Руководство по установке плагинов биометрии.

Установку биометрии необходимо производить по порядку, от 1го пункта, до 5го. 6й пункт необходимо выполнить, если вы используете сетевой контроллер

Лицензии

Для работы продукта необходимы лицензии:

- Если используется стетевые сканеры(которые работают не от usb), то необходима лицензия APIServer, если нет, то она не нужна
- Если необходима saas лицензия, то нужна лицензия APIPayment(до 10 устройств в рамках одного RMS), если lifetime, то APIFront(Для каждого устройства)

1. Установка сервера

Все операции в данном разделе производятся на сервере где находится iiko.

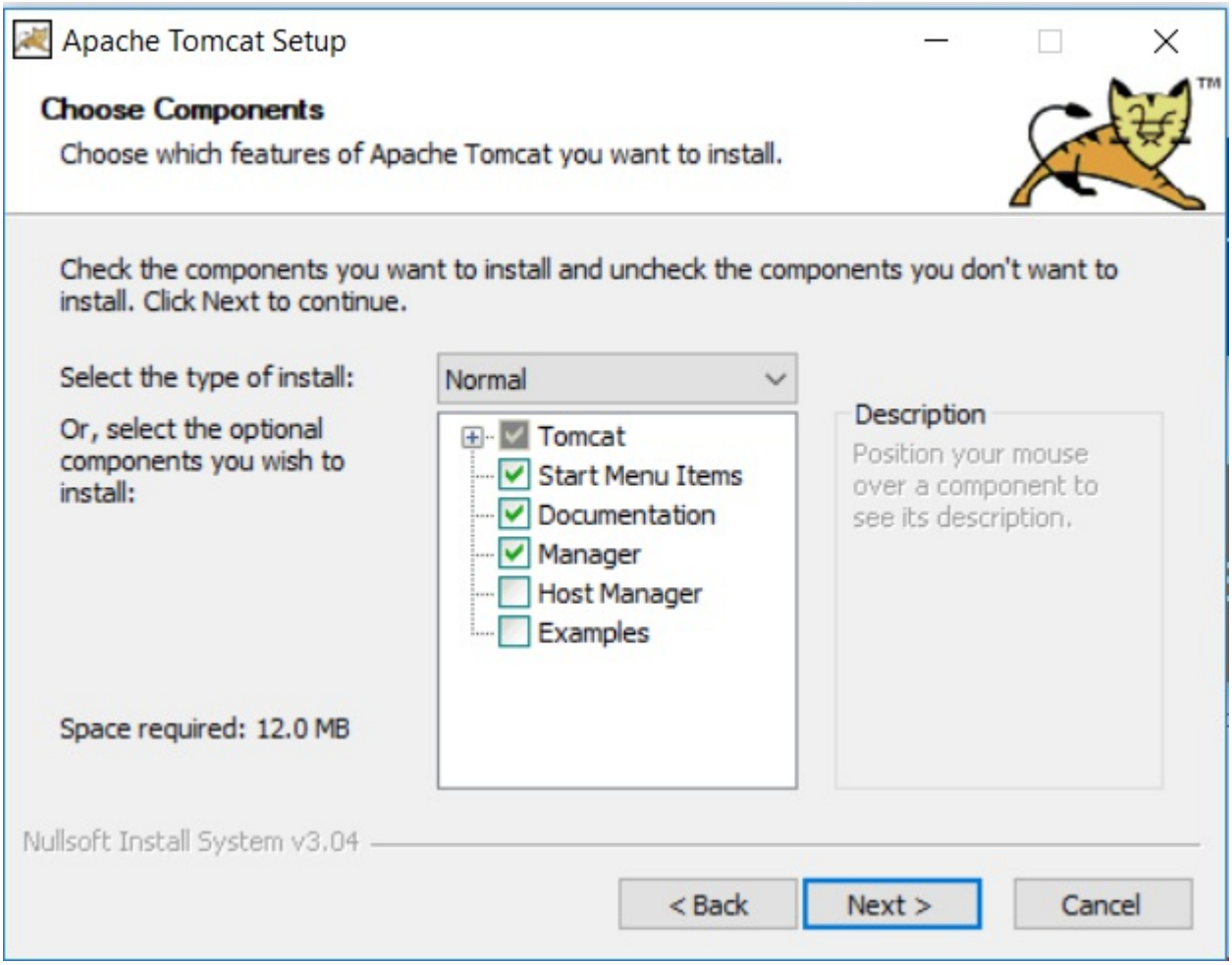
Внимание! Если клиент **iiko CLOUD** то все операции проводим на собственном хостинге.

Для CLOUD обязателен выбор H2 базы. Во всех остальных случаях, предпочтительной базой является mssql, так как iiko работает на ней,
это обеспечивает безопасность и целостность данных. Однако, при выборе базы H2 плагин также будет корректно функционировать.

