Интеграция AxelNAC PKI

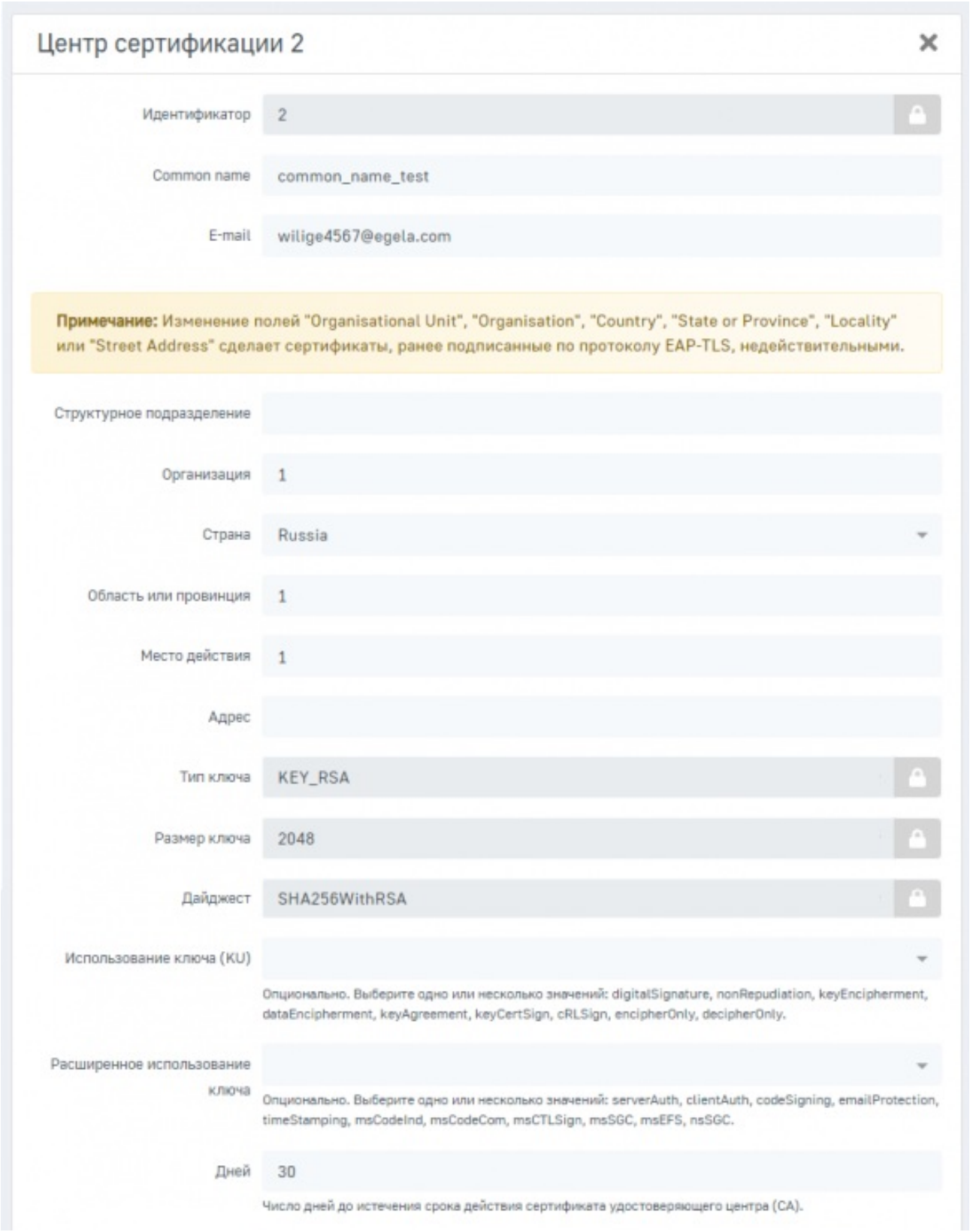
В данной статье описан процесс быстрой настройки AxelNAC PKI в AxelNAC. В описании не приводится расширенный поиск и устранение неисправностей в соединениях EAP-TLS. За дополнительной информацией обратитесь к документации по EAP-TLS, RADIUS и OpenSSL.

