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.

Вариант 1. Настройка самостоятельного выпуска сертификатов HTTPS

Создание сертификата сервером самостоятельно

1. Откройте файл **EventServer.ini** в каталоге **\UniServerAUTO\BIN20\BIN64**
2. Укажите значение параметра **Tls=1**
3. Укажите нужное значение HTTPS порта (**по умолчанию TlsPort=8443**)
4. Укажите значение параметра **Fqdn** - перечислите через «,» полное доменное имя сервера или IP адреса по которым клиенты будут обращаться к серверу. Например: **Fqdn=myserver.local, IP:192.168.0.42**
5. Сохраните файл и перезапустите сервер

```
[Server]
Tls=1
TlsPort=8443
Fqdn=myserver, myserver.local, 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 в папке сервера **Data\CA\certs\rootca.crt**. 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»

Установка корневого сертификата на клиентском ПК

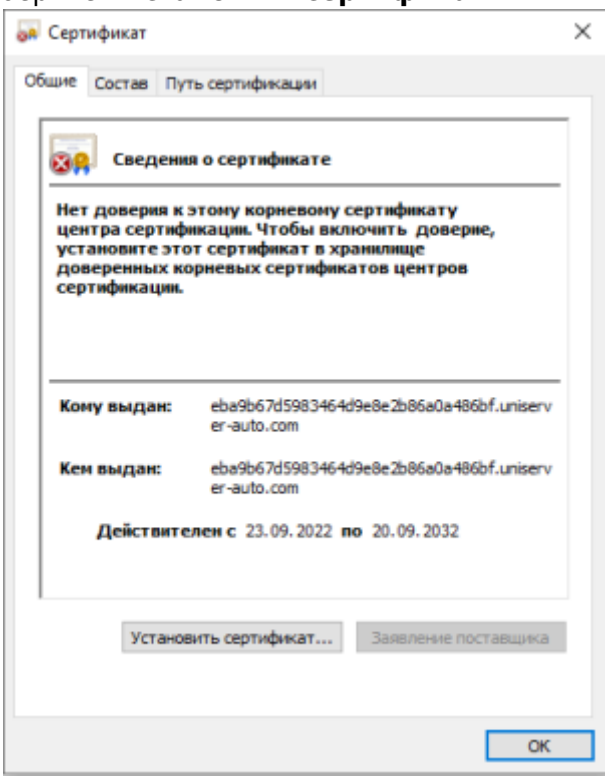
На каждом клиенте, который будет подключаться к серверу по HTTPS, необходимо установить корневой сертификат сервера в хранилище «Доверенные центры сертификации». Сделать это можно вручную, либо с помощью доменных политик или запуска скрипта на каждом клиенте.

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**

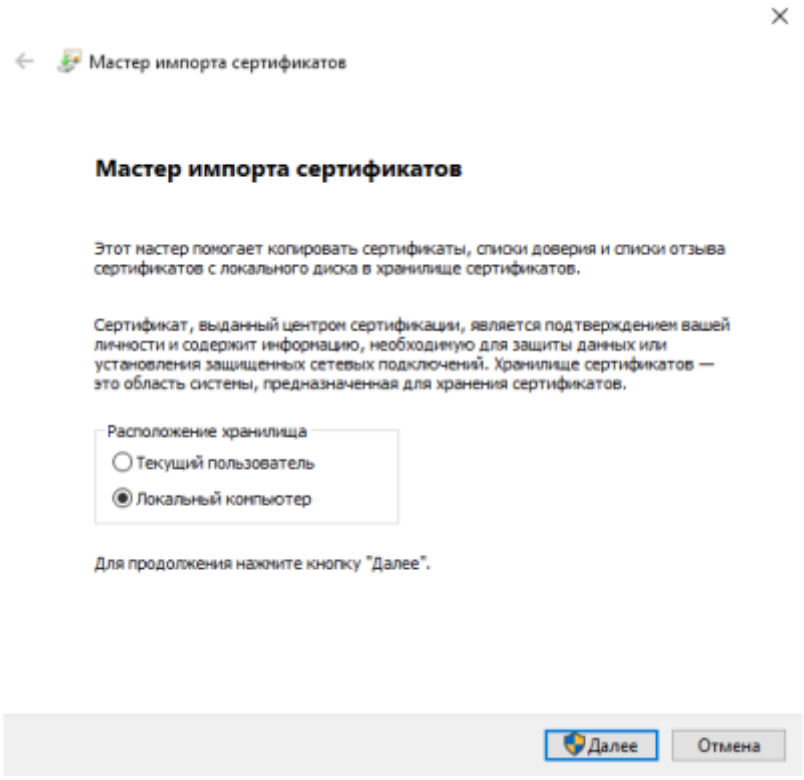
Для установки сертификата выполните следующие действия:

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

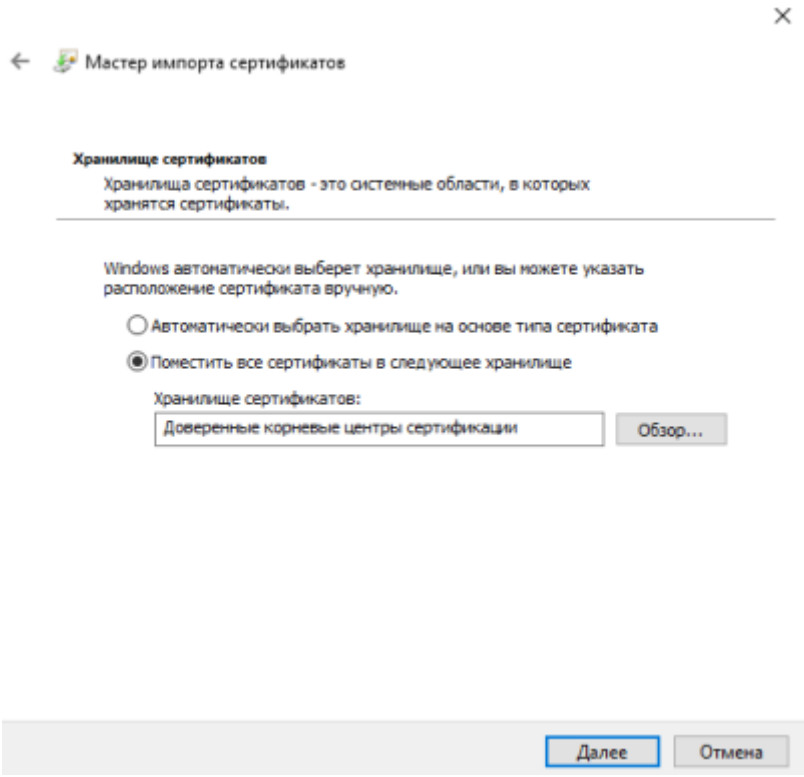


3. В окне «**Мастер импорта сертификатов**» выберите «**Локальный компьютер**» →

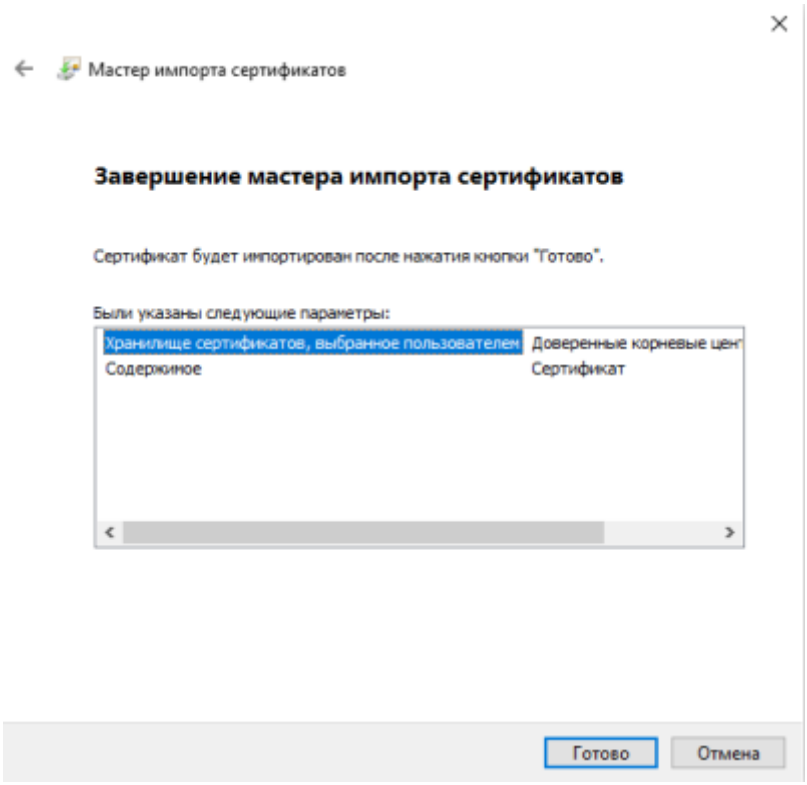
нажмите «**Далее**»



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!

Вариант 2. Настройка получения сертификатов HTTPS от сервера ACME

