

Установка корневого сертификата SkyDNS

Корневой сертификат или **сертификат SSL** - одна из частей системы безопасности сайтов. Сертификат SSL необходим для корректной работы сайтов с безопасным соединением (https). Если у Вас возникают проблемы с отображением страницы блокировки SkyDNS (браузер выдает сообщение **Не удается получить доступ к сайту**), то Вам необходимо скачать сертификат SkyDNS и настроить его использование в Вашем браузере.

Скачать корневой сертификат SkyDNS

Если при нажатии кнопки браузер открывает окно установки сертификата, отмените установку, кликните по кнопке правой клавишей мыши и выберите пункт **Сохранить объект как...**

Чтобы проверить работу страницы блокировки в https воспользуйтесь следующей инструкцией в конце статьи.

Сертификат не поддерживается в Yandex браузере.

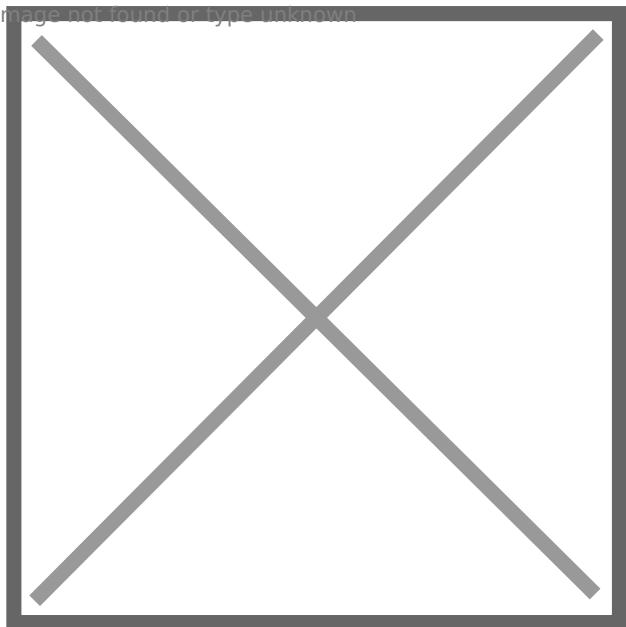
Браузер Mozilla Firefox не использует системные настройки, для установки сертификата воспользуйтесь инструкцией ниже.

Установка сертификата SkyDNS для Windows (браузеры Internet Explorer, Edge, Opera, Google Chrome)

Установка сертификата для браузеров **Internet Explorer, Edge, Opera, Google Chrome** производится через системные настройки.

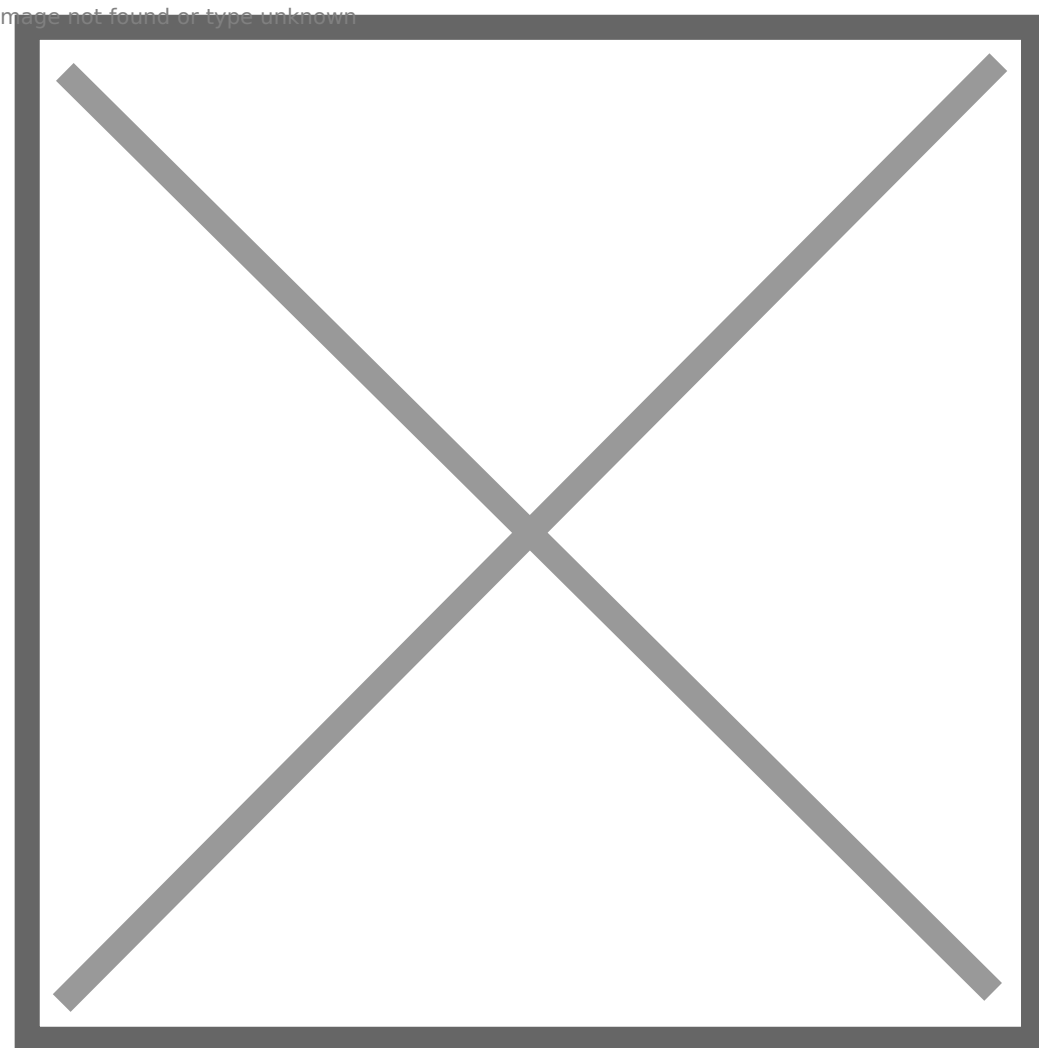
1. Нажмите кнопку **Пуск** и начните вводить словосочетание **Панель управления**. Когда появится иконка Панели Управления нажмите на нее.

Image not found or type unknown

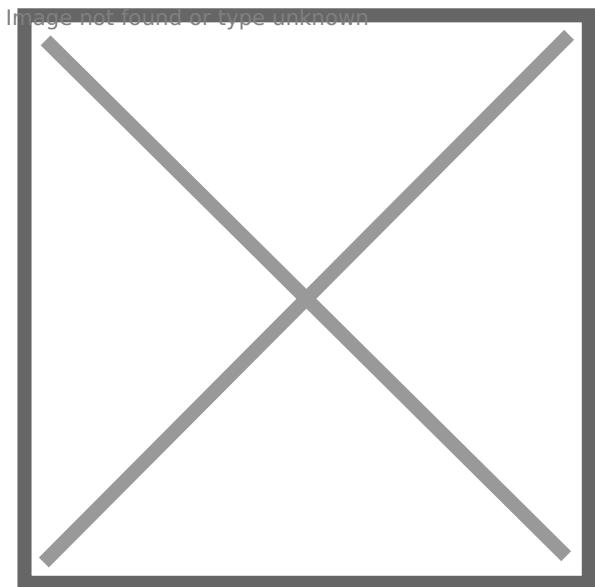


2. В поиске панели управления введите **Свойства браузера** и нажмите появившуюся иконку.

