Методы аутентификации сканера WinRS

Сканер WinRS является предустановленным в AxelNAC сканером соответствия. Данный сканер использует службу **winrm**, которая является встроенным протоколом в ОС Windows и выступает в роли транспорта безагентского сканера AxelNAC. При подключении к клиентскому устройству, сканеру необходимо пройти процесс аутентификации. В данной версии AxelNAC поддерживается три метода аутентификации сканера WinRS:

- Базовая аутентификация;
- Базовая аутентификация с использованием HTTPS;
- Аутентификация на основе сертификата.

Рассмотрим каждый из методов более подробно.

Базовая аутентификация

Описание метода аутентификации

Базовая аутентификация представляет собой аутентификацию на основе учетных данных (имя пользователя/пароль). Для процесса аутентификации необходимо создать локальную учетную запись с правами локального администратора для сканера на сканируемом устройстве.

Данный метод аутентификации сканера не рекомендуется, т.к. является небезопасным из-за использования транспортного протокола **HTTP**.

Конфигурация сканируемого устройства для базовой аутентификации сканера

Для того, чтобы реализовать метод базовой аутентификации сканера, необходимо выполнить следующие действия:

Шаг 1. Создайте учетную запись для сканера WinRS на сканируемом устройстве.

Шаг 2. Запустите интерфейс командной строки с правами администратора на сканируемом устройстве и разрешите использование незашифрованной аутентификации с помощью следующего набора команд:

```
winrm qc
cd WSman:\localhost\
cd Client
set-item AllowUnencrypted $true
set-item TrustedHosts "*"
cd ..\Service set-item AllowUnencrypted $true
cd Auth
set-item Basic $true
```

После этого сканируемое устройство полностью настроено для базовой аутентификации сканера.

Конфигурация AxelNAC

Шаг 1. Откройте веб-интерфейс AxelNAC. Перейдите в раздел **Конфигурация → Соответствие → Механизмы сканирования** , создайте новый механизм сканирования с типом WinRS.

Шаг 2. Выберите метод аутентификации **Базовый**.

Шаг 3. Укажите имя пользователя и пароль от учетной записи, которая будет использоваться для подключения сканера.

После этого базовая аутентификация сканера настроена.

Базовая аутентификация через HTTPS

Описание метода аутентификации

Базовая аутентификация через HTTPS представляет собой защищенную аутентификацию на основе учетных данных (имя пользователя/пароль) с использованием SSL-сертификата. Для процесса аутентификации необходимо создать на сканируемом устройстве локальную учетную запись с правами локального администратора для сканера, а также подготовить на нем SSL-сертификат для реализации защищенного соединения.

При выборе данного метода аутентификации, в окне конфигурации сканера соответствия появятся дополнительные поля:

- **Сертификат удостоверяющего центра** — поле для загрузки SSL-сертификата в формате **pem**;
- **Скрипт установки** — кнопка для загрузки скрипта, используемого для настройки метода аутентификации на сканируемом устройстве с помощью транспортного протокола **HTTPS**.

Для корректной аутентификации сканера WinRS необходимо использовать сертификат, выпущенный удостоверяющим центром.

Конфигурация метода аутентификации сканера по сертификату

Подготовка шаблонов сертификата

Для того, чтобы подготовить сертификаты для сканера и сканируемого устройства выполните следующие действия:

Шаг 1. Подключитесь к контроллеру домена и войдите в утилиту **Центр Сертификации**.

Шаг 2. В левой части окна выберите удостоверяющий центр, нажмите правой кнопкой мыши на раздел **Шаблоны сертификатов** и в выпадающем списке выберите **Управление**.

Шаг 3. Нажмите правой кнопкой мыши на предустановленный шаблон пользователя и выберите **Скопировать шаблон**.

Шаг 4. Настройте шаблон пользователя:

1. На вкладке **Совместимость** активируйте работу совместимости и выберите совместимость с **Windows Server 2003** и **Windows XP**.
2. На вкладке **Общие** укажите имя шаблона, периоды действия и обновления сертификата, а также активируйте флажок **Опубликовать сертификат в Active Directory** .
3. На вкладке **Обработка запроса** выберите в поле **Цель** значение **Подпись и шифрование**, активируйте флажок **Разрешить экспортировать закрытый ключ** и активируйте параметр **Подавать заявку для субъекта, не требуя ввода данных** .
4. На вкладке **Расширения** убедитесь, что для параметра **Политики применения** добавлено значение **Проверка подлинности сервера**.
5. На вкладке **Безопасность** добавьте пользователя, которому будет разрешено использовать шаблон и активируйте для него все необходимые разрешения.
6. На вкладке **Шифрование** в поле **Имя алгоритма** выберите значение **Определяется поставщиком служб шифрования**, и активируйте флажок **В запросах могут использоваться только следующие поставщики**, после чего выберите **Microsoft Enhanced Cryptographic Provider v1.0**.
7. На вкладке **Имя субъекта** активируйте флажок **Предоставляется в запросе**, после чего нажмите **Сохранить**.

