## 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.

🔇 Редактирован	ие 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 ht	tps 🔽					
Порт сервера данных: 9706						
Сервер печати и	используется 🔲					
Порт сервера пе	ечати: 9707					
	ОК Отмен	а				

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.

🔚 certmgr - [Сертификаты — текущий пользователь\Доверенные корнев 💻 🗖 🔜						
Файл Действие Вид Справка						
🗊 Сертификаты — текущий пользователь	Кому выдан	Кем выдан 🔷				
р Личное	🔄 AddTrust External CA Root	AddTrust Exterr				
Доверенные корневые центры сертификации	🔄 Baltimore CyberTrust Root	Baltimore Cybe				
Сертификаты	🔄 Certum CA	Certum CA				
Доверительные отношения в предприятии	🔄 Certum Trusted Network CA	Certum Trustec				
Промежуточные центры сертификации Объект пользователя Active Directory	🔄 Class 3 Public Primary Certificat	Class 3 Public F				
COMODO RSA Certification Au COMODO R						
р Сертификаты к которым нет доверия Гарария Соругіді (c) 1997 Microsoft C Copyright (c) 1						
Сторонние корневые центры сертификации	🔄 DigiCert Assured ID Root CA	DigiCert Assure				
Доверенные лица	🔄 DigiCert Global Root CA	DigiCert Global				
Поставщики сертификатов проверки подлиннос	🔄 DigiCert High Assurance EV Ro	DigiCert High A				
MSIEHistoryJournal	🔄 DST Root CA X3	DST Root CA X:				
Запросы заявок на сертификат	🔄 Entrust Root Certification Auth	Entrust Root Ce				
Доверенные корневые сертификаты смарт-карт	🔄 Entrust Root Certification Auth	Entrust Root Ce				
SYSTEM	🔄 Equifax Secure Certificate Auth	Equifax Secure				
	🔄 GeoTrust Global CA	GeoTrust Globa 🗸				
< >>	<	>				
Хранилище Доверенные корневые центры сертификации содержит 43 с						

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.

лиоо осуществлять урм подключение между оазой и тод, лиоо получать доверенный сертификат.

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

CLEVERENCE.RU — 3/3

Сервер Mobile SMARTS	Имя базы данных: Mobile SMARTS: К	урьер, Расширенный
Maraзин 15, Полный УТ1	,	
🚾 Магазин 15, Полный Роза	Параметры сервера данны	5 <sup>°°</sup>
🚾 1С Драйвер ТСД Инвент	Anner:	https://it02:10560
🚾 Магазин 15, Расширенны	Статус:	Базовое соединение закрыто: Непредвиденная ошибка при передаче.
Mobile SMARTS: Курьер,	Порт сервера данных:	10560
🚾 1С Драйвер ТСД Wi-Fi П	N.	_
мя Мал	учетная запись:	ПИспользуется (общие параметры)
🚾 тсд миур		Имя пользователя: foo
🚾 Магазин 15, Базовый Ку:		Пароль:
🚾 Магазин 15, Базовый 17:	Сжимать справочники и таблицы:	🗆 Рекомендуется использовать только в условиях неустойчивой сети или
🐻 Магазин 15, Расширенны		экономии платного траффика, так как скорость распаковки сжатых данн большинстве мобильных устройств мала!
🐻 Магазин 15, Расширенны	Donati Garadi Jorganoutor:	
	делать оэкапы документов.	

#### Не нашли что искали?

0

# Генерация самоподписанного тестового сертификата для веб-сервера Mobile SMARTS

Последние изменения: 2024-03-26

Для получения самоподписанного тестового сертификата в системах Windows<sup>®</sup> 8 и Windows Server<sup>®</sup> 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.

Windows PowerShell	ISE	- 🗆 🗙
Файл Правка Вид Сервис Отладка Дополнительные компоненты	Справка	
1 🙆 🖬 🤾 🖞 🖬 🔪 🔊 (*) 🕨 🔳	Se 🗵	
	Сценарий	🛞 Команды 🗙
PS C:\Users\1>		Модули: Все У Обновить
		Murr .
		A: ^
		Add-AppxPackage
		Add-AppxProvisionedPackage
		Add-BCDataCacheExtension
		Add-BitLockerKeyProtector
		Add-BitsFile
		Add-CertificateEnrollmentPolicyServer
		Add-Computer
		Add-Content
		Add-DnsClientNrptRule
		Add-UtcCluster i MMapping
		Add-History
		Add Joh Trigger
		Add-Job Higger
		Add-Member
		Add-MoPreference
		Add-NetEventNetworkAdapter
		Add-NetEventPacketCaptureProvider
		Add-NetEventProvider V
<		Эапустить оставить Копировать
		Стр. 1 Столб. 16 100%

