

# Настройка плагина для отчетов

## Настройка товаров в системах Лайм и iiko

1. интеграция с Лайм платная — 1500р/мес
2. чтобы лицензия работала корректно, нужно заменить номер id на 82055718.

Главное условие, для возможности пробития чеков Лайма в iiko - **это одинаковые названия товаров и типов оплаты.**

Также типы оплаты в iiko office должны быть настроены на прием извне

Для чистоты отчетов лучше делать настройки как можно схожими по смыслу.

Возвраты в системе iiko автоматически провести **невозможно**, так что для правильности отчетов это нужно делать вручную в iikoFront, на котором запущен плагин

Также, если при отправке чека была закрыта смена на iiko, то появившиеся открытые заказы следует удалить, так как они пройдут при следующем нажатии кнопки Провести в окне статуса плагина

## Настройки плагина

Заполнить файл PluginSettings.json следующим образом:

```
{
  "Login": "",
  "Password": "",
  "Address": "https://admin.lime-it.ru",
  "InstallationId": ,
  "Pin": "",
  "Port": "6666"
}
```

Где:

Login - Логин вашей учетной записи в системе Лайм  
Password - Ваш пароль от этой учетной записи  
Address - Для пользователей нашего сервера "https://admin.lime-it.ru/" или адрес вашего локального сервера  
InstallationId - Id вашей инсталляции(можно посмотреть в адресной строке)  
Pin : Пин пользователя в iiko, от имени которого будут пробиваться чеки  
Port - Свободный порт, на который будут приходить чеки от касс Лайм

Id инсталляции можно увидеть здесь:

[admin.lime-it.ru/installations/2627](https://admin.lime-it.ru/installations/2627)

## Разрешение на прослушивание порта

Для того, чтобы получать чеки нужно дать разрешение на прослушивание порта

Для это в командной строке, от имени **Администратора**, нужно выполнить следующую команду:

```
netsh http add urlacl url=http://+:6666/api/CashdeskServer/ user=YOURUSER
```

Где:

