# GeoIP-обогащение (Геоданными)

> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

> Официальная документация по данному разделу приведена в Онлайн-справке на продукт: https://support.kaspersky.com/KUMA/3.2/ru-RU/233257.htm

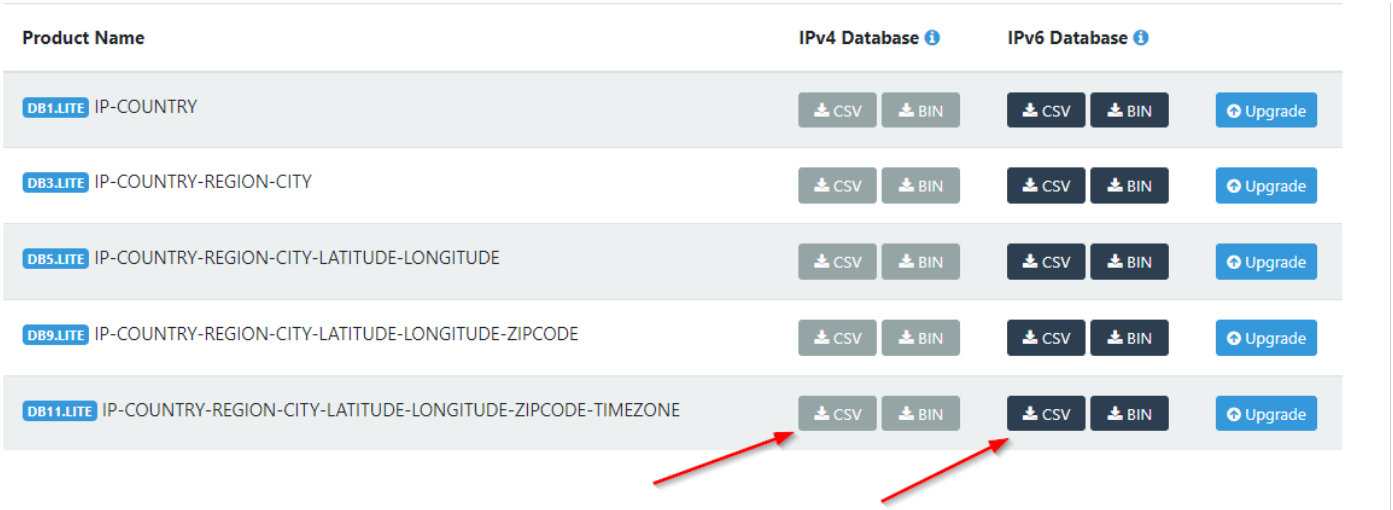
> Скачанная и конвертированная база (IP2Location) - https://box.kaspersky.com/f/b961a874400a4a0ab66b/

> Российская база (требуется регистрация) - https://geoip.noc.gov.ru/

## Скачивание БД

### IP2Location

Чтобы скачать базы необходимо зарегистрироваться.  После регистрации и входа на сайт переходим по ссылке:  https://lite.ip2location.com/database-download
И выбираем нужную нам БД (есть для ipv4 и ipv6) и скачиваем.




## MAXMIND

Скачивание БД также доступно после регистрации. Также при регистрации проверяется соответствие выбранной странны и ip, с которого вы регистрируетесь. При этом при выборе страны отсутствует Россия. Возможно проблему можно решить через VPN.

---

# Конвертация БД

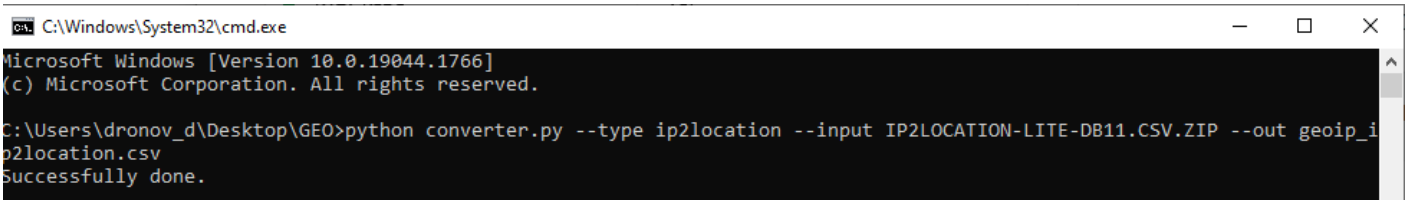
Перед импортом базы ее необходимо конвертировать в формат, понятный KUMA. Для конвертации данных используется скрипт. Актуальный скрипт и команды запуска тут:

https://support.kaspersky.com/help/KUMA/2.1/ru-RU/233259.htm

В простейшем случае команда запуска выглядит так:

```
python converter.py --type ip2location --input IP2LOCATION-LITE-DB11.CSV.ZIP --out geoip_ip2location.csv
```

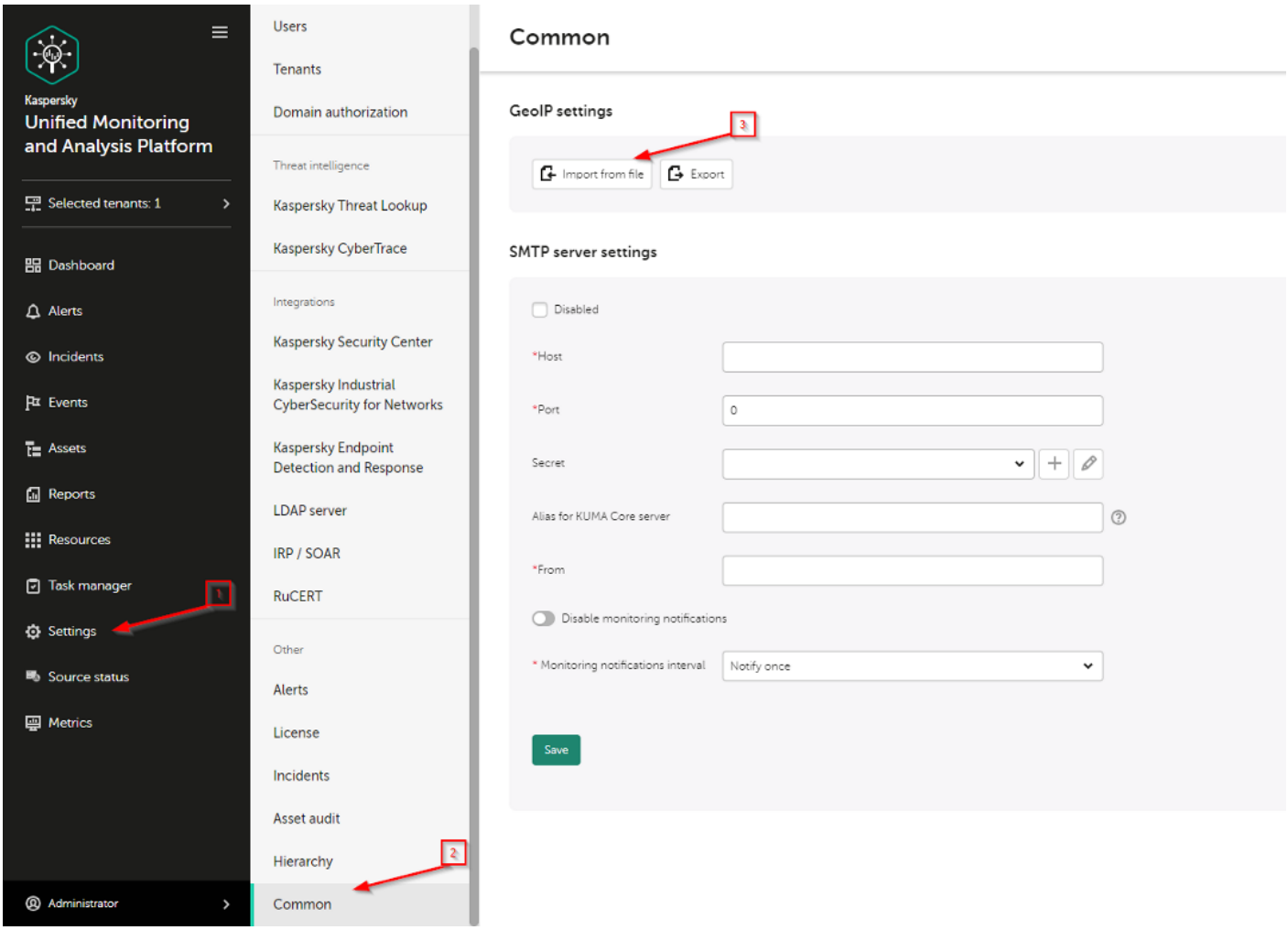
После запуска нужно подождать 20-30 сек и в случае успешной конвертации получим файл CSV:



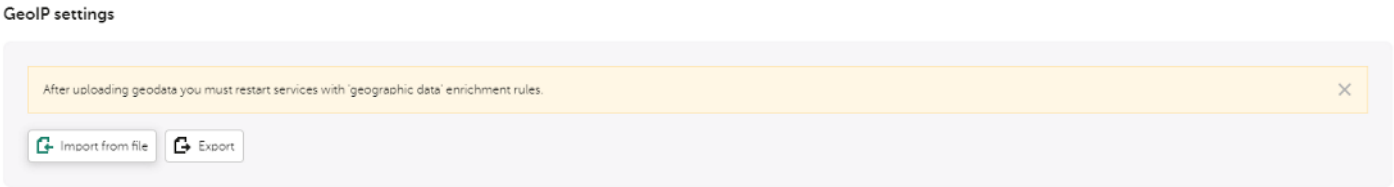

---

# Загрузка БД в KUMA

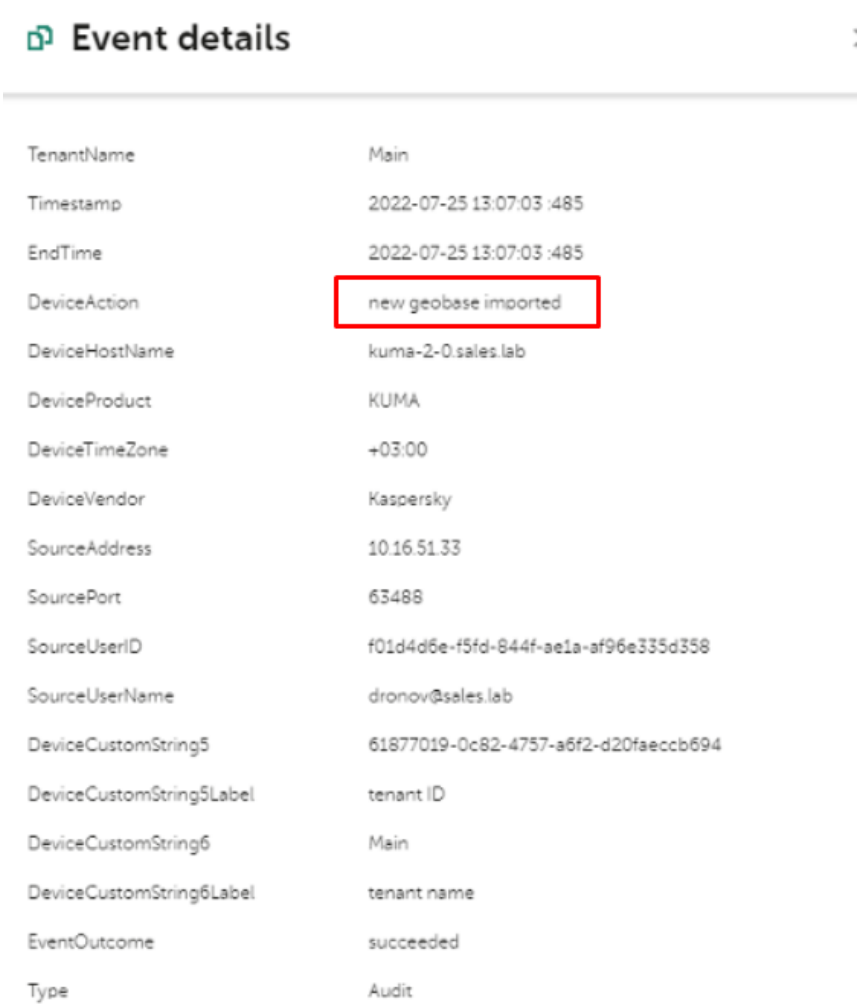
Загрузка БД (предварительно сконвертированной скриптом!) осуществляется по пути:
**Settings - Common - GeoIP settings - Import from file**




