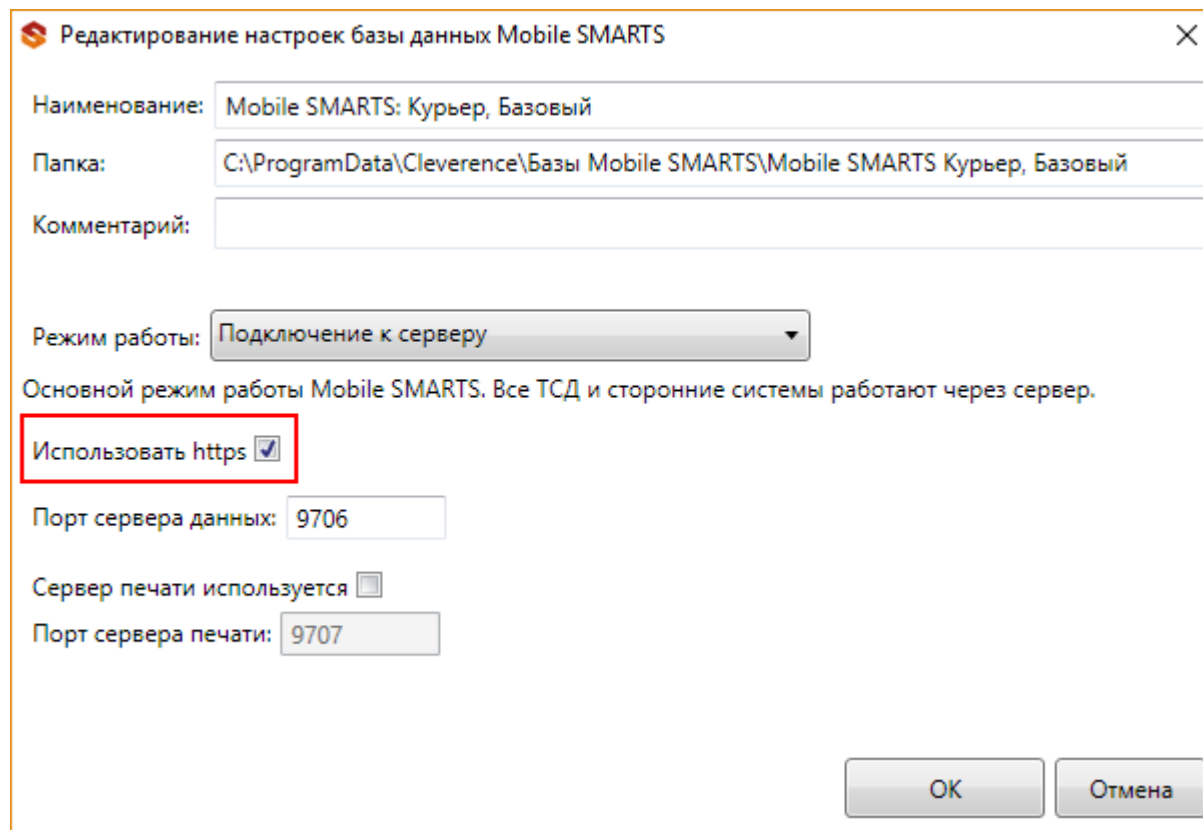


Установка сертификата HTTPS на сервер Mobile SMARTS

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.



Редактирование настроек базы данных Mobile SMARTS

Наименование: Mobile SMARTS: Курьер, Базовый

Папка: C:\ProgramData\Cleverence\Базы Mobile SMARTS\Mobile SMARTS Курьер, Базовый

Комментарий:

Режим работы: Подключение к серверу

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

Использовать https ☒

Порт сервера данных: 9706

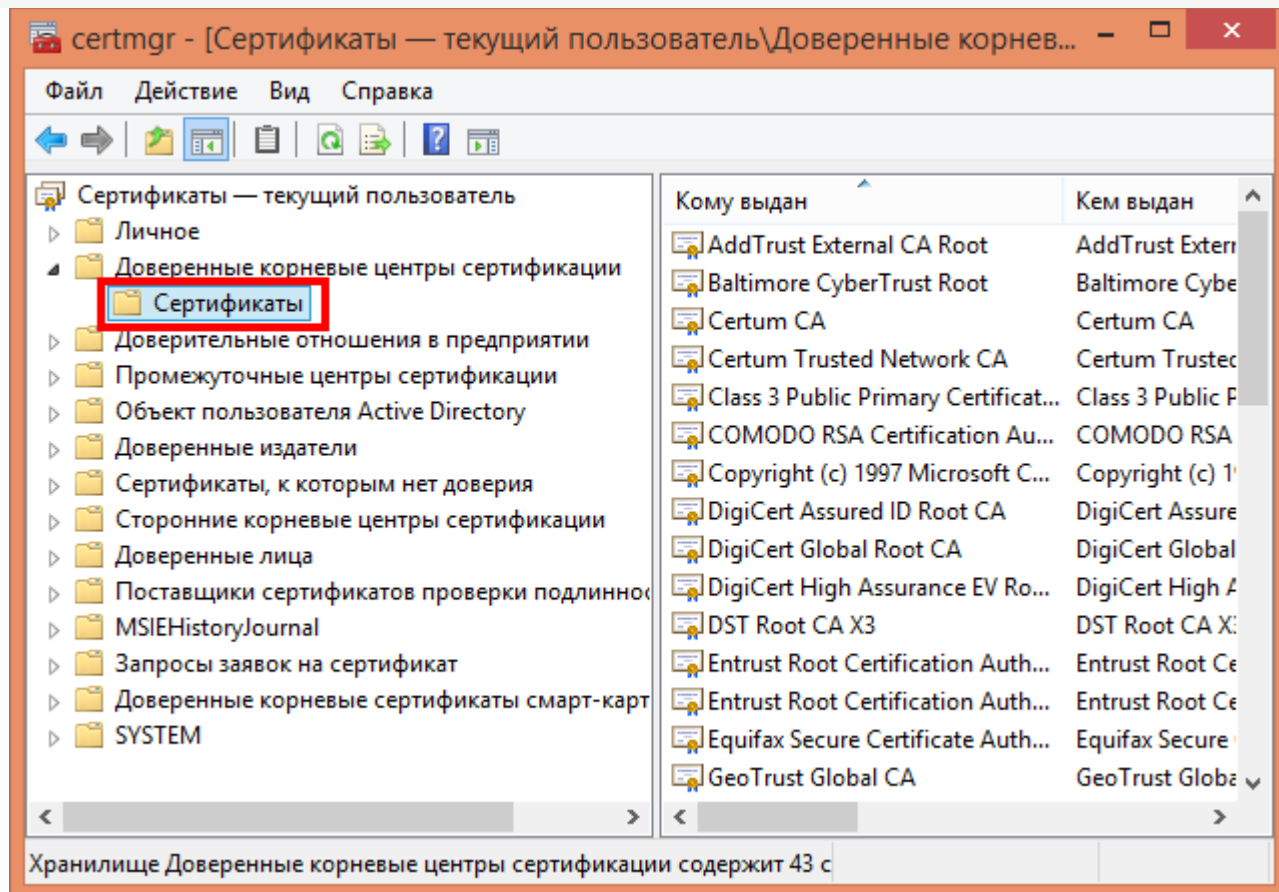
Сервер печати используется ☐

Порт сервера печати: 9707

OK Отмена

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

Можно работать без использования протокола HTTPS и сертификата, но при этом данные будут передаваться в открытом виде.



