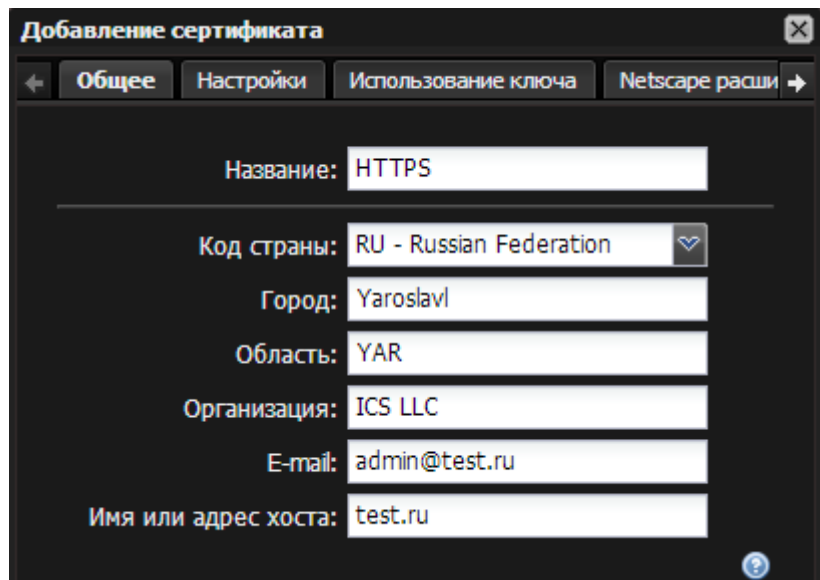


## Настройка HTTPS-фильтрации

Для того, чтобы получить возможность фильтровать HTTPS-трафик пользователей, необходимо сделать следующее:

1. Добавить корневой сертификат (CA) со стандартными настройками в модуле [сертификаты](#).