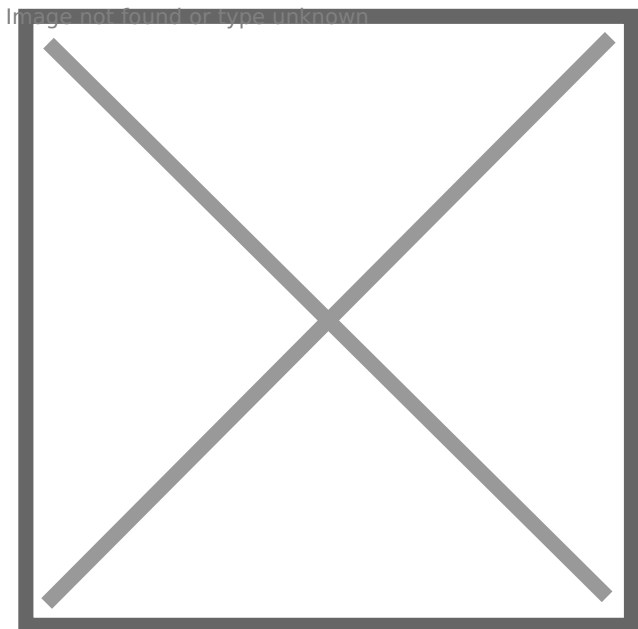
Image not found or type unknown



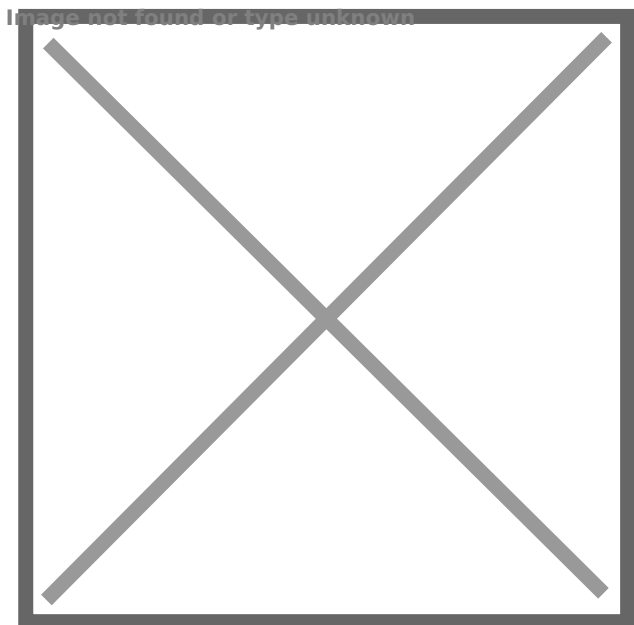
3. В Свойствах браузера перейдите на вкладку **Содержание** и нажмите кнопку **Сертификаты**.



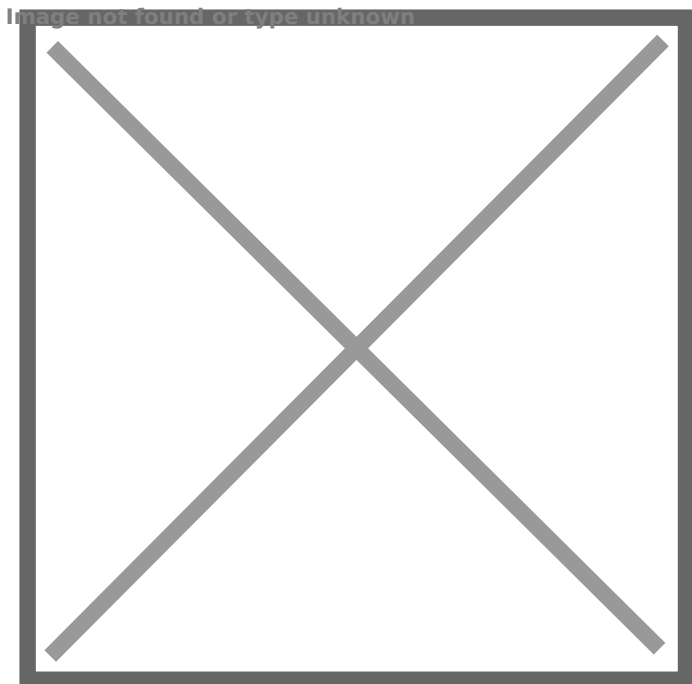
4. В окне Сертификаты перейдите на вкладку **Доверенные корневые центры сертификации** и нажмите кнопку **Импорт**.



5. В окне мастера импорта сертификатов на первом шаге нажмите кнопку **Далее**.

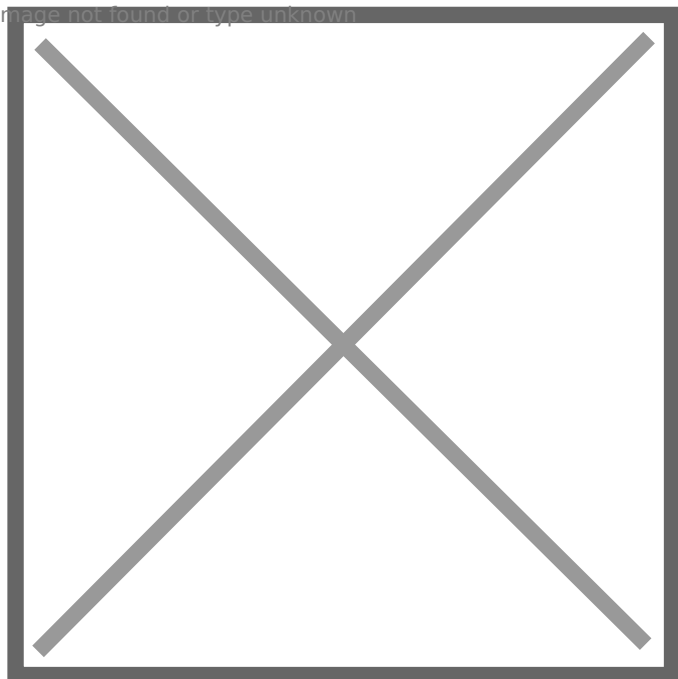


6. На втором шаге нажмите кнопку **Обзор** и выберите заранее загруженный файл сертификата SkyDNS.



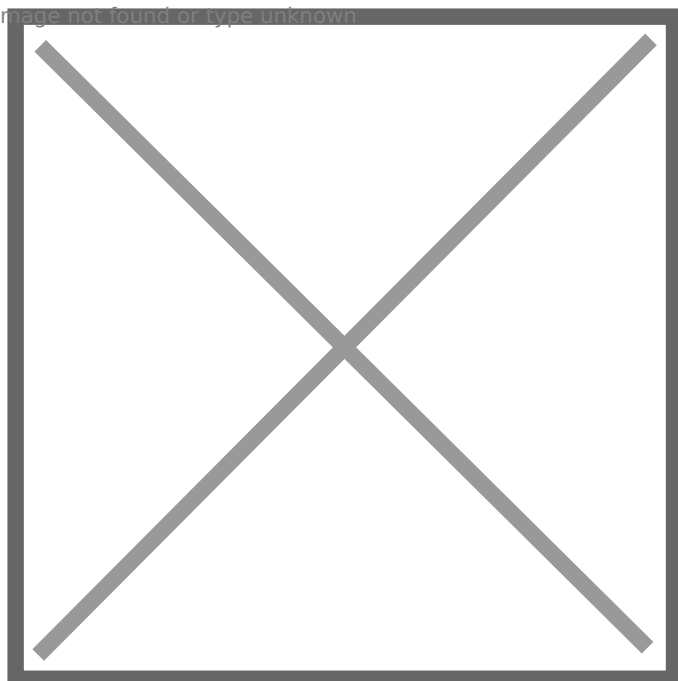
7. На третьем шаге убедитесь, что сертификат помещается в хранилище **Доверенных корневых центров сертификации**.

Image not found or type unknown



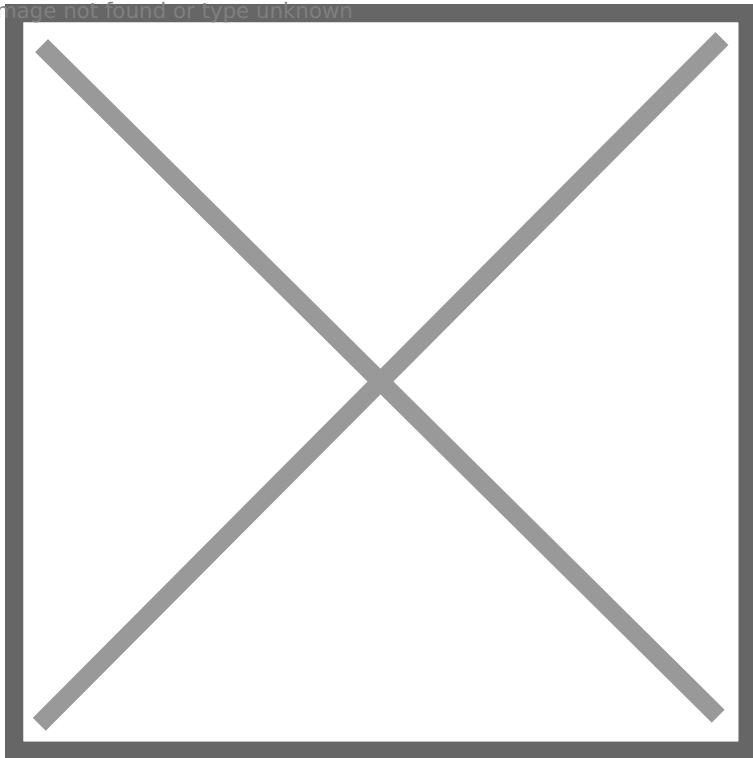
8. Подтвердите ранее проделанные действия, нажав на кнопку **Готово**.

