. **Проверка антивируса** — данный параметр позволяет включить проверку наличия включенного антивируса. В данный момент поддержана проверка **Kaspersky Endpoint Security** и **Windows Defender**. Также параметр **Проверка обновлений баз антивируса** становится доступным для взаимодействия;
3. **Проверка обновлений баз антивируса** — данный параметр позволяет включить проверку наличия обновлений баз антивируса. Также в поле ниже вы можете указать конкретное количество дней с момента последнего обновления (значение по умолчанию — 14 дней);
4. **Принадлежность пользователя к домену** — данный параметр позволяет включить проверку принадлежности пользователя по его SID к домену, указанному в источнике аутентификации, который ассоциирован с профилем подключения с работающим механизмом сканирования. Также параметр **Дополнительная проверка имени пользователя** становится доступным для взаимодействия;
5. **Дополнительная проверка имени пользователя** — данный параметр позволяет включить дополнительную проверку соответствия атрибута User-Name RADIUS-запроса подключающегося пользователя и APM при проверке на принадлежность пользователя к домену;
6. **Проверка обновлений безопасности ОС** — данный параметр позволяет включить проверку наличия конкретных пакетов обновлений ОС. Перечислите требуемые пакеты обновлений безопасности ОС в поле ниже;
7. **Запущенные службы** — данный параметр позволяет включить проверку наличия запущенных служб Windows. В поле ниже необходимо указать все требуемые службы через пробел. Также параметр **Проверка автозапуска служб** становится доступным для взаимодействия;
8. **Проверка автозапуска служб** — данный параметр позволяет проверить, включена ли автозагрузка перечисленных служб.

Вкладка «SSH»

На вкладке **SSH** находятся блоки **Настройки подключения**, **Опрос** и **Проверки**. Заполните параметры в них, чтобы настроить использование транспорта SSH.

Блок «Настройки подключения»



В данном блоке доступны следующие параметры:

1. **Включить SSH** — активируйте данный параметр для включения использования транспорта SSH;

   Если не активировать данный параметр, сканирование по данному протоколу проводиться не будет.

   Если параметры **Включить WinRS** и **Включить SSH** активированы — происходит параллельное подключение по обоим включенным протоколам. В этом случае проверка проводится в зависимости от типа ОС. В случае, если событие безопасности 1300006 настроено так, что при смене MAC-адреса устройство переводится в изоляцию, то для использования функционала автоматического определения ОС для одного и того же суппликанта эту опцию необходимо отключить.
2. **Порт** — порт для подключения (по умолчанию порт 22);
3. **SSH Центр сертификатов для аутентификации пользователя** — центры сертификации, использующиеся для подписи сертификата клиента. Показываются центры, созданные на вкладке **Центры сертификации**;
4. **Имя пользователя** — имя учетной записи на конечном хосте, к которому будет подключаться сканер.

После сохранения всех настроек в блоке появится еще один параметр:

5. **Установочный скрипт** — скачайте этот скрипт и запустите его на суппликанте. Он выполняет настройки Учетной записи с именем, указанным в параметре **Имя пользователя**, SSH-сервера и проверяет необходимые утилиты для проведения проверок. В настройках SSH-сервера скрипт устанавливает параметр **PubkeyAuthentication** в значение YES. Также он содержит параметр **TrustedUserCAKeys** с файлом открытого ключа удостоверяющего центра, указанного в параметре **SSH Центр сертификатов для аутентификации пользователя** .

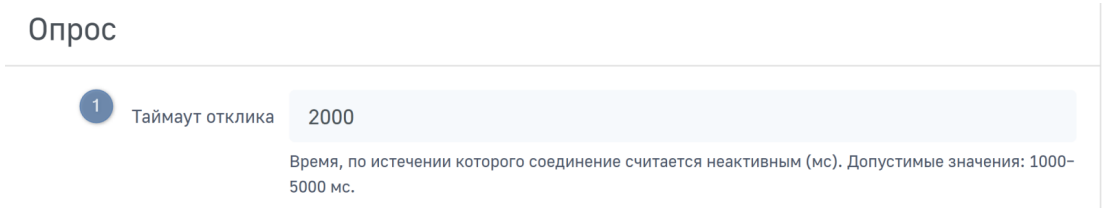
   Минимальная версия для реализации такого типа аутентификации - 9.2.p3. Проверка минимальной версии заложена в инсталляционный скрипт.

«Настройки SSH по умолчанию»

Для установки соединения с SSH-сервером AxelNAC использует методы обмена ключами, шифры и имитовставки, указанные в веб-интерфейсе.