Добавление сертификата

← Общее Настройки Использование ключа Netscape расши →

Название: HTTPS

Код страны: RU - Russian Federation

Город: Yaroslavl

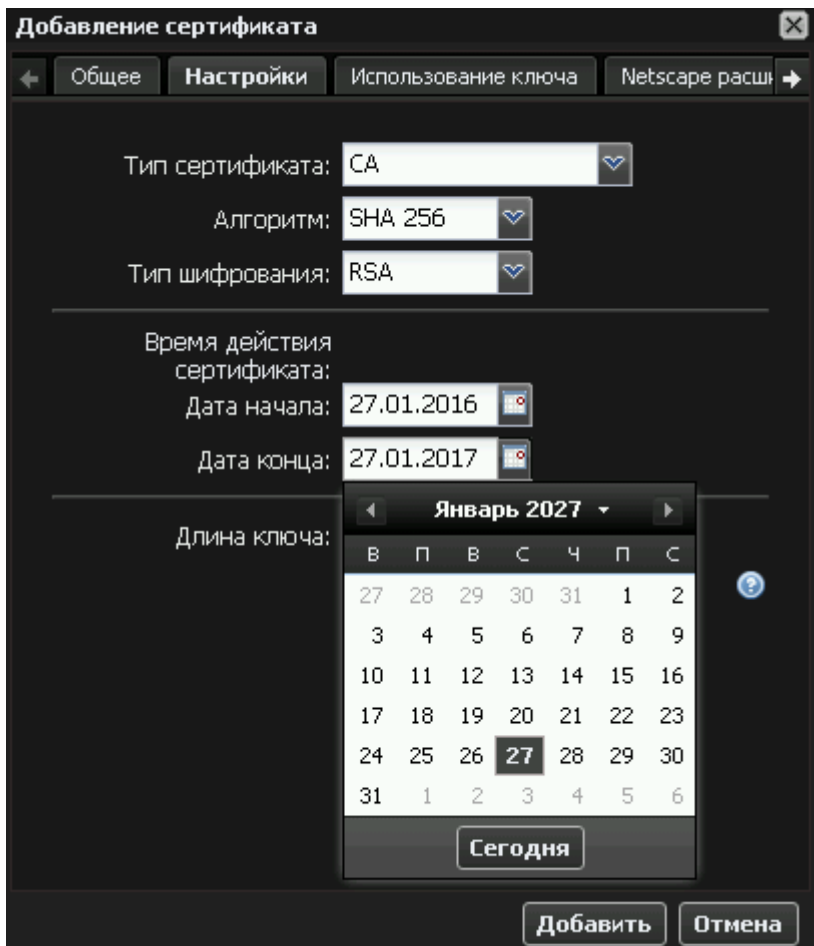
Область: YAR

Организация: ICS LLC

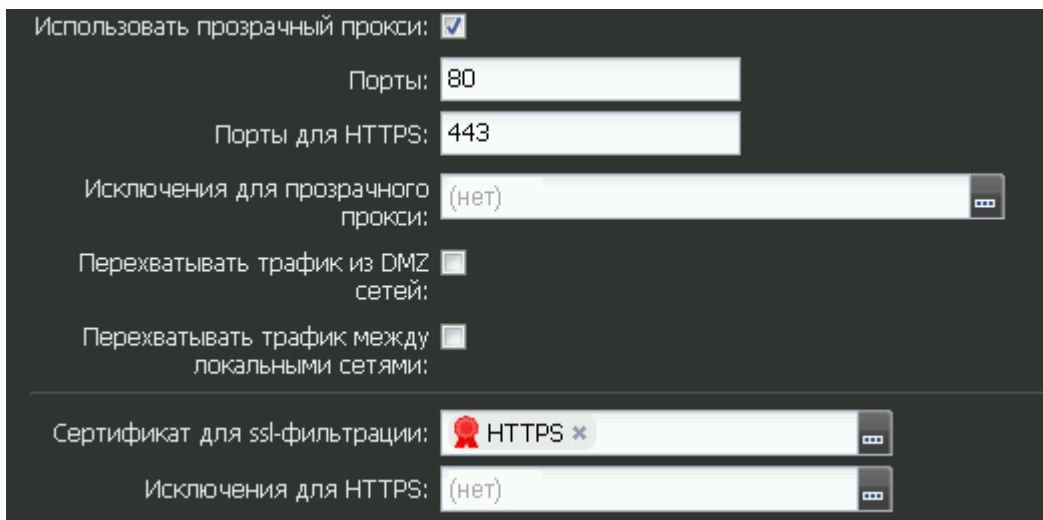
E-mail: admin@test.ru

Имя или адрес хоста: test.ru

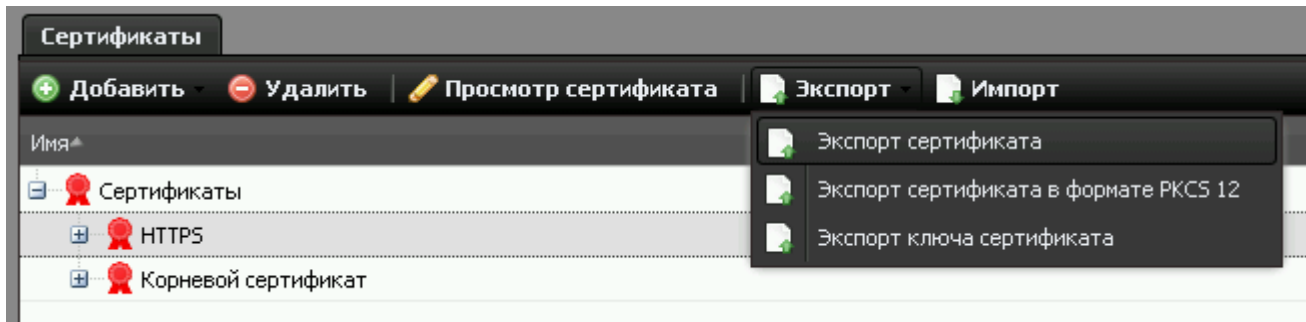
Для того, чтобы сертификат работал длительное время и не было необходимости менять его на конечных пользователях, установите дату окончания сертификата более чем 1 год (по умолчанию). Остальные параметры сертификата оставьте по умолчанию.



После нажатия кнопки «Добавить» система спросит, нужно ли шифрование ключа. Укажите «Не шифровать закрытый ключ».