Image not found or type unknown



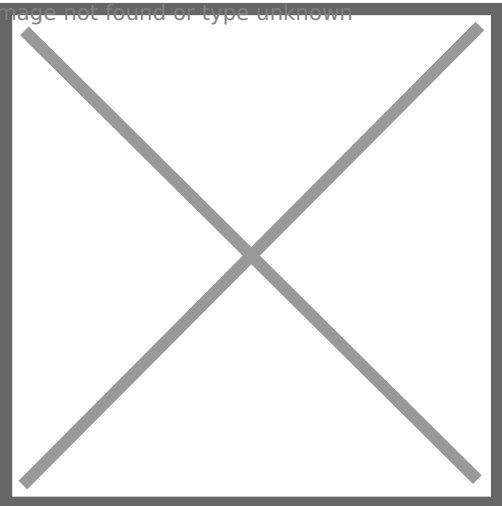
9. На вопрос системы нужно ответить **Да**.

Image not found or type unknown



10. Закрывать мастер импорта сертификатов, нажав **Ок**.

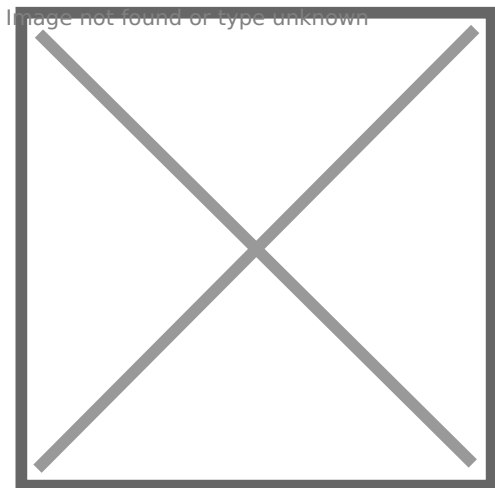
Image not found or type unknown



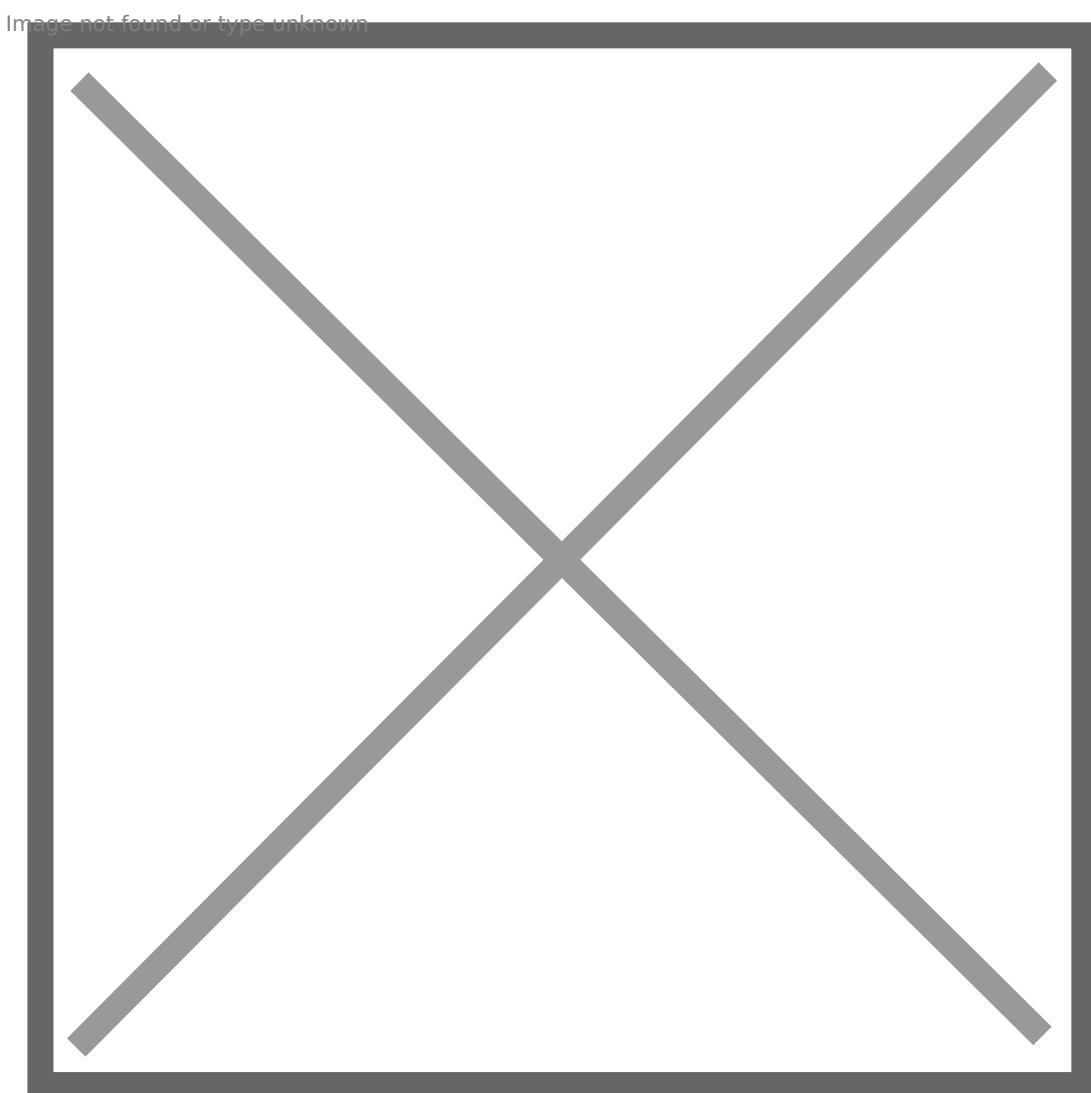
Установка сертификата SkyDNS в браузере Mozilla Firefox для всех платформ

Браузер Mozilla Firefox не использует системные настройки, поэтому установка сертификата в нем отличается от других браузеров.

1. Щелкните по иконке настроек в правом верхнем углу браузера и выберите пункт меню **Настройки**.

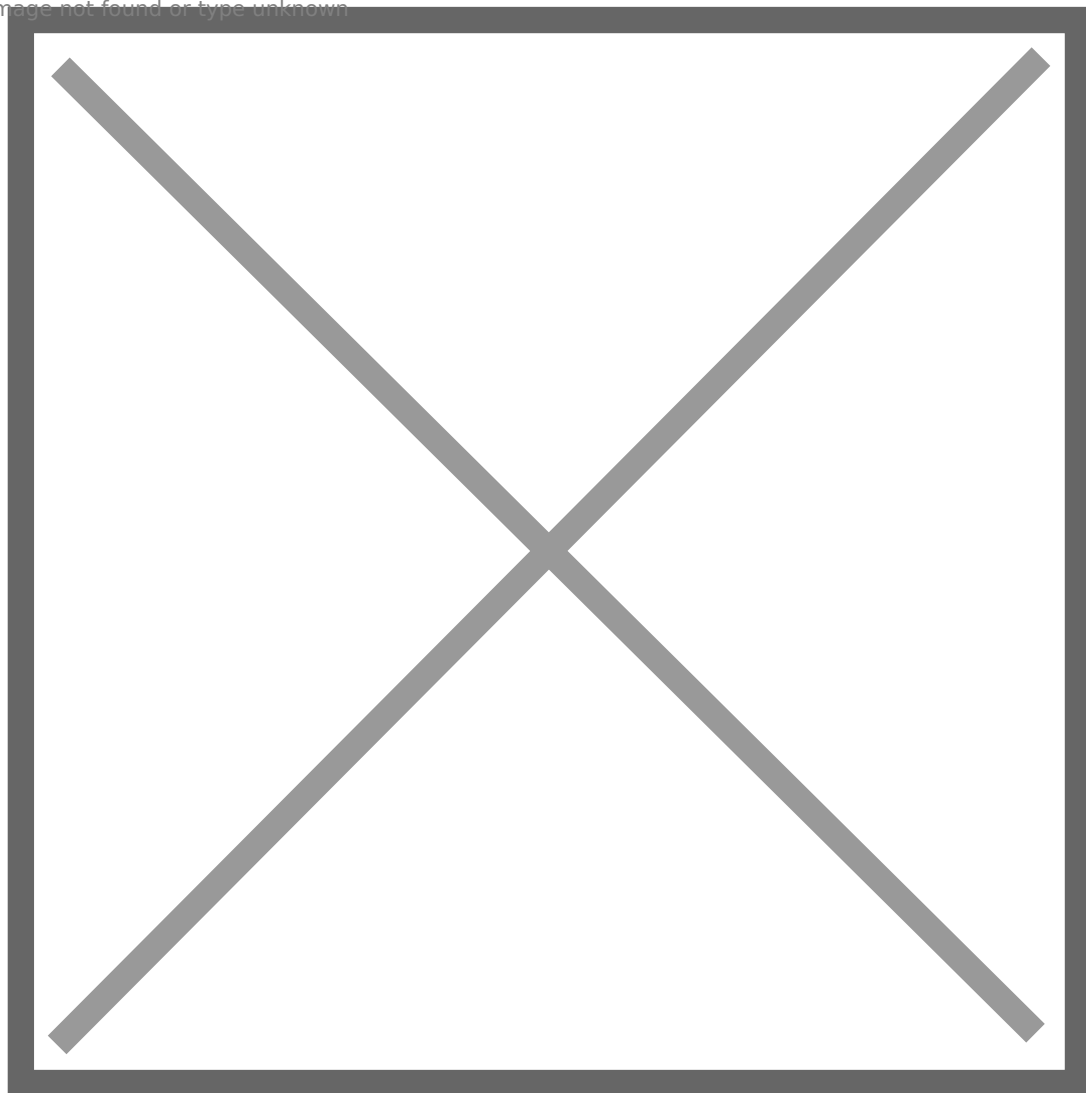


2. В левом меню выберите **Приватность и защита** затем прокрутите в самый низ страницы и нажмите кнопку **Просмотр сертификатов**.



