

Интеграция AxelNAC PKI

В данной статье описан процесс быстрой настройки AxelNAC PKI в AxelNAC. В описании не приводится расширенный поиск и устранение неисправностей в соединениях EAP-TLS. За дополнительной информацией обратитесь к документации по EAP-TLS, RADIUS и OpenSSL.

AxelNAC PKI по умолчанию интегрирован в поставляемую конфигурацию. Все сертификаты сохраняются в базе данных.

Создание центра сертификации

Для использования AxelNAC PKI необходимо создать новый центр сертификации. Для этого выполните следующие действия:

Шаг 1. Перейдите в веб-интерфейс AxelNAC в раздел **Конфигурация → Интеграция → PKI → Центры сертификации** и нажмите **Новый центр сертификации**. После этого появится форма для создания нового центра сертификации.

Центр сертификации 2

Идентификатор

2

Common name

common_name_test

E-mail

wilige4567@egela.com

Примечание: Изменение полей "Organisational Unit", "Organisation", "Country", "State or Province", "Locality" или "Street Address" сделает сертификаты, ранее подписанные по протоколу EAP-TLS, недействительными.

Структурное подразделение

Организация

1

Страна

Russia

Область или провинция

1

Место действия

1

Адрес

Тип ключа

KEY_RSA

Размер ключа

2048

Дайджест

SHA256WithRSA

Использование ключа (KU)

Опционально. Выберите одно или несколько значений: digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, cRLSign, encipherOnly, decipherOnly.

Расширенное использование ключа

Опционально. Выберите одно или несколько значений: serverAuth, clientAuth, codeSigning, emailProtection, timeStamping, msCodeInd, msCodeCom, msCTLSign, msSGC, msEFS, nsSGC.

Дней

30

Число дней до истечения срока действия сертификата удостоверяющего центра (CA).

OCSP URL

Опционально. URL-адрес OCSP-сервера, который будет добавлен в сертификат.

Сертификат

-----BEGIN CERTIFICATE-----

MIIDhzCCAm+gAwIBAgIBATANBgkqhkiG9w0BAQsFADBMMQswCQYDVQQG
EwJSVTEK
MAgGA1UECBMTEKMAgGA1UEBxMBMTEKMAgGA1UEChMBMTEZMBcG
A1UEAwwQY29t
bW9uX25hbWVfdGVzdDAeFw0yNDA2MjQxMzM4NTBaFw0yNDA3MjQxMzM
4NTBaMEwx
CzAJBgNVBAYTALJVMQowCAYDVQQIEwExMQowCAYDVQQHEwExMQowCA
YDVQQKEwEx
MRkwFwYDVQQDDDBBjb21tb25fbmFtZV90ZXN0MIIlBjANBgkqhkiG9w0BAQE
FAAOC
AQ8AMIIBCGKCAQEAtGpL31bfpJ8vZpiPrAB0P+Al1ahhy9WoxAus57uffoiSY
W9
4SK4c++NQyk09I+zMoLwS3fO6XAAG3HRAAdmsYcesRcR+f2Eqk9VVc8nBAF
M25lV
YmNfgg0332BI47YM74NmK71c9oSiYMzsY2Mvm1/CC6VcpQLMu80EoNf4cO
ZfO2gf
iwU7JaOMhhLAVRtvzdwZ9y+XzG37uS68BCGpszl6lqX2vInxsvMFYB90zdTs
wlk2
4Nh1+VJHDW8lZtJlgnEvR/T9OGUh7tXtqVlrdDie3lJBg2X++tXF7i0YluHx02
9
wHRzWlF5D2N+XK/yFfbtV/1gzdFswf/a3Njv9QIDAQABo3QwcjAPBgNVHR

Переподписать

Клонировать

Сбросить

Отмена

Пример заполнения формы создания центра сертификации

Шаг 2. Заполните все необходимые поля в форме и нажмите **Создать**.

Шаг 3. Вернитесь на страницу со списком центров сертификации и скопируйте ранее созданный сертификат в буфер обмена, нажав **Скопировать сертификат**.

Шаг 4. Перейдите в раздел **Конфигурация → Настройки системы → RADIUS → SSL-сертификаты PKI** и нажмите **Новый SSL-сертификат** или отредактируйте уже существующий сертификат.

Шаг 5. В открывшемся окне заполните все необходимые поля и вставьте скопированный сертификат в поле **Центр сертификации**.

