Вкладка «RADIUS»

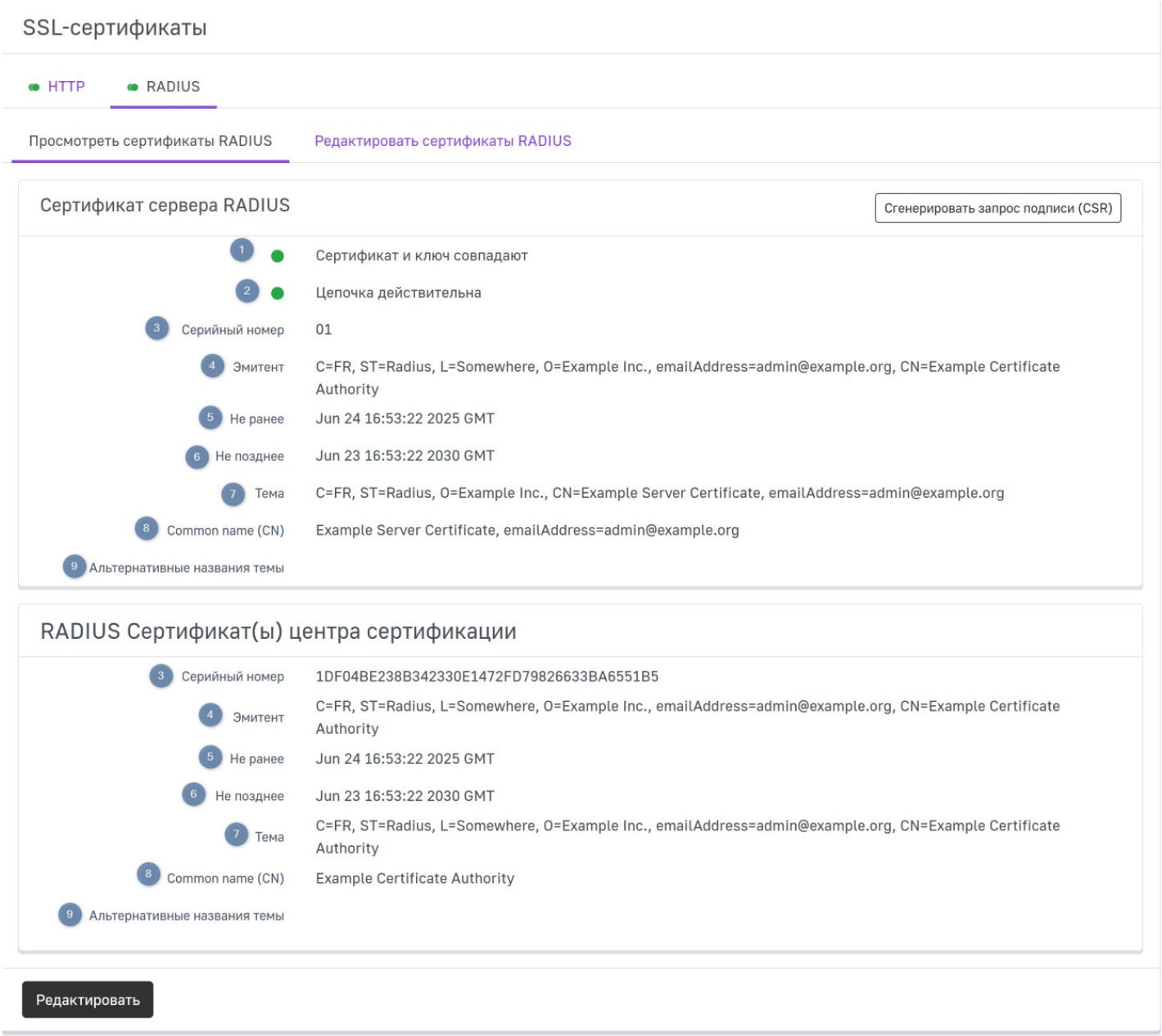
Вкладка «RADIUS» предназначена для управления сертификатами, используемыми сервером RADIUS. На данной вкладке можно просматривать действующие сертификаты RADIUS, проверять их валидность, формировать запросы на подписание (CSR), а также редактировать параметры сертификатов и управлять доверенными центрами сертификации.

Блок «Просмотреть сертификаты RADIUS»

В данном блоке можно просматривать действующие сертификаты RADIUS.

Сертификат сервера RADIUS — действующий сертификат RADIUS.

RADIUS Сертификат(ы) центра сертификации — сведения о сертификатах доверенных центров.