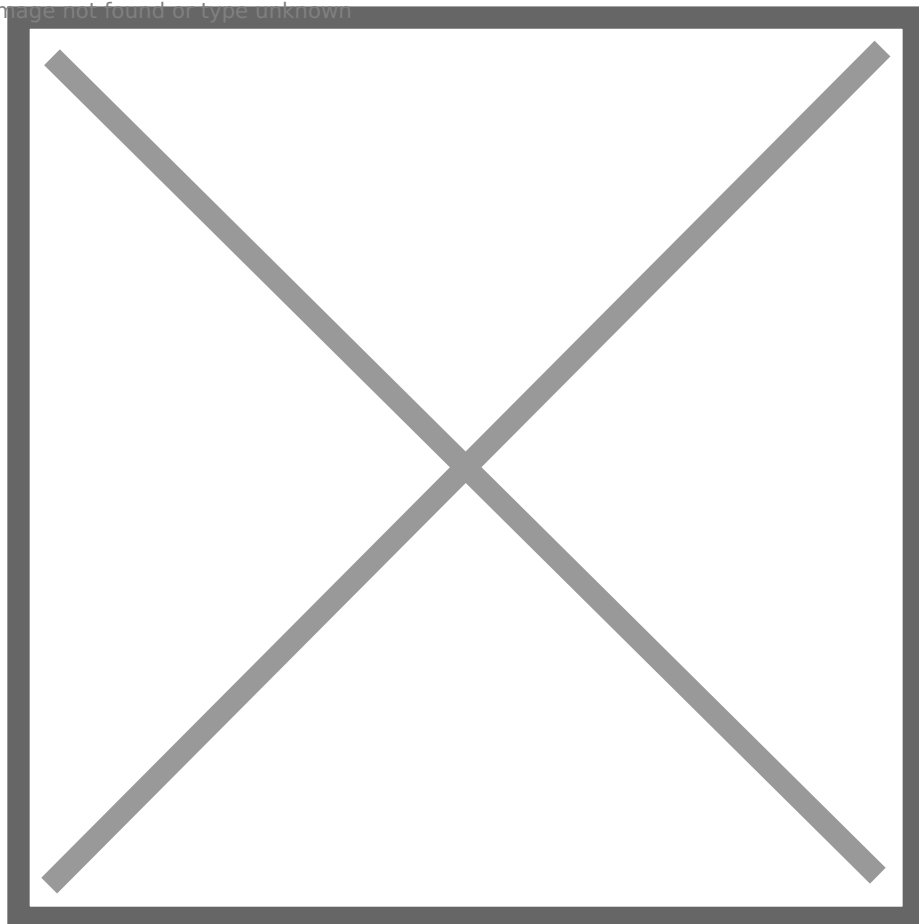
3. В окне Сертификатов выберите вкладку **Центры сертификации** и нажмите кнопку **Импортировать**.

Image not found or type unknown



4. Выберите заранее загруженный сертификат SkyDNS. В окне загрузки сертификата установите галочку **Доверять при идентификации веб-сайтов** и нажмите кнопку **ОК**.