Другие значение AxelNAC не использует по умолчанию, так как они являются менее защищенными.

Блок «Опрос»

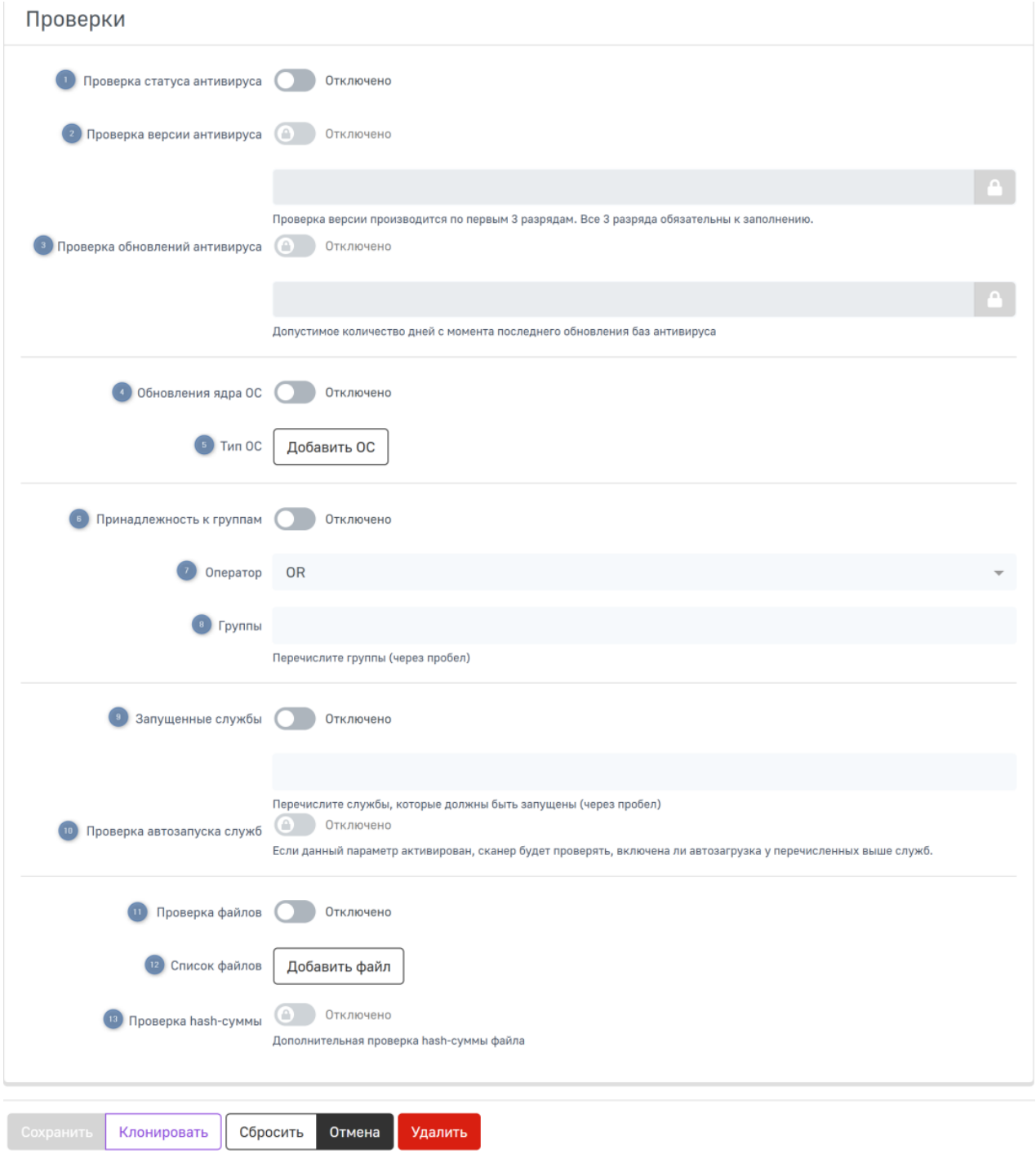


В данном блоке доступны следующие параметры:

1. **Таймаут отклика** — данный параметр задает таймаут для каждой операции (установка соединения, аутентификация, открытие канала коммуникации, выполнение операции, чтение результата, дисконнект-сообщение). Общий таймаут может составлять несколько секунд при последовательном выполнении операций. Допустимые значения: 1000–5000 мс. Рекомендуемое значение: 2000 мс. Уменьшение приведет к потере соединения при нестабильном соединении.

Блок «Проверки»

Для проведения проверок сканер использует пакеты **hostnamectl, systemctl, kesl-control, test, md5sum, who, id**. Отсутствие в системе пакетов влияет на функционал, они нужны для корректной работы.



