## 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:

- 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 **TIs=1**
- 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 компьютереклиенте, который будет подключаться к ПО по протоколу HTTPS.

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

## Получение сертификата от сервера АСМЕ

- 1. Откройте файл EventServer.ini в каталоге \UniServerAUTO\BIN20\BIN64
- 2. Укажите значение параметра TIs=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 компьютереклиенте, 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»

Сведени	а о сертификате
Нет доверия к центра сертифі установите это доверенных ко сертификации.	этому корневому сертификату икации. Чтобы включить доверие, т сертификат в хранилице рневых сертификатов центров
Кому выдан:	eba9b67d5983464d9e8e2b86a0a486bf.uniser er-auto.com
Кому выдан: Кем выдан:	eba9b67d5983464d9e8e2b86a0a486bf.unisen er-auto.com eba9b67d5983464d9e8e2b86a0a486bf.unisen er-auto.com
Кому выдан: Кем выдан: Действите	eba9b67d5983464d9e8e2b86a0a486bf.uniserv er-auto.com eba9b67d5983464d9e8e2b86a0a486bf.uniserv er-auto.com лен с 23.09.2022 по 20.09.2032

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

÷	🜮 Мастер импорта сертификатов	×
	Мастер импорта сертификатов	
	Этот настер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов с локального диска в хранилище сертификатов.	
	Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов — это область системы, предназначенная для хранения сертификатов.	
	Расположение хранилища О Текущий пользователь Покальный компьютер	
	Для продолжения нажните кнопку "Далее".	
	• Далее Отмена	

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

Хранилище сертифия Хранилища серти хранятся сертиф	атов ификатов - это систе икаты.	мные области, в ко	торых	
Windows автонат расположение се	ически выберет хра ртификата вручную	нилище, или вы мо»	кете указ	ать
ОАвтоматич	ески выбрать храни	лище на основе тип	а сертиф	ката
• Поместить	все сертификаты в с	следующее хранил	ще	
Хранилищ	е сертификатов:			
Доверен	ные корневые центра	ы сертификации		Обзор

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

÷	Ð	Мастер импорта сертификатов		×			
	Завершение мастера импорта сертификатов						
		Сертификат будет импортирован после нажатия кнопки	« "Готово".				
		Были указаны следующие параметры:					
		Хранилище сертификатов, выбранное пользователем Содержиное	Доверенные корневые цент Сертификат				
		٢	>				
			Готово Отмен	на			

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!

From: https://docuwiki.vesysoft.ru/ - База знаний

Permanent link: https://docuwiki.vesysoft.ru/doku.php?id=uniserver:https



Last update: 2025/04/19 01:16