Данный сертификат возможно получить, сформировав запрос к одному из доверенных центров сертификации.













Полученный сертификат необходимо установить в локальное хранилище сертификатов на той машине, на которой запущен веб-сервер Mobile SMARTS в раздел «Доверенные корневые центры сертификации\Сертификаты».

Для тестирования работы веб-сервера в защищенном режиме достаточно самостоятельно [сгенерировать самоподписанный тестовый сертификат](#) и установить его в хранилище сертификатов хост-машины на котором запущен веб-сервер.

Подключаться с ТСД через интернет по самоподписанному сертификату нельзя. Нужно сгенерировать настоящий сертификат на ip адрес, добавить на компьютер и импортировать в сервер MobileSMARTS и базу.
Либо осуществлять VPN подключение между базой и ТСД, либо получать доверенный сертификат.

Если сертификат не установлен или был установлен неправильно, то возникает ошибка и соединение с сервером будет закрыто.

Сервер Mobile SMARTS

-  Магазин 15, Полный УТ1
-  Магазин 15, Полный Роз
-  1С Драйвер ТСД Инвент
-  Магазин 15, Расширенн
-  Mobile SMARTS: Курьер,
-  1С Драйвер ТСД Wi-Fi П
-  Мал
-  тсд миур
-  Магазин 15, Базовый Куз
-  Магазин 15, Базовый 17
-  Магазин 15, Расширенн
-  Магазин 15, Расширенн

Имя базы данных: Mobile SMARTS: Курьер, Расширенный

Параметры сервера данны...

Адрес: <https://it02:10560>

Статус: Базовое соединение закрыто: Непредвиденная ошибка при передаче.

Порт сервера данных: 10560

Учетная запись:

☐ Используется (общие параметры)

Имя пользователя: foo

Пароль: ...

Сжимать справочники и таблицы:

☐ Рекомендуется использовать только в условиях неустойчивой сети или экономии платного трафика, так как скорость распаковки сжатых данных в большинстве мобильных устройств мала!

Делать бэкапы документов:

☒ [Открыть папку с бэкапами](#)

безопасность

Не нашли что искали?



Задать вопрос в техническую поддержку

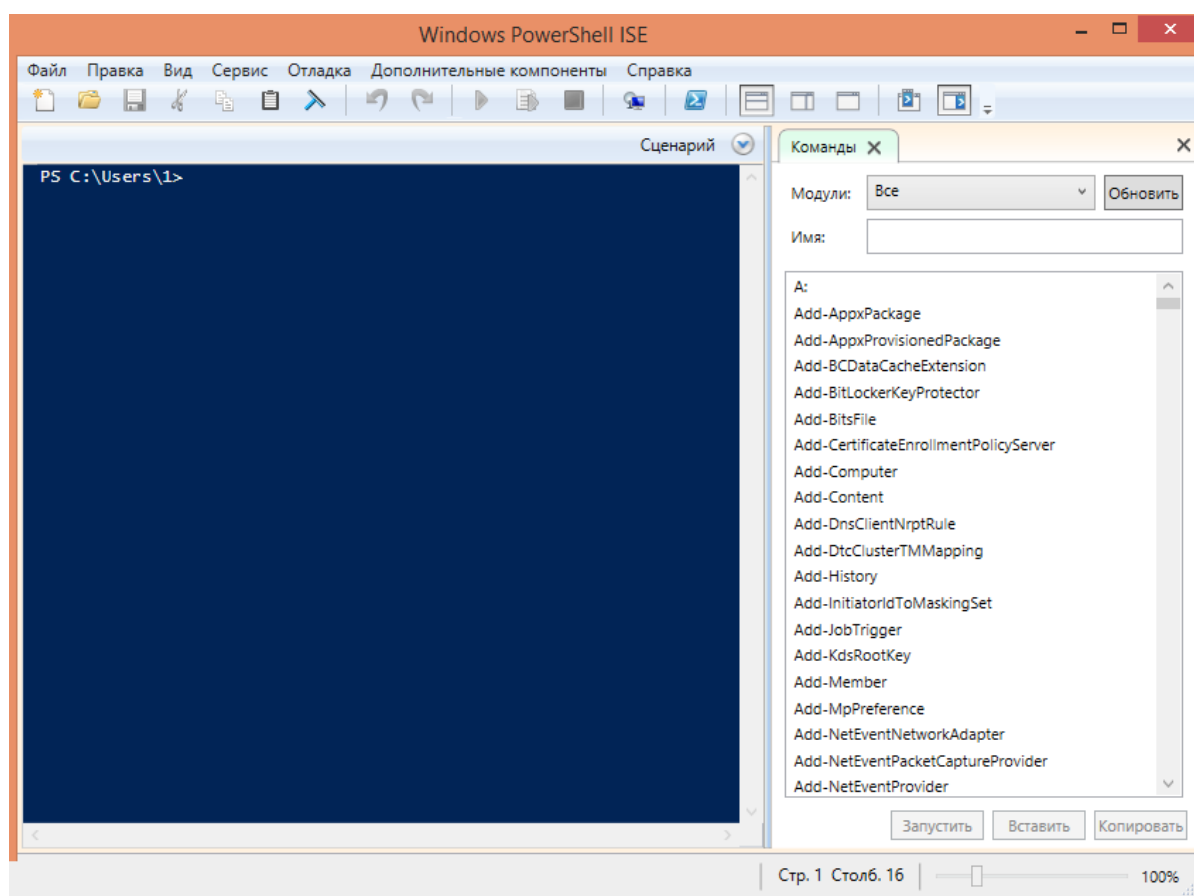
Генерация самоподписанного тестового сертификата для веб-сервера Mobile SMARTS

Последние изменения: 2024-03-26

Для получения самоподписанного тестового сертификата в системах Windows® 8 и Windows Server® 2012 легче всего воспользоваться Windows PowerShell 3.0.

Установка Windows PowerShell.

Для запуска консоли Windows PowerShell, выполните: Win+R, «PowerShell_ISE.exe», «Выполнить». Запускать консоль необходимо с правами локального администратора.



Далее, в окне консоли Windows PowerShell необходимо выполнить командлет «New-SelfSignedCertificate», для этого вводим команду:

```
New-SelfSignedCertificate -DnsName localhost -CertStoreLocation cert:LocalMachineMy
```

Данная команда запускает командлет, который производит генерацию самоподписанного сертификата для DNS имени localhost, и помещает его в раздел «Личные» локального хранилища сертификатов, иногда по неустановленным причинам сертификат может быть помещен в другой раздел локального хранилища, например «Промежуточные центры сертификации».