YOURUSER - имя пользователя Windows, работающего с iikoFront

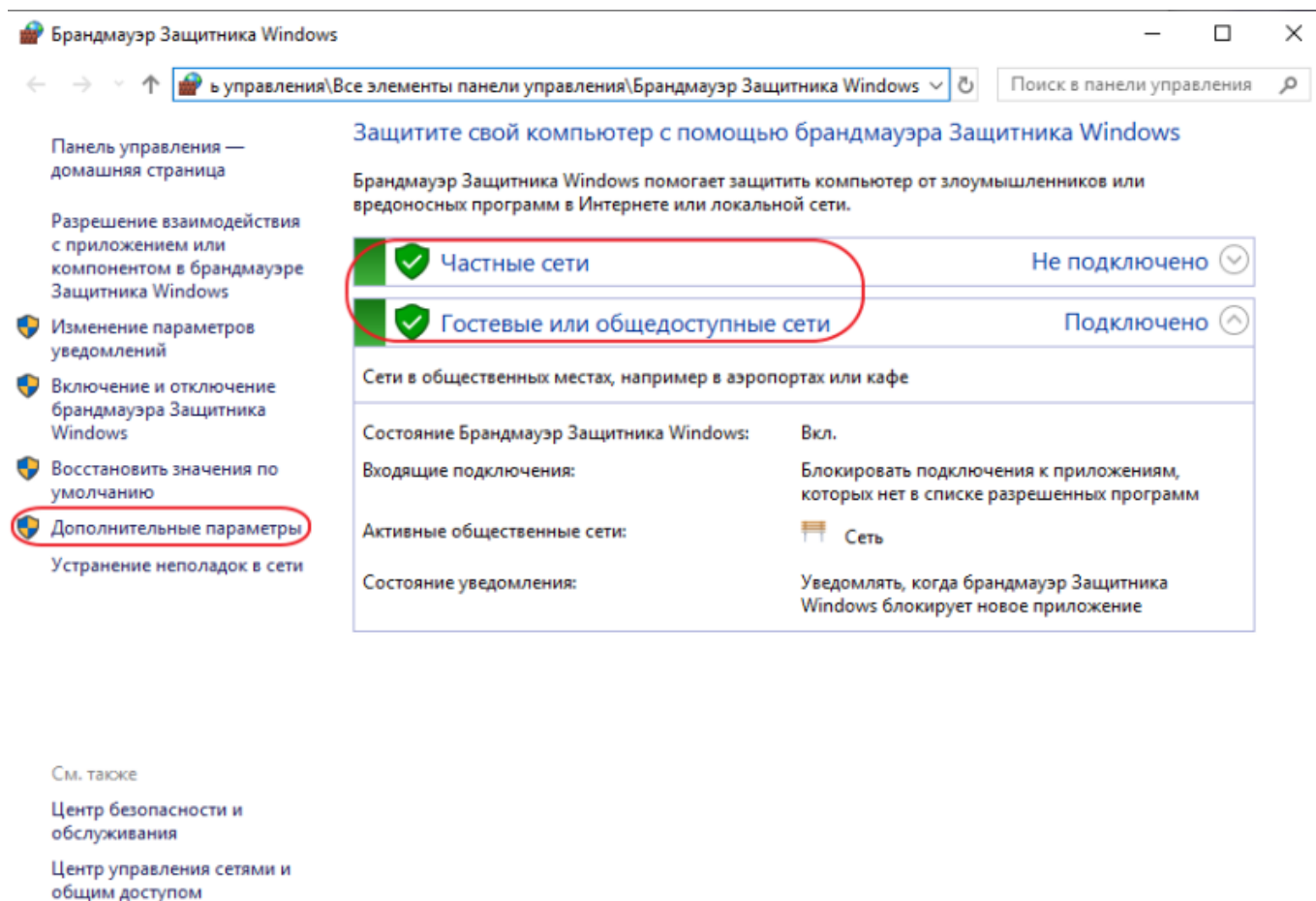
6666 - Порт из настроек плагина

Если при выполнении этой команды возникла ошибка 183 Невозможно создать файл, так как он уже существует, то, скорее всего, это разрешение уже было добавлено ранее

