

LogIQ. Замена TLS-сертификата для веб-интерфейса

Для того чтобы заменить TLS-сертификат для защищенного доступа к веб-интерфейсу системы необходимо выполнить следующие действия:

Шаг 1. Подключитесь к серверу системы по протоколу SSH и проверьте, что разделы с сертификатами примонтированы к контейнеру **logiq-apigw-1** в файле **docker-compose.services.yml**:

```
volumes:
  - /opt/logiq/services/apigw/nginx.conf:/etc/nginx/nginx.conf:ro
  - /opt/logiq/services/apigw/ssl:/etc/nginx/ssl:rw
```

Шаг 2. Поместите новые файлы сертификата и ключа в примонтированную папку.

Убедитесь, что новому ключу и сертификату выданы достаточные права.

Шаг 3. В файле **/opt/logiq/services/apigw/nginx.conf** закомментируйте неактуальные ключ и сертификат, после чего добавьте строки с новыми файлами сертификата и ключа и путь к этим файлам:

```
server {
    listen 5555;
    listen 5556 ssl;

#     ssl_certificate /etc/nginx/ssl/cert.crt;
#     ssl_certificate_key /etc/nginx/ssl/key.key;

    ssl_certificate /etc/nginx/ssl/logiq-app.axel.corp.cer;
    ssl_certificate_key /etc/nginx/ssl/logiq-app.axel.corp.key;
```

Шаг 4. Перезагрузите контейнер **nginx** с помощью следующей команды:

```
docker restart logiq-apigw-1
```

Если после перезапуска контейнера сертификат не обновился, отключите и заново запустите контейнер **nginx**.

ID статьи: 1544

Последнее обновление: 20 февр., 2026

Обновлено от: Егоров В.

Ревизия: 3

База знаний LogIQ -> Документация -> LogIQ. Замена TLS-сертификата для веб-интерфейса

<https://docs.axel.pro/entry/1544/>