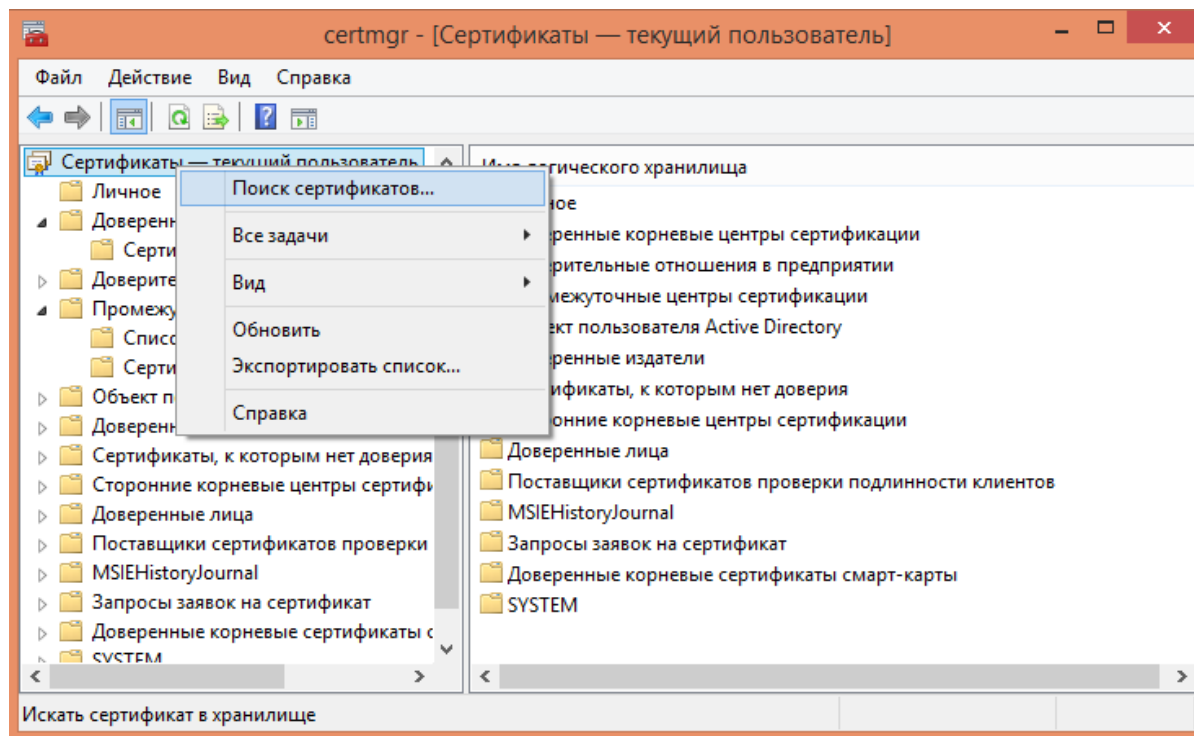
При успешном выполнении командлета в окне консоли появится информация, содержащая слепок сгенерированного сертификата.

```
PS C:\Windows\system32> New-SelfSignedCertificate -DnsName localhost -CertStoreLocation cert:\LocalMachine\My

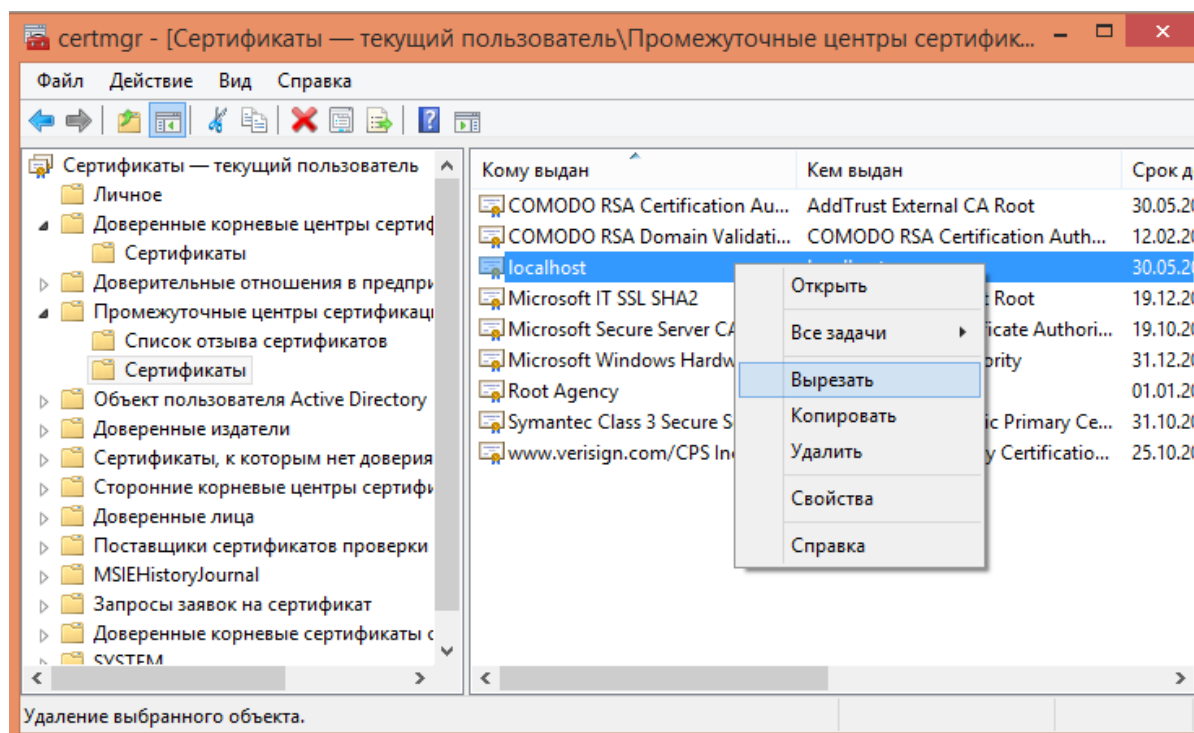
Каталог: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                               Subject
-----
E41C0ADC4FD58953F440C7FACE2097879D887C04  CN=localhost

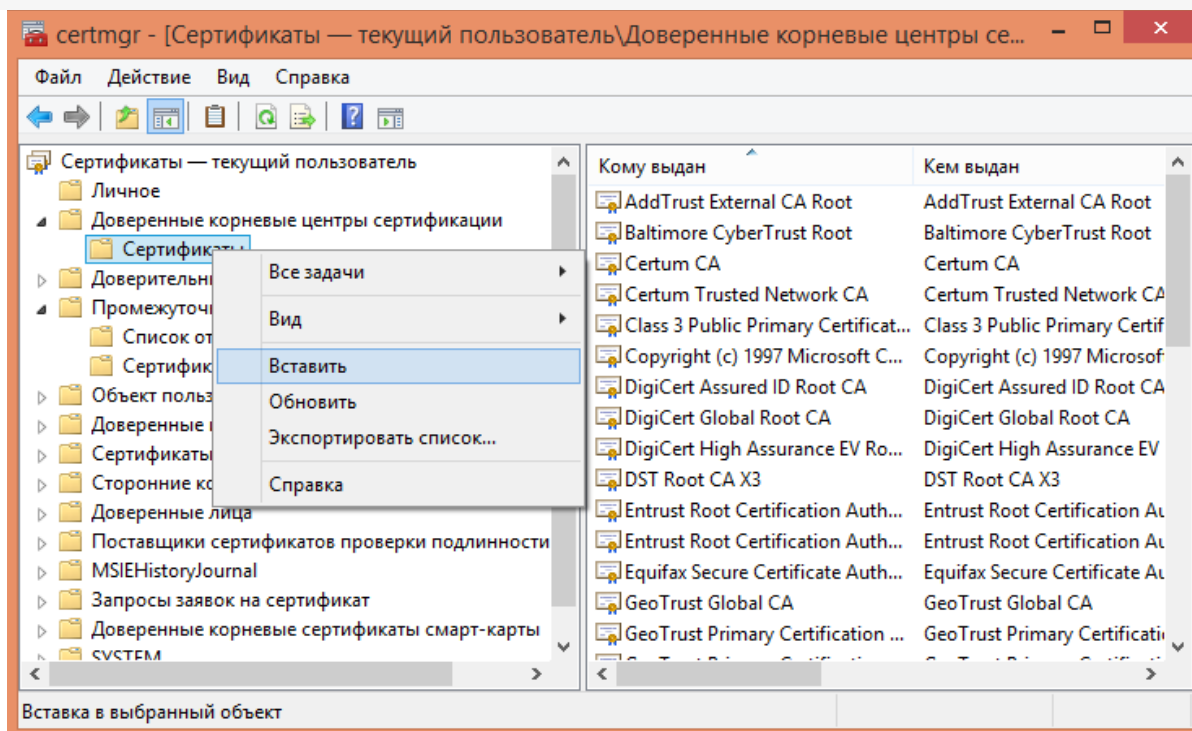
PS C:\Windows\system32>
```



