Безопасность базы Mobille SMARTS при работе с «1С:Фреш»

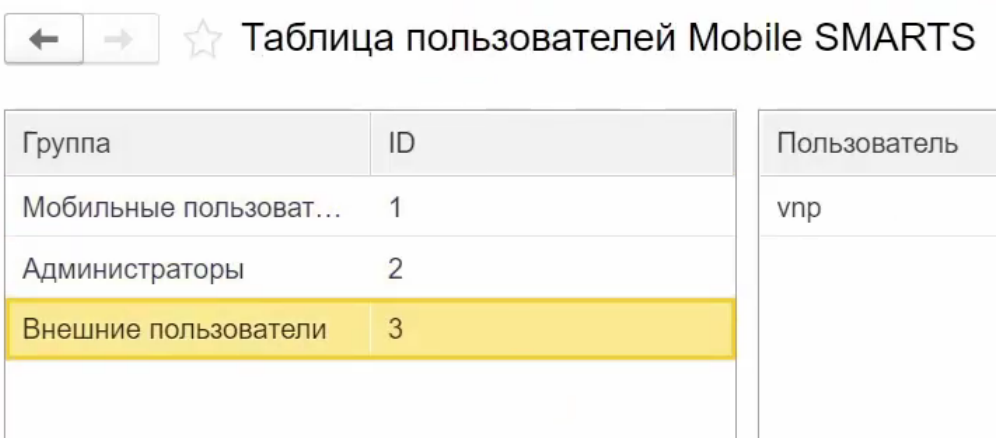
Последние изменения: 2024-03-26

Т.к. «1С:Фреш» находится в сети Интернет и имеет связь с сервером Mobile SMARTS на вашем ПК, то важным моментом становится безопасность передаваемых данных и самого сервера Mobile SMARTS. Для того чтобы обеспечить безопасность данных, сервера и вашего ПК, «Клеверенс» предлагает:

- использовать протокол https для шифрования передаваемых данных;
- поменять стандартные порты сервера и баз Mobile SMARTS на уникальные;
- включить авторизацию в базе по логину и паролю пользователя.

Как включить авторизацию по пользователю

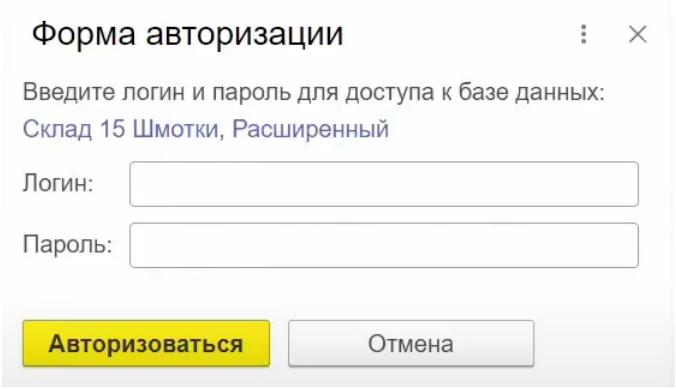
1. В обработке 1С создайте пользователей с разными правами:



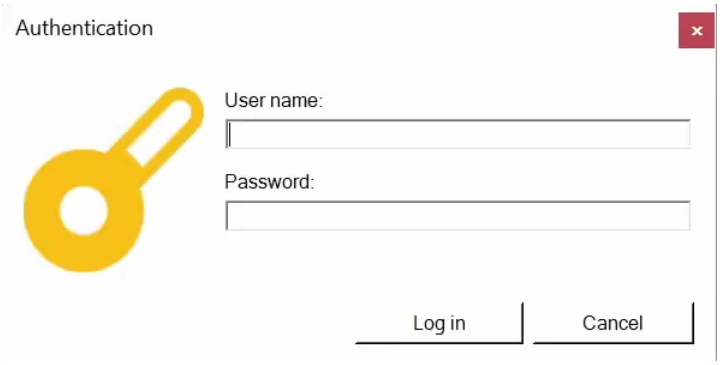
   - пользователь группы «**Администраторы**» может подключаться к Mobile SMARTS из внешней учетной системы («1С:Фреш»), с мобильного устройства, а также вносить правки в конфигурацию базы Mobile SMARTS.
   - пользователь группы «**Внешние пользователи**» могут подключаться к Mobile SMARTS из «1С:Фреш».

2. После этого включите доступ по https и аутентификацию по пользователю для базы Mobile SMARTS. Перезапустите сервер Mobile SMARTS.

3. При попытке открыть обработку «Клеверенса» в «1С:Фреш» будет появляться окно авторизации, где потребуется ввести данные пользователя.



4. **Пользователь с правами администратора также должен проходить авторизацию при попытке открыть панель управления Mobile SMARTS (всем остальным пользователям это запрещено).**



Не нашли что искали?

Задать вопрос в техническую поддержку