Шаг 6. Нажмите **Сохранить** и перезапустите службу **radiusd-auth**. Это позволит разрешить аутентификацию по протоколу EAP-TLS с использованием сертификатов, выданных PKI.

Перезагрузка данной службы может привести к таймауту текущих RADIUS-сессий аутентификации.

Создание шаблонов сертификатов

AxeINAC поддерживает создание шаблона сертификата, в котором будут собраны все настройки сертификата, например, срок его действия. Для этого выполните следующие действия:

Шаг 1. Перейдите в раздел **Конфигурация → Интеграция → PKI → Шаблоны**, нажмите **Новый шаблон** и выберите созданный ранее центр сертификации в выпадающем списке.

Шаг 2. В открывшемся окне заполните все необходимые поля.

Шаг 3. На вкладке **SCEP** активируйте параметр **Включить SCEP**, чтобы использовать **SCEP** в этом шаблоне.

Атрибуты **Common Name** и **Subject Alt Name**, предоставленные в CSR для получения сертификата через SCEP, будут переопределять значения в шаблоне PKI. Другие значения, такие как алгоритм подписи, использование ключа, расширенное использование ключа, будут взяты из шаблона PKI.

Шаг 4. Получите сертификат центра сертификации с помощью команды:

```
sscep getca -u http://ip_address/scep/template_name -c ./ca-prefix -i MyPKI -v -d
```

В результате вы получите сообщение следующего вида:

```
sscep: starting sscep, version 0.6.1
sscep: new transaction
sscep: transaction id: SSCEP transactionId
sscep: hostname: ip_address
sscep: directory: scep/template_name
sscep: port: 80
sscep: SCEP_OPERATION_GETCA
sscep: requesting CA certificate
sscep: scep msg: GET /scep/template_name?operation=GetCACert&message=MyPKI HTTP/1.0
sscep: server returned status code 200
sscep: MIME header: application/x-x509-ca-cert
sscep: valid response from server
sscep: MD5 fingerprint: 22:DE:09:17:8B:5F:94:1E:EB:0D:9C:12:EF:05:F0:C5
sscep: CA certificate written as ./ca-prefix
```

Шаг 5. Удалите секретную фразу закрытого ключа с помощью следующей команды:

```
openssl rsa -in PRIVATEKEY.key -out private.key Enter pass phrase for PRIVATEKEY.key:
writing RSA key
```

Шаг 6. Отправьте CSR и получите сертификат, используя команду:

```
scep enroll -c ./ca-prefix -k ./private.key -r ./MYCSR.csr -u http://ip_address/scep/template_name -S sha1 -I ./cert.crt
```

Создание сертификата

После настройки центра сертификации вы можете выпускать сертификаты из веб-интерфейса AxelINAC. Чтобы выпустить сертификат, выполните следующие действия:

Шаг 1. Перейдите в раздел **Конфигурация → Интеграция → PKI → Сертификаты**, нажмите **Новый сертификат** и выберите созданный ранее шаблон сертификата в выпадающем списке.

Шаг 2. В открывшемся окне заполните все необходимые поля и нажмите **Сохранить**.

После создания сертификат можно отправить пользователю по электронной почте или загрузить в формате p12.

Формат PEM

AxelINAC PKI выпускает сертификаты в формате PKCS12; если нужно преобразовать сертификат в формат PEM, можно воспользоваться командами:

```
openssl pkcs12 -in ИмяВашегоСертификата.p12 -nocerts -out ИмяВашегоСертификата.key -nodes
openssl pkcs12 -in ИмяВашегоСертификата.p12 -out ИмяВашегоСертификата.pem -clcerts -nokeys
```

Отзыв сертификата

Чтобы отозвать сертификат, перейдите в раздел **Конфигурация → Интеграция → PKI → Сертификаты** и нажмите **Отозвать** справа от имени сертификата.

Если сертификат отозван, восстановить его нельзя, поэтому нужно создать его новую версию. При этом потребуется указать причину отзыва.

ID статьи: 1817

Последнее обновление: 22 апр., 2025

Обновлено от: Егоров В.

Ревизия: 5

База знаний AxelINAC -> Документация -> Система контроля доступа к сети «AxelINAC». Версия 2.2.0 -> AxelINAC. Руководство администратора -> Интеграция PKI -> Интеграция AxelINAC PKI

<https://docs.axel.pro/entry/1817/>