В блоке присутствуют следующие информационные поля:

1. **Сертификат и ключ совпадают** — показывает, валиден ли сертификат и соответствует ли закрытый ключ сертификату;
2. **Цепочка действительна** — отражает корректность и действительность цепочки сертификатов до доверенного центра сертификации или самоподписанного сертификата;
3. **Серийный номер** — уникальный идентификатор сертификата, отображающий SHA1-хэш открытой части сертификата;
4. **Эмитент** — организация или центр сертификации, выдавший сертификат;
5. **Не ранее** — дата, начиная с которой сертификат считается действительным;
6. **Не позднее** — дата окончания срока действия сертификата;
7. **Тема** — данные владельца сертификата;
8. **Common name (CN)** — основное имя субъекта, указанное в сертификате;
9. **Альтернативные названия темы** — дополнительные имена субъекта, на которые распространяется действие сертификата.

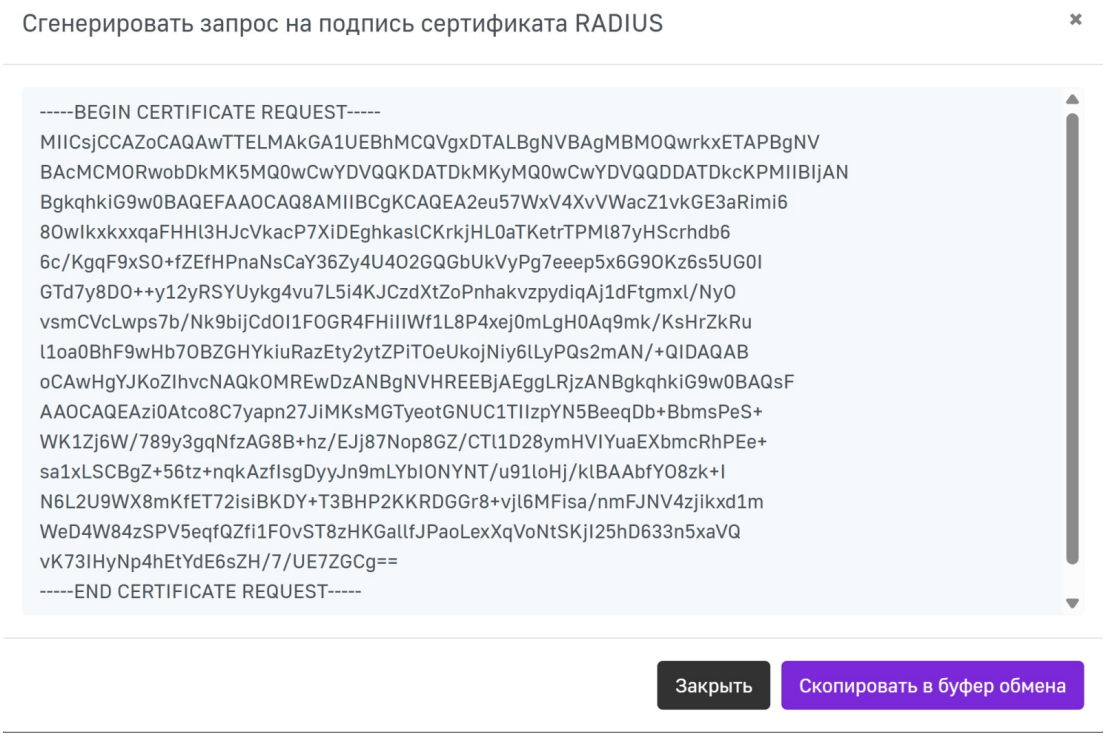
Чтобы отредактировать параметры сертификата, нажмите **Редактировать**.

В случае, если необходимо сгенерировать новый запрос подписи сертификата (CSR), который может быть отправлен в центр сертификации для получения действительного SSL-сертификата, нажмите Сгенерировать запрос подписи (CSR). При нажатии открывается окно с параметрами, которые необходимо заполнить.

В данном меню необходимо заполнить следующие параметры:

1. **Страна** — страна владельца сертификата;
2. **Состояние** — регион или область владельца сертификата;
3. **Город** — город владельца сертификата;
4. **Название организации** — официальное наименование организации, которой принадлежит сертификат;
5. **Common name** — имя субъекта.

Чтобы сгенерировать запрос, заполните все параметры и нажмите Сгенерировать. При этом откроется новое окно, в котором находится сертификат.