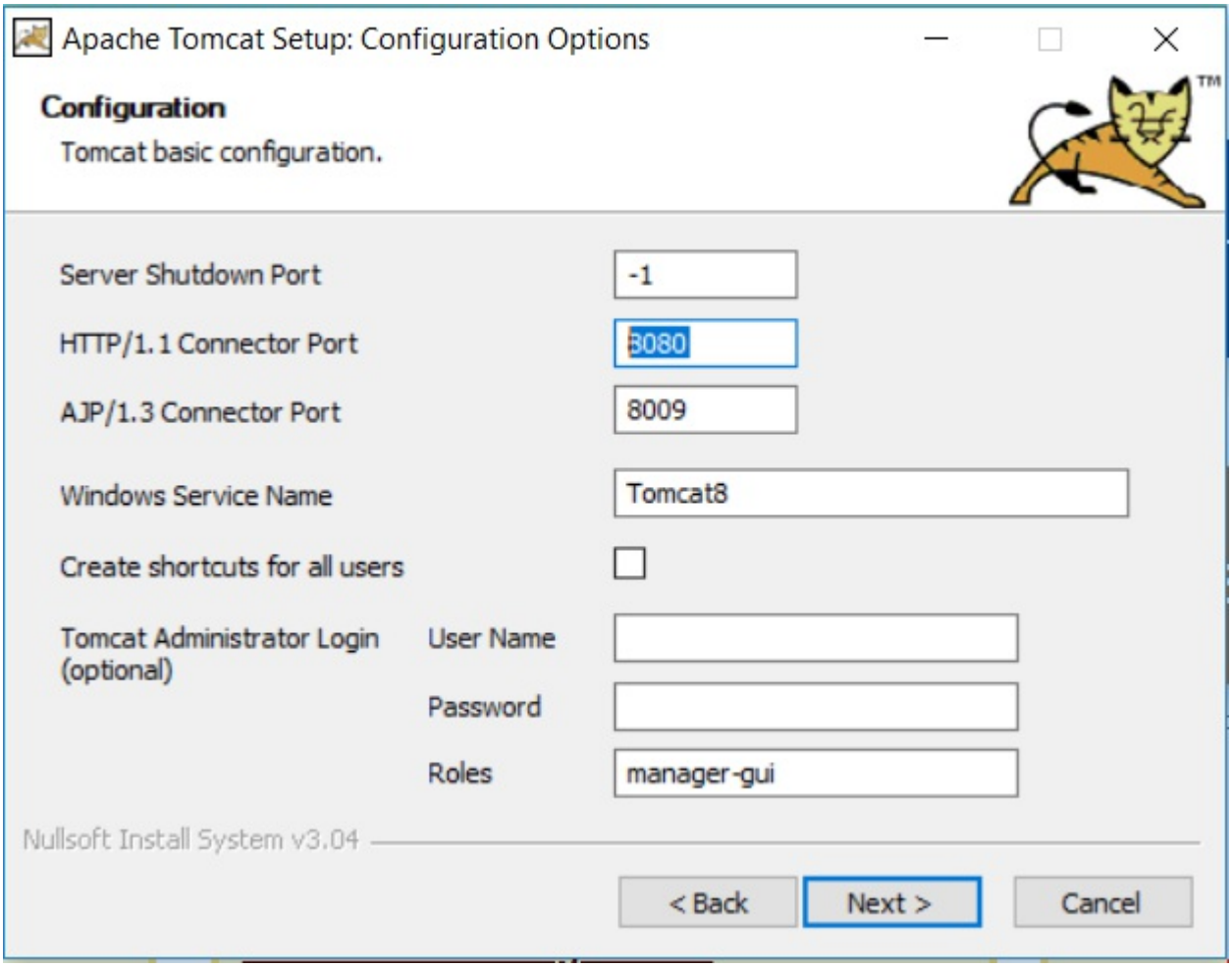
Если на компьютере **нет папки iiko\iikoRMS\Server**, то можно установить чистый tomcat(он будет выполнять функцию сервера, в Server он *уже* есть).

Установка TOMCAT

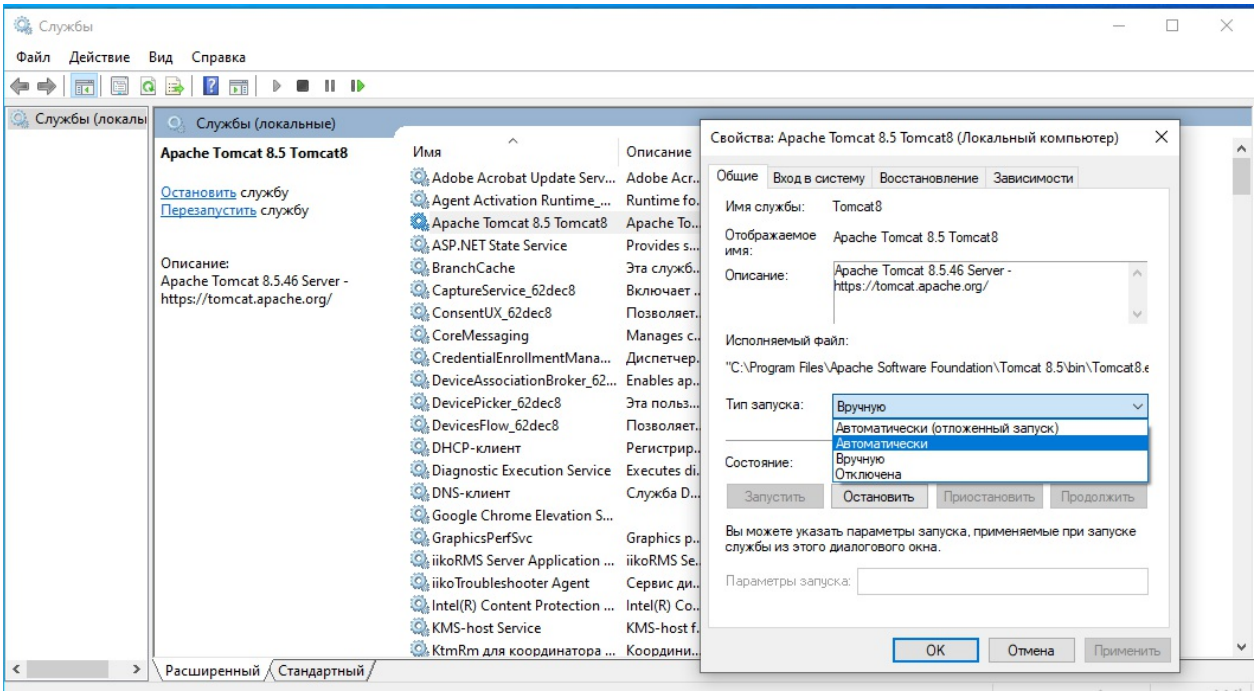
- Для начала, нужно установить Java Runtime Environment из папки Server/tomcat_and_jre_setup, там лежат инсталляторы для 64х и 32х битной архитектуры
- Далее необходимол установить Apache Tomcat из папки Server/tomcat_and_jre_setup
  При установке необходимо выбрыть тип Normal. Рекомендуется дать службе однозначное имя, чтобы потом было проще ее искать.