Далее необходимо открыть оснастку «Сертификаты» с правами локального администратора, для этого запустите соответствующий файл «certmgr.msc» и произведите поиск сгенерированного сертификата по его DNS имени «localhost».



Далее, найденный сертификат необходимо переместить в раздел «Доверенные корневые центры сертификации\Сертификаты».



Если описанный способ не сработал, попробуйте альтернативные способы получения сертификата:

- [Как создать самоподписанный сертификат в Windows](#)
- [Выпуск собственного SSL-сертификата](#)

Не нашли что искали?



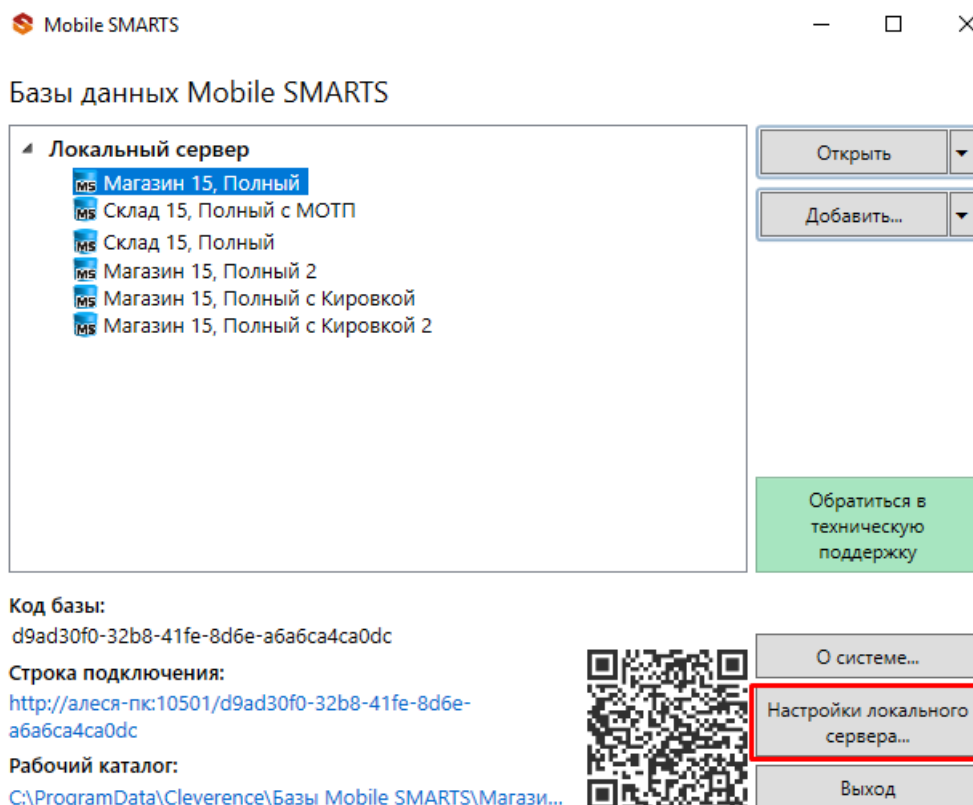
Задать вопрос в техническую поддержку

Изменение типовых портов в настройках сервера Mobile SMARTS

Последние изменения: 2024-03-26

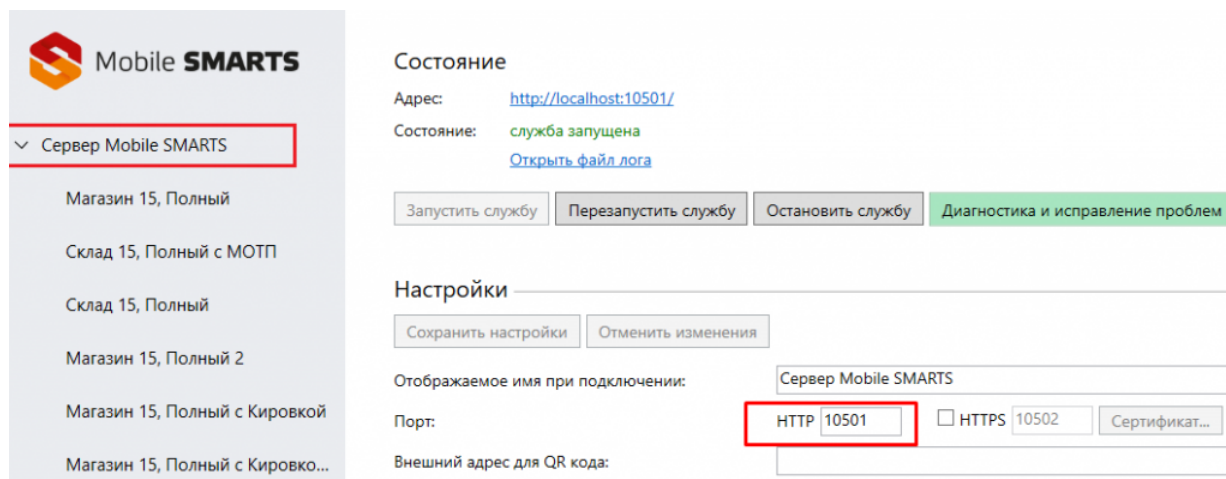
Как изменить порт сервера Mobile SMARTS

1. Запустите **менеджер баз Mobile SMARTS** и нажмите на кнопку «Настройки локального сервера».