Шаг 5. Создайте шаблон для выпуска сертификата AxelNAC. Для этого скопируйте предыдущий сертификат и на вкладке **Расширения** для параметра **Политики применения** замените значение **Проверка подлинности сервера** на **Проверка подлинности клиента**.

Шаг 6. Добавьте созданные шаблоны в удостоверяющий центр. Для этого нажмите правой кнопкой мыши на свободном участке окна удостоверяющего центра и в выпадающем окне нажмите **Создать → Выдаваемый шаблон сертификата**. Выберите ранее созданные шаблоны и нажмите **Ok**.

Подготовка сертификата и приватного ключа для клиента

Для того, чтобы сгенерировать сертификат и ключ с помощью шаблонов Active Directory, выполните следующие действия:

Шаг 1. Подключитесь к контроллеру домена, запустите утилиту **Выполнить** с помощью комбинации **Win+R** и введите **mmc**, для запуска утилиты **Консоль управления**.

Шаг 2. На вкладке **Файл** выберите **Добавить или удалить оснастку**.

Шаг 3. Добавьте оснастку **Сертификаты** и сконфигурируйте её:

1. Выберите параметр **Учетной записи компьютера** и нажмите **Далее**.
2. Выберите параметр **Локальным компьютером** и нажмите **Готово**.

Шаг 4. В добавленной оснастке нажмите правой кнопкой мыши на папке **Сертификаты**, выберите параметр **Все задачи**, затем **Запросить новый сертификат** и сконфигурируйте запрос:

1. Нажмите **Далее**, затем еще раз **Далее**.
2. Активируйте флажок для шаблона, который будет использоваться для выпуска сертификата и нажмите на поле для добавления данных для подачи заявки.
3. В окне **Свойства сертификата** для имени субъекта выберите тип **Общее имя** и укажите FQDN сканируемого устройства с указанием домена (**например:** gp.axeldemo.pro), затем нажмите **Ok**.
4. Проверьте, чтобы пользователь для сертификата был активен и нажмите **Заявка**, затем **Готово**.

При генерации сертификата для кластерной инсталляции AxelNAC необходимо указывать FQDN кластера с указанием домена.

Шаг 5. Экспортируйте закрытый ключ сертификата, указав в окне **Безопасность** параметр **Пароль** и укажите восьмизначный пароль.

После выполнения действий будут создан файл **cert.pfx**, который является контейнером сертификата пользователя.

Конфигурация AxelNAC

Шаг 1. Откройте веб-интерфейс AxelNAC. Перейдите в раздел **Конфигурация → Соответствие → Механизмы сканирования** , создайте новый механизм сканирования с типом WinRS.

Шаг 2. Выберите метод аутентификации **Базовый через HTTPS**.

Шаг 3. Укажите имя пользователя и пароль от учетной записи, которая будет использоваться для подключения сканера.

Шаг 4. Добавьте сертификат удостоверяющего центра в формате **.pem**.

После этого базовая аутентификация сканера через HTTPS настроена.

Конфигурация сканируемого устройства

Сканируемое устройство может быть настроено двумя способами: в автоматическом и в ручном режиме. Ниже приведено описание этих способов.

Автоматическая конфигурация сканируемого устройства

Для того, чтобы настроить сканируемое устройство в автоматическом режиме, выполните следующие действия:

Шаг 1. На сканируемом устройстве создайте локальную учетную запись, которая будет использоваться для аутентификации с использованием HTTPS и наделите ее правами администратора.

Шаг 2. Скачайте скрипт конфигурации сканируемого устройства в окне конфигурации механизма сканирования, нажав **Скачать скрипт установки**.

Шаг 3. Запустите скрипт на сканируемом устройстве.

Убедитесь, что вы настроили механизм сканирования перед скачиванием скрипта установки. В ином случае, скрипт может быть сформирован некорректно.

