Настройка ПО "UniServer AUTO" для работы по протоколу HTTPS

Для корректной работы системы по протоколу HTTPS при первом запуске ПО генерирует 2 сертификата:

1. **Корневой сертификат** (срок действия 10 лет)
2. **Рабочий сертификат** (срок действия 90 дней)

Корневой сертификат необходимо установить вручную на каждом компьютере-клиенте, который будет подключаться к ПО по протоколу HTTPS. Во время работы система периодически проверяет срок действия рабочего сертификата и если до его окончания остается менее 10 дней - автоматически перевыпускает его.

В ПО «UniServer AUTO» реализовано 2 способа выпуска рабочего сертификата:

1. **Создание сертификата сервером самостоятельно** - подходит для взаимодействия с сервером с помощью IP адреса или доменного имени в локальной сети или с помощью «белого» IP адреса для взаимодействия через интернет.
2. **Получение сертификата от сервера ACME** - подходит для взаимодействия с сервером с помощью доменного имени через интернет.

Для корректной работы ПО по протоколу HTTPS необходимо использовать ОС Windows Vista и выше.

Создание сертификата сервером самостоятельно

1. Откройте файл **EventServer.ini** в каталоге **\UniServerAUTO\BIN20\BIN64**
2. Укажите значение параметра **Tls=1**
3. Укажите значение параметра **Fqdn** - перечислите через «,» IP адреса и локальные доменные имена (если имеются) по которым клиенты будут подключаться к серверу. Например: **Fqdn=myserver.local, IP:127.0.0.1, IP:192.168.0.42**

В дальнейшем каждый раз, после изменения параметра **Fqdn**, необходимо перевыпустить сертификат. Для этого удалите файлы имеющиеся в папке **DATA/CA/** и перезапустить сервер!

После сохранения файла и перезапуска сервера будут сгенерированы корневой и рабочий сертификаты. Корневой сертификат необходимо вручную установить на каждом компьютере-клиенте, который будет подключаться к ПО по протоколу HTTPS.

Далее перейдите к пункту «Установка корневого сертификата на клиентском ПК»

Получение сертификата от сервера ACME

1. Откройте файл **EventServer.ini** в каталоге **\UniServerAUTO\BIN20\BIN64**
2. Укажите значение параметра **Tls=1**
3. Укажите значение параметра **Port=80**
4. Укажите значение параметра **TlsPort=443**
5. Укажите значение параметра **Fqdn** - перечислите через «,» доменные имена по которым клиенты будут подключаться к серверу. Например: **Fqdn=myuniserver.company.net**. **ПО должно быть доступно по всем перечисленным доменным именам через интернет!**
6. В параметре **AcmeUrl** укажите URL каталога сервера ACME. Например: **AcmeUrl=https://acme-v02.api.letsencrypt.org/directory**

Можно использовать собственный сервер **Windows Server Active Directory Certificate Services** через промежуточную службу https://github.com/glatzert/ACME-Server-ACDS либо сервис letsencrypt.org

После сохранения файла и перезапуска сервера будут сгенерированы корневой и рабочий сертификаты. Корневой сертификат необходимо вручную установить на каждом компьютере-клиенте, который будет подключаться к ПО по протоколу HTTPS.

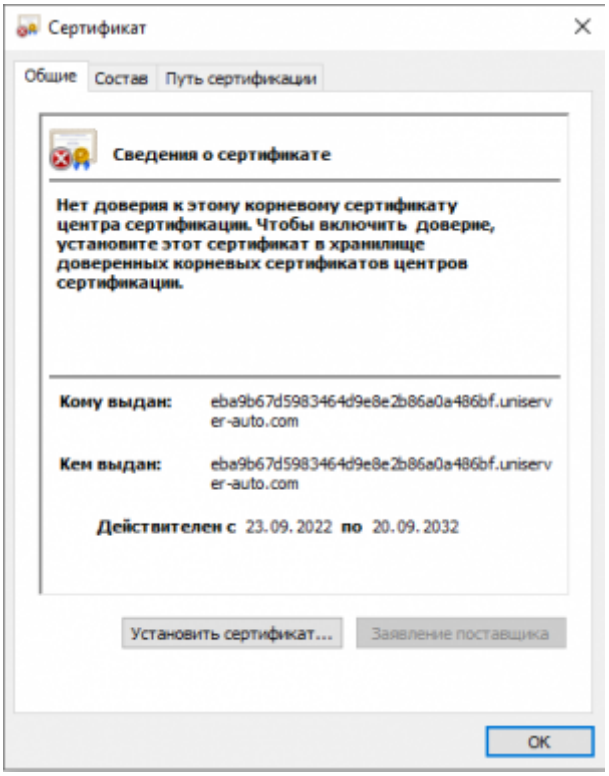
Установка корневого сертификата на клиентском ПК