2. В открывшемся окне нажмите кнопку «Остановить службу».

3. Измените порт сервера Mobile SMARTS.



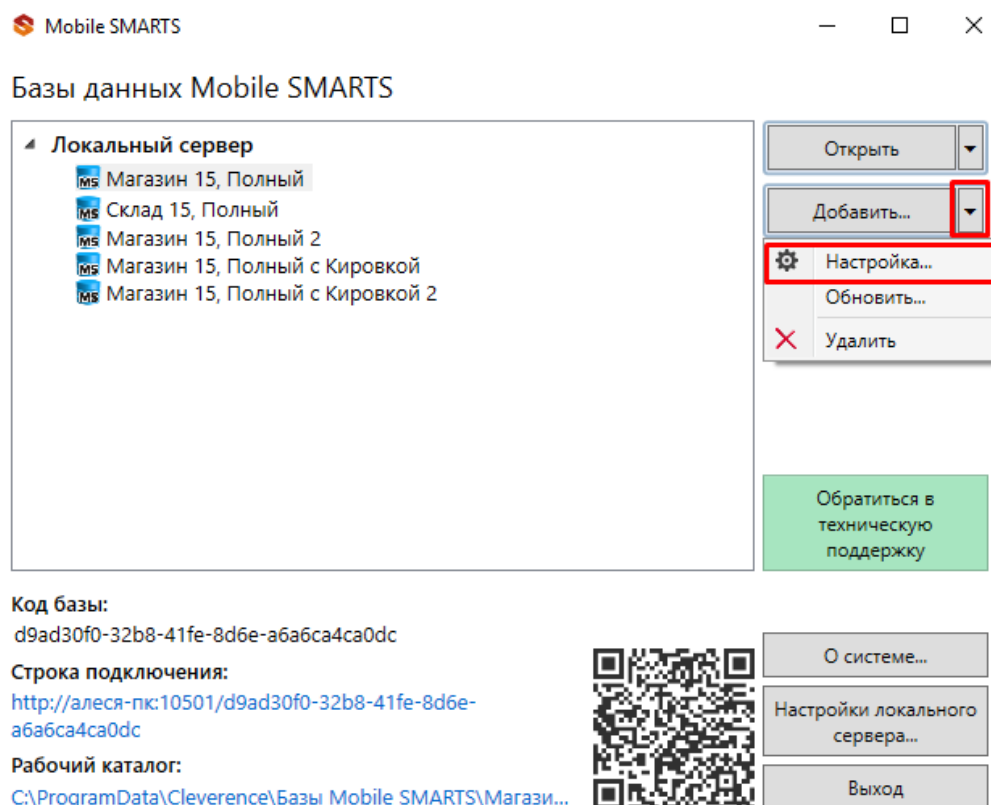
4. Нажмите на кнопку «Сохранить настройки».

5. Запустите службу.


Если изменить порт, не останавливая службу, изменения вступают в силу только после сохранения настроек и перезапуска сервера.

Как изменить порт базы Mobile SMARTS

1. Запустите менеджер баз Mobile SMARTS.
2. Выберите нужную вам базу и откройте выпадающий список возле кнопки «Добавить».
3. Нажмите кнопку «Настройка».



4. Измените порт базы данных Mobile SMARTS. Нажмите кнопку «Ок».

 Редактирование настроек базы данных Mobile SMARTS ✕

Код базы:

Наименование:

Папка:

Комментарий:

Режим работы:

Подключение к серверу ▾

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

Использовать https ☐

Сертификат...

Аутентификация по пользователю ☐

Порт сервера данных:

Сервер печати используется ☐

Порт сервера печати:

OK

Отмена

У каждой базы должен быть свой уникальный порт. Для вступления в силу произведенных настроек перезапуск сервера Mobile SMARTS не требуется.



безопасность

Не нашли что искали?



Задать вопрос в техническую поддержку

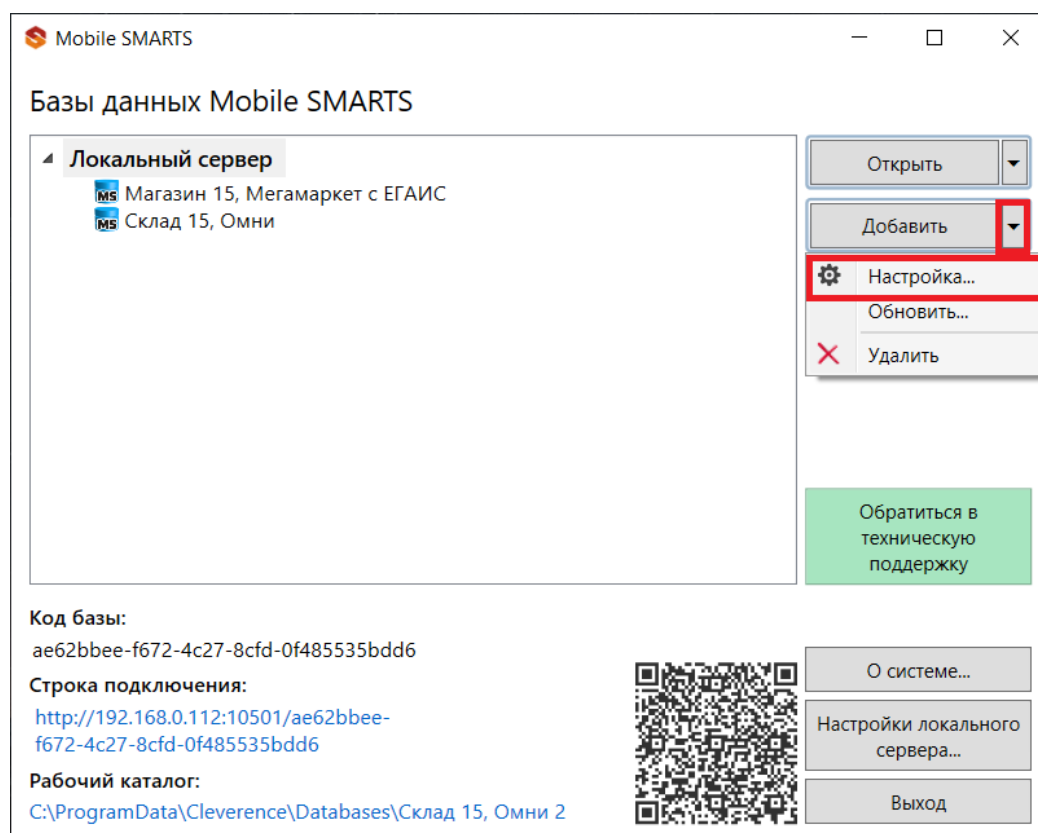
Аутентификация по пользователю в Mobile SMARTS

Последние изменения: 2024-03-26

Еще одна защитная мера, которая повышает безопасность работы — это аутентификация по пользователю.

Рекомендуется использовать аутентификацию по пользователю и закрытое соединение https совместно. Если не **включать использование https**, то трафик не шифруется и может быть перехвачен.

