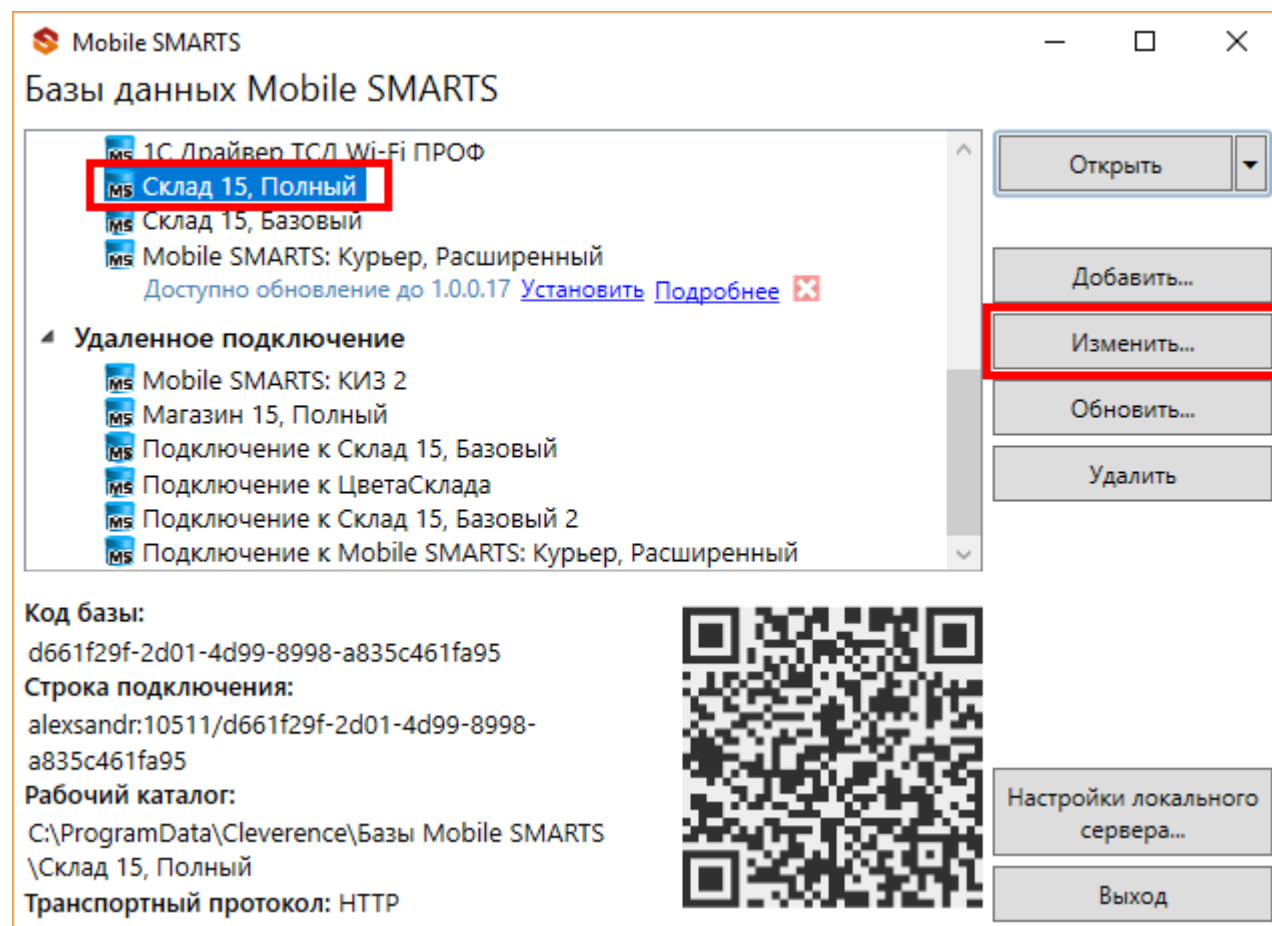


# Доступ к серверу Mobile SMARTS по протоколу HTTPS


Последние изменения: 2024-03-26

Для того, чтобы данные в момент передачи на сервер невозможно было перехватить используется специальный протокол https, который шифрует все передаваемые данные – это безопасное соединение, которое гарантирует, что информация которая передается на сервер остается защищенной.

