

## 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.

SSL-сертификаты

HTTP

RADIUS

Просмотреть сертификаты HTTP

Редактировать сертификаты HTTP

Сертификат сервера HTTPS

Сгенерировать запрос подписи (CSR)

1

Сертификат и ключ совпадают

2

Цепочка действительна

3

Серийный номер

488C3622AA264F7DD663A3930EAFEB93096A19C7

4

Эмитент

C=RU, ST=MO, L=Moscow, O=AxeI PRO, CN=127.0.0.1, emailAddress=support@axel.pro

5

Не ранее

Jun 24 16:53:01 2025 GMT

6

Не позднее

Jun 22 16:53:01 2035 GMT

7

Тема

C=RU, ST=MO, L=Moscow, O=AxeI PRO, CN=127.0.0.1, emailAddress=support@axel.pro

8

Common name (CN)

127.0.0.1, emailAddress=support@axel.pro

9

Альтернативные названия темы

DNS:\* DNS:192.0.2.1

Редактировать

В блоке присутствуют следующие информационные поля:

- Сертификат и ключ совпадают** — показывает, валиден ли сертификат и соответствует ли закрытый ключ сертификату;
- Цепочка действительна** — отражает корректность и действительность цепочки сертификатов до доверенного центра сертификации или самоподписанного сертификата;
- Серийный номер** — уникальный идентификатор сертификата, отображающий SHA1-хэш открытой части сертификата;
- Эмитент** — организация или центр сертификации, выдавший сертификат;
- Не ранее** — дата, начиная с которой сертификат считается действительным;
- Не позднее** — дата окончания срока действия сертификата;
- Тема** — данные владельца сертификата;
- Common name (CN)** — основное имя субъекта, указанное в сертификате;
- 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.

1

Страна

Требуется указать страну.

2

Состояние

Требуется указать область.

3

Город

Требуется указать город.

4

Название организации

Требуется указать имя организации.

5

Common name

Требуется Common name.

Заккрыть

Сгенерировать

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.

-----BEGIN CERTIFICATE REQUEST-----  
MIICsjCCAzoCAQAwTTElMAkGA1UEBhMCQUYxDTALBqNVBAqMBMQwrlxETAPBqNV  
BAcMCMQwrlLdkMKyMQ0wCwYDVQQKDATDkMKyMQ0wCwYDVQQDDATDkMKyMIIBIJAN  
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtmMOv44qWpPkaRI4H1sTHwJImmk  
xEFlwDcBnaMk8u0+RfMOvujrBGykGAhxZaF8g6neduWoqxTWa61/yRcwmOn/spJV  
r19fy8nZiaEzuFbJKZhQgErVm4fUktCM7+eqRDJQKzkuxoRcwxS7Qs74m67BS+SJ  
+CisA9/JExoXvs1YrSMQ+4VaYl/mBxySA1wkh8jNnVLXAYWMfLEH78qsfWHjICsg  
q7On4eti7FwSxDE7X0Rm16itXH4iT4AR5HF7jsZmnG1N1VanQvPTfj34k5Njs7sD  
+PIA0dAHRDoDFN53K0+kfXi0TBibGXQGZ/TBCGkNMaYtZiITl3k9TMeIXQIDAQAB  
oCAwHgYJKoZihvCAQKQOMREwDzANBqNVHREEBjAEgqLQsIANBgkqhkiG9w0BAQsF  
AAQCAQEAT162PivLb7IR4fAVMEM80qP5UrP3DVJOnFLA9BpRKfOP6s89a7wGLTMg  
KXmK676001ikx5D6pKYvWpfuBSLmPxRj0x0c4HN17uFU6D26nS9/27Qum19JQW1  
jnzRlpntxWr7QAqL04i7mNOu+x46hR2lT10uq+FkLVwgYrh4w3u2V5+pvAUJIsP  
WHSImzS6N+iuPVb8HC8mD2i6NPjAc9CrSqnVAONxc58+39VthoW0T0bJPJ1vD0do  
BxTAFnmjtlvhLxiRDKf7i9+5JfBtH+gw6ed3vtCOH+MIWepsYMeLScRselictePA  
nmn6QEPBvoRzFzDIKCDktakftCblog==  
-----END CERTIFICATE REQUEST-----

Заккрыть

Скопировать в буфер обмена

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.

## SSL-сертификаты

● HTTP ● RADIUS

Просмотреть сертификаты HTTP

Редактировать сертификаты HTTP

1 Использовать Let's Encrypt ☐ Отключено

2 Сертификат сервера HTTPS

```
-----BEGIN CERTIFICATE-----
MIIEsDCCA5igAwIBAgIU5Iw2IqomT33WY60TDq/rkwlqGccwDQYJKoZIhvcNAQEL
Lf5fgufFEmKQNoMY+ml6Tenuq8jMJeG/s+1xYg2rd2S4fMc1HnlfwZtsAgASxg9y
DDWAocAA6LnD/9GXms0L7to9SLsYUB2b17x0xqXPaJsv8d/htbLFi94EYON+Kei1
OdAL9CINvAQPX9F7E/qodUT9i18fDMcdolGw+ZTf4FFKWZSATpCSxJJBUegWcWK
5cZ3JAhU3Loh4C1yrlvd00IB66aQCGp8C5/zCn5bjWf2TZIHUzRmfoUe7/f0pMpw
dTF1Ag==
-----END CERTIFICATE-----
```



3 Автопоиск промежуточных CA сервера HTTPS ☐ Отключено

4 Сертификат(ы) промежуточного центра сертификации (CA)

Добавить сертификат промежуточного центра сертификации (CA)

5 Валидация цепочки сертификатов ☒ Включено

6 Закрытый ключ сервера HTTPS

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAtmMOy44gWpPkgRI4H1sTHwIJIImmKxEFlwDcBnaMk8u0+RfMO
vujrBGyGKAhxZaF8g6neduWoqxTWa61/yRcwmOn/spJvR19fy8nZiaEzuFbJKZhQ
hLuvtdwirZ77+q9lgNH/jFNNxJs4SKOSuRvyzMn0XKU3XhCGm3APyBYXmitWQMBI
zJ1mzLg8CwQ6LjxwGQ4vTkvmEJ6pl6iq6Tm1GV2MKrp1WPP6zLfnCU=
-----END RSA PRIVATE KEY-----
```



Сохранить

Сбросить

Отмена

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: 1304

Последнее обновление: 26 сент., 2025

Обновлено от: Ильина В.

Ревизия: 12

База знаний AxelINAC -> Документация -> Система контроля доступа к сети «AxelINAC». Версия 2.0.1 -> AxelINAC. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Настройки системы» -> Страница «SSL-сертификаты» -> Вкладка «HTTP»

<https://docs.axel.pro/entry/1304/>