- Когда откроется такое же окно, как на скриншоте ниже, в выделенном поле необходимо указать *СВОБОДНЫЙ* порт для tomcat (по умолчанию 8080)

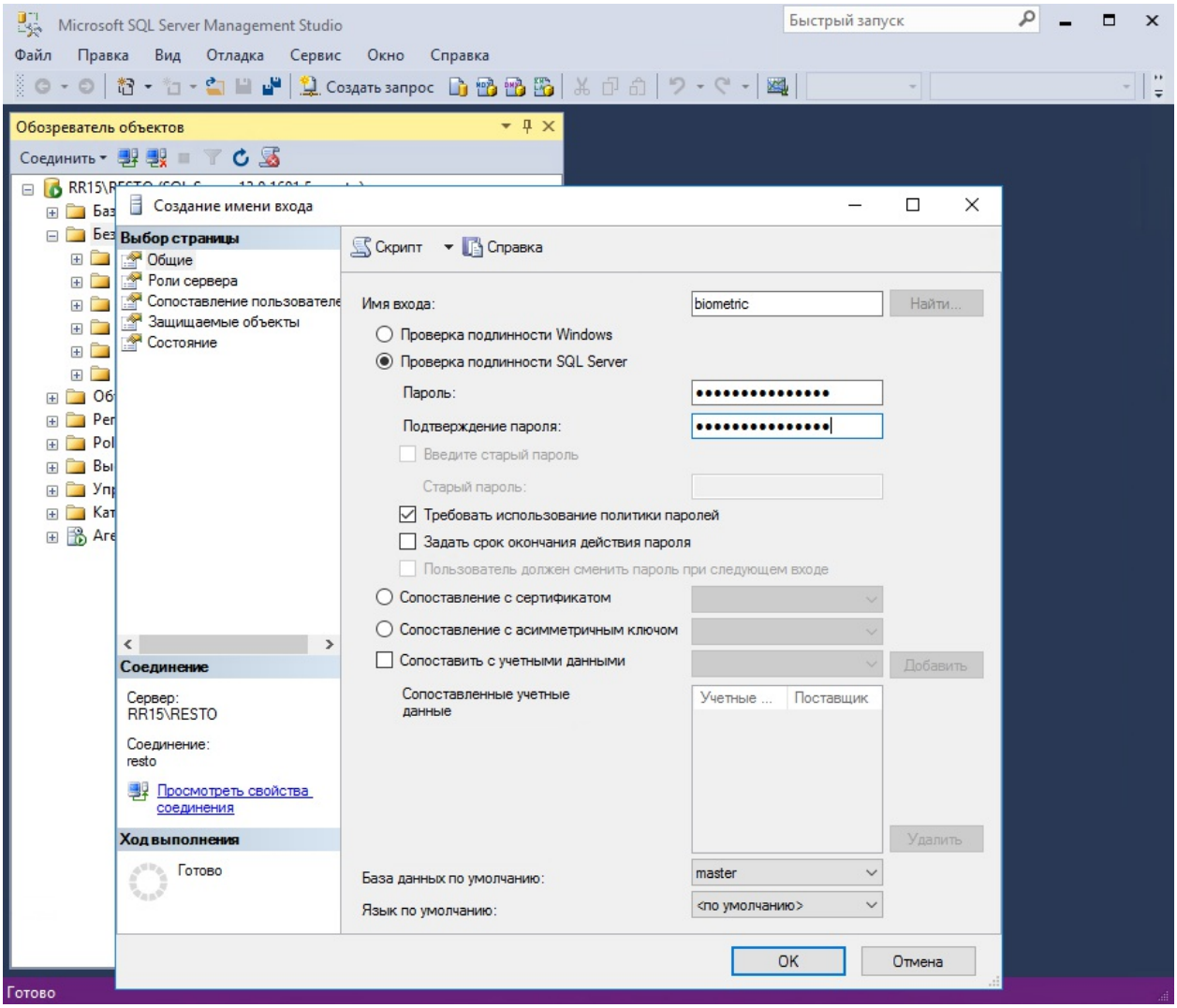


После завершения установки tomcat, необходимо перевести службу в автозагрузку:

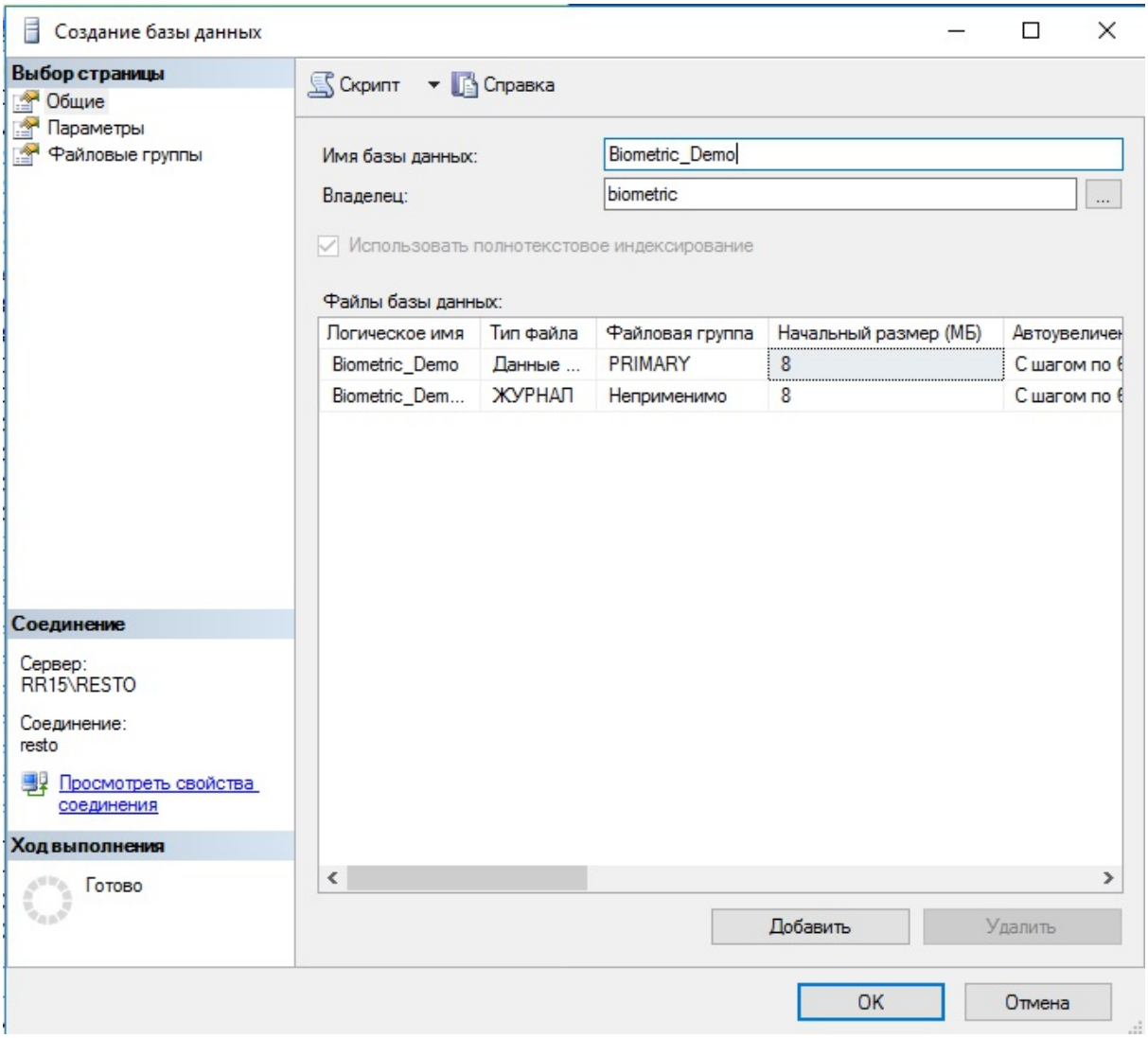


MSSQL База данных

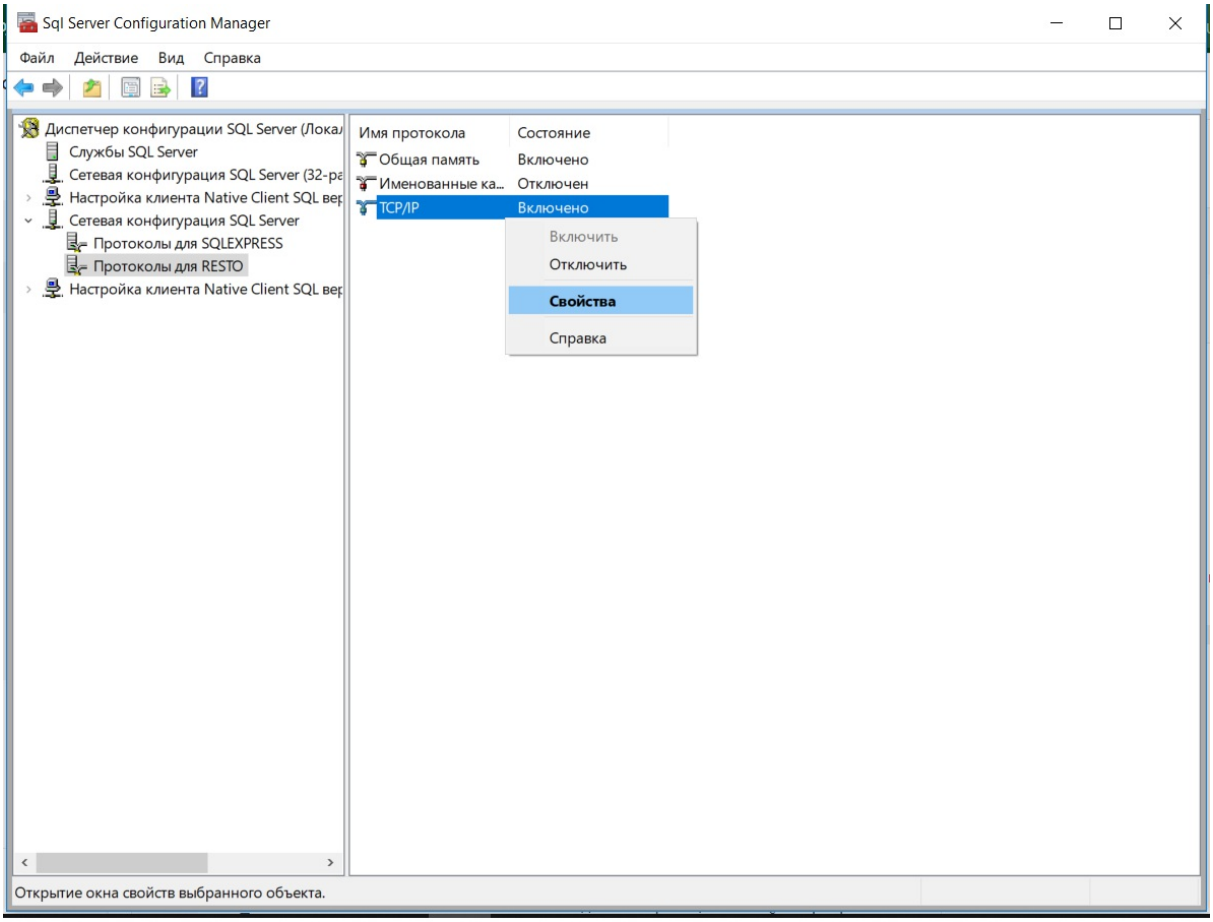
- Необходимо создать пользователя для базы данных и дать ему все полномочия (вкладка "Роли сервера") (Пример: BeOpenBiometricUser_"название ресторана")



