

# Конфигурация сканеров соответствия в AxeINAC

Для того, чтобы проверки на соответствие требованиям корректно работали в AxeINAC (взаимодействовали и генерировали события безопасности внутри AxeINAC), необходимо добавить механизм сканирования, настроить события безопасности и связать механизм сканирования с профилем подключения в AxeINAC.

## Добавление механизма сканирования

Для того, чтобы добавить новый механизм сканирования в AxeINAC, выполните следующие действия:

**Шаг 1.** В разделе **Конфигурация → Соответствие → Механизмы сканирования** нажмите **Новый механизм сканирования**.

**Шаг 2.** Заполните параметры на открывшейся странице и нажмите **Создать**.

Для каждого сканера существуют общие параметры:

- **Имя** — имя механизма сканирования;
- **Роли** — Будут затронуты только устройства с указанными ролями (необязательно);
- **Сканирование перед регистрацией** — Запуск сканирования при появлении устройства в регистрационной VLAN;
- **Сканирование при регистрации** — Запуск сканирования сразу после регистрации на Captive-портале;
- **Сканирование после регистрации** — Запуск сканирования в производственной сети (**pfdhcplistener** должен принимать продуктивный dhcp-трафик).

### Специфичные параметры для WinRS:

- **Метод аутентификации** — метод аутентификации, который будет использоваться при подключении к устройству:
    - **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.
  - **Имя пользователя** — имя пользователя локальной учетной записи для подключения к WinRS;
  - **Пароль** — пароль локальной учетной записи для подключения к WinRS;
  - **Порт** — порт для подключения (по умолчанию порт 5985 — для базовой аутентификации, порт 5985 — для аутентификации по сертификату и HTTPS);
  - **Роли** — список ролей узлов, для которых будет срабатывать механизм фильтрации;
  - **Запрещенный список доменов** — список доменов, для которых запрещено подключение к сети с данным механизмом фильтрации;
  - **Разрешенный список доменов** — список доменов, для которых разрешено подключение к сети с данным механизмом фильтрации;
  - **Обновление ОС** — данный параметр позволяет включить проверку наличия обновлений ОС. Также вы можете указать конкретное количество дней с момента последнего обновления (значение по умолчанию — 30 дней);
  - **Проверка антивируса** — данный параметр позволяет включить проверку наличия включенного антивируса. В данный момент поддержана проверка **Kaspersky Endpoint Security** и **Windows Defender**;
  - **Проверка обновлений баз антивируса** — данный параметр позволяет включить проверку наличия обновлений баз антивируса. Также вы можете указать конкретное количество дней с момента последнего обновления (значение по умолчанию — 14 дней);
  - **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;
  - **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;
  - **Проверка обновлений безопасности ОС** — данный параметр позволяет включить проверку наличия конкретных пакетов обновлений ОС. В поле ниже необходимо указать все требуемые пакеты обновлений через пробел;
  - **Запущенные службы** — данный параметр позволяет включить проверку наличия запущенных служб Windows. В поле ниже необходимо указать все требуемые службы через пробел;
  - **Проверка автозапуска служб** — данный параметр позволяет проверить, включена ли автозагрузка перечисленных служб.
- 
- Для успешного подключения к сканируемому устройству, необходимо создать на нем локальную учетную запись с правами администратора;
  - По умолчанию таймаут ответа на каждый из запросов, отправляемых WinRS при сканировании, имеет значение в 300 с.

## Настройка событий безопасности

Для того чтобы настроить события безопасности, перейдите в раздел **Конфигурация → Соответствие → События безопасности** и нажмите **Новое событие безопасности**.

Подробный процесс настройки событий безопасности описан в статье [Конфигурация событий безопасности](#).

Для того, чтобы связать событие безопасности с механизмом сканирования, необходимо выбрать сканер в поле **Событие** строки **Триггеры события** и указать идентификатор события сканера.