После добавления БД необходимо перезапустить все сервисы, где настроено обогащение по GeoIP (при выполнении тестов было достаточно выполнить reload, а не restart)

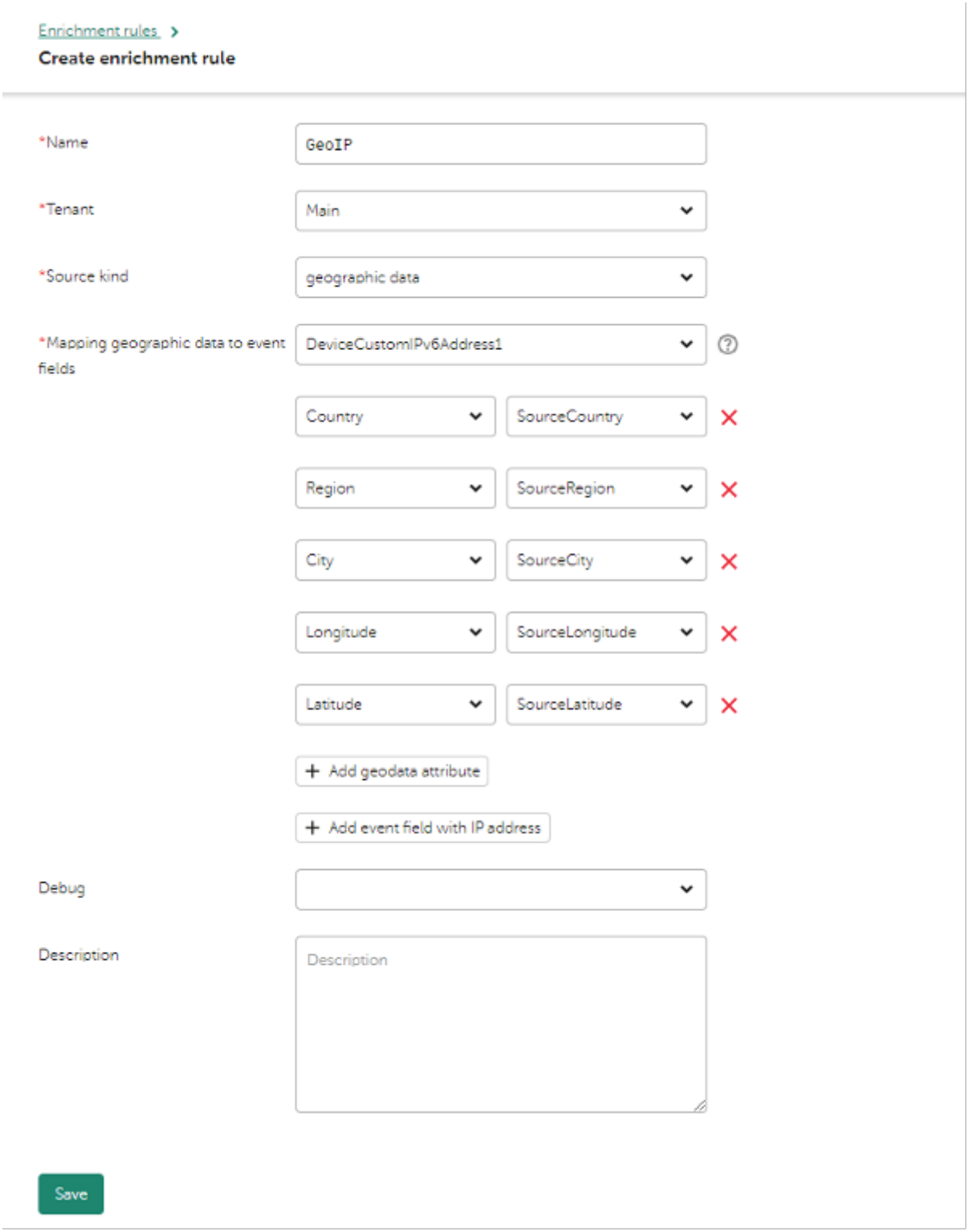



> При импорте нового файла с данными GeoIP ранее добавленные данные перезапишутся (с созданием события аудита). Поэтому если нужно внести незначительные изменения для кастомизации сопоставления рекомендуется скачать текущую БД из интерфейса KUMA, после чего внести туда изменения и подгрузить обратно.