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

 ----- ----- 

 E41C0ADC4FD5 895 3F440C7FACE2097879D887C04
 CN=localhost

PS C:\Windows\system32>

🚡 certmgr - [(	ертификаты — текущий пользователь] 🛛 – 🗖 🗙						
Файл Действие Вид Справка							
🗊 Сертификаты — текуший пользователь 🗸	И						
📔 Личное Поиск сертификатов	100						
⊿ ☐ Доверен⊦ ☐ Серти Все задачи	<ul> <li>ренные корневые центры сертификации</li> </ul>						
⊳ ☐ Доверите Вид	рительные отношения в предприятии иежуточные центры сертификации						
Списс Обновить	кт пользователя Active Directory						
Серти Экспортировать список.							
<ul> <li>Объект п</li> <li>Доверенн</li> </ul>	ификаты, к которым нет доверия онние корневые центры сертификации						
Сертификаты, к которым нет доверия	🛗 Доверенные лица						
🕟 🚞 Сторонние корневые центры сертиф	📔 Поставщики сертификатов проверки подлинности клиентов						
Доверенные лица	MSIEHistoryJournal						
Поставщики сертификатов проверки	📔 Запросы заявок на сертификат						
MSIEHistoryJournal	🛄 Доверенные корневые сертификаты смарт-карты						
Запросы заявок на сертификат	SYSTEM						
Доверенные корневые сертификаты с	» 🧰 Доверенные корневые сертификаты с						
Искать сертификат в хранилище							

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».

🖀 certmgr - [Сертификаты — текущий пользователь\Промежуточные центры сертифик 🗕 🗖 💌							
Файл Действие Вид Справка							
🗢 🔿 📶 🔏 🖻 🔀 📴 🔂 🛛 🖬							
<ul> <li>Сертификаты — текущий пользователь</li> <li>Личное</li> <li>Доверенные корневые центры сертиф</li> <li>Сертификаты</li> </ul>	Кому выдан COMODO RSA Certification Au COMODO RSA Domain Validati	Кем выдан AddTrust External CA COMODO RSA Certif	A Root fication Auth	Срок д 30.05.20 12.02.20			
<ul> <li>Сертификаты</li> <li>Доверительные отношения в предпри</li> <li>Промежуточные центры сертификаци</li> <li>Список отзыва сертификатов</li> <li>Сертификаты</li> <li>Объект пользователя Active Directory</li> <li>Доверенные издатели</li> <li>Сертификаты, к которым нет доверия</li> <li>Сторонние корневые центры сертифи</li> <li>Доверенные лица</li> <li>Поставщики сертификатов проверки</li> <li>MSIEHistoryJournal</li> </ul>	Iocalhost       Image: Construction of the second sec	Открыть Все задачи ► Вырезать Копировать Удалить Свойства Справка	: Root icate Authori ority ic Primary Ce y Certificatio	30.05.2 19.12.2 19.10.2 31.12.2 01.01.2 31.10.2 25.10.2			
<ul> <li>Запросы заявок на сертификат</li> <li>Доверенные корневые сертификаты с</li> <li>Сустем</li> <li>Удаление выбранного объекта.</li> </ul>	٢	_		>			

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

🚡 certmgr - [Сертиф	оикаты — текущий пользова	ате	аль∖Доверенные корневые це	ентры се 🗕 🗖 💙	ĸ
Файл Действие Вид	Справка				
🗢 🔿 🖄 📰 📋	Q 🗟 🚺 🖬				
Сертификаты — текул Личное Доверенные корн Сертификаты Промежуточа Список от Сертифик Объект полз Объект полз Объект полз Объект полз Сертификаты Сертификаты Сертификаты Сертификаты Сертификаты Сертификаты Сертификаты Сертификаты Сертификаты Соверенные лица МSIEHistoryJourna Запросы заявок н	щий пользователь евые центры сертификации Все задачи Вид Вставить Обновить Экспортировать список Справка ификатов проверки подлинности а сертификат евые сертификат	* *	Кому выдан AddTrust External CA Root Baltimore CyberTrust Root Certum CA Certum Trusted Network CA Copyright (c) 1997 Microsoft C Copyright (c) 1997 Microsoft C DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert High Assurance EV Ro DST Root CA X3 Entrust Root Certification Auth Equifax Secure Certificate Auth GeoTrust Global CA	Кем выдан AddTrust External CA Root Baltimore CyberTrust Root Certum CA Certum Trusted Network CA Class 3 Public Primary Certif Copyright (c) 1997 Microsof DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert High Assurance EV DST Root CA X3 Entrust Root Certification At Entrust Root Certification At Equifax Secure Certificate At GeoTrust Global CA	
	>	*		Second services and second services and second services and second	<b>`</b> ~
Вставка в выбранный объ	ект				

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

- Как создать самоподписанный сертификат в Windows
- Выпуск собственного SSL-сертификата