Ручная конфигурация сканируемого устройства

Для того, чтобы настроить сканируемое устройство в ручном режиме, выполните следующие действия:

Шаг 1. На сканируемом устройстве создайте локальную учетную запись, которая будет использоваться для аутентификации с использованием HTTPS и наделите ее правами администратора.

Шаг 2. Включите поддержку транспортного протокола **HTTPS** для службы **winrm**:

1. Отключите в домене проверку отзыва сертификатов (CDP/CRL) (опционально, для случаев, когда подключающаяся машина не введена в домен и не имеет возможности обратиться к службе CDP/CRL для просмотра отозванных сертификатов).
2. Ранее выгруженный контейнер сертификата в формате **PFX** установите на сканируемом устройстве и включите транспортный протокол **HTTPS** для службы **winrm** (сертификат необходимо установить в хранилище **Сертификаты (локальный компьютер) → Личное** .
3. Скопируйте значение поля **Отпечаток** в сертификате, оно вам понадобится на следующем этапе.
4. Убедитесь, что в доверенных корневых сертификатах установлен сертификат Центра сертификации (например, **axeldemo.pro**) и включите транспортный протокол **HTTPS** для службы **winrm**:

   ```
   winrm quickconfig -transport:https
   winrm create winrm/config/Listener?Address=*+Transport=HTTPS '@{Hostname="gp.axeldemo.pro";CertificateThumbprint="6cfe3df4a69f750debdcd878389dfb09cd3b17c0"}'
   ```

   - **Hostname** должен совпадать с **CN** ранее созданного сертификата (например, gp.axeldemo.pro).
   - **CertificateThumbprint** должен быть равен отпечатку ранее созданного сертификата.
5. Активируйте аутентификацию по сертификатам с помощью следующей команды:

   ```
   Set-Item -Path WSMan:\localhost\Service\Auth\Certificate -Value $true
   ```

6. Проверьте, что транспортный протокол включен с помощью следующей команды:

   ```
   winrm enumerate winrm/config/listener
   ```

   При успешном выполнении команды вы получите результат, как на рисунке ниже:

```
PS C:\Windows\system32> winrm enumerate winrm/config/listener
Listener
    Address = *
    Transport = HTTP
    Port = 5985
    Hostname
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint
    ListeningOn = 10.31.208.11, 127.0.0.1, 169.254.110.170, 192.168.56.1, ::1, fe80::2c7c:cb73:dacb:27c2%7, fe80::6765:7432:74de:66b1%14, fe80::f15f:ffe2:

Listener
    Address = *
    Transport = HTTPS
    Port = 5986
    Hostname = AxelNB1
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint = 6cfe3df4a69f750debdcd878389dfb09cd3b17c0
    ListeningOn = 10.31.208.11, 127.0.0.1, 169.254.110.170, 192.168.56.1, ::1, fe80::2c7c:cb73:dacb:27c2%7, fe80::6765:7432:74de:66b1%14, fe80::f15f:ffe2:
```

7. Если вы ошиблись при настройке сертификата, выполните следующую команду для того, чтобы удалить listener:

   ```
   winrm delete winrm/config/Listener?Address=*+Transport=HTTPS
   ```

Аутентификация по сертификату

Описание метода аутентификации

Аутентификация по сертификату представляет собой аутентификацию для которой не требуется указание имени пользователя/пароля для доступа к локальной учетной записи, а в качестве аутентификатора используется сертификат.

При выборе данного метода аутентификации, в окне конфигурации сканера соответствия появятся дополнительные поля:

- **Файл сертификата** — поле для загрузки файла сертификата. В данное поле необходимо загрузить сертификат в формате **pem**, содержащий открытую часть ключа. Поле **CN** в сертификате должно соответствовать имени локальной учетной записи, созданной на сканируемом устройстве;
- **Отпечаток CA сертификата** — поле для указания SHA1 сертификата, следующего по очереди (SHA1 сертификата удостоверяющего центра/внутреннего удостоверяющего центра);
- **Сертификат центра сертификации для SSL в HTTPS** — поля для загрузки сертификата удостоверяющего центра в формате **pem**;
- **Закрытый ключ** — поле для загрузки закрытого ключа сертификата в формате **key**;
- **Пароль для закрытого ключа** — поле для указания парольной фразу для доступа к закрытому ключу;
- **Скрипт установки** — кнопка для загрузки скрипта, используемого для настройки метода аутентификации на сканируемом устройстве с помощью транспортного протокола **HTTPS**.