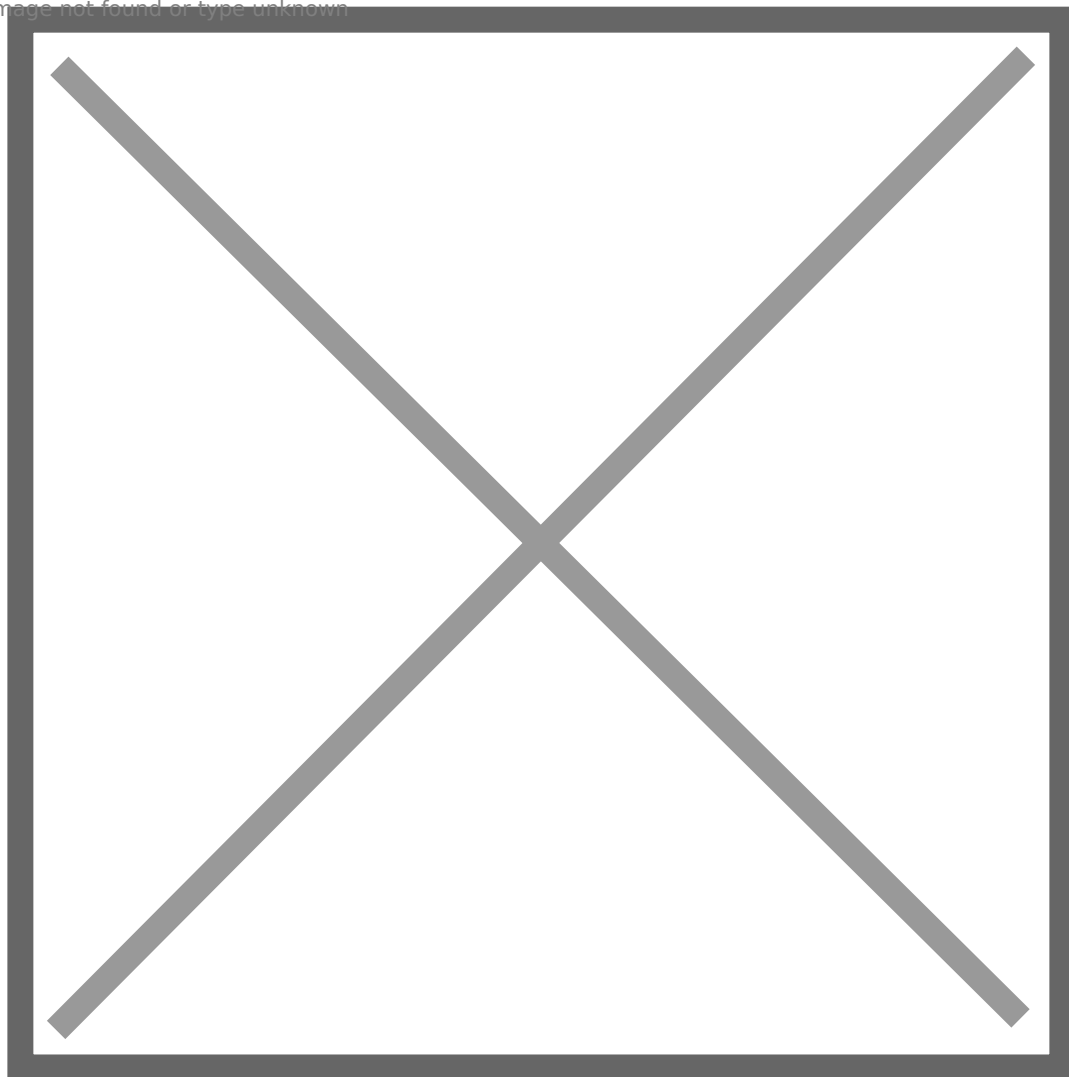
Image not found or type unknown



Установка сертификата SkyDNS в Mac OSX

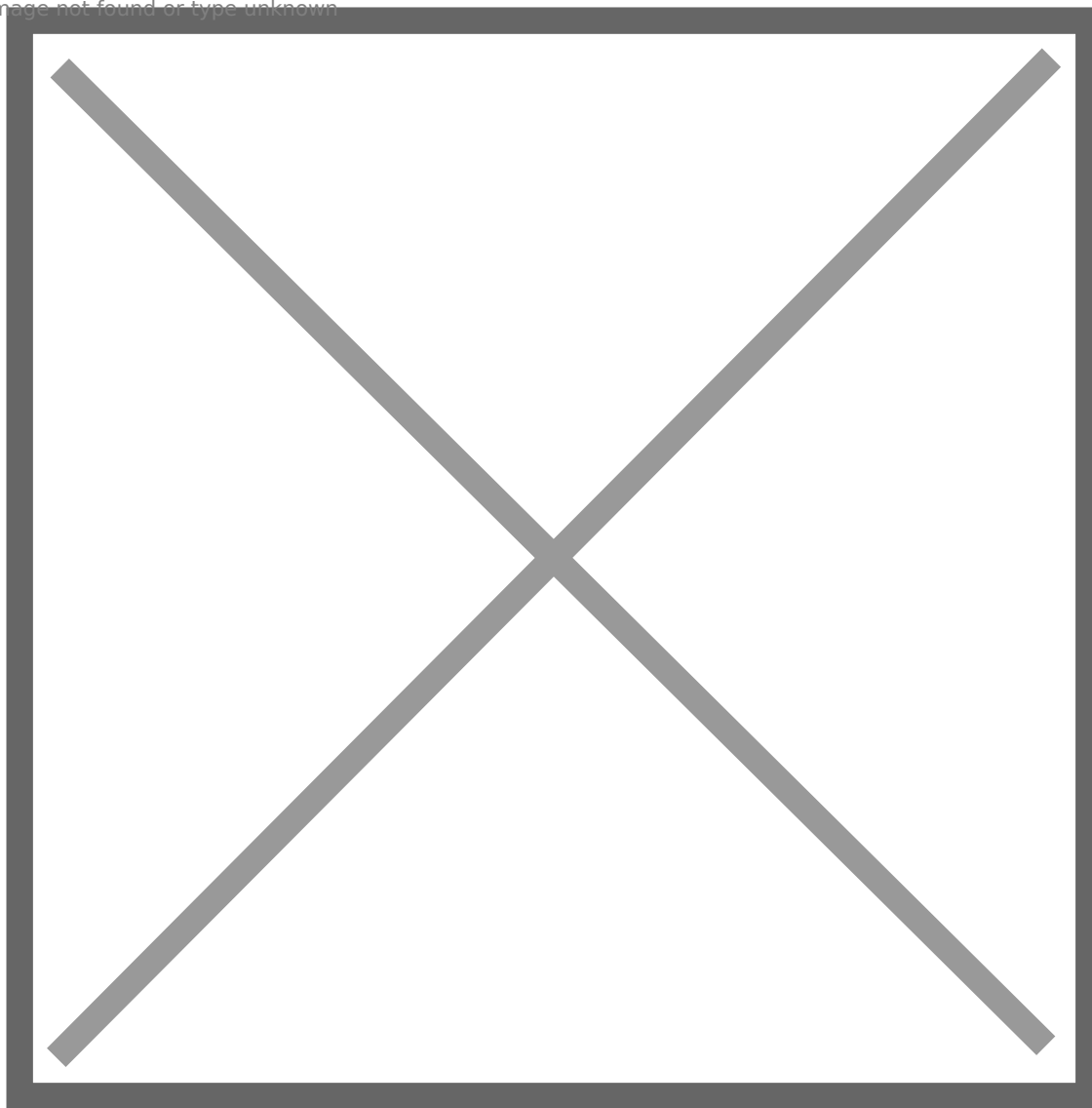
1. Нажмите сочетание клавиш **CTRL+SPACE** и в поиске Spotlight введите **Связка ключей**. Откройте приложение Связка ключей.

Image not found or type unknown



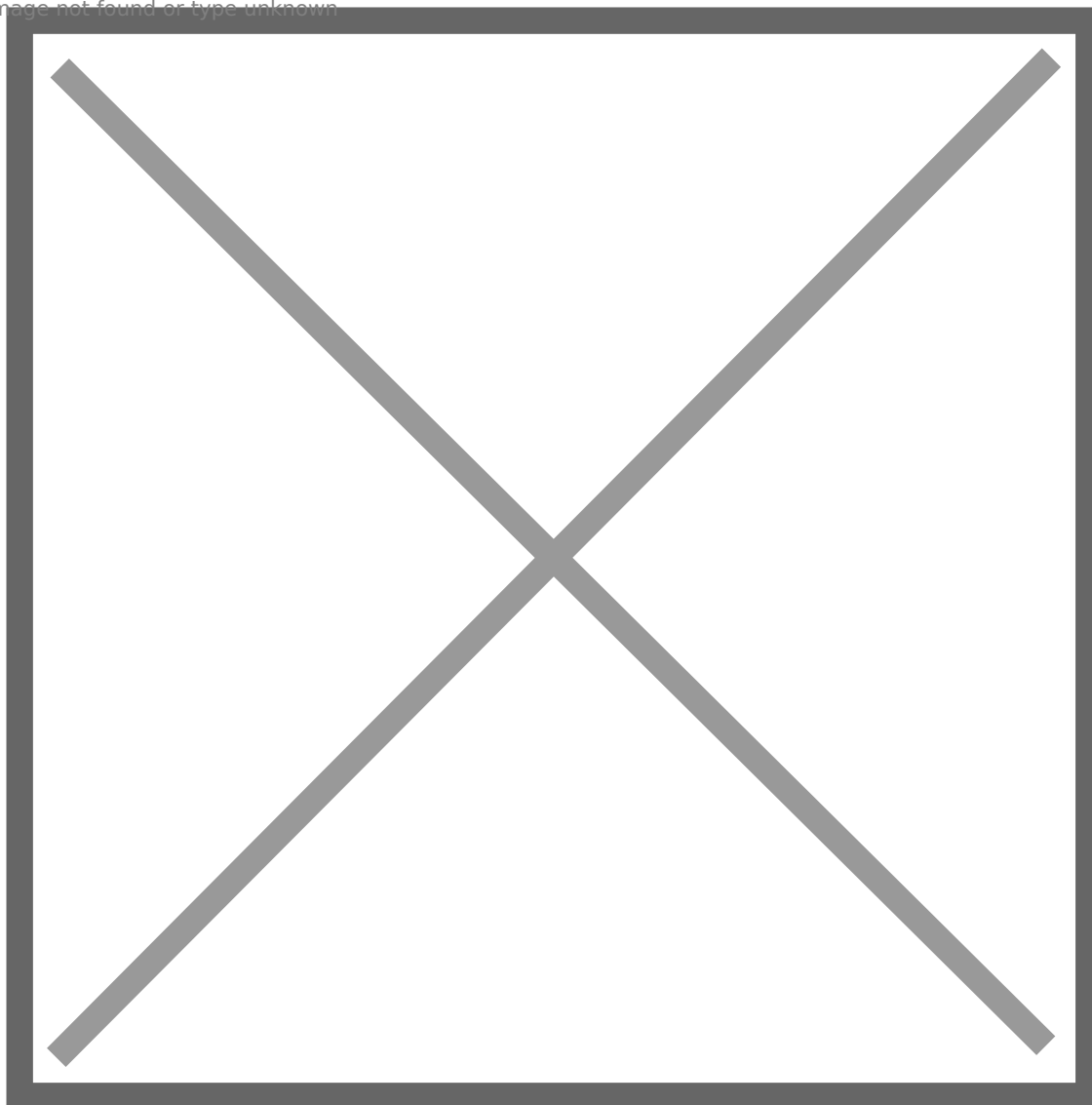
2. В приложении Связка ключей выберите параметр **Вход** и категорию **Сертификаты**.

Image not found or type unknown



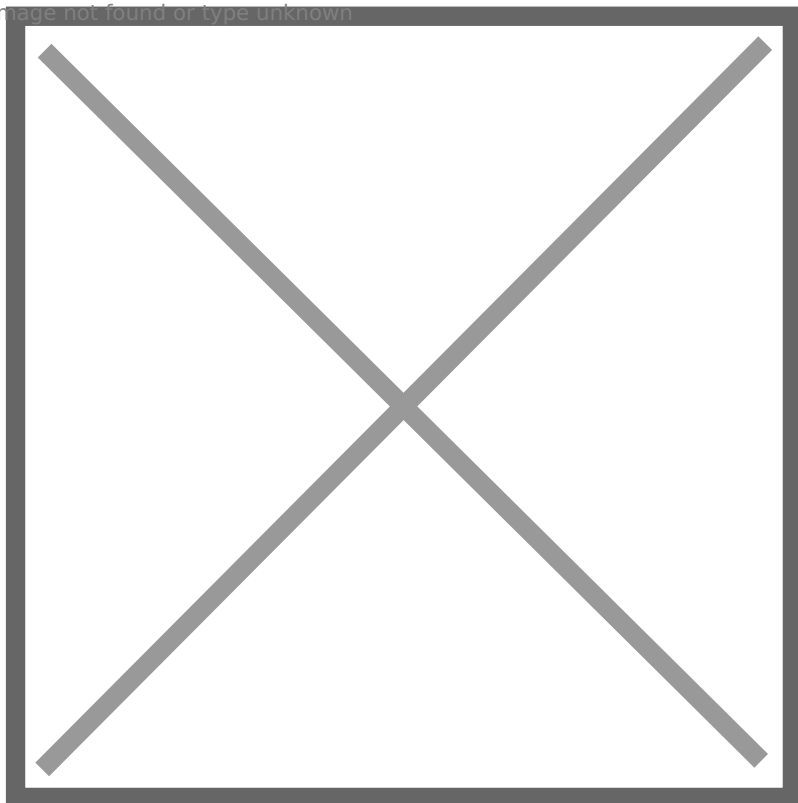
3. Перетащите заранее загруженный сертификат SkyDNS в правую часть окна приложения Связка ключей, где хранятся остальные сертификаты.

