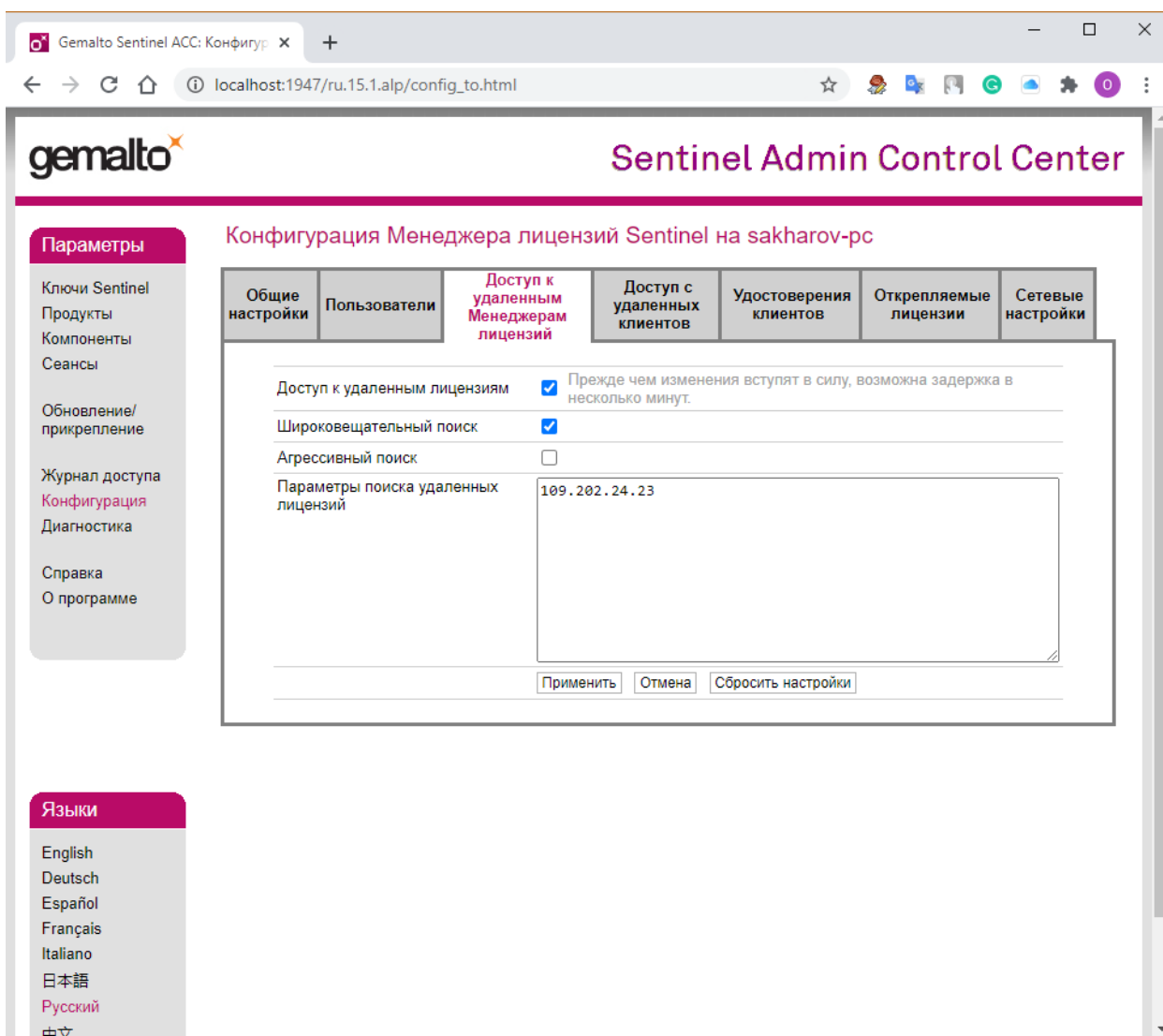


Установка сетевого ключа

Пользовательские компьютеры

На компьютерах пользователей установка выполняется согласно **Руководству пользователя** – нужно установить находящийся на диске с дистрибутивом драйвер аппаратного ключа HASPUserSetup.exe и дистрибутив программы. Если компьютеры пользователей и сервер лицензий находятся в одной локальной сети, то больше на компьютерах пользователей никаких действий не требуется. Если в компьютеры и сервер не в одной локальной сети, то на компьютере пользователя нужно запустить страницу Sentinel HASP Admin Control Center в браузере по адресу <http://localhost:1947> и в меню **Конфигурация – Доступ к удаленным менеджерам лицензий** указать IP адрес сервера с установленным сетевым ключом (на скриншоте адрес 109.202.24.23):



