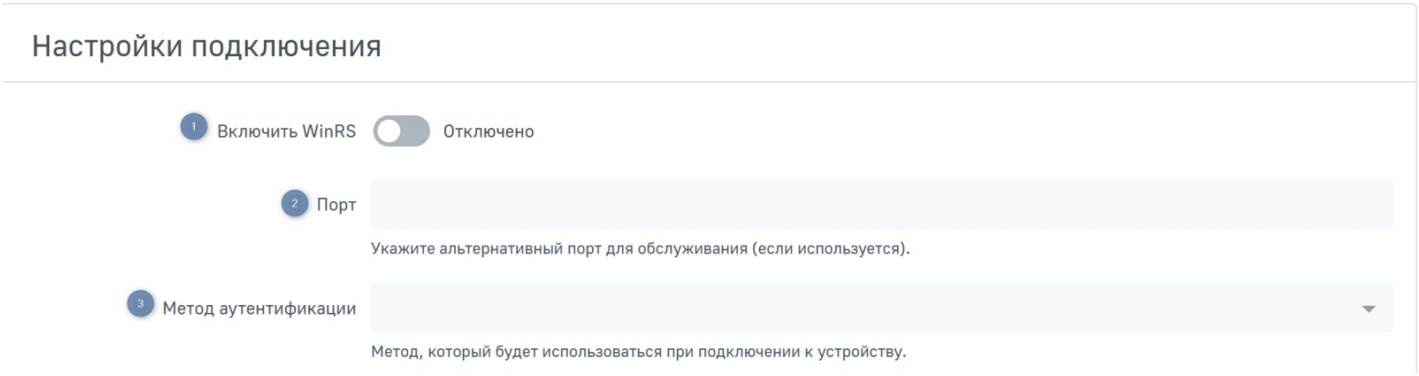
Конфигурация протокола WinRS для подключения к сканируемому устройству

На вкладке **WinRS** находятся блоки **Настройки подключения**, **Фильтры** и **Проверки**. Заполните параметры в них, чтобы настроить сканер соответствия с использованием протокола 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 протоколу WinRS проводиться не будет.

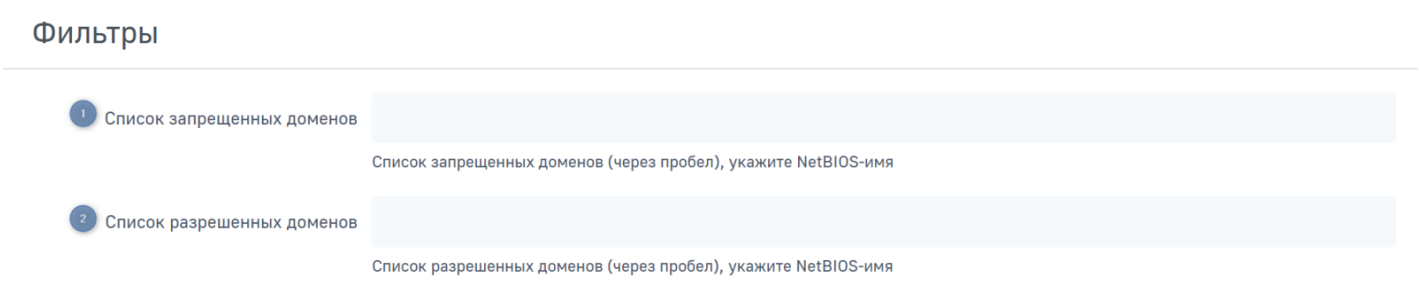
   Если параметры **Включить WinRS** и **Включить SSH** активированы — происходит параллельное подключение по обоим включенным протоколам. В этом случае проверка проводится в зависимости от типа ОС конечного устройства.
2. **Порт** — порт для подключения (по умолчанию создается порт 5985 — для базовой аутентификации, 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;
     - **Цепочка сертификатов УЦ** — файл с цепочкой сертификатов;
     - **Закрытый ключ** — закрытый ключ для расшифровки цепочки сертификатов;
     - **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 на конечном хосте, к которому будет подключаться сканер.
   - **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.

При выборе метода аутентификации **По сертификату** необходимо включить выполнение неподписанных скриптов через командную строку. Для этого используйте команду **PowerShell -executionpolicy RemoteSigned -file <имя_скрипта>**.