- Необходимо создать базу данных (Пример: BeOpenBiometricServer_"название ресторана") и назначить созданного пользователя владельцем этой базы



- Необходимо открыть SQL Server Configuration Manager, развернуть вкладку "Сетевая конфигурация SQL Server", нажать на вкладку "Протоколы" для вашего сервера.
  Протокол TCP/IP необходимо перевести в состояние Enabled.



Далее, необходимо открыть "Свойства", перейти на вкладку "ip-адреса", и, для каждого ip(ip1…ip10,ipall) в поле TCP-port ввести "1433"

- Заходим в папку "Biometric\Server\tomcat", если вы *НЕ устанавливали* TOMCAT, копируем ее содержимое в папку "C:\Program Files\iiko\Server\Tomcat 7\webapps", если вы *устанавливали* TOMCAT "C:\Program Files\Apache Software Foundation\Tomcat 8.5\webapps"

- Далее необходимо зайти в папку webapps\fingers\WEB-INF\classes открыть файл application.properties и отредактировать его

```
Если у БД дефолтный инстанс : раскоментировать(убрать "#" перед строкой) конфиг для дефолтного инстанса
Если у БД не дефолтный инстанс : раскоментировать(убрать "#" перед строкой) конфиг для не дефолтного инстанса

SERVER_IP - ip сервера SQL;
DATABASE_NAME - заменяем на имя базы данных (то, которе задали при создании)
USERNAME – заменяем на имя пользователя для авторизации на SQL сервере (то, которе задали при создании)
PASSWORD – заменяем на пароль указанного пользователя
TOKEN - токен для доступа к серверу биометрии. Не менять.

Подробнее про формирование jdbc строки подкючения можно прочитать тут:
https://docs.microsoft.com/ru-ru/sql/connect/jdbc/building-the-connection-url?view=sql-server-2017
```

После любых изменение файла application.properties необходимо перезагрузить tomcat

Чтобы проверить, что база успешно запустилась, можно в браузере в строку url написать "http://адрес:порт_tomcat/fingers/user/all" если сервер не вернул ошибку 404, то все хорошо

H2 База данных

- Заходим в папку "Biometric\Server\tomcat", если вы *НЕ устанавливали* TOMCAT, копируем ее содержимое в папку

"C:\Program Files\iiko\Server\Tomcat 7\webapps", если вы *устанавливали* TOMCAT "C:\Program Files\Apache Software Foundation\Tomcat 8.5\webapps"

- Далее необходимо зайти в папку webapps\fingers\WEB-INF\classes открыть файл application.properties и отредактировать его

```
Нужно раскоментировать конфиг для H2(убрать "#" перед строкой)

DATABASE_PATH - заменяем на путь до базы данных (К примеру "C:\\test", на диске C:\\ будет создан файл базы данных "test")
TOKEN - токен для доступа к серверу биометрии. Не менять.
```

После любых изменение файла application.properties необходимо перезагрузить tomcat.

Чтобы проверить, что база успешно запустилась, можно в браузере в строку url написать "http://адрес:порт_tomcat/fingers/user/all" если сервер не вернул ошибку 404, то все хорошо

2. Установка драйверов для контроллеров

Если вы не испульзуете механизм авторизации с iikoOffice с помощью биомерии:
Драйвер необходимо установить на все компьютеры которые будут общаться с контроллерами (т.е и на фронтовые терминалы и на компьютер с бэком)
В архиве **Drivers** лежат две папки и установщик, тут очень важно делать все в описанном порядке!

