

# Использование стороннего сертификата в Nginx

InfoWatch Traffic Monitor knowledge base

Exported on 11/12/2020

# 1 Table of Contents

1 Table of Contents.....	2
2 Задача.....	3
3 Решение.....	4

## 2 Задача

Использовать wild-сертификат для Nginx, чтобы не было ошибки в Web-консоли управления.

### 3 Решение

Если сертификат с расширением pfx, то для его использования необходимо выполнить следующую инструкцию:

1. Извлекаем из сертификата публичный ключ (считаем, что pfx-ключ находится в папке root)

```
# openssl pkcs12 -in ~/your_cert.pfx -clcerts -nokeys -out ~/iw_console.cer
```

2. Извлекаем из сертификата закрытый ключ

```
# openssl pkcs12 -in ~/your_cert.pfx -nocerts -nodes -out ~/iw_console.key
```

3. Переносим полученные файлы в папку сертификатов

```
# mv ~/iw_console.* /opt/iw/tm5/etc/certification
```

4. Изменяем файл конфигурации Nginx /etc/nginx/nginx-iw.conf

```
Было
...
    ssl_certificate      /opt/iw/tm5/etc/certification/web-server.pem;
    ssl_certificate_key  /opt/iw/tm5/etc/certification/web-server.key;
...

Стало
...
    ssl_certificate /opt/iw/tm5/etc/certification/iw_console.cer;
    ssl_certificate_key /opt/iw/tm5/etc/certification/iw_console.key;
...
```

5. Перезапускаем Nginx

```
# service nginx restart
# service php-fpm restart
```