Аутентификацию по пользователю можно включить во время установки базы продукта на ПК или с помощью **менеджера баз** («Пуск» --> «Cleverence Soft» --> «Mobile SMARTS»). Для этого нажмите откройте меню кнопки «Добавить» и нажмите «Настройка».



Чтобы пользоваться аутентификацией, необходимо предварительно **создать пользователей в панели управления Mobile SMARTS** и назначить им определенные роли (оператор, администратор).

Редактирование настроек базы данных Mobile SMARTS

Код базы: 21e6d501-e8c1-44e0-b0cd-f30a369b1822

Наименование: Магазин 15 Вещевой, Расширенный

Папка: C:\ProgramData\Cleverence\Databases\Магазин 15 Вещевой, Расширенный

Комментарий:

Режим работы: Подключение к серверу

Основной режим работы Mobile SMARTS. Все мобильные устройства и сторонние системы работают через сервер.

Использовать https ☐ Сертификат...

Аутентификация по пользователю ☒

Порт сервера данных: 51824

Сервер печати используется ☒

Порт сервера печати: 51825

OK Отмена

Из соображений безопасности при создании пароля для администратора и других пользователей рекомендуем использовать сложный пароль (длина около 8 символов, прописные и строчные буквы, цифры).

Также во вкладке «Свойства» панели управления Mobile SMARTS установите для параметра «Вход по штрихкоду» значение «Нет». После этого при входе будет запрашиваться логин и пароль.

Конфигурация *

Магазин 15 Вещевой*

- Типы документов
- Операции
- Структура номенклатуры
- Общие вычисляемые поля
- Структура таблиц
- Серверные события и расширения
- Пользователи и группы
- Структура складов
- Штрихкоды контейнеров
- Оборудование
- Этикетки
- Данные
 - Документы
 - Номенклатура
 - Новые товары
 - Таблицы
 - БизнесПроцессы
 - Цены
 - ДисконтныеКарты
 - ЛовВажности

Свойства

. Главное	
Имя	Магазин 15 Вещевой
Версии компонентов	
Версия Android клиента от	3.3.0.24804
Версия CE\Mobile клиента от	3.3.0.24804
Версия редактора	2.7.1.0
Версия сервера	2.7.1.0
Интерфейс	
Использовать всплывающие сообщения	Нет
Отображать детальные сообщения об ошибках	Нет
Показывать количество серверных документов на кнопках	Нет
Текст выбора склада	
Контроль версий	
Автор	Клеверенс
Версия	31594
Машина автора	Клеверенс
Последнее обновление	06.05.2022 12:40
Прочее	
Возврат чужих документов при обмене	Нет
Вход по штрихкоду	Нет
запрашивать возврат документов при смене пользователя	Да
Комментарий	Типовая конфигурация Магазин 15 Вещевой
Пароль для выхода	*****

В режиме с включенной аутентификацией все компоненты системы будут требовать обязательного ввода логина и пароля. Все права пользователей, логины и пароли добавляются в панели управления Mobile SMARTS.



безопасность

Не нашли что искали?