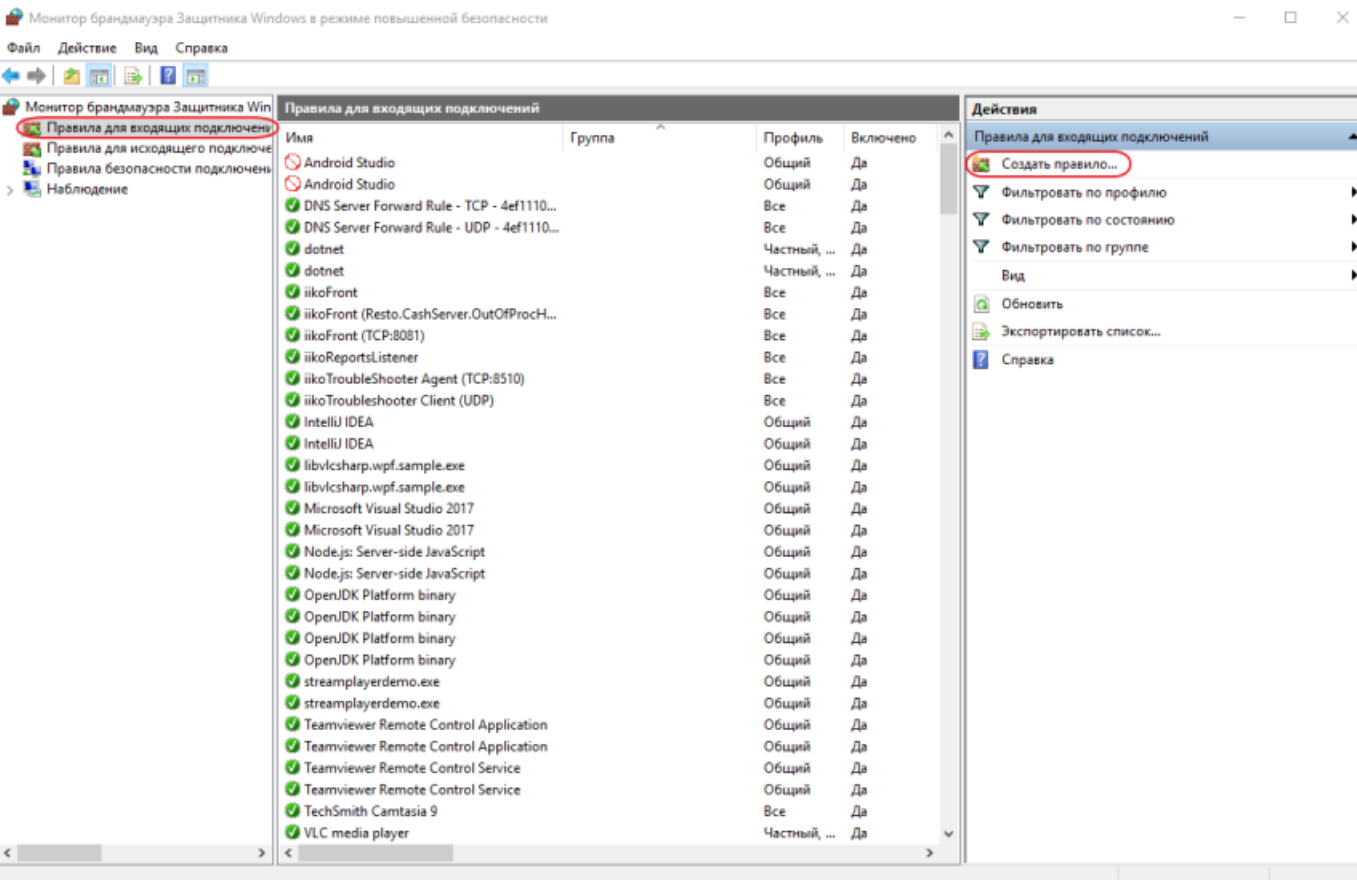
## Разрешение на входящие запросы

Для начала, проверяем, включен ли брандмауэр(найти его можно в панели управления)


Если он включен, то переходим в Дополнительные параметры



В открывшемся окне выбираем Правила для входящих подключений.  
Нажимаем Создать правило



Выбираем правило для Порта

 Мастер создания правила для нового входящего подключения

## Тип правила

Выберите тип правила брандмауэра, которое требуется создать.

### Шаги:

- Тип правила
- Протокол и порты
- Действие
- Профиль
- Имя

Правило какого типа вы хотите создать?

☐ Для программы

Правило, управляющее подключениями для программы.

☒ Для порта

Правило, управляющее подключениями для порта TCP или UDP.

☐ Предопределенные

BranchCache - обнаружение кэширующих узлов (использует WSD)

Правило, управляющее подключениями для операций Windows.

☐ Настраиваемые

Настраиваемое правило.

< Назад

Далее >

Отмена

Протокол TCP

Определенный порт: Порт из настроек плагина

## Мастер создания правила для нового входящего подключения



## Протокол и порты

Укажите протоколы и порты, к которым применяется данное правило.

## Шаги

- Тип правила
- Протокол и порты
- Действие
- Профиль
- Имя

Укажите протокол, к которому будет применяться это правило.

- ☒ Протокол TCP
- ☐ Протокол UDP

Укажите порты, к которым будет применяться это правило.

- ☐ Все локальные порты
- ☒ Определенные локальные порты:

Пример: 80, 443, 5000-5010

< Назад

Далее >

Отмена

Разрешить подключение

## Действие

Укажите действие, выполняемое при соответствии подключения условиям, заданным в данном правиле.

### Шаги:

- Тип правила
- Протокол и порты
- Действие
- Профиль
- Имя

Укажите действие, которое должно выполняться, когда подключение удовлетворяет указанным условиям.

☒ **Разрешить подключение**

Включая как подключения, защищенные IPSec, так и подключения без защиты.