Image not found or type unknown



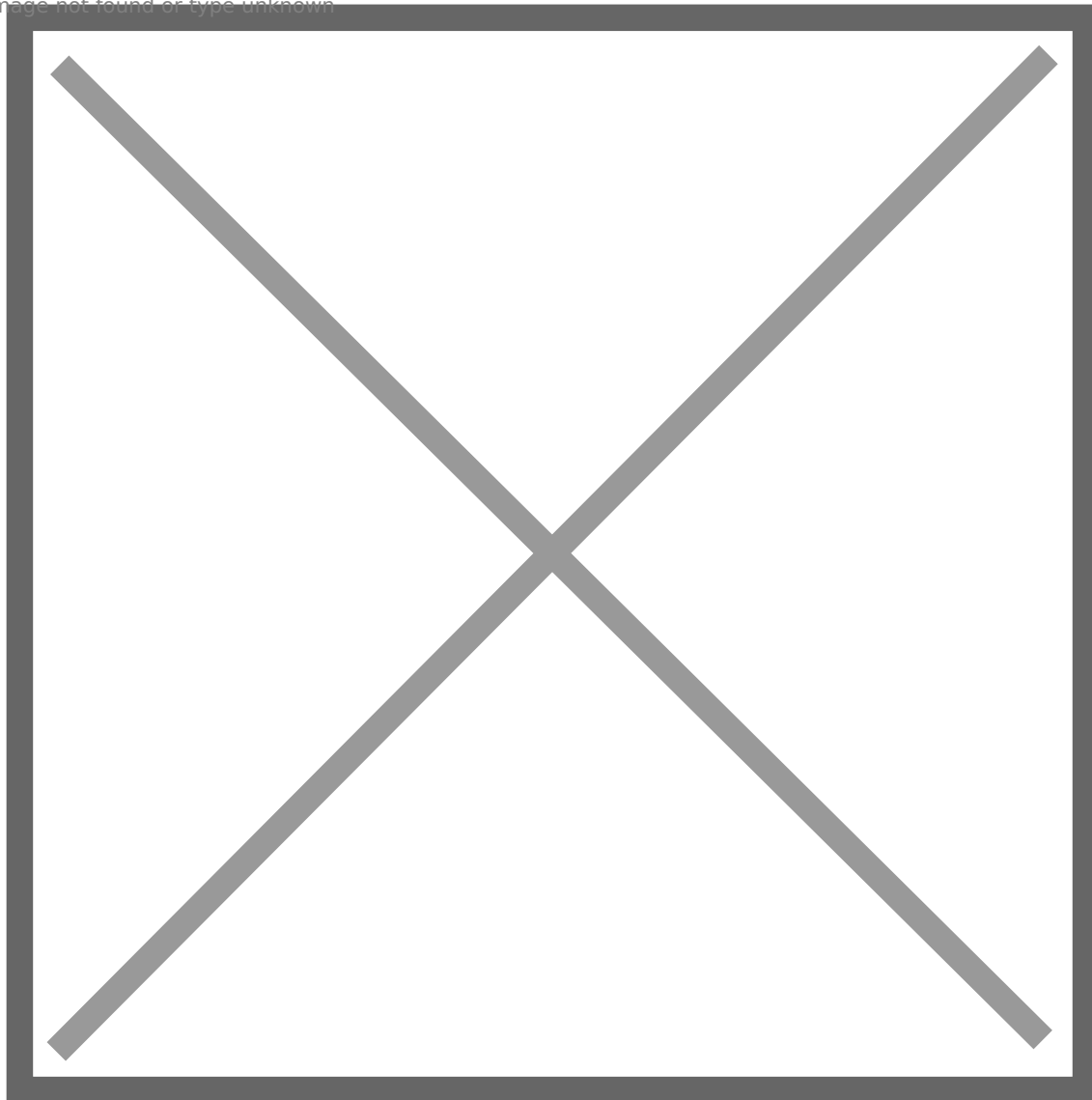
4. Щелкните правой кнопкой мыши по сертификату SkyDNS и выберите пункт меню **Свойства сертификата**. В открывшемся окне разверните пункт **Доверие** и в **Параметрах использования сертификата** выберите **Всегда доверять**. Закройте окно сертификата.

Image not found or type unknown



5. В приложении Связка ключей убедитесь, что сертификат SkyDNS помечен как надежный для данной учетной записи.

Image not found or type unknown

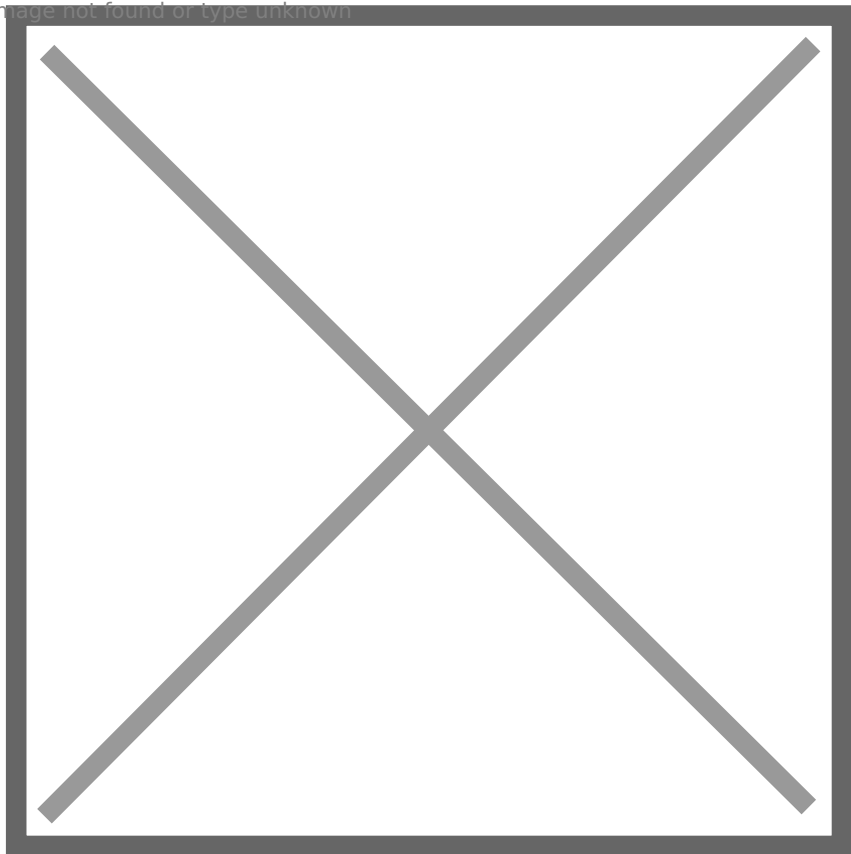


Установка корневого сертификата SkyDNS на устройства под управлением OS Android и iOS

Установка сертификата SkyDNS в Android:

1. [Скачать сертификат](#). После скачивания автоматически откроется окно добавления сертификата.
2. Ввести название сертификата, в поле "**Использовать аккаунт**" выбрать "**VPN и приложения**". Нажать "**ОК**".

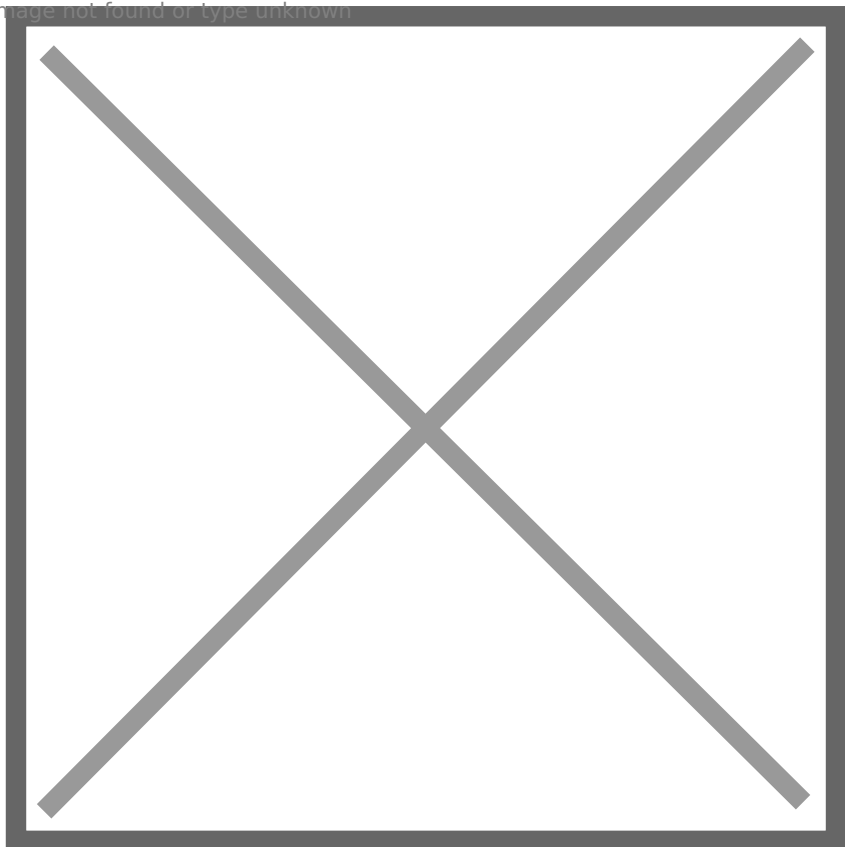
Image not found or type unknown



Установка сертификата SkyDNS в iOS:

1. [Скачать сертификат на устройство](#). Открыть скачанный файл.