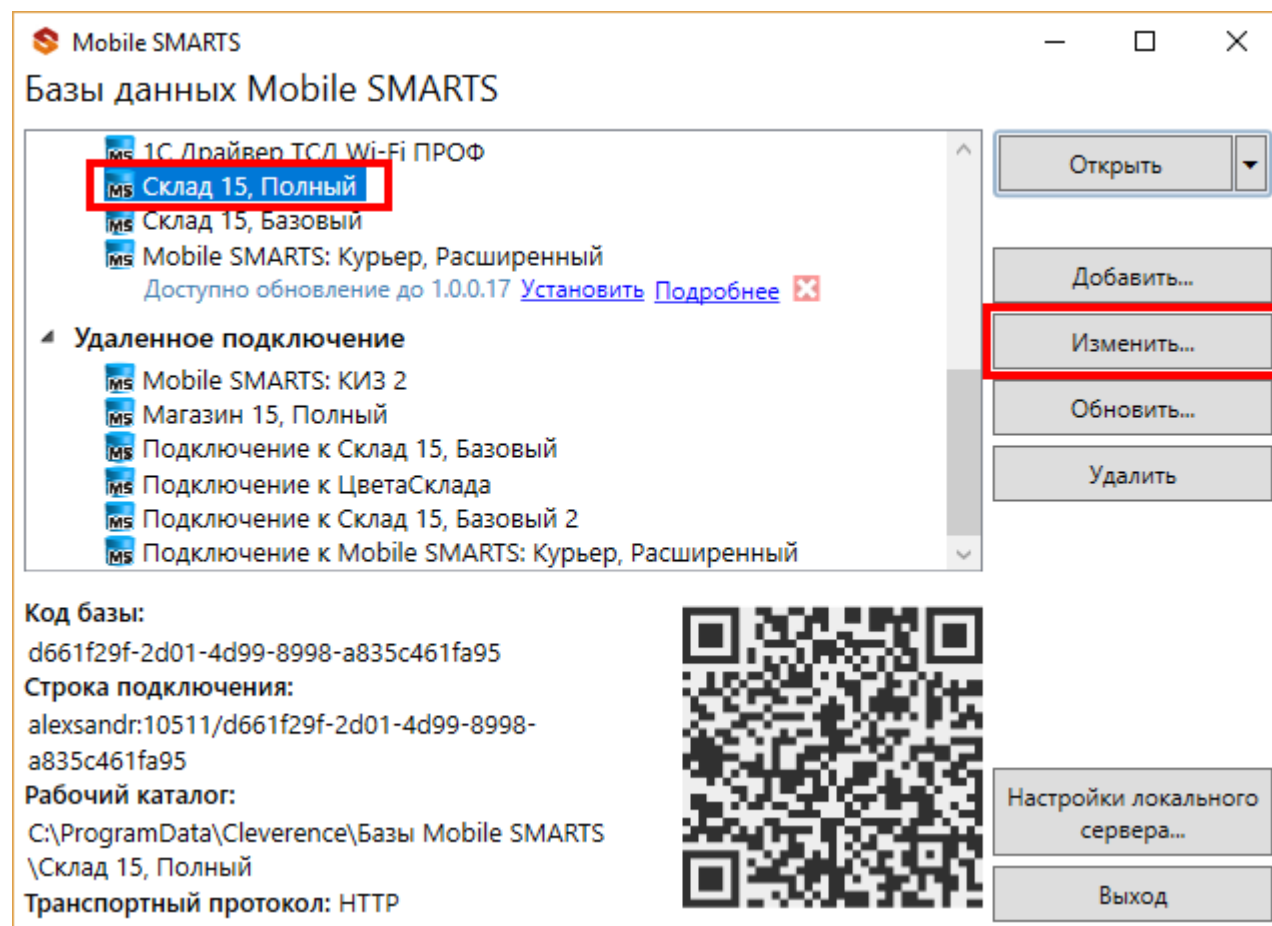
Задать вопрос в техническую поддержку

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 — □ ✕

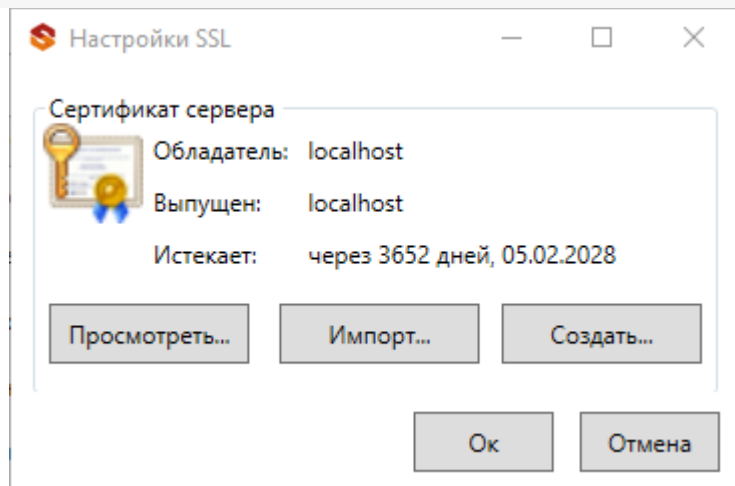
Сертификат сервера

 Обладатель:

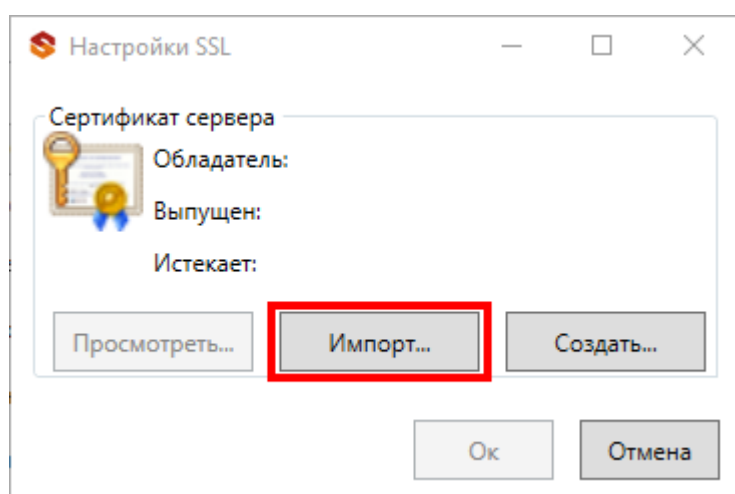
Выпущен:

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?

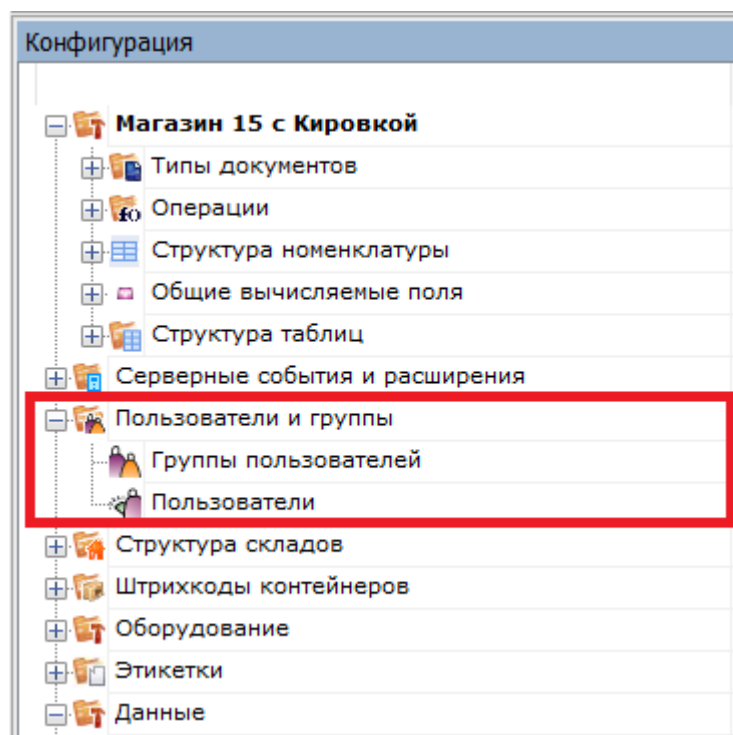


Задать вопрос в техническую поддержку

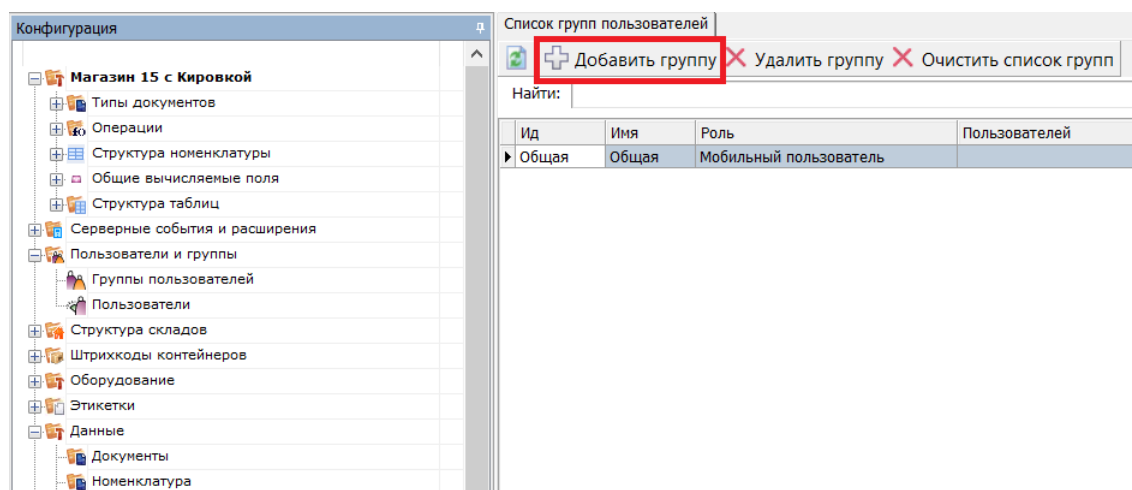
Заведение пользователей и групп пользователей в Mobile SMARTS

Последние изменения: 2024-03-26

Для работы в **режиме с включенной аутентификацией** необходимо завести пользователей, задать им логины и пароли. В панели управления Mobile SMARTS узел «Пользователи и группы» содержит данные о пользователях и группах, в которых они состоят.



Заведение групп пользователей



Группы определяют роль пользователей и список **типов документов**, доступных для обработки пользователям такой группы.