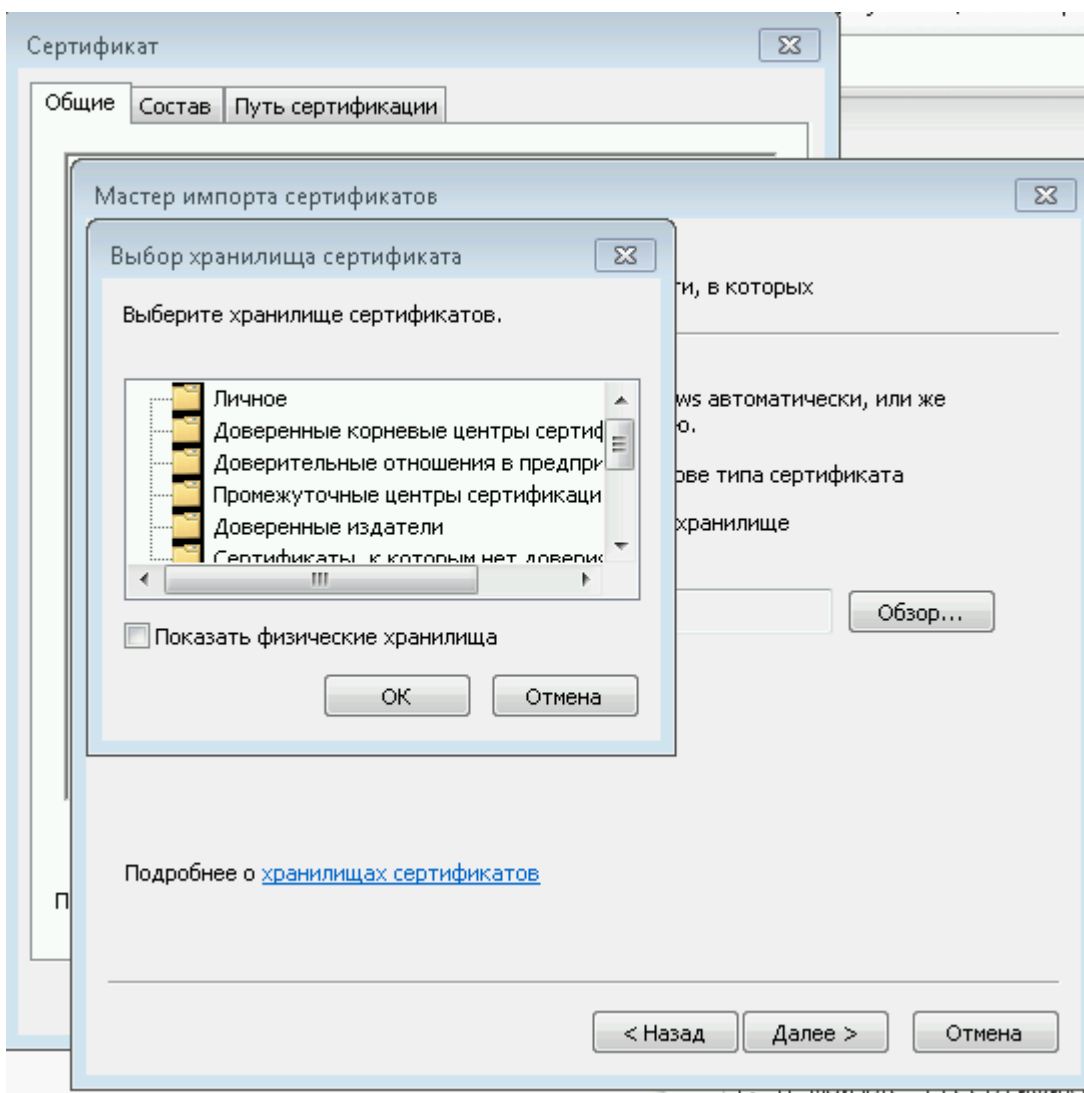


2. Выбрать данный сертификат в поле «Сертификат для ssl-фильтрации» модуля [прокси](#). После этого правила фильтрации начнут работать, однако в связи с подменой сертификата при запросе браузер пользователя будет сообщать о некорректном сертификате. Чтобы исключить данную ошибку, необходимо сделать следующее:



3. В модуле [сертификаты](#) экспортировать данный сертификат на машину конечного пользователя. Экспорт ключа сертификата не требуется.

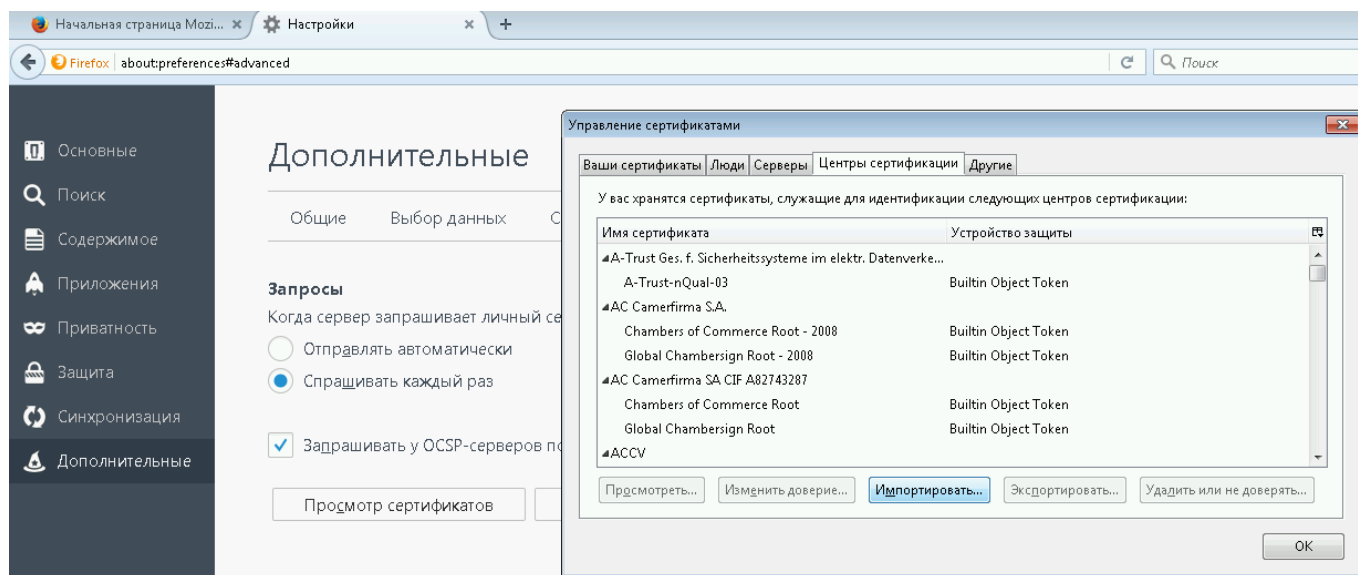
4. На каждом клиентском компьютере добавить сертификат в доверенные корневые центры сертификации.