Image not found or type unknown



2. Нажать **Установить** в открывшемся окне установки сертификата, затем в появившемся предупреждении, затем в окне установки профиля.

Image not found or type unknown

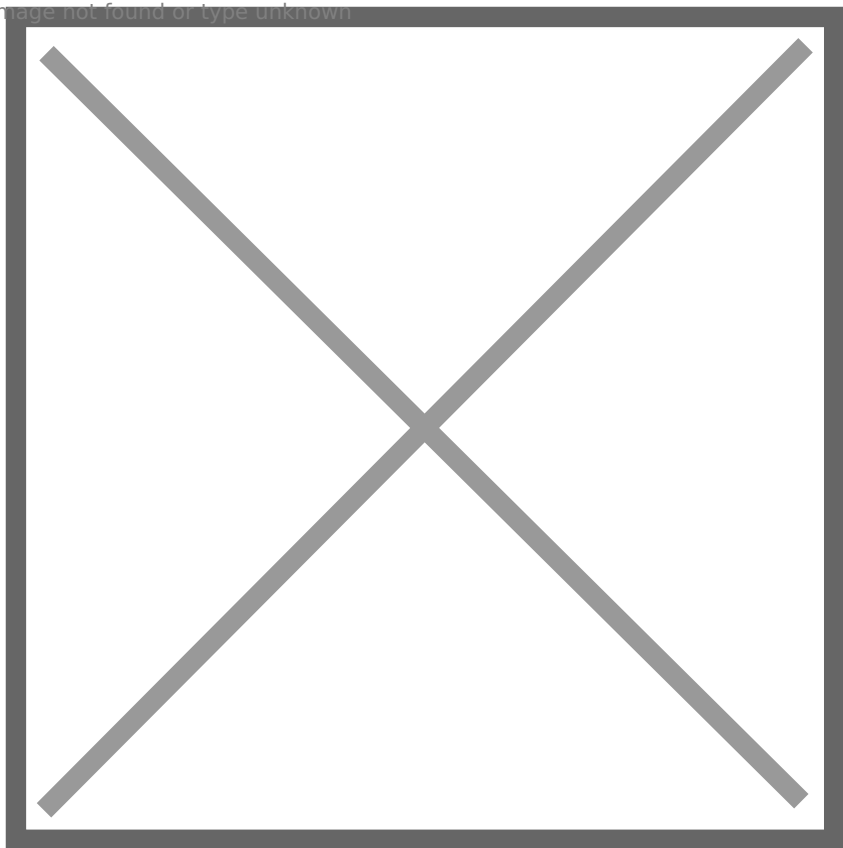
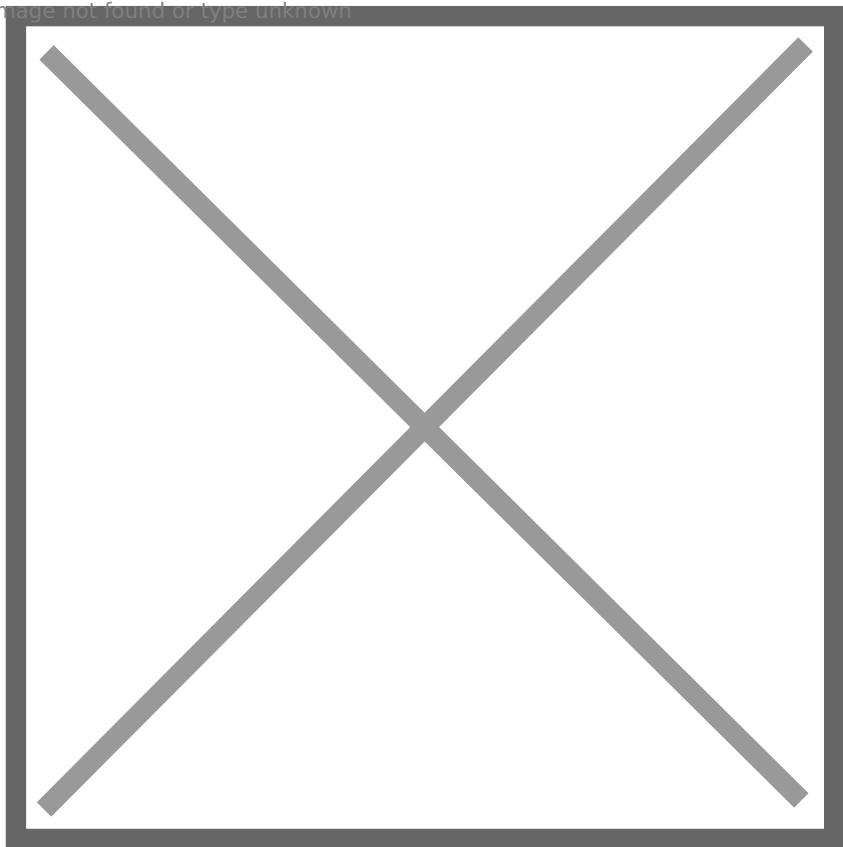
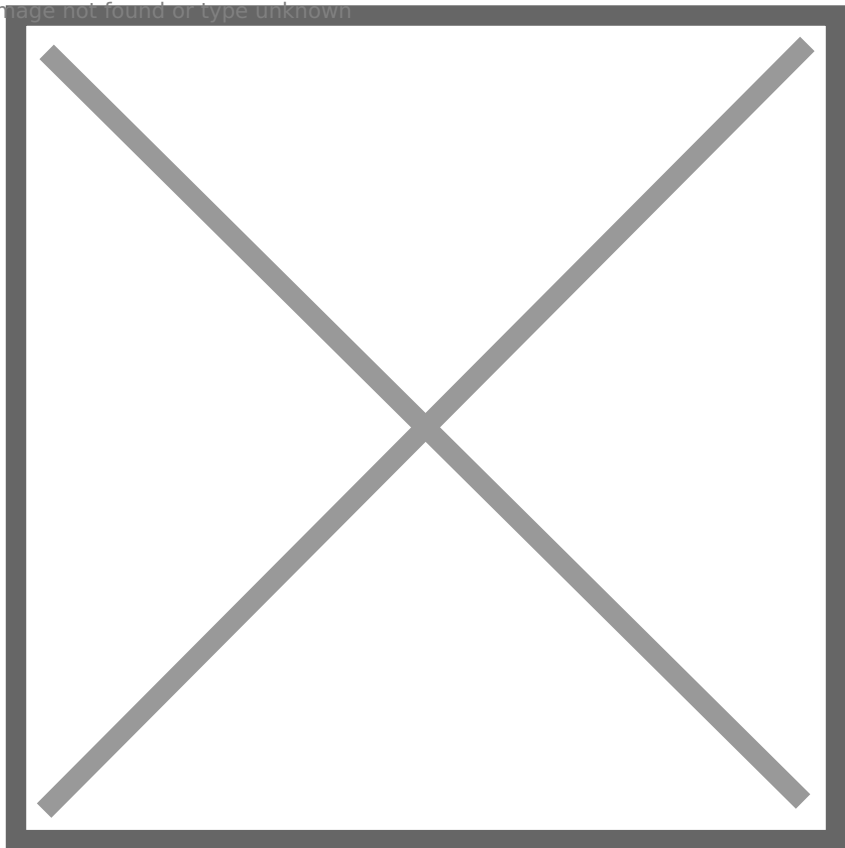


Image not found or type unknown



3. Нажать **Готово** для завершения установки.

Image not found or type unknown



4. Перейти в Настройки - Об этом устройстве - Управление сертификатами. Включить переключатель **Доверять сертификату**.

