

??????? ?????????? SSL- ?????????????: unable to get local issuer certificate

?????????

В логах компонентов появляется ошибка:

```
[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed:  
unable to get local issuer certificate
```

?????????

Не удалось проверить цепочку доверия SSL-сертификата.

Возможные причины:

- Отсутствие поля **Subject Alternative Name (SAN)** в сертификате сервера.
- Отсутствие данных о поставщике (центр сертификации, CA) в сертификате сервера.

????????????????

??????????? ???????? SAN:

```
openssl x509 -in /path/to/server.crt -noout -ext subjectAltName
```

Норма: вывод содержит `DNS:` или `IP:` записи. Ошибка: пустой вывод или `No extensions in certificate` — SAN отсутствует.

Решением является перевыпуск сертификата с полем SAN. В SAN указать все адреса сервера:

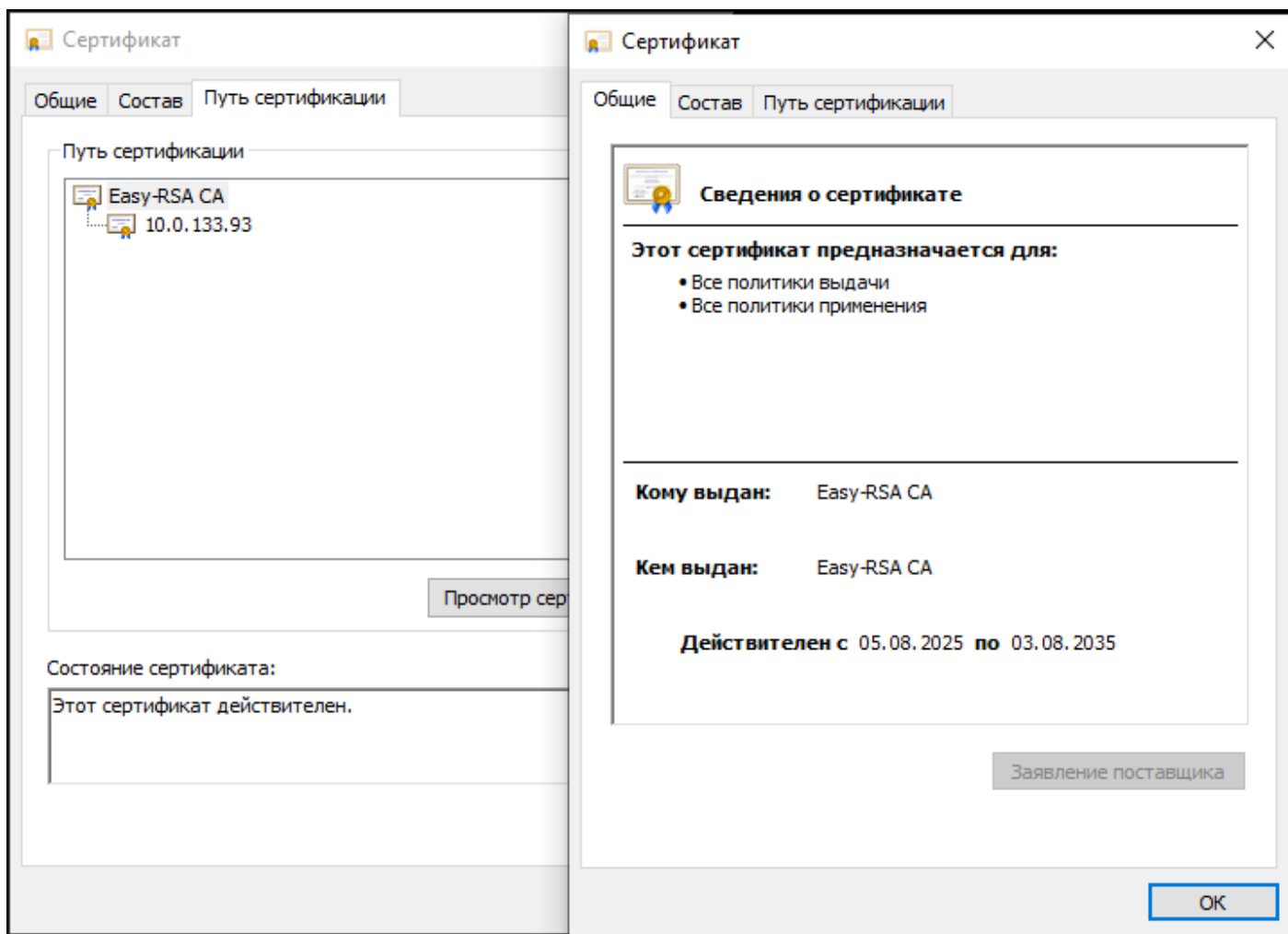
DNS:server.example.com

DNS:server

IP:10.0.0.1

????????? ??????? ?????? ? ????????????? ??????????????.

В Windows откройте данные по сертификату, перейдите во вкладку «Путь сертификации» и обратите внимание на цепочку: сертификат сервера должен быть вторым от СА-сертификата. Если СА-сертификата в цепочке нет - возникнет ошибка проверки сертификата сервера.



Решением является перевыпуск сертификата с корректной цепочкой сертификации (наличие данных о центре сертификации).

После перевыпуска, нужно внедрить сертификаты методом обновления Мониторинга и/или ПринтМенеджера.

Пример офлайн обновления с указанием переменных для установки собственных сертификатов:

```
sudo -E SSL_CERT=/path/server.crt SSL_KEY=/path/server.key SSL_CERT_CA=/path/ca.crt  
./install.sh
```

????????? ??????????

- [Требования к сертификатам безопасности](#)
-

Revision #17

Created 2026-05-18 10:00:18 UTC by DD

Updated 2026-07-15 10:30:47 UTC by Артём Сидельников