Сервер

Сетевой ключ может быть установлен на сервере с ОС Windows/Linux или на любом пользовательском компьютере. На сервере/компьютере с ОС Windows, устанавливается тот же драйвер аппаратного ключа HASPUserSetup.exe, затем нужно запустить страницу Sentinel HASP Admin Control Center в браузере по адресу <http://localhost:1947> и в меню **Конфигурация – Доступ с удаленных клиентов** указать IP адреса, с которых можно запускать программу – см. прилагаемый скриншот. Если разрешено всем - то указать allow=all.

gemalto Sentinel Admin Control Center

Конфигурация Менеджера лицензий Sentinel на sakharov-pc

Параметры

- Ключи Sentinel
- Продукты
- Компоненты
- Сеансы
- Обновление/прикрепление
- Журнал доступа
- Конфигурация
- Диагностика
- Справка
- О программе

Языки

- English
- Deutsch
- Español
- Français
- Italiano
- 日本語
- Русский
- 中文

Общие настройки | Пользователи | **Доступ к удаленным Менеджерам лицензий** | Доступ с удаленных клиентов | Удостоверения клиентов | Открепляемые лицензии | Сетевые настройки

Доступ с удаленных клиентов

- Никто
- Только идентифицируемые клиенты
- Любой, но облачные лицензии требуют удостоверения
- Любой, облачные лицензии могут использоваться без удостоверения

Публичный адрес для доступа с удостоверением

Хранение секретов удостоверений

- Обычный текст
- Зашифрован ключом хранилища, предоставленным с Sentinel AdminAPI

Ограничения доступа

allow=all

Показать недавних клиентов

Записи обрабатываются в том порядке, в котором они указаны. После обнаружения совпадения обработка прекращается. allow=all добавляется в конце списка

Применить | Отмена | Сбросить настройки

C:\Program Files (x86)\Common Files\Aladdin Shared\HASP\hasplm.ini

На компьютере (сервере) с установленным сетевым ключом необходимо добавить новое правило для входящих подключений в брандмауэр Защитника Windows:

Зайдите на **Брандмауэр и безопасность сети – Дополнительные параметры** и выберите **Правила для входящих подключений**:

Монитор брандмауэра Защитника Windows в режиме повышенной безопасности

Файл Действие Вид Справка

Монитор брандмауэра Защитника Windows

- Правила для входящих подключений
- Правила для исходящего трафика
- Правила безопасности подключения
- Наблюдение