Image not found or type unknown

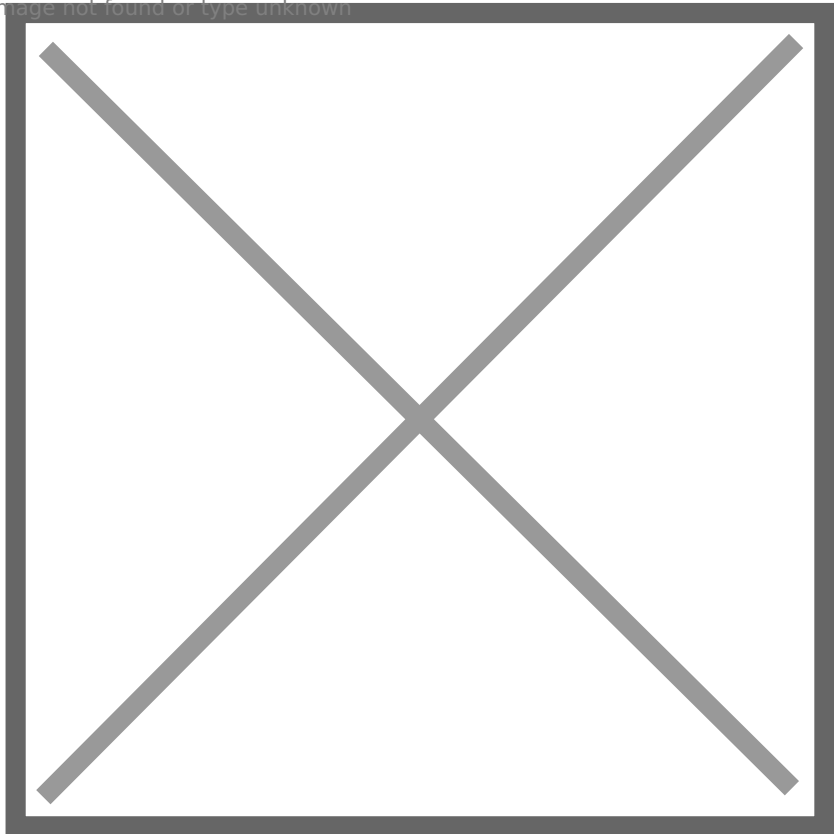


Image not found or type unknown

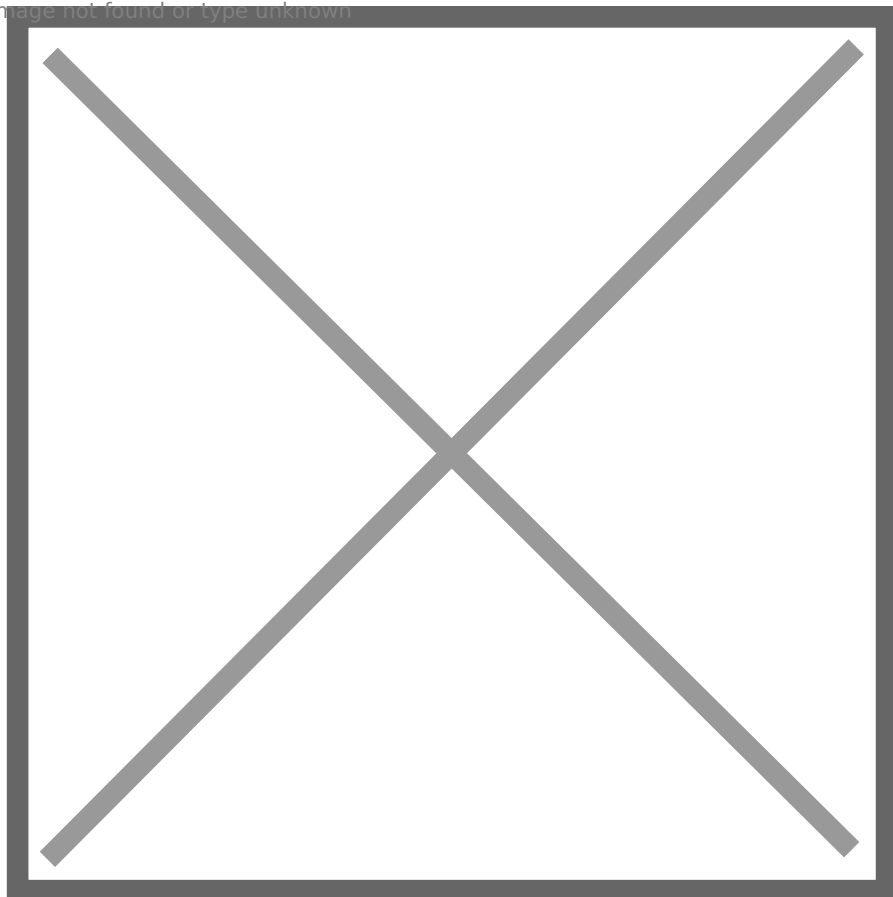
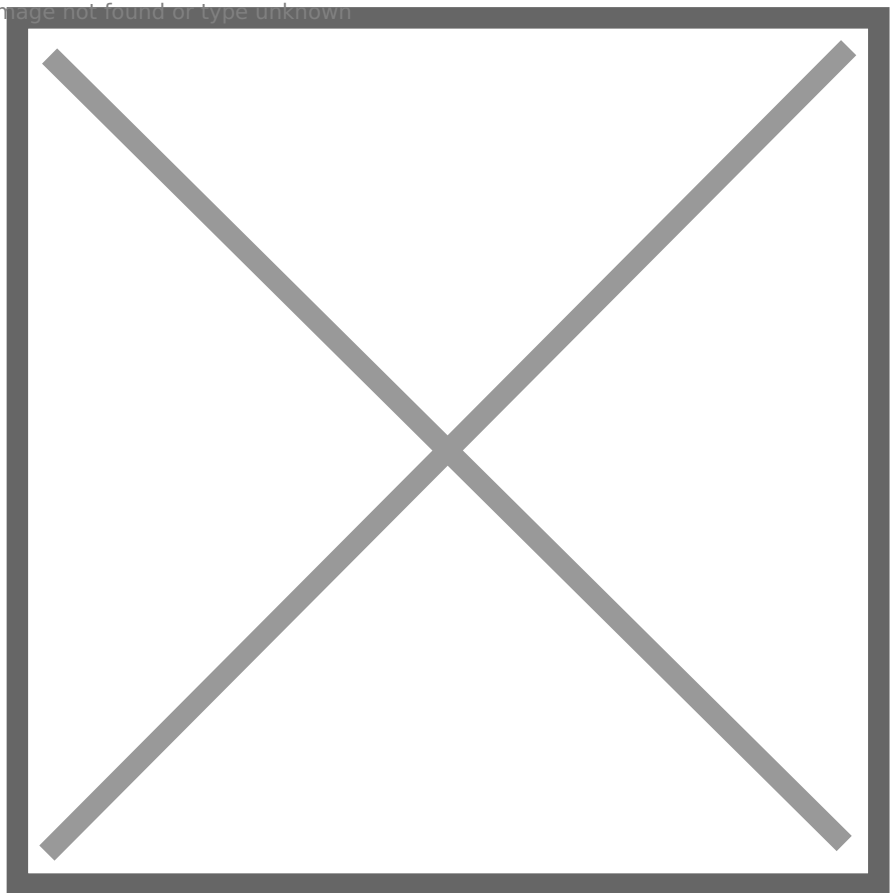


Image not found or type unknown



Ручная установка сертификата с помощью консоли

Установка сводится к двум шагам:

1. Скопировать файл с сертификатом в определенный каталог.
2. Запустить команду для импорта сертификата.

Для Deb (Debian / Ubuntu / Astra Linux)

Копируем файл в каталог **/usr/local/share/ca-certificates**:

```
cp /foo/bar/cert.crt /usr/local/share/ca-certificates/
```

Выполняем установку:

```
update-ca-certificates
```

Для RPM (Rocky Linux / РЕД ОС / RHEL / CentOS / Fedora)

Копируем файл в каталог **/etc/pki/ca-trust/source/anchors**:

```
cp /foo/bar/cert.crt /etc/pki/ca-trust/source/anchors/
```

Выполняем установку:

```
update-ca-trust
```

Проверка корректности работы страницы блокировки после установки сертификата

Теперь можно проверить блокировку сайтов по протоколу **https**. При попытке зайти на заблокированный сайт у Вас должна отобразиться страница блокировки. Если страница блокировки не отображается, либо отображается оповещение браузера о недействительном сертификате - повторите шаги по установке сертификата.

Если после повторной настройки останутся нерешенные вопросы или проблемы - обращайтесь в нашу [службу технической поддержки](#).

Revision #11

Created 22 November 2023 10:07:48 by Виктор

Updated 7 February 2024 06:58:18 by Виктор