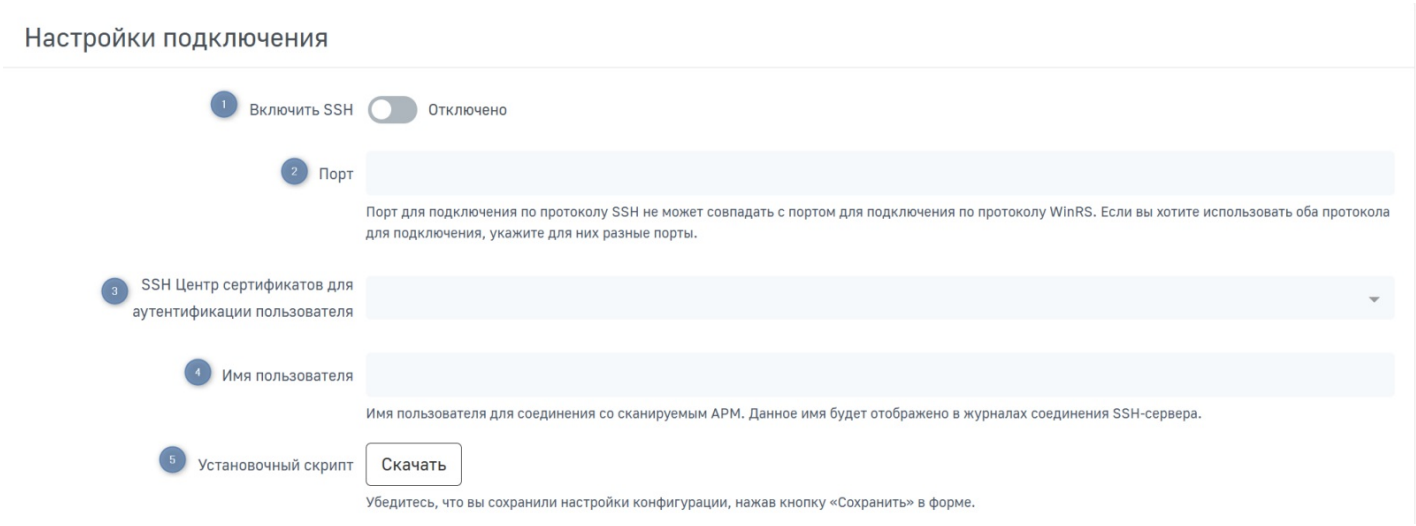
Конфигурация протокола SSH для подключения к сканируемому устройству

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 оконечного устройства.
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** .

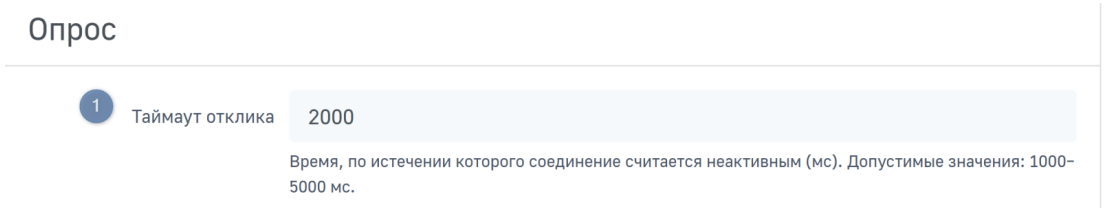
   Минимальная версия для реализации такого типа аутентификации - 9.2.p3. Проверка минимальной версии заложена в инсталляционный скрипт.