☐ **Разрешить безопасное подключение**

Включая только подключения с проверкой подлинности с помощью IPSec. Подключения будут защищены с помощью параметров IPSec и правил, заданных в разделе правил безопасности подключений.

Настроить...

☐ **Блокировать подключение**

< Назад

Далее >

Отмена

Выбрать доменный, частный и публичный



## Профиль

Укажите профили, к которым применяется это правило.

### Шаги:

- Тип правила
- Протокол и порты
- Действие
- Профиль
- Имя

Для каких профилей применяется правило?

☒ Доменный

Применяется при подключении компьютера к домену своей организации.

☒ Частный

Применяется, когда компьютер подключен к частной сети, например дома или на работе.

☒ Публичный


Применяется при подключении компьютера к общественной сети.

< Назад

Далее >

Отмена

Ввести говорящее имя, чтобы случайно не удалить и не забыть, зачем оно нужно

 Мастер создания правила для нового входящего подключения

## Имя

Укажите имя и описание данного правила.

### Шаги:

- Тип правила
- Протокол и порты
- Действие
- Профиль
- Имя

Имя:

Входящие чеки Лайма для ііко

Описание (необязательно):

< Назад

Готово

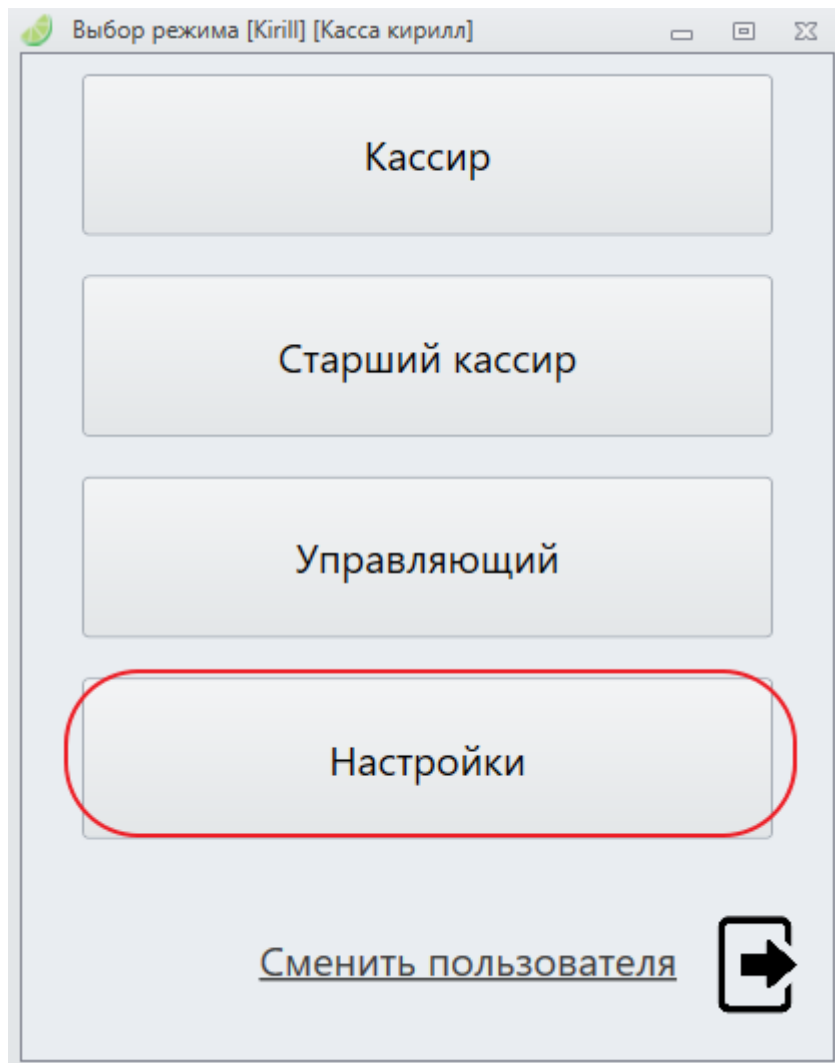
Отмена

**Готово!**

## Настройка плагина в кассе

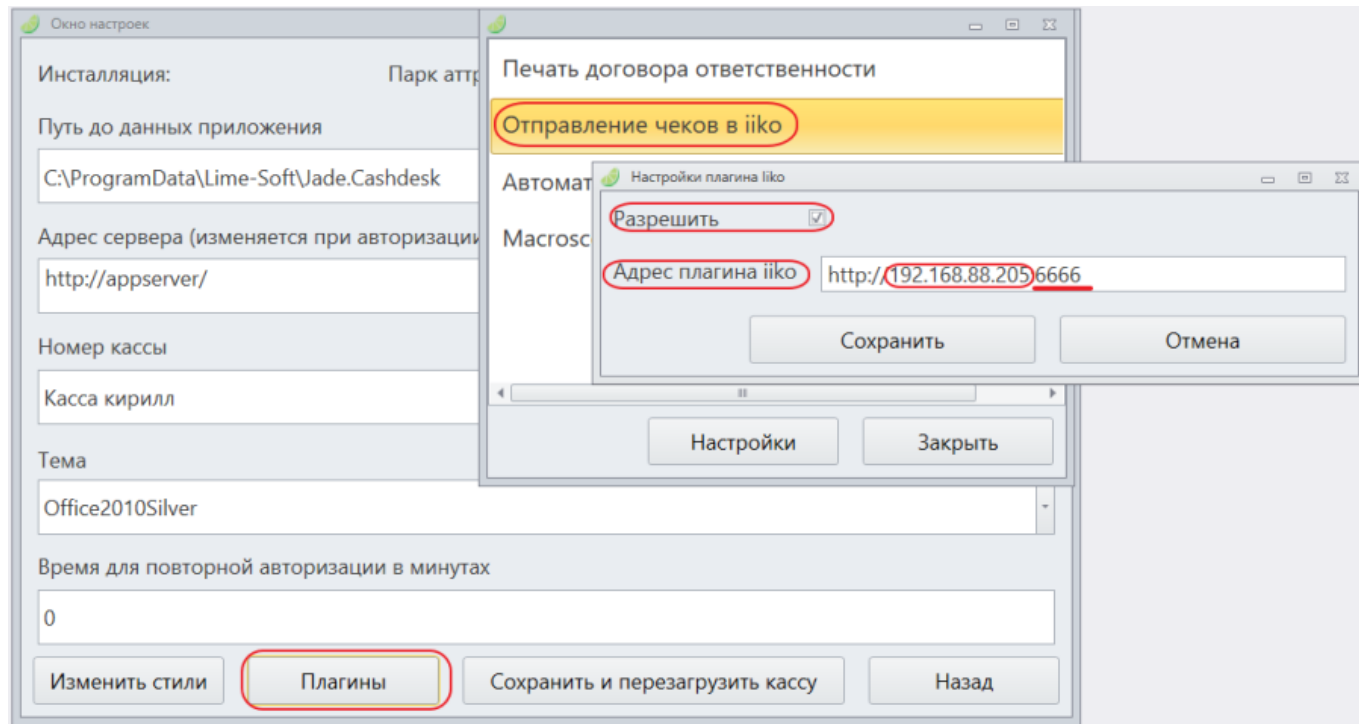
Заходим в кассу с учетной записи администратора Заходим в настройки





В окне настроек нажимаем кнопку Плагины Из появившегося списка выбираем Отправление чеков в iiko Ставим галочку в поле Разрешить В поле Адрес плагина iiko адрес компьютера в локальной сети с запущенным плагином в iiko в формате:

```
http://(ip компьютера в локальной сети):(Порт из настроек плагина iiko)
```



[public](#), [doc](#), [iiko](#)

From:

<https://wiki.lime-it.ru/> -

Permanent link:

[https://wiki.lime-it.ru/doku.php/public/iiko/report\\_setting](https://wiki.lime-it.ru/doku.php/public/iiko/report_setting)

Last update: **15:33 11/12/2023**