Группа пользователей: Новая *

Идентификатор:
1

Имя группы: **1**
Операторы ТСД

Автономная работа: ☐

Роль: Мобильный пользователь **2**

Автозапуск документа при старте:

Операция при входе пользователя: При начале работы пользователя

Операция при выходе пользователя: При завершении работы пользоват

Типы документов: **3**

☒ Возврат
☒ Инвентаризация
☒ МаркировкаОстатков
☒ Настройки
☒ Перемещение
☒ Переоценка
☒ ПодборЗаказа
☒ Поступление
☒ Продажа
☒ ПросмотрСправочников
☒ СборШК
☒ Списание

Сохранить Отмена

1. Имя группы может быть любым.
2. Обязательно нужно указать «Роль» (мобильный пользователь, внешнее подключение, администратор) в зависимости от прав, предоставляемых пользователям данной группы.
 - о обычная работа на ТСД («Мобильный пользователь»);
 - о обмен данными между учетной системой, сервером и ТСД («Внешнее подключение»);
 - о работа с конфигурацией («Администратор»).
3. При заведении новой группы отмечаем для неё те типы документов, которые будут доступны пользователям из этой группы. Если не отметить ни одного типа документа или в конфигурации нет еще ни одного типа документа, мы получим предупреждение об ошибке: «Группа пользователей должна иметь хотя бы одну операцию».

Заведение пользователей

Конфигурация

Магазин 15 с Кировкой

- Типы документов
- Операции
- Структура номенклатуры
- Общие вычисляемые поля
- Структура таблиц
- Серверные события и расширения
- Пользователи и группы
 - Группы пользователей
 - Пользователи**
- Структура складов
- Штрихкоды контейнеров
- Оборудование
- Этикетки
- Данные

Список групп пользователей | Список пользователей

Добавить пользователя ✕ Удалить пользователя ✕ Очистить список пользователей

Найти:

Ид	Имя	Группа	Роль	Описание
▶ оператор	оператор	Общая	Мобильный пользова...	

При заведении пользователя выберите группу, в которую вы хотите его добавить. Впишите имя пользователя, назначьте ему пароль и штрихкод, а также выберите склады, на которых он может работать.

Новый пользователь *

Идентификатор:
1

Имя пользователя:
Иванов

Пароль пользователя:

Штрихкод пользователя:

Имя группы:
Операторы ТСД

Описание:

Склады:

☒ Общий

Сохранить

Отмена

При аутентификации на ТСД Mobile SMARTS не спрашивает имени пользователя, а только его пароль. Соответственно, у каждого пользователя пароль должен быть уникальный и отсутствие пароля запрещено.



безопасность

Не нашли что искали?



Задать вопрос в техническую поддержку

Настройка блокировки доступа по IP встроенными средствами сервера Mobile SMARTS

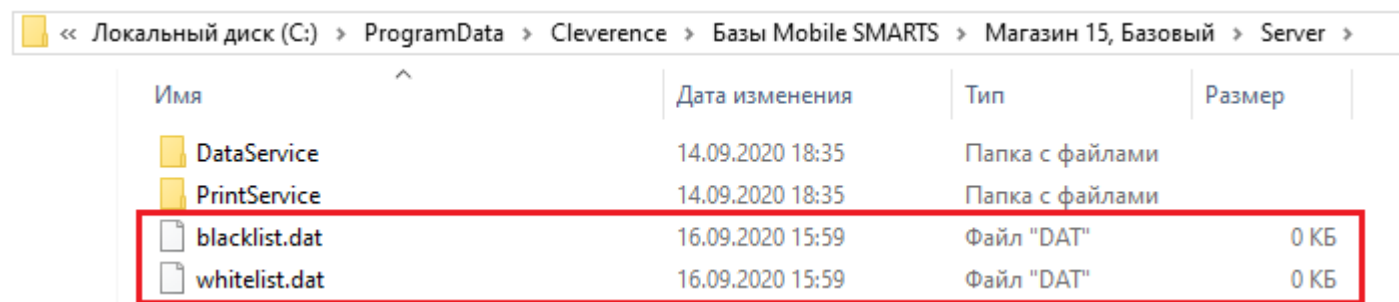
Последние изменения: 2024-03-26

Для защиты сервера Mobile SMARTS (особенно опубликованного в сети Интернет) от несанкционированного доступа клиентских мобильных устройств можно воспользоваться такой функцией платформы, как блокировка IP-адреса. Данная функция подразумевает создание списка IP-адресов устройств, которым будет запрещен доступ к открытому серверу.

Файлы со списками адресов создаются вами самостоятельно (например, с помощью программы «Блокнот») и должны иметь следующий вид:

- **blacklist.dat** — список запрещенных ip адресов;
- **whitelist.dat** — список разрешенных ip адресов.

Оба файла должны быть помещены в папку «Server» той базы, с которой вы работаете (путь к этой папке по умолчанию — «C:\ProgramData\Cleverence\Databases\Имя вашей базы\Server», может быть другим, в зависимости от того, куда вы поместили папку базы).

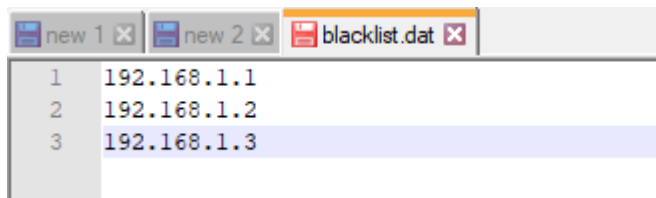


<< Локальный диск (C:) > ProgramData > Cleverence > Базы Mobile SMARTS > Магазин 15, Базовый > Server >				
Имя	Дата изменения	Тип	Размер	
DataService	14.09.2020 18:35	Папка с файлами		
PrintService	14.09.2020 18:35	Папка с файлами		
blacklist.dat	16.09.2020 15:59	Файл "DAT"	0 КБ	
whitelist.dat	16.09.2020 15:59	Файл "DAT"	0 КБ	

В итоге, при попытке мобильного устройства обратиться к серверу Mobile SMARTS, происходит проверка, не внесен ли текущий IP-адрес устройства в один из этих списков. «Whitelist.dat» имеет больший приоритет чем «blacklist.dat» — если IP-адрес найден в whitelist, то blacklist проверяться не будет.

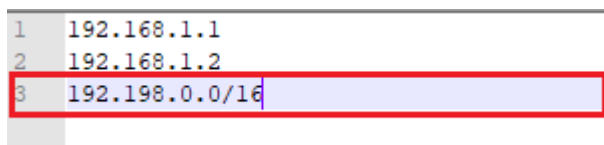
При создании обоих файлов можно использовать следующие правила записи IP-адресов для блокировки:

1. Если вы хотите, чтобы проверка происходила по конкретному адресу — записывайте в строку один IP-адрес (например, 192.168.1.1).



1	192.168.1.1
2	192.168.1.2
3	192.168.1.3

2. Если проверка требуется по битовой маске, формат записи будет следующим — 192.198.0.0/16 (в данном случае проверка затронет диапазон от 192.198.0.1 — 192.198.255.255).



1	192.168.1.1
2	192.168.1.2
3	192.198.0.0/16

3. Если нужна проверка по диапазону адресов, запись будет иметь следующий вид — 192.198.0.1-

192.198.0.100 (в данном случае проверяется вхождение в диапазон от 1 до 100).

1	192.168.1.1
2	192.168.1.2
3	192.198.0.1-192.198.0.100

Кроме того, добавление IP-адреса в whitelist.dat поможет избежать блокировки данного адреса из-за ввода неправильного пароля или ШК при авторизации пользователя на мобильном устройстве (с одного IP допускается 10 попыток в минуту).

Не нашли что искали?



Задать вопрос в техническую поддержку