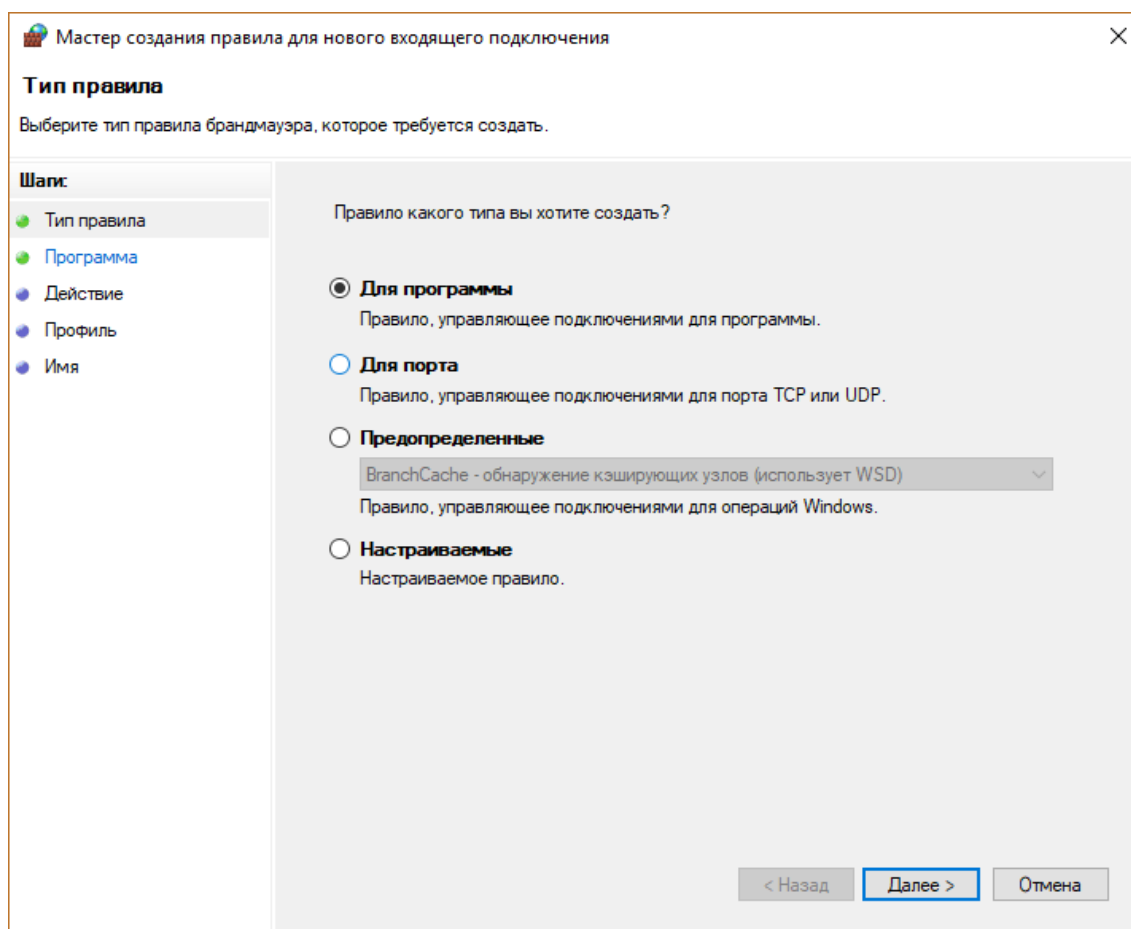
Правила для входящих подключений

Имя	Группа
Обнаружение кэширующих узлов BranchCache	BranchCache
Получение содержимого BranchCache	BranchCache
Сервер размещенного кэша BranchCache	BranchCache
mDNS (UDP-In)	mDNS
mDNS (UDP-In)	mDNS
Secure Socket Tunneling Protocol (SSTP)	Сетевые подключения
Беспроводной дисплей (входящий трафик)	Беспроводные переносные устройства
Обратный канал инфраструктуры беспроводных переносных устройств	Беспроводные переносные устройства
Беспроводные переносные устройства	Беспроводные переносные устройства
Беспроводные переносные устройства	Беспроводные переносные устройства
Удаленный рабочий стол — пользователь	Диспетчер задач
Удаленный рабочий стол — пользователь	Диспетчер задач
Удаленный рабочий стол — теневая копия	Диспетчер задач
Домашняя группа: входящий трафик	Домашняя группа
Домашняя группа: входящий трафик	Домашняя группа
Журналы и оповещения производителей	Журналы
Журналы и оповещения производителей	Журналы
Журналы и оповещения производителей	Журналы
Журналы и оповещения производителей	Журналы