Для корректной аутентификации сканера WinRS необходимо использовать сертификаты, выпущенные удостоверяющим центром.

Конфигурация метода аутентификации сканера по сертификату

Подготовка шаблонов сертификата

Для того, чтобы подготовить сертификаты для сканера и сканируемого устройства выполните следующие действия:

Шаг 1. Подключитесь к контроллеру домена и войдите в утилиту **Центр Сертификации**.

Шаг 2. В левой части окна выберите удостоверяющий центр, нажмите правой кнопкой мыши на раздел **Шаблоны сертификатов** и в выпадающем списке выберите **Управление**.

Шаг 3. Нажмите правой кнопкой мыши на предустановленный шаблон пользователя и выберите **Скопировать шаблон**.

Шаг 4. Настройте шаблон пользователя:

1. На вкладке **Совместимость** активируйте работу совместимости и выберите совместимость с **Windows Server 2003** и **Windows XP**.
2. На вкладке **Общие** укажите имя шаблона, периоды действия и обновления сертификата, а также активируйте флажок **Опубликовать сертификат в Active Directory**.
3. На вкладке **Обработка запроса** выберите в поле **Цель** значение **Подпись и шифрование**, активируйте флажок **Разрешить экспортировать закрытый ключ** и активируйте параметр **Подавать заявку для субъекта, не требуя ввода данных**.
4. На вкладке **Расширения** убедитесь, что для параметра **Политики применения** добавлено значение **Проверка подлинности сервера**.
5. На вкладке **Безопасность** добавьте пользователя, которому будет разрешено использовать шаблон и активируйте для него все необходимые разрешения.
6. На вкладке **Шифрование** в поле **Имя алгоритма** выберите значение **Определяется поставщиком служб шифрования**, и активируйте флажок **В запросах могут использоваться только следующие поставщики**, после чего выберите **Microsoft Enhanced Cryptographic Provider v1.0**.
7. На вкладке **Имя субъекта** активируйте флажок **Предоставляется в запросе**, после чего нажмите **Сохранить**.

Шаг 5. Создайте шаблон для выпуска сертификата AxelNAC. Для этого скопируйте предыдущий сертификат и на вкладке **Расширения** для параметра **Политики применения** замените значение **Проверка подлинности сервера** на **Проверка подлинности клиента**.

Шаг 6. Добавьте созданные шаблоны в удостоверяющий центр. Для этого нажмите правой кнопкой мыши на свободном участке окна удостоверяющего центра и в выпадающем окне нажмите **Создать → Выдаваемый шаблон сертификата**. Выберите ранее созданные шаблоны и нажмите **Ok**.

Подготовка сертификата и приватного ключа для клиента

Для того, чтобы сгенерировать сертификат и ключ с помощью шаблонов Active Directory, выполните следующие действия:

Шаг 1. Подключитесь к контроллеру домена, запустите утилиту **Выполнить** с помощью комбинации **Win+R** и введите **mmc**, для запуска утилиты **Консоль управления**.

Шаг 2. На вкладке **Файл** выберите **Добавить или удалить оснастку**.

Шаг 3. Добавьте оснастку **Сертификаты** и сконфигурируйте её:

1. Выберите параметр **Учетной записи компьютера** и нажмите **Далее**.
2. Выберите параметр **Локальным компьютером** и нажмите **Готово**.

Шаг 4. В добавленной оснастке нажмите правой кнопкой мыши на папке **Сертификаты**, выберите параметр **Все задачи**, затем **Запросить новый сертификат** и сконфигурируйте запрос:

1. Нажмите **Далее**, затем еще раз **Далее**.
2. Активируйте флажок для шаблона, который будет использоваться для выпуска сертификата и нажмите на поле для добавления данных для подачи заявки.
3. В окне **Свойства сертификата** для имени субъекта выберите тип **Общее имя** и укажите FQDN сканируемого устройства с указанием домена (**например:** gp.axeldemo.pro), затем нажмите **Ок**.
4. Проверьте, чтобы пользователь, для которого создается сертификат, был активен и нажмите **Заявка**, затем **Готово**.

При генерации сертификата для кластерной инсталляции AxelNAC необходимо указывать FQDN кластера с указанием домена.

Шаг 5. Экспортируйте закрытый ключ сертификата, указав в окне **Безопасность** параметр **Пароль** и укажите восьмизначный пароль.

