

# Mikrotik: работа с сертификатами

## Курс «Настройка оборудования MikroTik»

Освоить MikroTik вы можете с помощью онлайн-курса «Настройка оборудования MikroTik». В курсе изучаются все темы из официальной программы MTCNA. Автор – официальный тренер MikroTik. Материал подходит и тем, кто уже давно работает с оборудованием MikroTik, и тем, кто еще не держал его в руках. В состав входят 162 видеоурока, 45 лабораторных работ, вопросы для самопроверки и конспект. [Узнать подробности](#)

Документация от производителя: <https://wiki.mikrotik.com/wiki/Manual:System/Certificates>

Что требуется:

- Mikrotik
- Желательно но не обязательно: белый IP
- Желательно но не обязательно: FQDN (полное доменное имя, в примере это vpn.mydomain.ru)

## Создание сертификатов

Прежде чем начать любые работы с сертификатами стоит убедиться что на Mikrotik'e настроен клиент NTP, в противном случае при достаточном расхождении часов шифрование работать не будет.

Настройка описана здесь: [Mikrotik: настройка времени](#)

## Создание корневого сертификата (CA - Certification Authority)

Корневой сертификат нужен для подписывания других выдаваемых сертификатов, необходим если вы сами выпускаете сертификаты

- Открываем System / Certificates
- Создаем новый, заполняем поля:
  - Вкладка General
    - Name: Любое понятное имя, например CA.mydomain.ru
    - Country: RU
    - State: 24 (можно писать что угодно, я предпочитаю Край/Регион/Область или их цифровые коды)
    - Locality: YourCity (город)
    - Organization: MyCompany (наименование компании)
    - Unit: IT (подразделение)
    - Common Name: Необходимо указать белый IP или полное доменное имя (например 100.100.100.100)

- Subject Alt.Name: Желательно указать DNS-имя и/или белый IP (например 100.100.100.100). Можно указывать сразу несколько опций.
- Key Size: 2048 (или 4096 если вы параноик)
- Days Valid: 3650 (10 лет или дефолтные 365 на 1 год)
- Вкладка Key Usage
  - Key Usage: должны быть включены только «crl sign» и «key cert. sign»
- Проверяем все ли заполнено верно
- Нажимаем Apply - сертификат создан
- Нажимаем Sign чтобы подписать сертификат
  - Certificate: Выбираем свой сертификат (если он выбран)
  - CA: ничего не указываем (т.к. у нас его еще нет)
  - CA CRL Host: (Желательно, но не обязательно) Указываем белый IP или FQDN имя роутера для списка отозванных сертификатов, например 100.100.100.100
  - Нажимаем Start
  - Ждем окончания процесса подписания, закрываем все окна
- В результате этих действий должен появиться сертификат с нашим именем и он должен иметь флаги KLAB

## Создание сертификата сервера

Для создания сертификата сервера должно быть создано CA-сертификат как это описано выше

- Открываем System / Certificates
- Создаем новый, заполняем поля:
  - Вкладка General
    - Name: Любое понятное имя, например vpn.mydomain.ru
    - Country: RU
    - State: 24 (можно писать что угодно, я предпочитаю Край/Регион/Область или их цифровые коды)
    - Locality: YourCity (город)
    - Organization: MyCompany (наименование компании)
    - Unit: IT (подразделение)
    - Common Name: Необходимо указать белый IP или полное доменное имя
    - Subject Alt.Name: Желательно указать DNS-имя и/или белый IP. Можно указывать сразу несколько опций
    - Key Size: 2048 (или 4096 если вы параноик)
    - Days Valid: 3650 (10 лет или дефолтные 365 на 1 год)
  - Вкладка Key Usage
    - Key Usage: должны быть включены только «digital signature», «key encipherment», «tls server»
- Проверяем все ли заполнено верно
- Нажимаем Apply - сертификат создан
- Нажимаем Sign чтобы подписать сертификат
  - Certificate: Выбираем свой сертификат (если он выбран)
  - CA: выбираем сертификат CA
  - CA CRL Host: пропускаем
  - Нажимаем Start
  - Ждем окончания процесса подписания
- Проверяем галку «Trust», закрываем все окна
- В результате этих действий должен появиться сертификат с нашим именем и он должен

иметь флаги KИT

## То же самое командами

В консоле:

```
/certificate
add name=CA common-name=100.100.100.100 country=RU state=24
locality=Krasnoyarsk organization=Company days-valid=3650 key-usage=key-
cert-sign,crl-sign
add name=server common-name=server country=RU state=24 locality=Krasnoyarsk
organization=Company days-valid=3650 key-usage=digital-signature,key-
encipherment,tls-server
sign CA ca-crl-host=100.100.100.100 name=CA
sign server ca=CA name=server
```

## Создание сертификата клиента

Для создания сертификата сервера должно быть создан CA-сертификат как это описано выше

- Открываем System / Certificates
- Создаем новый, заполняем поля:
  - Вкладка General
    - Name: Любое понятное имя, например Client1
    - Country: RU
    - State: 24 (можно писать что угодно, я предпочитаю Край/Регион/Область или их цифровые коды)
    - Locality: YourCity (город)
    - Organization: MyCompany (наименование компании)
    - Unit: IT (подразделение)
    - Common Name: Необходимо указать имя клиента (как вариант - белый IP или полное доменное имя)
    - Subject Alt.Name: Оставляем пустым
    - Key Size: 2048 (или 4096 если вы параноик)
    - Days Valid: 3650 (10 лет или дефолтные 365 на 1 год) - в зависимости от вашего доверия к клиенту
  - Вкладка Key Usage
    - Key Usage: должны быть включены только «tls client»
- Проверяем все ли заполнено верно
- Нажимаем Apply - сертификат создан
- Нажимаем Sign чтобы подписать сертификат
  - Certificate: Выбираем свой сертификат (если он выбран)
  - CA: выбираем сертификат CA
  - CA CRL Host: пропускаем
  - Нажимаем Start
  - Ждем окончания процесса подписания
- В результате этих действий должен появиться сертификат с нашим именем и он должен иметь флаги KИ

## Экспорт сертификатов

Экспорт с помощью GUI:

- Открываем нужный сертификат
- Нажимаем Export
- Выбираем формат PEM (по умолчанию) или PKCS12 (если сертификат создавался на этом же роутере то он выгрузится вместе с корневым сертификатом CA)
- В меню Files появляется экспортированный сертификат с расширением .crt

Экспорт с помощью командной строки:

```
/certificate  
export-certificate CA  
export-certificate Client1
```

Если требуется выгрузить приватный ключ (файл .key), это можно сделать командой:

```
/certificate  
export-certificate Client1 export-passphrase=secret-pa$$word
```

Где secret-pa\$\$word - пароль.

Если нужно удалить пароль, можно перенести сертификат на компьютер и выполнить:

```
openssl rsa -in Client1.key -out Client2.key
```

В новом файле Client2.key пароль будет удален

## Импорт сертификатов

- Загружаем сертификаты в Files
- Открываем System / Certificates
- Нажимаем Import
- Выбираем сертификат, при необходимости указываем Passphrase (пароль)

[mikrotik](#), [certificate](#), [cert](#), [crt](#), [key](#), [сертификат](#), [выпуск](#)

From:  
<https://wiki.rtzra.ru/> - RTzRa's hive

Permanent link:  
<https://wiki.rtzra.ru/software/mikrotik/mikrotik-generate-certificate>

Last update: **2025/11/10 13:02**