Действия

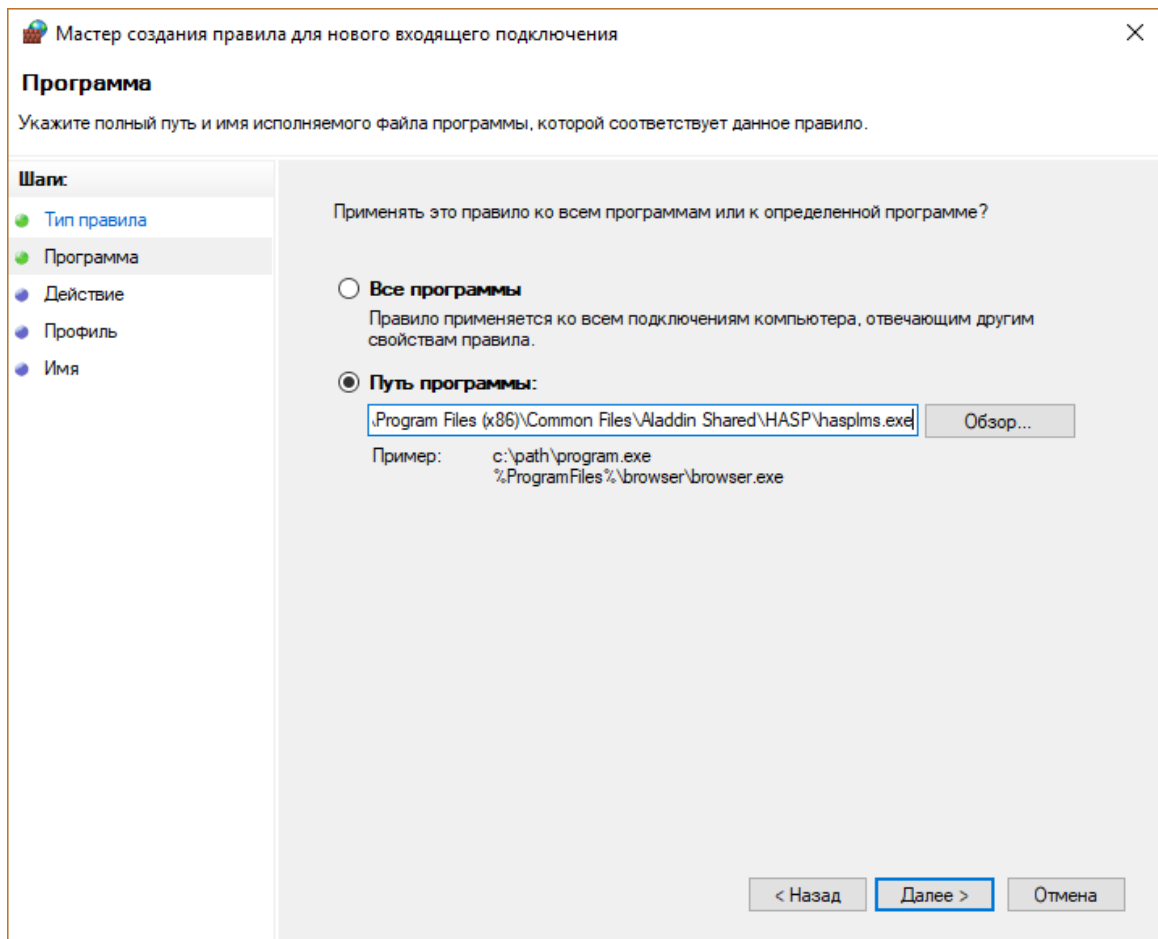
- Правила для входящих подключений
- Создать правило...
- Фильтровать по профилю
- Фильтровать по состоянию
- Фильтровать по группе
- Вид
- Обновить
- Экспортировать список...
- Справка

Затем кликните на **Создать правило** и выберите **Для программы**:

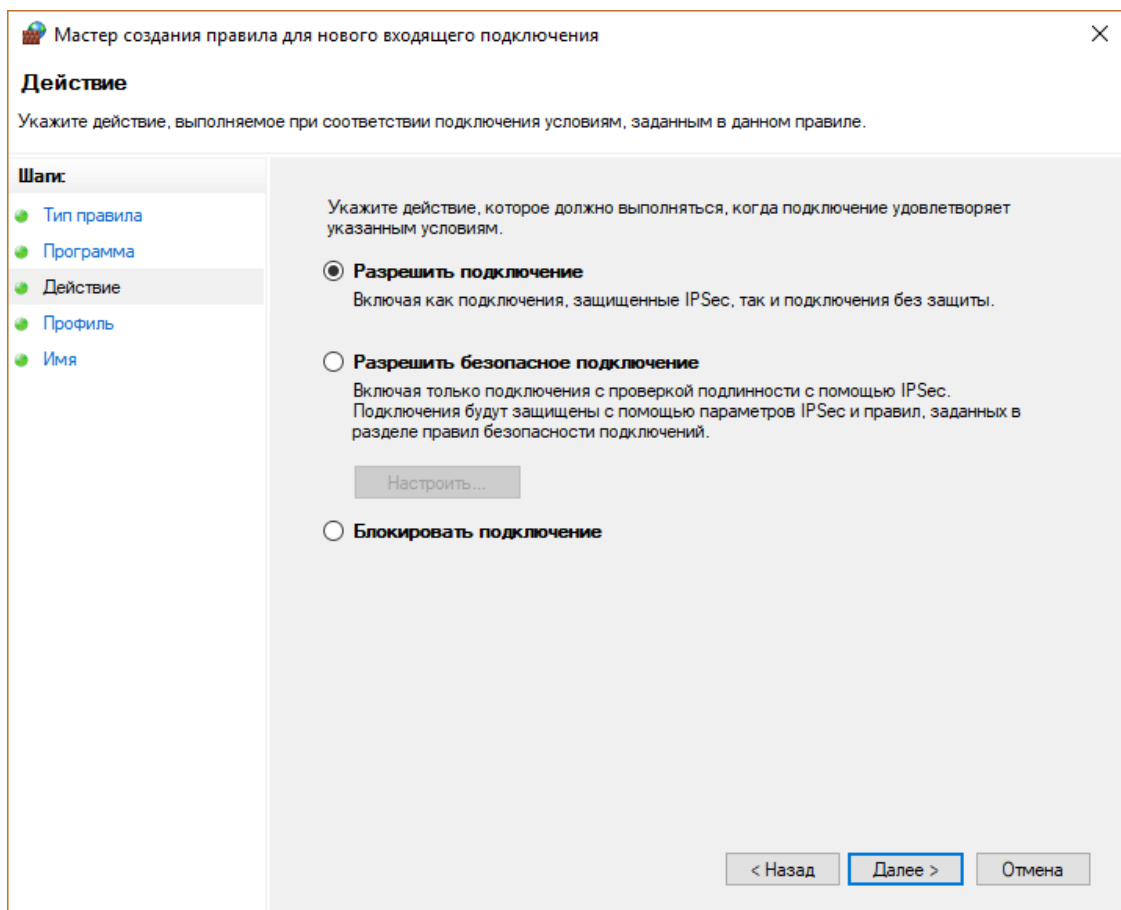


Затем укажите путь к менеджеру лицензий:

C:\Program Files (x86)\Common Files\Aladdin Shared\HASP\hasplms.exe



Далее – Разрешить подключение



Далее укажите профиль, к которому будет применяться правило:

Мастер создания правила для нового входящего подключения

Профиль

Укажите профили, к которым применяется это правило.

Шаги:

- Тип правила
- Программа
- 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

Далее укажите имя, например такое: Sentinel License Manager

Мастер создания правила для нового входящего подключения

Имя

Укажите имя и описание данного правила.

Шаги:

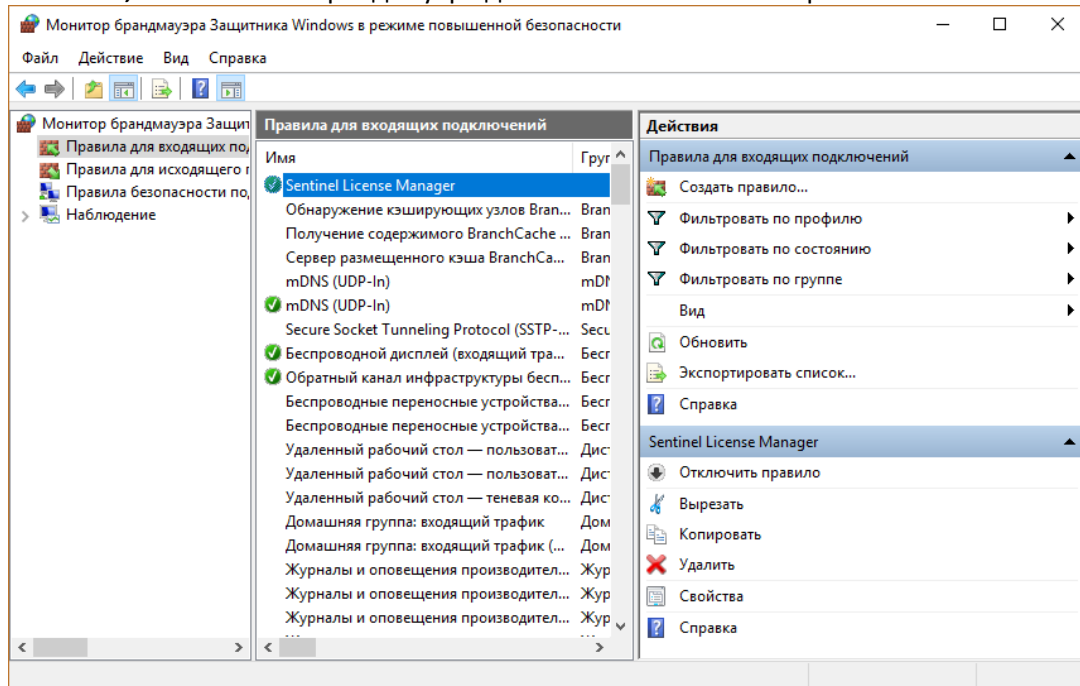
- Тип правила
- Программа
- Действие
- Профиль
- Имя**

Имя:

Описание (необязательно):

< Назад **Готово** Отмена

Нажмите **Готово**, после этого в брандмауэре должно появиться новое правило:



После всех этих действий на пользовательских компьютерах ключ должен появиться в списке **Ключи Sentinel** (см. пример на скриншоте ниже). Программы будут запускаться на компьютерах пользователей в соответствии с записанными на ключе лицензиями.