Для работы через протокол https необходимо указать это в настройках базы данных.



Для работы мобильных приложений с базой данных в защищенном режиме (через https) необходимо наличие на сервере установленного и зарегистрированного корневого сертификата.

 Редактирование настроек базы данных Mobile SMARTS ✕

Наименование:

Папка:

Комментарий:

Режим работы:

*Основной режим работы Mobile SMARTS. Все ТСД и сторонние системы работают через сервер.*

Использовать https ☒

Аутентификация по пользователю ☐


Порт сервера данных:

Сервер печати используется ☐


Порт сервера печати:

Сертификат можно установить, только от имени Администратора.

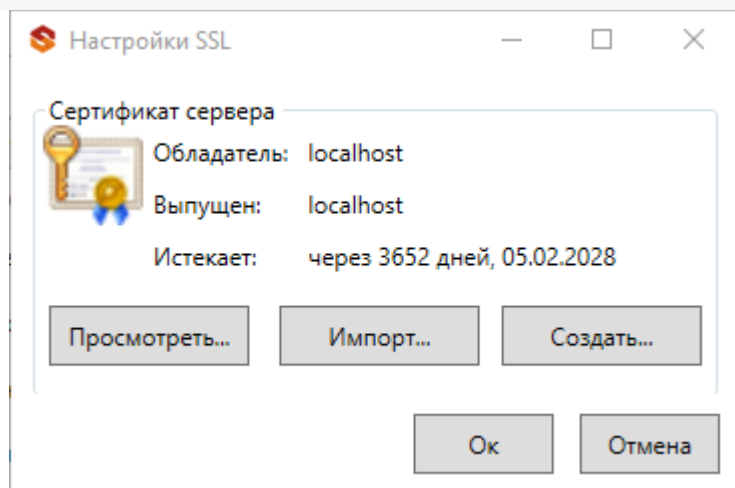
Для тестирования работы веб-сервера в защищенном режиме достаточно самостоятельно сгенерировать самоподписанный тестовый сертификат.

 Настройки SSL — □ ✕

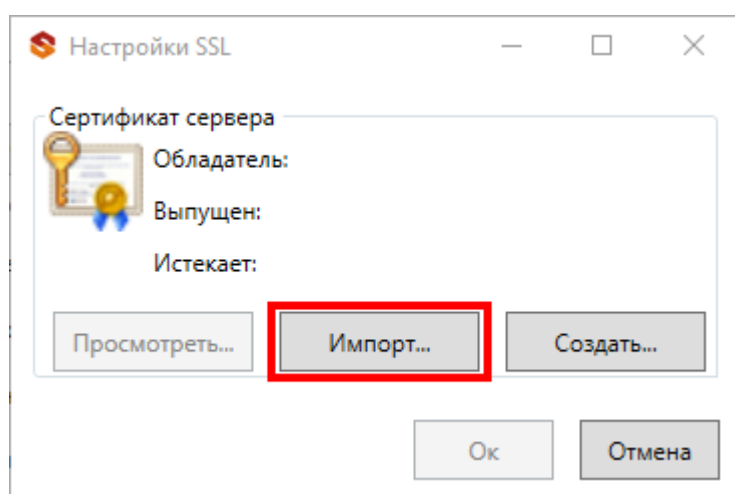
Сертификат сервера

 Обладатель:  
Выпущен:  
Истекает:

Созданный самоподписанный тестовый сертификат установится автоматически.



Настоящий сертификат возможно получить, сформировав запрос к одному из доверенных центров сертификации. Полученный сертификат необходимо установить (импортировать) в локальное хранилище сертификатов на той машине, на которой запущен веб-сервер Mobile SMARTS в раздел "Доверенные корневые центры сертификации\Сертификаты"



 безопасность

Не нашли что искали?



Задать вопрос в техническую поддержку