После выполнения действий будут создан файл **cert.pfx**, который является контейнером сертификата пользователя.

Конфигурация AxelNAC

Для того, чтобы настроить AxelNAC для аутентификации сканера с помощью сертификата, выполните следующие действия:

Шаг 1. Выпустите сертификат для AxelNAC, используя ранее созданный шаблон.

Шаг 2. Переместите ранее созданный контейнер сертификатов в AxelNAC, используя следующую команду и введите пароль для доступа к AxelNAC:

```
scp C:\Users\{Имя пользователя}\downloads\{Контейнер сертификата}.pfx root@{IP-адрес AxelNAC}:~/{Контейнер сертификата}.pfx
```

Шаг 3. Подключитесь к AxelNAC по SSH, создайте и переместите сертификат в удобную директорию с помощью следующего набора команд:

```
mkdir scan_winrs_cert
mv /root/{Контейнер сертификата}.pfx scan_winrs_cert/
cd scan_winrs_cert
```

Шаг 4. В рабочей директории необходимо разделить сертификат на 3 части: Открытый ключ, сертификат УЦ, приватный ключ. Во время разделения сертификатов у вас запросят пароль от контейнера:

```
openssl pkcs12 -in {Контейнер сертификата}.pfx -clcerts -nokeys -out Axelnac_cert.crt
openssl pkcs12 -in {Контейнер сертификата}.pfx -cacerts -nokeys -out Axeldemo_CA.crt
openssl pkcs12 -in {Контейнер сертификата}.pfx -nocerts -out Axelnac_private_key.key
```

Шаг 5. Скорректируйте содержимое сертификатов: при экспорте через **openssl** могут появиться лишние данные, поэтому необходимо оставить только информацию о сертификатах (начиная с **------BEGIN CERTIFICATE------** и заканчивая **------END CERTIFICATE------**). Также необходимо инвертировать порядок указанных сертификатов так, чтобы первым был **сертификат УЦ** ближайший к клиенту.

Шаг 6. Полученные сертификаты необходимо перенести на АРМ, у которой есть доступ к веб-интерфейсу AxelNAC:

```
scp  root@{IP-адрес AxelNAC}:~/scan_winrs_cert/Axelnac_cert.crt C:\Users\{Имя пользователя}\downloads\Axelnac_cert.crt
scp  root@{IP-адрес AxelNAC}:~/scan_winrs_cert/Axeldemo_CA.crt C:\Users\{Имя пользователя}\downloads\Axeldemo_CA.crt
scp  root@{IP-адрес AxelNAC}:~/scan_winrs_cert/Axelnac_private_key.key C:\Users\{Имя пользователя}\downloads\Axelnac_private_key.key
```

Шаг 7. Для получения отпечатка сертификата на linux, воспользуйтесь командой:

```
openssl x509 -in cert.crt -fingerprint -sha1 -noout
```

Шаг 8. Откройте веб-интерфейс AxelNAC. Перейдите в раздел **Конфигурация → Соответствие → Механизмы сканирования**, создайте новый механизм сканирования с типом WinRS.

Шаг 9. Выберите метод аутентификации **Сертификат**.

Шаг 10. Добавьте сертификаты в соответствии с полями, где Axelnac_cert.crt - файл сертификата, Axeldemo_CA.crt — сертификат удостоверяющего центра, Axelnac_private_key.key — закрытый ключ. Также укажите пароль от закрытого ключа, если он есть.

Шаг 11. В поле **Отпечаток CA сертификата** укажите отпечаток сертификата центра сертификации.

Отпечаток CA сертификата должен быть равен отпечатку вышестоящего сертификата (например, промежуточного центра или удостоверяющего центра).

После этого аутентификация сканера с использованием сертификатов настроена.

Конфигурация сканируемого устройства

Сканируемое устройство может быть настроено двумя способами: в автоматическом и в ручном режиме. Ниже приведено описание этих способов.

Автоматическая конфигурация сканируемого устройства

Для того, чтобы настроить сканируемое устройство в автоматическом режиме, выполните следующие действия:

Шаг 1. На сканируемом устройстве создайте локальную учетную запись, которая будет использоваться для аутентификации с использованием сертификата и наделите ее правами администратора.

Шаг 2. Скачайте скрипт конфигурации сканируемого устройства в окне конфигурации механизма сканирования, нажав **Скачать скрипт установки**.

Шаг 3. Запустите скрипт на сканируемом устройстве.