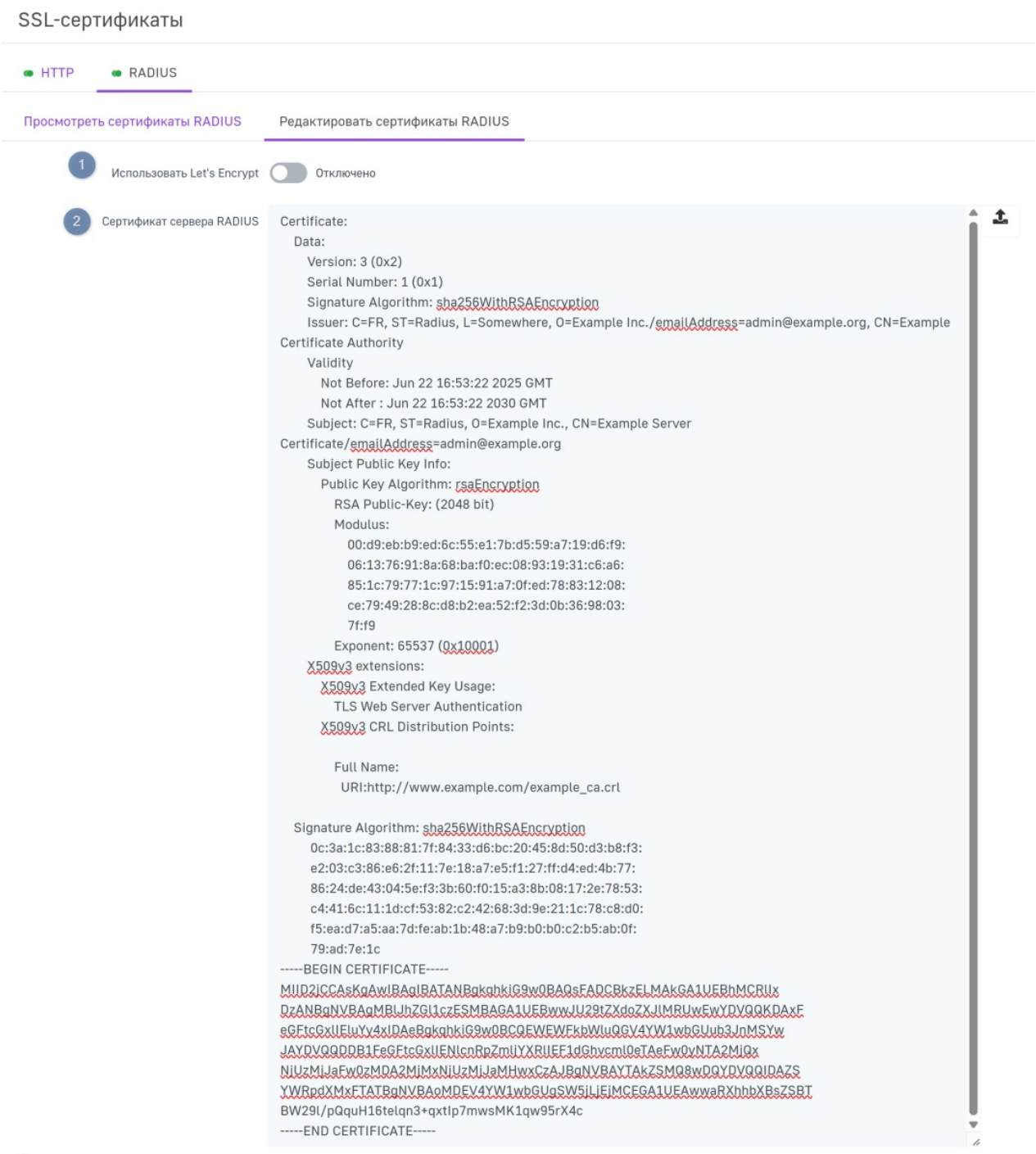


Нажмите Скопировать в буфер обмена, чтобы скопировать сертификат в буфер обмена.