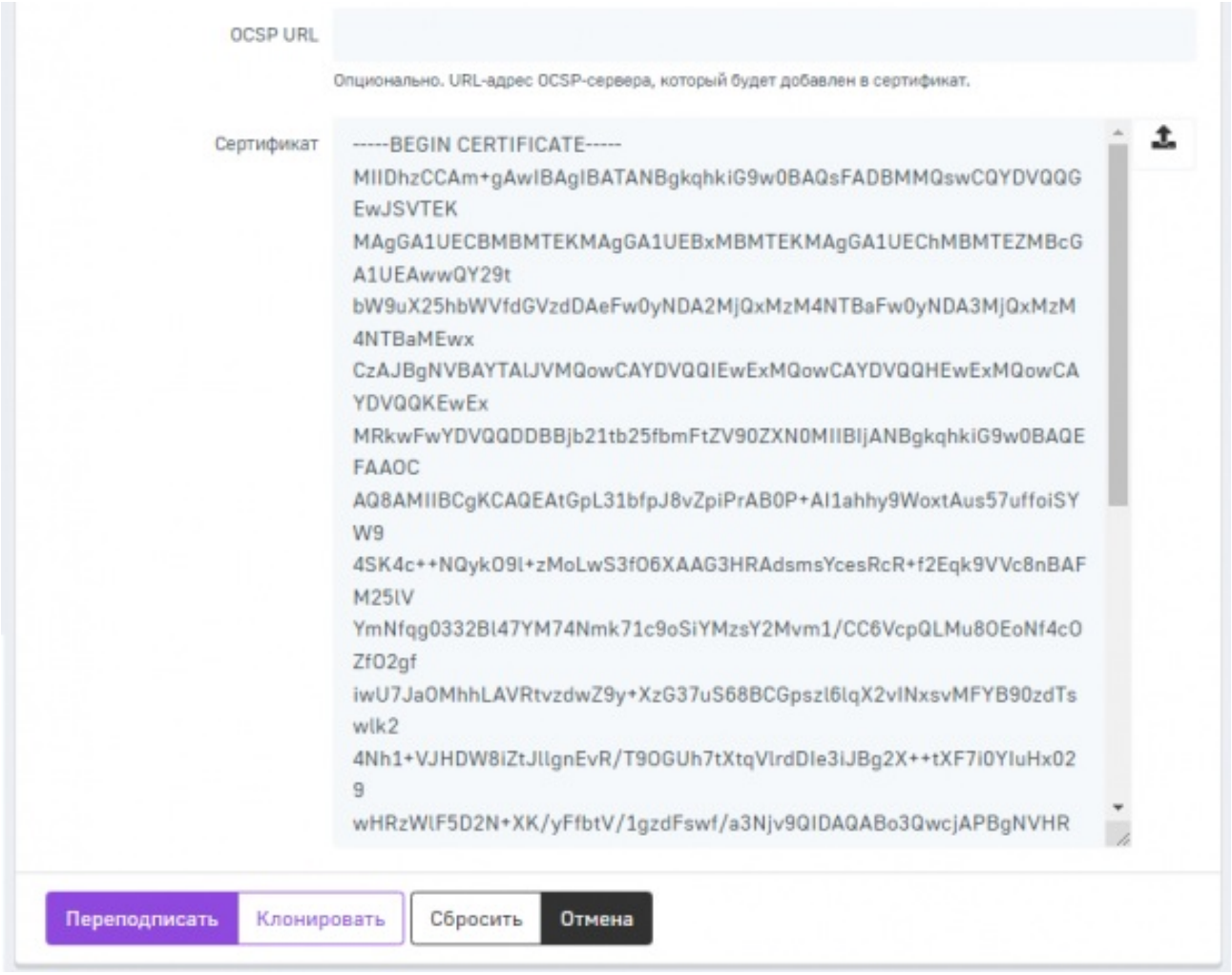
AxelNAC PKI по умолчанию интегрирован в поставляемую конфигурацию. Все сертификаты сохраняются в базе данных.

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.





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

AxelNAC 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 -l ./cert.crt

Создание сертификата

После настройки центра сертификации вы можете выпускать сертификаты из веб-интерфейса AxelNAC. 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

AxelNAC 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: 986
Последнее обновление: 22 апр., 2025
Обновлено от: Егоров В.
Ревизия: 5
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.1.0 -> AxelNAC. Руководство администратора -> Интеграция PKI -> Интеграция AxelNAC PKI
https://docs.axel.pro/entry/986/