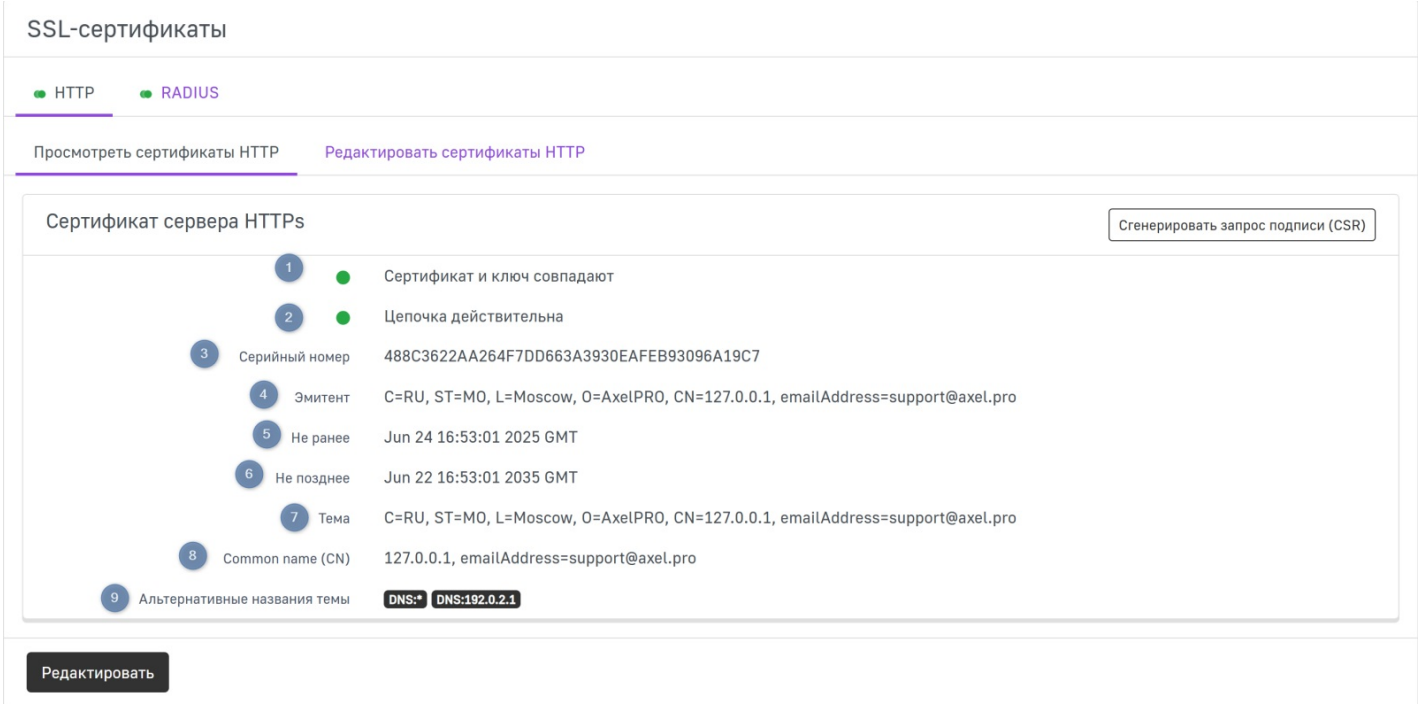
# Вкладка «HTTP»

На данной вкладке можно просматривать действующие сертификаты HTTPS, проверять их валидность, создавать запросы на подписание (CSR), а также редактировать параметры сертификатов, включая использование Let's Encrypt и добавление промежуточных сертификатов.

## Блок «Просмотреть сертификаты HTTP»

В данном блоке можно просматривать текущие SSL-сертификаты, проверять их корректность и срок действия, а также формировать запросы на выпуск новых сертификатов.