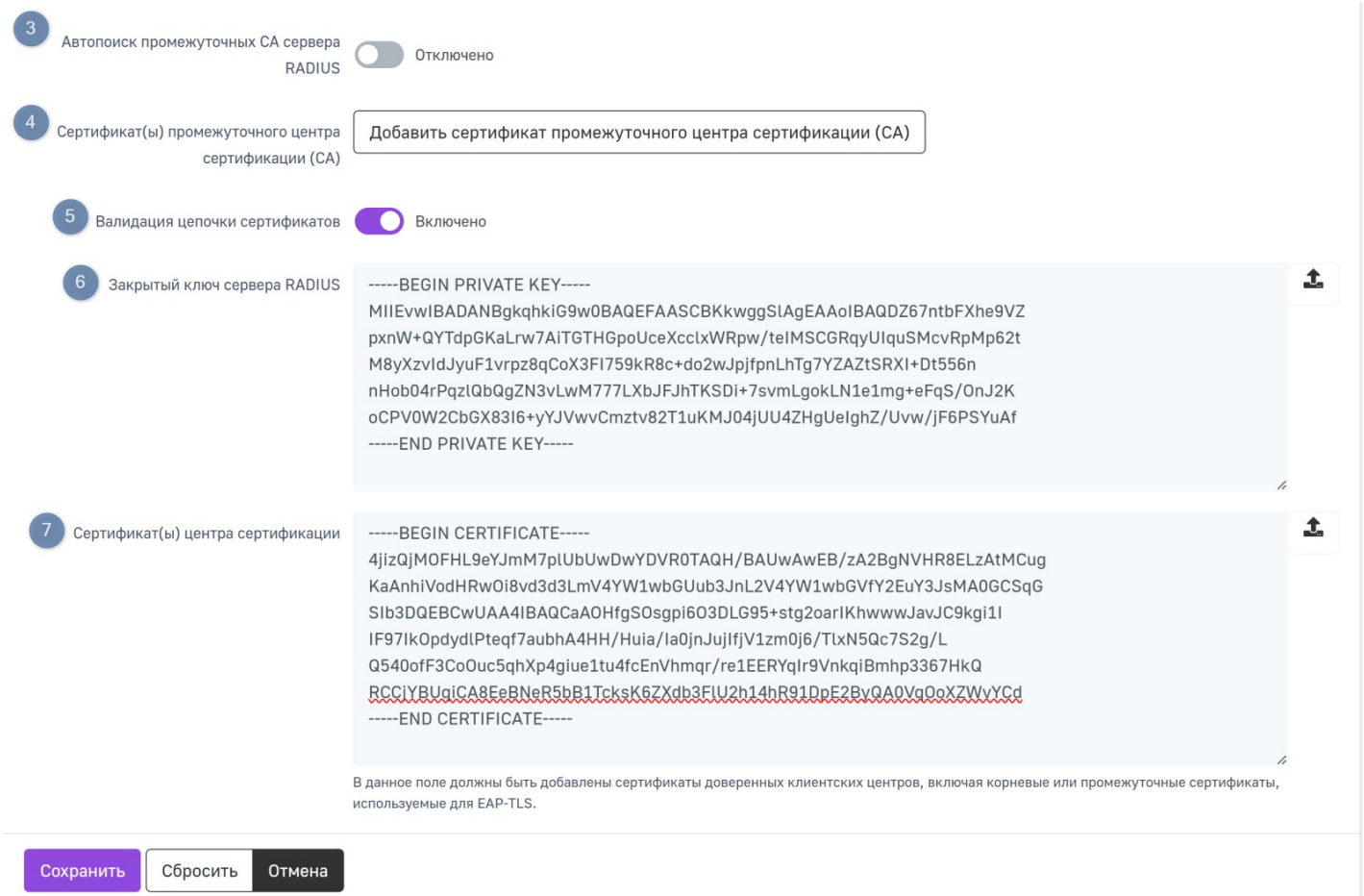
Блок «Редактировать сертификаты RADIUS»

В данном блоке можно отредактировать SSL-сертификаты, используемые RADIUS-сервером, а также задать параметры их проверки и хранения.

В меню доступны следующие настройки:



1. **Использовать Let's Encrypt** — при активации данного параметра система использует доверенные удостоверяющие центры Let's Encrypt для автоматического выпуска и продления сертификатов. При активации данного параметра все последующие параметры заменяются на:
    1. **Common name** — указывает общее имя для сертификата;
    2. **Сертификат(ы) центра сертификации** — сертификаты доверенных центров, включая корневые и промежуточные сертификаты, используемые при аутентификации по EAP-TLS. Сертификат должен быть в формате PEM.
2. **Сертификат сервера RADIUS** — загружаемый SSL-сертификат, используемый RADIUS-сервером. Сертификат должен быть в формате PEM;



3. **Автопоиск промежуточных CA сервера HTTPs** — при активации данного параметра система автоматически определяет и загружает промежуточные сертификаты центра сертификации, скрывая параметр **Сертификат(ы) промежуточного центра сертификации (CA)**. Сертификат должен быть в формате PEM;
4. **Сертификат(ы) промежуточного центра сертификации (CA)** — список сертификатов промежуточных центров сертификации. Сертификат должен быть в формате PEM;
5. **Валидация цепочки сертификатов** — при активации данного параметра выполняется проверка корректности цепочки сертификатов до доверенного центра сертификации;
6. **Закрытый ключ сервера RADIUS** — закрытый ключ, используемый для сертификата сервера RADIUS. Ключ должен быть в формате PEM, а также иметь тип шифрования RSA или не иметь пароля;
7. **Сертификат(ы) центра сертификации** — сертификаты доверенных центров, включая корневые и промежуточные сертификаты, используемые при аутентификации по EAP-TLS. Сертификат должен быть в формате PEM.

Чтобы сохранить параметры, нажмите **Сохранить**. Чтобы сбросить введенные параметры на последние сохраненные, нажмите **Сбросить**.

ID статьи: 1305
Последнее обновление: 16 окт., 2025
Обновлено от: Ильина В.
Ревизия: 7
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.0.1 -> AxelNAC. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Настройки системы» -> Страница «SSL-сертификаты» -> Вкладка «RADIUS»
https://docs.axel.pro/entry/1305/