- Распаковываем папку **ThirdParty** заходим в ThirdParty\64bit, если у вас 64х рахрядная система, или в ThirdParty\32bit, если у вас 32х разрядная система. Запускаем от имени Администратора, соответственно, **Register_SDK_x64.bat** или **Register_SDK_x86**. Дожидаемся регистрации всех dll
- Устанавливаем драйвер **ZKOnline** (тоже от имени Администратора)
  Если вы испульзуете механизм авторизации с iikoOffice с помощью биомерии:
- На фронтовые терминалы устанавливаем драйвера так, как описано выше;
- На компьютер с iiko office, если у вас 64х разрядная система устанавливаем драйвера из папки ThirdPartyForAuthInBack\1(Register_SDK_x86.bat от админа), затем из папки ThirdPartyForAuthInBack\2(Register_SDK_x64.bat от админа), если у вас 32х разрядная система, то устанавливаем драйвера из папки ThirdPartyForAuthInBack\32bit(Register_SDK_x86.bat от админа)
- Устанавливаем драйвер **ZKOnline** (тоже от имени Администратора)

3. Установка плагина для iiko Office

- В папке Biometric\Back\BeOpen.iiko.Back.Biometric есть папка **Office**, копируем файлы из нее в папку `"C:\Program Files\iiko\iikoRMS\Office"`
- В папке Biometric\Back\BeOpen.iiko.Back.Biometric есть папка **Plugins**, копируем файлы из нее в папку `"C:\Program Files\iiko\iikoRMS\Office\Plugins"`

Если вы хотите использовать систему авторизации в iiko office с помощью отпечатка:

- В папку C:\Program Files\iiko\iikoRMS\Office необходимо копировать файл CorFlag.exe из папки ForRunningOfficeAs32bit
- Запустить командную строку от админа, переместиться в папку C:\Program Files\iiko\iikoRMS\Office и прописать команду Corflags.exe /32bit+ BackOffice.exe

4. Установка плагинов для iiko Front

BeOpen.iiko.Front.Biometric

- Копируем папку с плагином в `"C:\Program Files\iiko\iikoRMS\Front.Net\Plugins"`

BeOpen.Front.Plugins.AgentExtensionsContext

- Копируем папку с **AgentExtensionsContext** в папку `"C:\Program Files\iiko\iikoRMS\Front.Net\Plugins"`

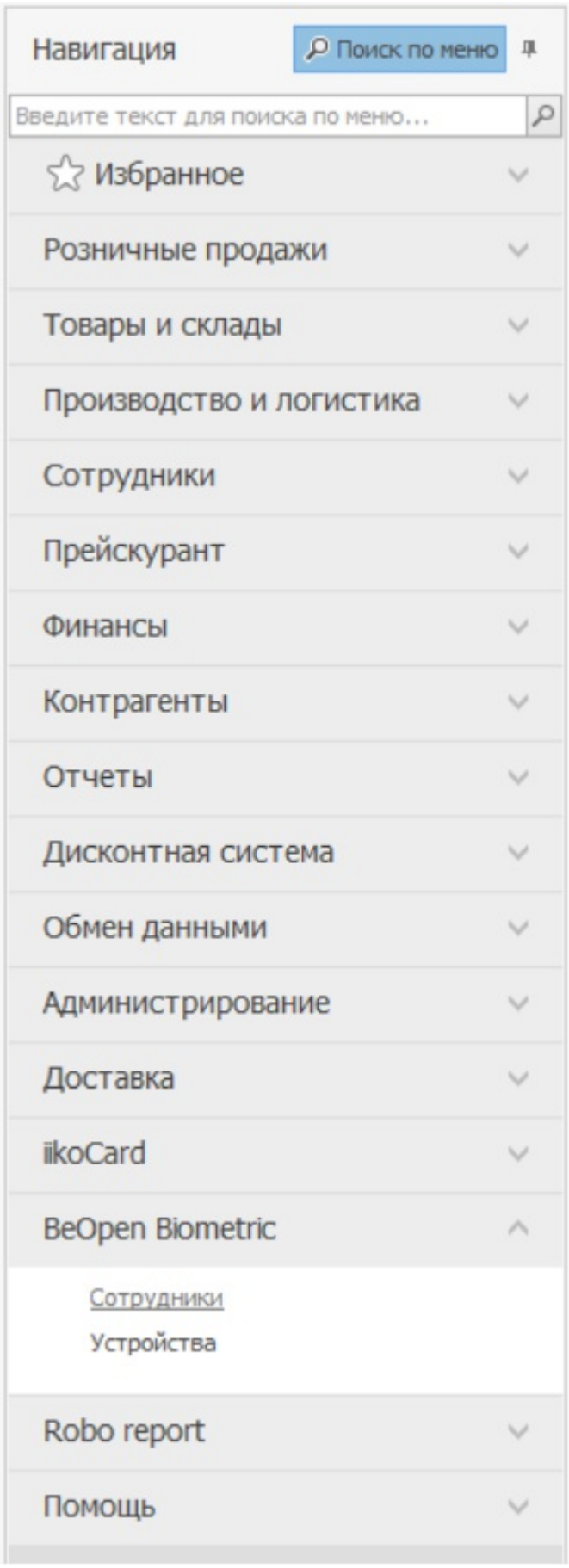
- Конфигурируем плагин. Для этого заходим в папку с плагином и открываем файл **«BeOpen.Front.Plugins.AgentExtensionsContext.dll.config»** :

```
<userSettings>
    <BeOpen.Front.Plugins.AgentExtensionsContext.Properties.Settings>
        <setting name="PipeName" serializeAs="String">
            <value>BeOpenAgentExtensions</value>
        </setting>
    </BeOpen.Front.Plugins.AgentExtensionsContext.Properties.Settings>
</userSettings>
```