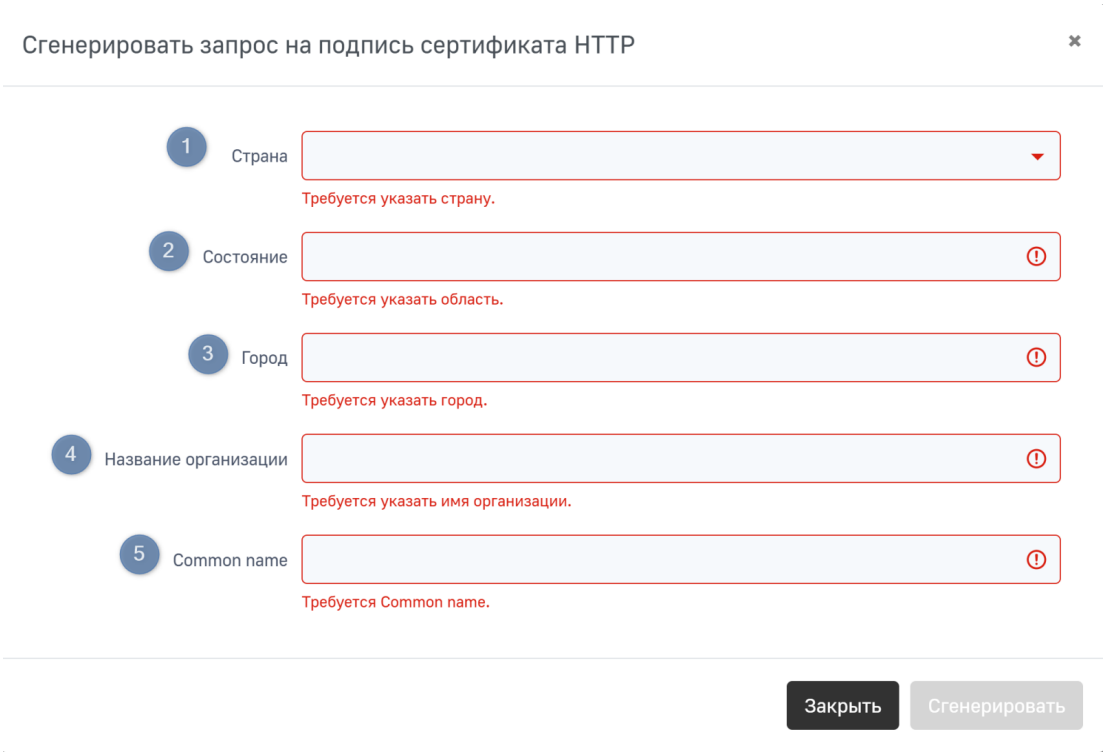



В блоке присутствуют следующие информационные поля:

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**.

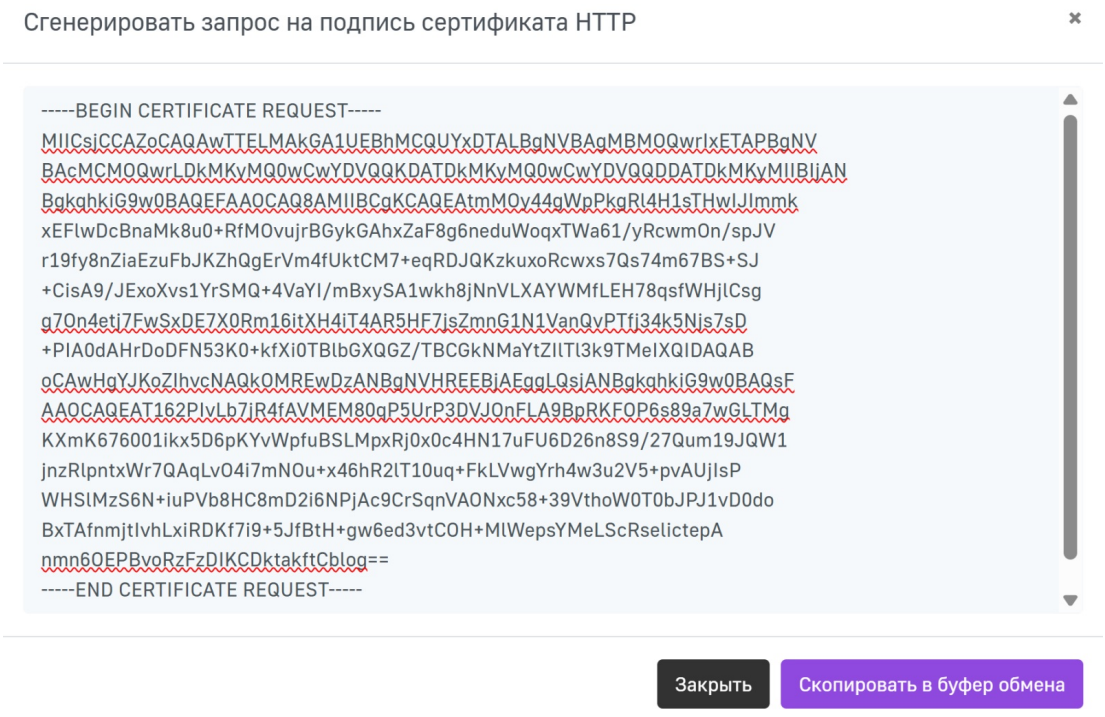
В случае, если необходимо сгенерировать новый запрос подписи сертификата (CSR), который может быть отправлен в центр сертификации для получения действительного SSL-сертификата, нажмите Сгенерировать запрос подписи (CSR). При нажатии открывается окно с параметрами, которые необходимо заполнить.




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.