Файл корневого сертификата **rootca.ctr** можно двумя способами:

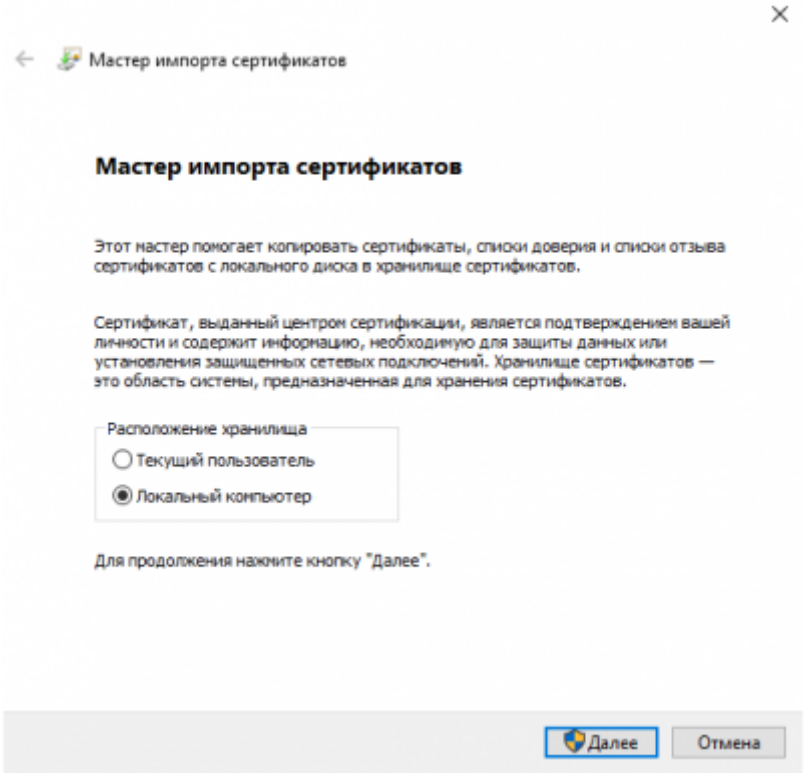
1. В каталоге **/UniServer AUTO/BIN20/DATA/CA/certs/**
2. Скачать с сервера по адресу **http://<адрес сервера>:<порт>/core/rootca.crt**

Для установки сертификата выполните следующие действия:

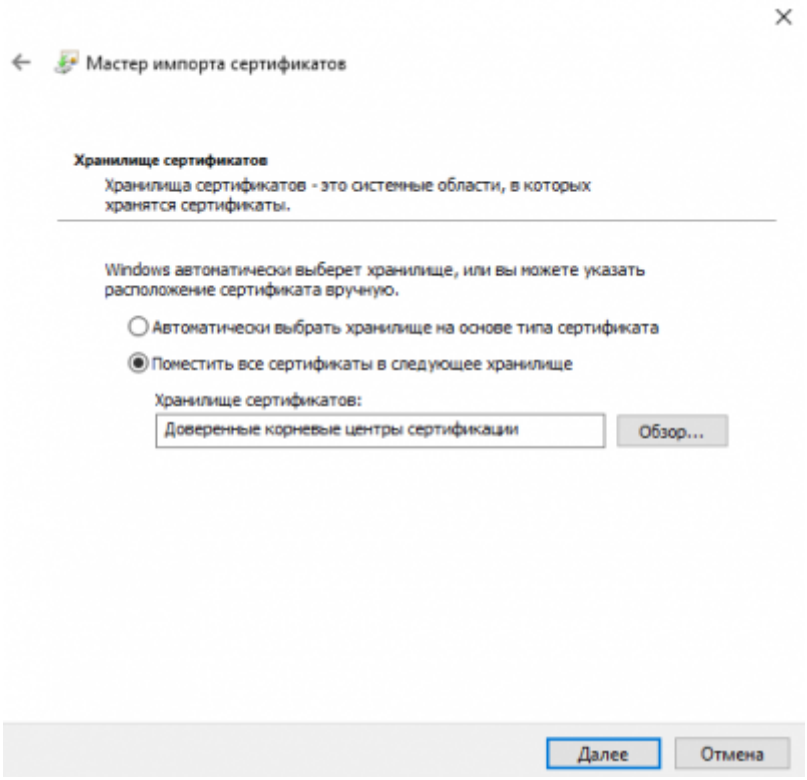
1. Дважды кликните по файлу **rootca.ctr**
2. В открывшемся окне выберите «**Установить сертификат**»



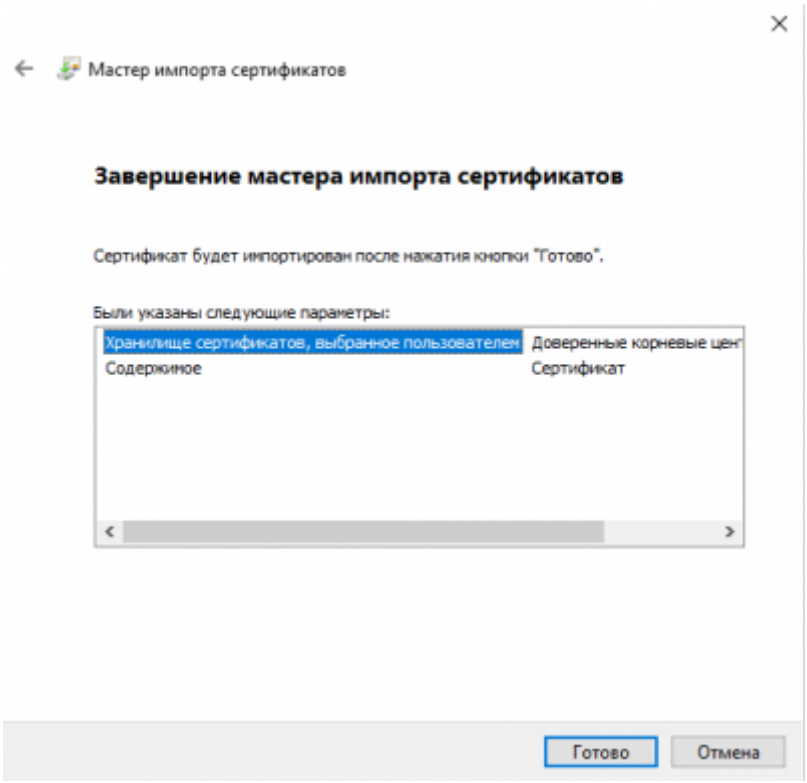
3. В окне «**Мастер импорта сертификатов**» выберите «**Локальный компьютер**» → нажмите «**Далее**»



4. Выберите «**Поместить все сертификаты в следующее хранилище**» → нажмите «**Обзор**» → выберите «**Доверенные корневые центры сертификации**» → нажмите «**Далее**»



5. В окне «**Завершение мастера импорта сертификатов**» нажмите «**Готово**» → выберите «**ОК**»



На этом установка корневого сертификата завершена. Так же сертификат можно установить с помощью утилиты certmgr.exe из Windows SDK (https://developer.microsoft.com/en-us/windows/downloads/windows-sdk/) Команда для установки

```
certmgr.exe /add rootca.crt /s /r localMachine root /all
```

Не забудьте после установке сертификата обязательно перезапустите браузер в котором будите работать!