В данном блоке доступны следующие параметры:

1. **Проверка статуса антивируса** — при активации данного параметра запускаются проверки версии антивируса и даты обновления баз. Также параметры **Проверка версии антивируса** и **Проверка обновлений антивируса** становятся доступными для взаимодействия;
2. **Проверка версии антивируса** — при активации данного параметра выполняется проверка версии антивируса, указанной в поле ниже. В поле необходимо указывать первые 3 октета версии антивируса;
3. **Проверка обновлений антивируса** — при активации данного параметра производится проверка даты последнего обновления и сравнение с максимально допустимым значением, указанным в поле ниже;

   В данном блоке проводятся проверки антивируса KESL.

4. **Обновления ядра ОС** — при активации данного параметра выполняется проверка соответствия минимальной версии ядра ОС;
5. **Тип ОС** — при нажатии кнопки **Добавить ОС**, показывает поле для выбора типа ОС и установки минимально допустимой ее версии ядра. В поле необходимо указывать первые 3 октета типа ОС;

   Проверка версии ядра производится по первым трем октетам.

6. **Принадлежность к группам** — при активации данного параметра проверяется принадлежность активного пользователя, использующего GUI, к группам, указанным в поле **Группы**;
7. **Оператор** — выбор оператора:
   - **OR** — проверка считается успешной при наличии хотя бы 1 группы из списка ниже;

    - **AND** — проверка считается успешной при соответствии всех групп из списка ниже.
8. **Группы** — список групп, к которым должен принадлежать пользователь;
9. **Запущенные службы** — при активации данного параметра указанные в поле ниже службы, которые участвуют в проверке, будут проверены на статус Active. Любой другой статус службы будет обработан как ошибочный и приведет к появлению триггера. Параметр позволяет дополнительно выполнить проверку автозапуска служб. Также параметр **Проверка автозапуска служб** становится доступным для взаимодействия;
10. **Проверка автозапуска служб** — при активации данного параметра при загрузке системы выполняется проверка активности автозагрузки у перечисленных служб;
11. **Проверка файлов** — при активации данного параметра выполняется проверка места расположения файла в системе. Также параметр **Проверка hash-суммы** становится доступным для взаимодействия;

    Проверка некоторых системных директорий может быть недоступна, например **root**, **proc** (конкретный набор зависит от дистрибутива). Это связано с тем, что данные директории являются системными и доступ к ним для пользователя запрещен.

12. **Список файлов** — при нажатии кнопки **Добавить файл**, показывается поля, которые необходимо заполнить путем к файлу, а также его hash-суммой. Путь и название файла могут быть указаны как на английском, так и на русском языке;
13. **Проверка hash-суммы** — при активации данного параметра выполняется дополнительная проверка целостности файла по hash-сумме.

    В случае, если hash-сумма не указана, данная проверка будет пропущена и для протокола SSH не будет вызван триггер **ScanIsFailed** и **HashDoesNotMatch**.

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**, **Хост**, **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 экспортировать 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.

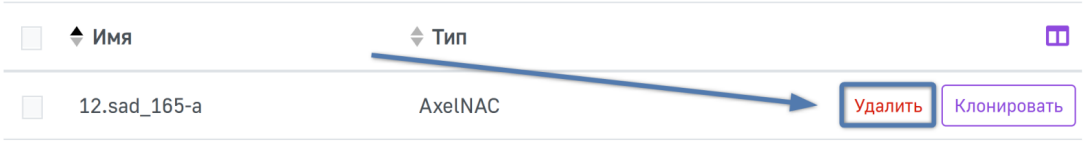
Клонирование механизма сканирования

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

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

Удаление механизма сканирования

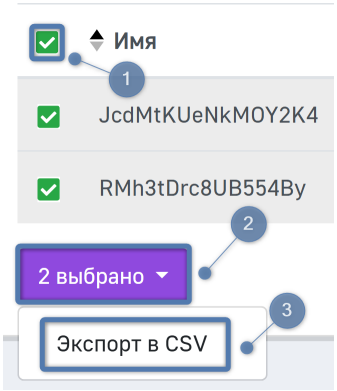
Для того чтобы удалить механизм сканирования, нажмите **Удалить**. После этого подтвердите удаление.



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.



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: 1945
Последнее обновление: 20 мая, 2026
Обновлено от: Егоров В.
Ревизия: 9
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.2.0 -> AxelNAC. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Соответствие» -> Страница «Механизмы сканирования» -> Вкладка «Механизмы сканирования»
https://docs.axel.pro/entry/1945/