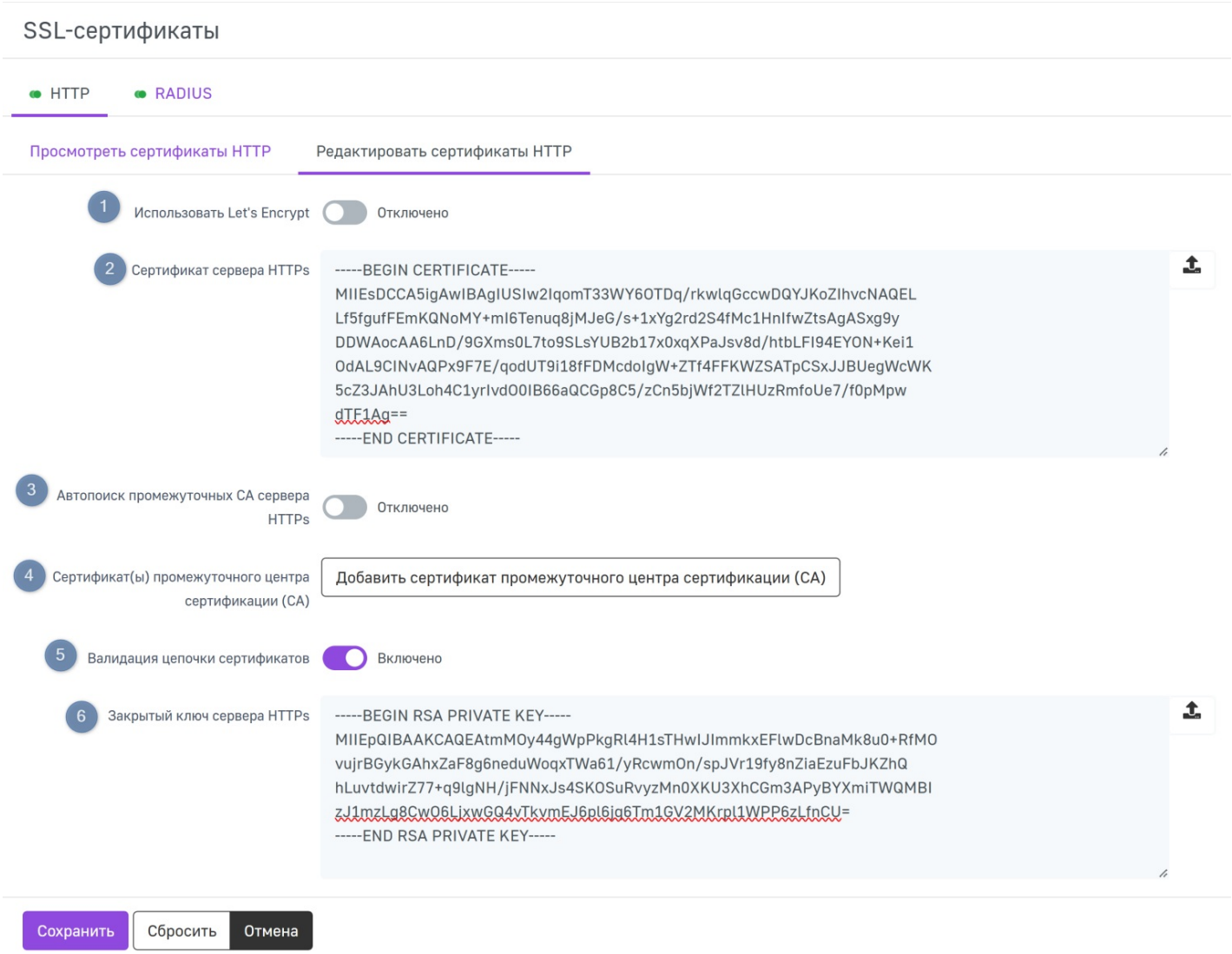
Чтобы сгенерировать запрос, заполните все параметры и нажмите Сгенерировать. При этом откроется новое окно, в котором находится сертификат.




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

## Блок «Редактировать сертификаты HTTP»

В данном блоке можно отредактировать SSL-сертификаты, используемые веб-интерфейсом и Captive-порталом AxelNAC, а также задать параметры их проверки и хранения.




В данном 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 сервера HTTPs** — загружаемый SSL-сертификат, применяемый для защищенного соединения веб-интерфейса. 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 HTTPs** — закрытый ключ, соответствующий загруженному SSL-сертификату сервера HTTPs. Ключ должен быть в формате PEM, а также иметь тип шифрования RSA или не иметь пароля.

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

---

ID статьи: 1507
Последнее обновление: 19 янв., 2026
Обновлено от: Ильина В.
Ревизия: 1
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.1.0 -> AxelNAC. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Настройки системы» -> Страница «SSL-сертификаты» -> Вкладка «HTTP»
https://docs.axel.pro/entry/1507/