Убедитесь, что вы настроили механизм сканирования перед скачиванием скрипта установки. В ином случае, скрипт может быть сформирован некорректно.

Ручная конфигурация сканируемого устройства

Для того, чтобы настроить сканируемое устройство в ручном режиме, выполните следующие действия:

Шаг 1. На сканируемом устройстве создайте локальную учетную запись, которая будет использоваться для аутентификации с использованием сертификата и наделите ее правами администратора.

Шаг 2. Включите поддержку транспортного протокола **HTTPS** для службы **winrm**:

1. Отключите в домене проверку отзыва сертификатов (CDP/CRL) (опционально, для случаев, когда подключающаяся машина не введена в домен и не имеет возможности обратиться к службе CDP/CRL для просмотра отозванных сертификатов).
2. Ранее выгруженный контейнер сертификата в формате **PFX** установите на сканируемом устройстве и включите транспортный протокол **HTTPS** для службы **winrm** (сертификат необходимо установить в хранилище **Сертификаты (локальный компьютер) → Личное**.
3. Скопируйте значение поля **Отпечаток** в сертификате, оно вам понадобится на следующем этапе.
4. Убедитесь, что в доверенных корневых сертификатах установлен сертификат Центра сертификации (например, **axeldemo.pro**) и включите транспортный протокол **HTTPS** для службы **winrm**:

   ```
   winrm quickconfig -transport:https
   winrm create winrm/config/Listener?Address=*+Transport=HTTPS '@{Hostname="gp.axeldemo.pro";CertificateThumbprint="6cfe3df4a69f750debdcd878389dfb09cd3b17c0"}'
   ```

- **Hostname** должен совпадать с **CN** ранее созданного сертификата (например, gp.axeldemo.pro).
- **CertificateThumbprint** должен быть равен отпечатку ранее созданного сертификата.

5. Активируйте аутентификацию по сертификатам с помощью следующей команды:

   Set-Item -Path WSMan:\localhost\Service\Auth\Certificate -Value $true

6. Проверьте, что транспортный протокол включен с помощью следующей команды:

   winrm enumerate winrm/config/listener

   При успешном выполнении команды вы получите результат, как на рисунке ниже:

```
PS C:\Windows\system32> winrm enumerate winrm/config/listener
Listener
    Address = *
    Transport = HTTP
    Port = 5985
    Hostname
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint
    ListeningOn = 10.31.208.11, 127.0.0.1, 169.254.110.170, 192.168.56.1, ::1, fe80::2c7c:cb73:dacb:27c2%7, fe80::6765:7432:74de:66b1%14, fe80::f15f:ffe2:

Listener
    Address = *
    Transport = HTTPS
    Port = 5986
    Hostname = AxelNB1
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint = 6cfe3df4a69f750debdcd878389dfb09cd3b17c0
    ListeningOn = 10.31.208.11, 127.0.0.1, 169.254.110.170, 192.168.56.1, ::1, fe80::2c7c:cb73:dacb:27c2%7, fe80::6765:7432:74de:66b1%14, fe80::f15f:ffe2:
```

7. Если вы ошиблись при настройке сертификата, выполните следующую команду для того, чтобы удалить listener:

   winrm delete winrm/config/Listener?Address=*+Transport=HTTPS

Шаг 3. Настройте строку запуска в интерфейсе командной строки с помощью следующего набора команд:

```
$password = ConvertTo-SecureString "password123" -AsPlainText -Force
$Cred = New-Object System.Management.Automation.PSCredential ("winrm-test", $password)
New-Item -Path WSMan:\localhost\ClientCertificate -Subject 'winrm-test' -URI * -Issuer 618d20af4ddda24981085e8f229e7d7b0c0e653f -Credential $cred ` -Force
```

Issuer должен быть равен отпечатку вышестоящего сертификата (например, промежуточного центра или удостоверяющего центра).

Созданную привязку можно проверить с помощью следующей команды:

dir WSMan:\localhost\ClientCertificate

Шаг 4. Если вы ошиблись при настройке, выполните следующую команду для отмены привязки:

Remove-Item -Recurse -Path WSMan:\localhost\ClientCertificate*

ID статьи: 135
Последнее обновление: 5 февр., 2025
Обновлено от: Егоров В.
Ревизия: 12
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 1.0.0 -> AxelNAC. Руководство администратора -> Конфигурация сканеров соответствия -> Методы аутентификации сканера WinRS
https://docs.axel.pro/entry/135/