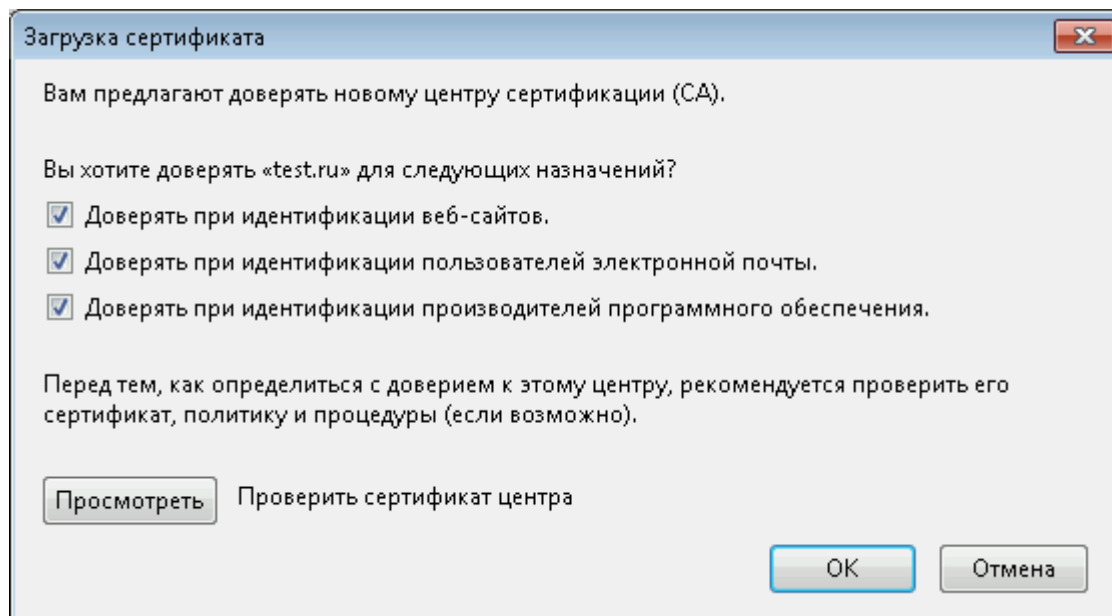
Это делается следующим образом (на примере Windows 7): дважды кликните на сертификат. Нажмите кнопку «Установить сертификат». Откроется мастер импорта сертификата. Когда мастер спросит выбор места хранения сертификата, выберите «поместить все сертификаты в следующее хранилище», нажмите кнопку «Обзор» и выберите «доверенные корневые центры сертификации».

Таким образом, сертификат будет импортирован в глобальное хранилище системы. Он будет работать для тех браузеров, которые используют системные хранилища сертификатов,

например, Internet Explorer, Chrome, Yandex. Если же браузер использует собственное хранилище, как, к примеру, Firefox, то импорт необходимо произвести непосредственно в настройках браузера. Это делается следующим образом (для Mozilla Firefox):



Зайдите в настройки браузера, перейдите в Дополнительные - Сертификаты - Просмотр сертификатов - Импортировать и укажите скачанный с ИКС сертификат.



Отметьте все флажки и импортируйте сертификат.

From: <https://188.225.32.134/> - **Документация**

Permanent link: <https://188.225.32.134/doku.php?id=https>

Last update: **2020/01/27 16:28**