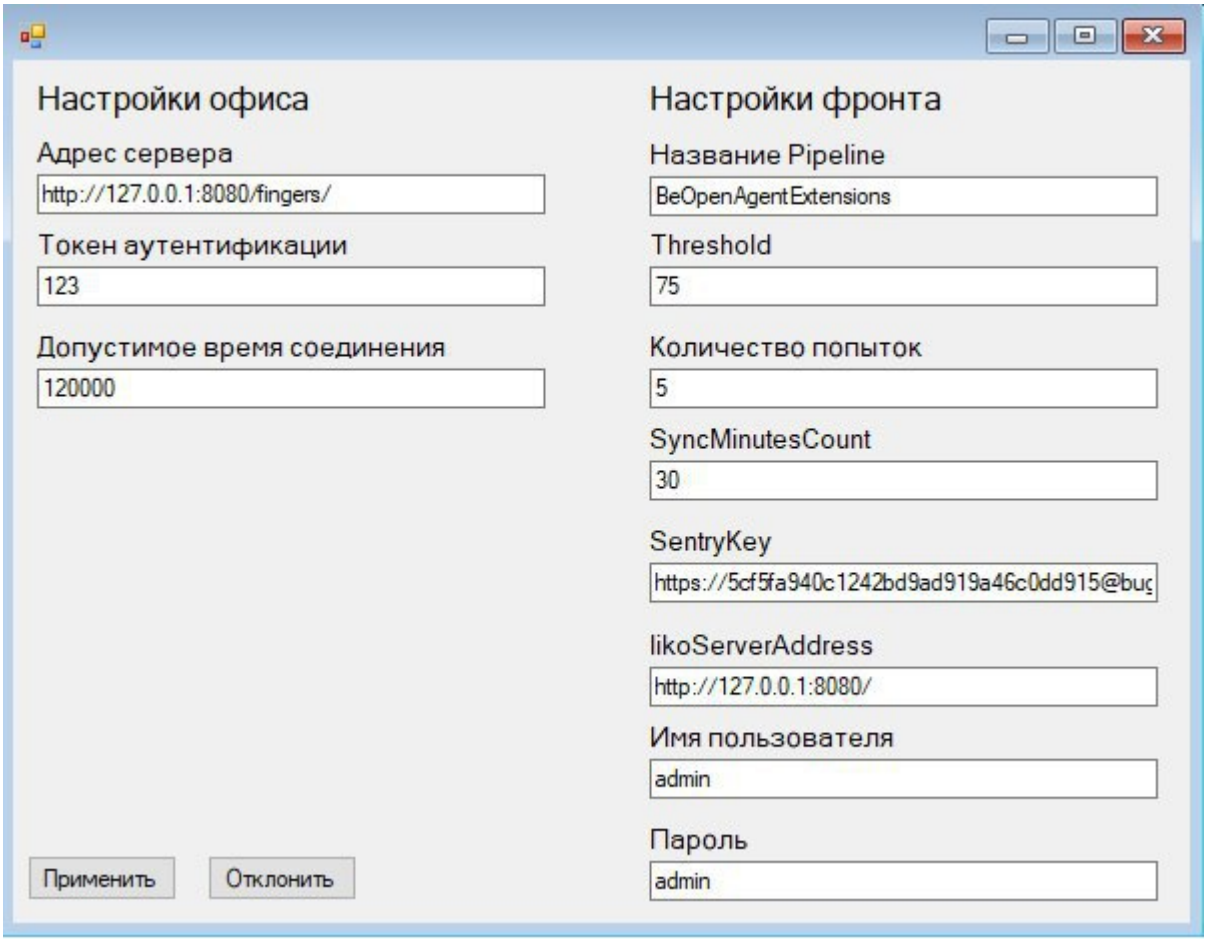
PipeName - название канала связи для общения с **Front.Biometric**.

5. Конфигурация back и front плагинов

- Необходимо зайти в backoffice. Слева, в меню, появится вкладка BeOpenBiometric, необходимо зайти в нее, нажать на кнопку "Соткудники"
  или "Устройства".



- После этого появится окно:



- Левая колонка относится к back плагину, здесь :

  i. **Адрес сервера** – адрес сервера биометрии с указанием порта.
  Например: http://192.168.0.1:8110/fingers/
  Приставка "/fingers/" обязательна!!!
  ii. **Токен аутентификации** - токен сервера биометрии. Не менять.
  iii. **Допустиомое время соежинения** - таймаут ожидания ответа сервера. По умолчанию 12000.

- Правая колонка относится к front плагину, здесь :

  i. **Название Pipeline** - название канала связи для общения с **AgentExtensionsContext**, должно совпадать с названием в конфиге плагина **AgentExtensionsContext**.
  ii. **Порог** - пороговый процент распознавания отпечатка(% совпадения отпечатка для корректного срабатывания. Если у вас плохо читается отпечаток, можно его понизить).
  iii. **Количесвто попыток** - Максимальное количество попыток прикладывания пальца к сканеру.
  iv. **Количество минут на синхронизацию** - настройка периодичности синхронизации в минутах.
  v. **Ключ Sentry** - SSH ключ багтрекера. Не менять.
  vi. **Адрес сервера iiko** – адрес сервера биометрии с указанием порта. Например http://192.168.0.1:8110/
  vii. **Имя пользователя** - Имя пользователя front и back
  viii. **Пароль** - Пароль пользователя front и back

