Базовая аутентификация сканера AxelNAC с использованием протокола HTTPS

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 **AxelNAC** необходимо использовать сертификат, выпущенный удостоверяющим центром.

Конфигурация метода аутентификации сканера по SSL-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 **Ок**.

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 ее:

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 сертификата был активен и нажмите **Заявка**, затем **Готово**.

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 → Сканеры**, создайте новый механизм сканирования с типом AxelNAC.

Шаг 2. Перейдите на вкладку WinRS и 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. Ранее выгруженный контейнер сертификата в формате **PFX** установите на сканируемом устройстве (сертификат необходимо установить в хранилище **Сертификаты (локальный компьютер) → Личное**).

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"}'
   ```

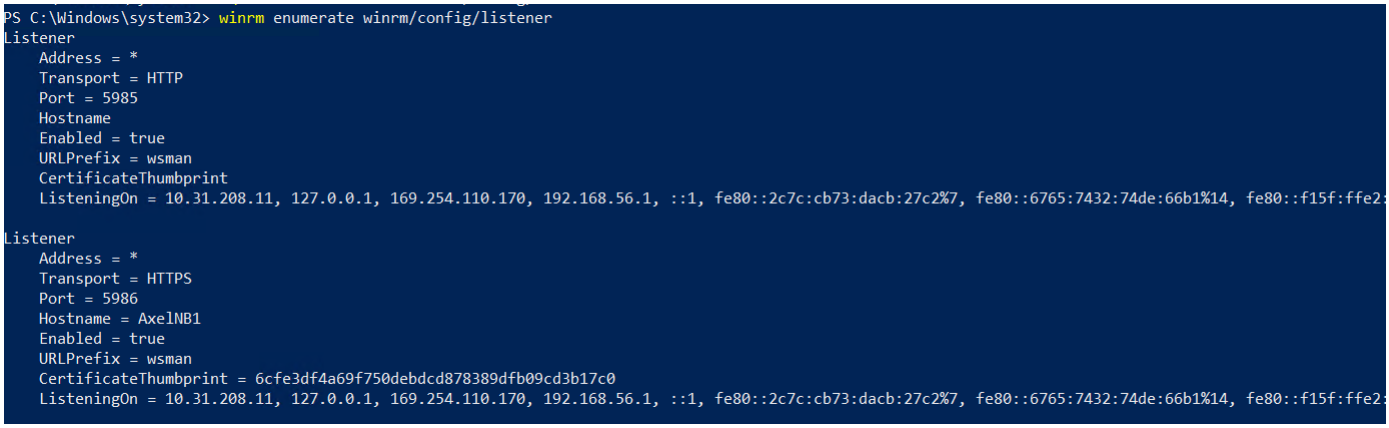
   - **Hostname** должен совпадать с **CN** ранее созданного сертификата (например, gp.axeldemo.pro).
   - **CertificateThumbprint** должен быть равен отпечатку ранее созданного сертификата.
5. Активируйте аутентификацию по сертификатам с помощью следующей команды:

   ```
   Set-Item -Path WSMan:localhostServiceAuthCertificate -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:



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

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

ID статьи: 982
Последнее обновление: 18 дек., 2025
Обновлено от: Ильина В.
Ревизия: 7
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.1.0 -> AxelNAC. Руководство администратора -> Конфигурация сканеров соответствия -> Методы аутентификации сканера AxelNAC по протоколу WinRS -> Базовая аутентификация сканера AxelNAC с использованием протокола HTTPS
https://docs.axel.pro/entry/982/