«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»

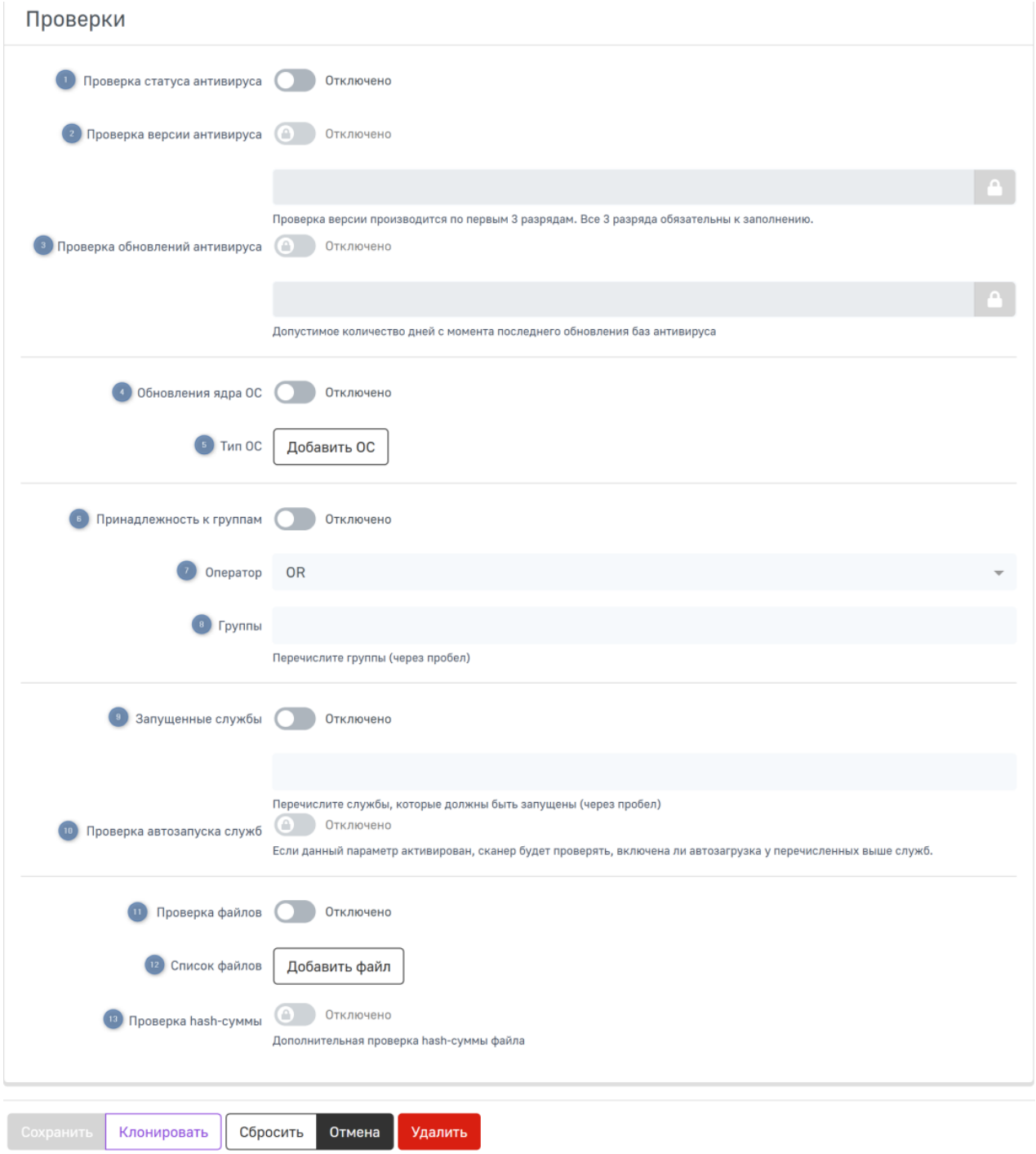


В данном блоке доступны следующие параметры:

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**.

ID статьи: 1416
Последнее обновление: 20 февр., 2026
Обновлено от: Ильина В.
Ревизия: 37
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.1.0 -> AxelNAC. Руководство администратора -> Конфигурация сканеров соответствия -> Конфигурация сканеров соответствия в AxelNAC -> Добавление механизма сканирования -> Конфигурация протокола SSH для подключения к сканируемому устройству
https://docs.axel.pro/entry/1416/