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

Блок «Фильтры»

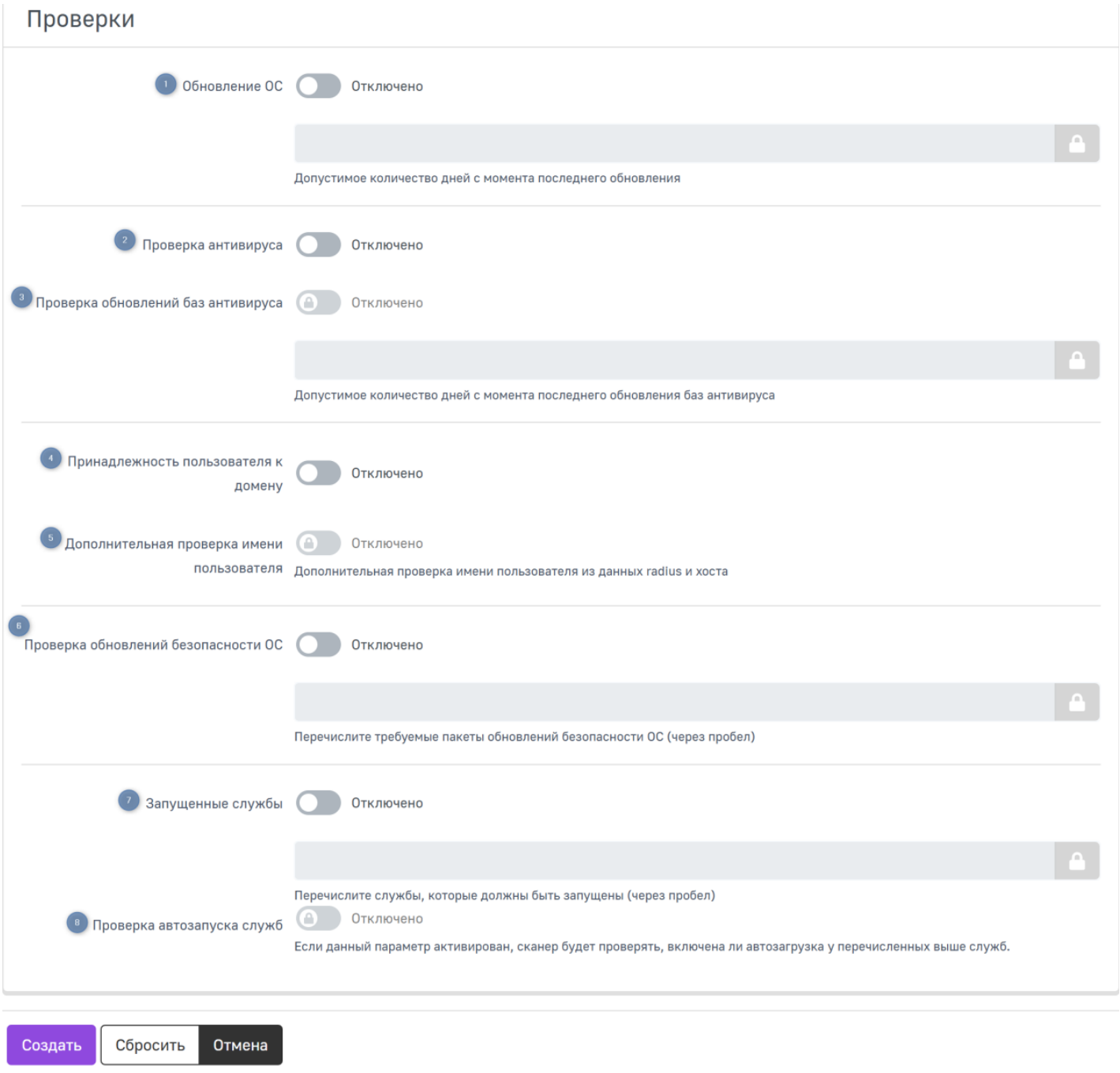
В случае, если в имени домена указано WORKGROUP, проверки из данного блока не выполняются. Это связано с тем, что данное имя присваивается для устройств, не введенных в домен.



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;

   В данном поле не рекомендуется указывать следующие проверки:
   • **Некритические обновления:** Данное поле предназначено для проверки критических обновлений и обновлений безопасности.
   • **Обновления, которые по умолчанию включены только на версии Windows, содержащих патч KB5066835 (Oct 14, 2025) for Windows 11 24H2/25H2":** В других дистрибутивах эти обновления могут отсутствовать, что приведет к срабатыванию триггера.
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.

ID статьи: 1415
Последнее обновление: 6 апр., 2026
Обновлено от: Ильина В.
Ревизия: 26