#### Список идентификаторов триггеров и условий их срабатывания во время сканирования для сканера WinRS:

- **ScanIsFailed** — не удалось подключиться к клиентскому устройству через сканер WinRS;
- **ScanIsSuccess** — удалось подключиться к клиентскому устройству через сканер WinRS (при этом неважно было ли проведено сканирование дальше);
- **OsIsNotUpdated** — срабатывание при выполнении хотя бы одного из условий:
  - Последний поиск обновлений был выполнен больше значения поля "Допустимое количество дней с момента последнего обновления";
  - В списке обновлений на установку есть хотя бы одно обновление типа **Critical Updates** или **Security Update**.
- **OsKBPatchesAreNotInstalled** — среди списка обновлений на установку есть хотя бы одно из значений "Обновления требуемые для проверки" с типом **Critical** или **Security**;
- **AntivirusIsNotInstalled** — не удалось найти установленный антивирус;
- **AntivirusDefenderIsNotInstalled** — не установлен антивирус Windows Defender;
- **AntivirusKESIsNotInstalled** — не установлен антивирус Kaspersky Endpoint Security;
- **AntivirusIsNotTurnedOn** — нет ни одного запущенного антивируса;
- **AntivirusDefenderIsNotTurnedOn** — антивирус Windows Defender не запущен;
- **AntivirusKESIsNotTurnedOn** — антивирус Kaspersky Endpoint Security не запущен;
- **AntivirusIsNotUpdated** — антивирус не содержит обновленные антивирусные базы;
- **AntivirusDefenderIsNotUpdated** — срабатывание при выполнении хотя бы одного из условий:
  - Статус антивируса Windows Defender — **не обновлен**;
  - Дата последнего успешного поиска обновлений больше значения **Допустимый порог устаревания антивирусных баз**.
- **AntivirusKESIsNotUpdated** — срабатывание при выполнении хотя бы одного из условий:
  - Статус антивируса Kaspersky Endpoint Security — **не обновлен**;
  - Дата последнего успешного поиска обновлений больше значения **Допустимый порог устаревания антивирусных баз**.
- **ServiceIsNotRunning** — срабатывание если отсутствует служба со статусом **running**(запущена) в списке сервисов Windows;
- **ServiceIsNotStartAutomatically** — срабатывание при отсутствии флага **automatic** у службы автозагрузки;
- **HostDataIsNotValid** — срабатывание при выполнении хотя бы одного из условий:
  - Не была найдена активная сессия на стороне хоста;
  - На стороне хоста обнаружено более одной активной сессии;
  - Имя пользователя хоста не совпадает с данными переданными через RADIUS.
- **ADDataIsMissing** — срабатывание при выполнении хотя бы одного из условий:
  - SID пользователя не найден;
  - Пользователь не найден в AD.
- **UsernameMatchingIsFailed** — срабатывание при несовпадении значений Username хоста и данных из AD;
- **FQDNMatchingIsFailed** — срабатывание при несовпадении значений FQDN хоста и данных из AD;
- **SIDMatchingIsFailed** — срабатывание при несовпадении значений SID хоста и данных из AD.

После завершения настройки перезагрузите содержимое базы данных, связанное с событиями безопасности с помощью следующей команды:

```
pfcmd reload security_events
```

ОС Windows не позволяет корректно определять идентификаторы обновлений и патчей не имеющих тип **Critical** или **Security**, например обновления с типом **Drivers**.

## Добавление механизма сканирования в профиль подключения

После того как процесс и логика работы сканера настроены, необходимо добавить сканер в профиль подключения:

**Шаг 1.** Перейдите в раздел **Конфигурация** → **Политики и контроль доступа** → **Профили подключения** и откройте/создайте профиль подключения.

**Шаг 2.** На открывшейся странице в строке **Сканеры** нажмите на кнопку **Добавить сканер** и укажите имя сканера, который вы хотите добавить, затем нажмите **Сохранить**.

---

ID статьи: 589

Последнее обновление: 8 дек., 2025

Обновлено от: Егоров В.

Ревизия: 19

База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.0.1 -> AxelNAC. Руководство администратора -> Конфигурация сканеров соответствия -> Конфигурация сканеров соответствия в AxelNAC

<https://docs.axel.pro/entry/589/>