#### Не нашли что искали?



# 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).

Редактирова	ние 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 режил через сервер.	л работы Mobile SMARTS. Все мобильные устройства и сторонние системы работают					
Использовать ht	ttps 🗌 Сертификат					
Аутентификация	а по пользователю 🔽					
Порт сервера да	анных: 51824					
Сервер печати и	используется 🔽					
Порт сервера печати: 51825						
	ОК 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 *	<b>ņ</b>	Свойства	
	^	2↓ □	
🖃 🛐 Магазин 15 Вещевой*		У Главное	
🕀 🌆 Типы документов		Имя	Магазин 15 Вещевой
🕀 🌠 Операции		У Версии компонентов	
Приктура номенклатуры		Версия Android клиента от	3.3.0.24804
Общие вычисляемые поля		Версия CE\Mobile клиента от	3.3.0.24804
🕂 🌠 Структура таблиц		Версия редактора	2.7.1.0
Серверные события и расширения		Версия сервера	2.7.1.0
		Интерфейс	
на пользователи и группы		Использовать всплывающие сообщения	Нет
🕀 🎆 Структура складов		Отображать детальные сообщения об ошибках	Нет
🕂 🙀 Штрихкоды контейнеров		Показывать количество серверных документов на кнопках	Нет
🕂 🛐 Оборудование		Текст выбора склада	
Этикетки		<ul> <li>Контроль версий</li> </ul>	
		Автор	Клеверенс
_ т данные		Версия	31594
🌆 Документы		Машина автора	Клеверенс
🎬 Номенклатура		Последнее обновление	06.05.2022 12:40
		У Прочее	
🖃 🛅 Таблицы		Возврат чужих документов при обмене	Нет
БизнесПроцессы		Вход по штрихкоду	Нет 🗸 🗸
Пены		Запрашивать возврат документов при смене пользователя	Да
		Комментарий	Типовая конфигурация Магазин 15 Вещевой
дисконтныетарты		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.



## Не нашли что искали?



# 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.

S Mobile SMARTS	– 🗆 🗙
Базы данных Mobile SMARTS	
мя 1С. Драйвер ТСЛ. Wi-Fi ПРОФ ^ мя Склад 15, Полный мя Склад 15, Базовый	Открыть 🔻
Mobile SMARTS: Курьер, Расширенный Доступно обновление до 1.0.0.17 <u>Установить</u> <u>Подробнее</u>	Добавить
<ul> <li>Удаленное подключение</li> </ul>	Изменить
мя Mobile SMARTS: КИЗ 2 мя Магазин 15, Полный мя Подключение к Склад 15, Базовый	Обновить
мя Подключение к ЦветаСклада мя Подключение к Склад 15, Базовый 2 мя Подключение к Mobile SMARTS: Курьер, Расширенный	Удалить
Код базы: d661f29f-2d01-4d99-8998-a835c461fa95 Строка подключения: alexsandr:10511/d661f29f-2d01-4d99-8998- a835c461fa95 Рабочий каталог: C:\ProgramData\Cleverence\Базы Mobile SMARTS	Настройки локального сервера
\Склад 15, Полный Транспортный протокол: НТТР	Выход

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

💲 Редактирова	ние настроек базы данных Mobile SMARTS	×
Наименование:	Склад 15, Полный	
Папка:	C:\ProgramData\Cleverence\Базы Mobile SMARTS\Склад 15, Полный	
Комментарий:		
Режим работы:	Подключение к серверу 🗸	
Основной режи	и работы Mobile SMARTS. Все ТСД и сторонние системы работают через сервер.	
Использовать h	ttps 🔽 Сертификат	
Аутентификация	а по пользователю	
Порт сервера да	анных: 9708	
Сервер печати и	используется	
Порт сервера п	ечати: 9709	
	ОК Отмен	a

Сертификат можно установить, только от имени Администратора.

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

💲 Настройки SS	L		-	_		$\times$
Сертификат сер Обла, Выпул Истек	овера цатель: цен: ает:					
Просмотреть	И	мпорт		С	оздать.	
			Ок		Отм	іена

Созданный самоподписанный тестовый сертификат установится автоматически.