- Далее необходимо зайти в папку C:\Program Files\iiko\iikoRMS\Front.Net\Plugins\BeOpen.iiko.Front.Biometric открыть блокнотом от имени администратора файл BeOpen.iiko.Front.Biometric.dll.config

```xml
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral,
    PublicKeyToken=b77a5c561934e089">
      <section name="BeOpen.iiko.Front.Biometric.Properties.Settings" type="System.Configuration.ClientSettingsSection, System,
      Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission=
      "false" />
    </sectionGroup>
  </configSections>
  <runtime>
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
      <dependentAssembly>
        <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30ad4fe6b2a6aeed" culture="neutral" />
        <bindingRedirect oldVersion="0.0.0.0-12.0.0.0" newVersion="12.0.0.0" />
      </dependentAssembly>
      <dependentAssembly>
        <assemblyIdentity name="System.Runtime.InteropServices.RuntimeInformation" publicKeyToken="b03f5f7f11d50a3a" culture="
        neutral" />
        <bindingRedirect oldVersion="0.0.0.0-4.0.2.0" newVersion="4.0.2.0" />
      </dependentAssembly>
    </assemblyBinding>
  </runtime>
  <userSettings>
    <BeOpen.iiko.Front.Biometric.Properties.Settings>
      <setting name="IsCashServer" serializeAs="String">
        <value>True</value>
      </setting>
      <setting name="ClearUnclosedAttendances" serializeAs="String">
        <value>False</value>
      </setting>
      <setting name="ClearingTimeout" serializeAs="String">
        <value>30</value>
      </setting>
    </BeOpen.iiko.Front.Biometric.Properties.Settings>
  </userSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.7.2" /></startup></configuration>

```

В случае, если плагин устанлен на главной кассе, значение поля IsCashServer должно быть True, если нет - False.
В случее, если вы не используете usb сканеры на кассе, значение поля UseUsbScanners должно быть False.
В случае, если вы хотите удалять незакрытые явки после закрытия кассовой сметы, значаения поля ClearUnclosedAttendances должно быть True, если нет - False.
Значение поля ClearingTimeout устанавливает времая, после истечения которого будут удаляться явки

ЕСЛИ ВЫ НЕ *ИСПОЛЬЗУЕТЕ* СЕТЕВОЙ СКАНЕР (СКАНЕР ОТПЕЧАТКОВ, КОТОРЫЙ ПОДКЛЮЧАЕТСЯ НАПРЯМУЮ В ЛОКАЛЬНУЮ СЕТЬ И ИСПОЛЬЗУЕТСЯ ДЛЯ РЕГИСТРАЦИИ ЯВОК), НАСТРОЙКА *ЗАВЕРШЕНА*, ЕСЛИ ВЫ *ИСПОЛЬЗУЕТЕ* СЕТЕВОЙ СКАНЕР, ВЫПОЛНЯЙТЕ ПУНКТ 6

6. Настройка сетевого контроллера

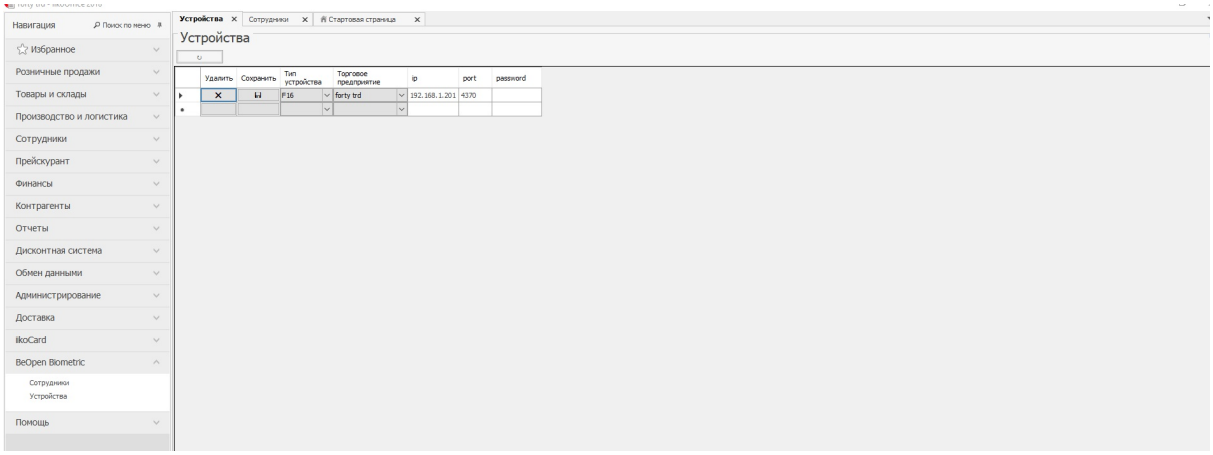
Перед выездом для установки сетевого контроллера необходимо его подготовить! Для этого:

- Подключаем сканер к сети
- На рабочий компьютер скачиваем архив Drivers_forSyncTime.zip, запускаем bat-файл Register_SDK.bat из папки ThirdParty(от администратора), запускаем ZKOnline.exe(от администратора)
- Скачиваем архив ThirdParty , запускаем программу Third Party/Search Panels and Modify IPAddress.exe
- В IPAdress записан IP найденного в сети устройства, записываем его в поле колонки "ip"
- Скачиваем архив **Scanner.Util(net scanner only)**
- Запускаем **StandaloneSDKDemo**
- Заходим во вкладку **Terminal**
- В **TCP/IP** вводим IP устройства и порт(4370).
- Нажимаем кнопку **Connect**
- Переходим во вкладку **OtherMng** и нажимаем кнопку **SYNCTime**

Действия на клиенсткой машине:

- Открываем вкладку "Устройства" в бэке
- Запускаем программу Third Party/Search Panels and Modify IPAddress.exe
- В IPAdress записан IP найденного в сети устройства, записываем его в поле колонки "ip"

- В Поле колонки "port" пишем 4370
- Выбираем тип устройства и торговое предприятие
- Жмем кнопку "сохранить"



По всем вопросам просьба писать на beopensoft@open-s.info