UniServer AUTO может получать сертификаты от сервера ACME (Automatic Certificate Management Environment).

В качестве сервера ACME, выдающего сертификаты, может быть использован **https://letsencrypt.org/** (если есть доступ к серверу из интернета), специально созданный сервер (**https://smallstep.com/blog/private-acme-server/**) или Windows Server Active Directory Certificate Services через промежуточную службу (**https://github.com/glatzert/ACME-Server-ACDS**).

Чтобы сервер ACME, например Let's Encrypt, мог проверить принадлежность домена, обычный HTTP сервер должен работать на порту 80.

Принадлежность домена определяется через запрос страницы вида **http://myserver.example.com/.well-known/acme-challenge/8LxPlzYN...9vzCdduk**. Если сервер ответит правильно, то считается, что домен **myserver.example.com** действительно принадлежит вам, и вы можете получить TLS-сертификат для этого домена.

Включение шифрованного транспортного механизма TLS и настройка

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 «,» полное доменное имя сервера по которому клиенты будут обращаться к нему. Можно указать несколько имен, разделяя их запятыми (сервер ACME будет проверять все имена, поэтому все они должны быть для него доступны). Например: **Fqdn=myserver.example.com**
6. В параметре **AcmeUrl** укажите URL каталога сервера ACME. Например: **AcmeUrl=https://acme-v02.api.letsencrypt.org/directory**
7. Сохраните файл и перезапустите сервер

```
[Server]
Tls=1
Port=80
TlsPort=443
Fqdn=myserver.example.com
AcmeUrl=https://acme-v02.api.letsencrypt.org/directory
```

Выдача сертификатов для IP-адресов обычно не поддерживается серверами ACME.