💲 Настро	ойки SSL		_		$\times$
Сертифи	кат сервера Обладатель: Выпущен: Истекает:	localhost localhost через 3652 дне	й, 05.02	2.2028	
Просм	отреть	Импорт	Ок	Создать Отм	ена

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"



#### Не нашли что искали?



# 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.

Конфигурация				
🖃 🍯 Магазин 15 с Кировкой				
🕀 🛅 Типы документов				
🕀 🌠 Операции				
🕀 🧮 Структура номенклатуры				
🕀 🖬 Общие вычисляемые поля				
🕀 🎬 Структура таблиц				
🗄 📆 Серверные события и расширения				
🕂 🙀 Пользователи и группы				
и Пользователи				
🕀 🙀 Структура складов				
🕀 🎁 Штрихкоды контейнеров				
🕀 🛐 Оборудование				
🕂 👘 Этикетки				
🚔 🛐 Данные				

## Заведение групп пользователей



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

🌄 Группа пользователей: Новая \*

Х

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.
  - обычная работа на ТСД («Мобильный пользователь»);
  - обмен данными между учетной системой, сервером и ТСД («Внешнее подключение»);
  - 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		пользователей Список поль	зователей		
🖃 🛐 Магазин 15 с Кировкой	^ 📓 🔂 До	бавить пользователя 🗙	Удалить пользовате	еля 🗙 Очистить спис	ок пользователей
💼 🌇 Типы документов	Наити:				
🕀 🌠 Операции	Ид	Имя	Группа	Роль	Описание
🕀 🧮 Структура номенклатуры	• оператор	оператор	Общая	Мобильный пол	ьзова
庄 🖬 Общие вычисляемые поля					
🕀 🌠 Структура таблиц					
🕀 🎆 Серверные события и расширения					
🚔 🌠 Пользователи и группы					
- 🎋 Группы пользователей					
🛉 Пользователи					
🕀 🌠 Структура складов					
🕀 🔯 Штрихкоды контейнеров					
🗄 🛐 Оборудование					
🕀 🜇 Этикетки					
🖃 🛐 Данные					

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.

CLEVERENCE.RU — 3/3

Идентификатор:	Имя пользователя:				
1	Иванов	Иванов			
Пароль пользователя:		Штрихкод пользовател	я:		
***		***			
Имя группы:					
Операторы ТСД	2	e			
Описание:					
Склады:					
<b>У</b> Общий					

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

### Не нашли что искали?

	-	×
C	2	
	2	2

## Изменение типовых портов в настройках сервера Mobile SMARTS

Последние изменения: 2024-03-

## Как изменить порт сервера Mobile SMARTS

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

S Mobile SMARTS		_		×
Базы данных Mobile SMARTS				
<ul> <li>Локальный сервер</li> </ul>		Откры	ыть	-
мы Магазин 15, Полный мы Склад 15, Полный с МОТП мы Склад 15, Полный мы Магазин 15, Полный 2 мы Магазин 15, Полный с Кировкой мы Магазин 15, Полный с Кировкой 2		Добави	1ТЬ	•
		Обрат технич подде	иться в нескую ержку	
Код базы:				
d9ad30f0-32b8-41fe-8d6e-a6a6ca4ca0dc		0		
Строка подключения:		Осис	теме	
http://алеся-пк:10501/d9ad30f0-32b8-41fe-8d6e- абабса4са0dc		Настройки серв	локальн ера	юго
Рабочий каталог:	10 C C C C C C C C C C C C C C C C C C C			
C\ProgramData\Cleverence\Eazu Mobile SMARTS\Marazu	The ALCHO	Вы	ход	

C:\ProgramData\Cleverence\Базы Mobile SMARTS\Maraзи...

- 2. В открывшемся окне нажмите кнопку «Остановить службу».
- 3. Измените порт сервера Mobile SMARTS.

Mobile SMARTS	Состояние Aдрес: <u>http://localhost:10501/</u>
✓ Сервер Mobile SMARTS	Состояние: служба запущена Открыть файл лога
Магазин 15, Полный	Запустить службу Перезапустить службу Остановить службу Диагностика и исправление проблем
Склад 15, Полный с МОТП	
Склад 15, Полный	Настройки Отменить изменения
Магазин 15, Полный 2	Отображаемое имя при подключении: Cepвер Mobile SMARTS
Магазин 15, Полный с Кировкой	Порт:
Магазин 15, Полный с Кировко	Внешний адрес для QR кода:

- 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».



- C:\ProgramData\Cleverence\Базы Mobile SMARTS\Maraзи...
- 4. Измените порт базы данных Mobile SMARTS. Нажмите кнопку «Ок».

Редактирова	ние настроек базы данных Mobile SMARTS X
Код базы:	d9ad30f0-32b8-41fe-8d6e-a6a6ca4ca0dc
Наименование:	Магазин 15, Полный
Папка:	C:\ProgramData\Cleverence\Базы Mobile SMARTS\Магазин 15, Полный
Комментарий:	
Режим работы:	Подключение к серверу 🗸
Основной режи	и работы Mobile SMARTS. Все ТСД и сторонние системы работают через сервер.
Использовать h	ttps 🗌 Сертификат
Аутентификация	я по пользователю
Порт сервера да	анных: 18690
Сервер печати і	используется
Порт сервера п	ечати: 18691
	ОК Отмена

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



#### Не нашли что искали?



# 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 ір адресов;
- whitelist.dat список разрешенных ір 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 ІР-адресов для блокировки:

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



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).



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).



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?