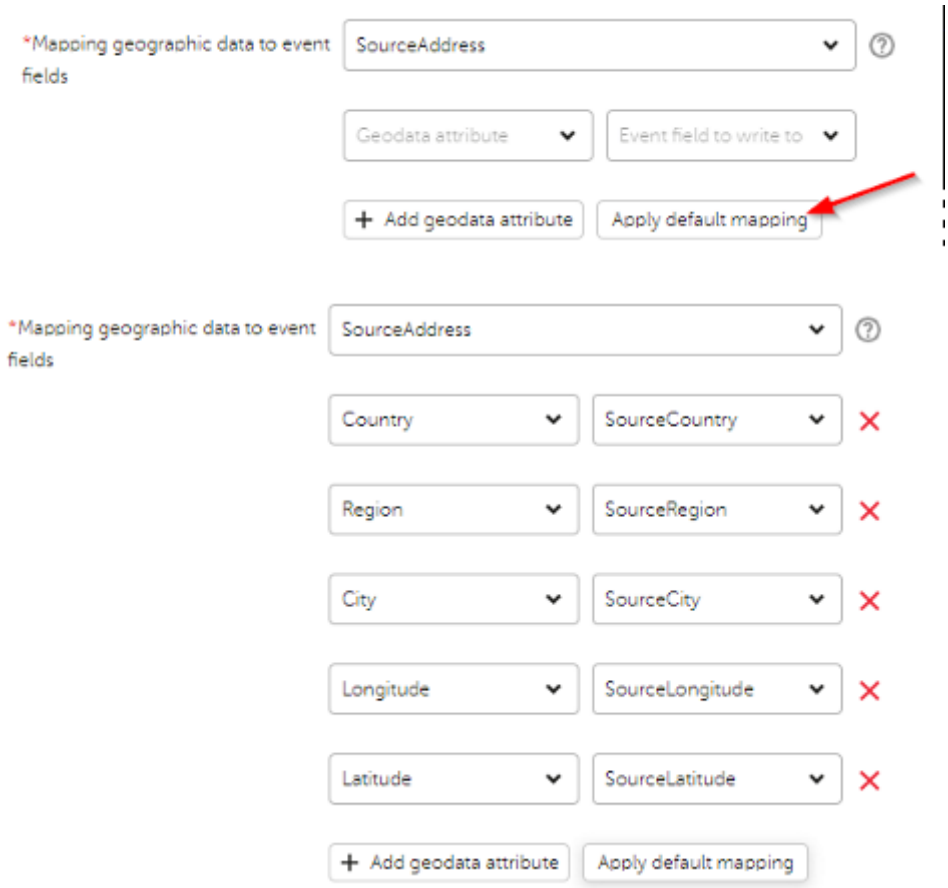



# Обогащение GeoIP

- В разделе **Ресурсы - Правила Обогащения** создаем новое правило
- В поле Source kind выбираем geographic data
- В поле Mapping geographic data to event fields выбираем поле события KUMA, в котором присутствует нужный для обогащения ip-адрес
- Здесь же выбираем Geodata attribute и соответствующее поле события KUMA Event field to write to
- Для GeoIP добавлены новые поля событий, но можно использовать любые




Сопоставление по умолчанию доступно, если в качестве источника IP выбрано одно из полей событий SourceAddress, DestinationAddress и DeviceAddress.
При выборе других полей в качестве источника сопоставление по умолчанию не доступно.




Далее нужно созданное правило выше закрепить в коллекторе в части обогащения. Пример того, как выглядит обогащенное событие:

| | |
|---|---|
| SourceAddress | 8.8.8.8 |
| SourceCity | Mountain View |
| SourceCountry | United States of America |
| SourceLatitude | 37.40599 |
| SourceLongitude | -122.078514 |
| SourcePort | 49048 |
| SourceProcessName | Advapi |
| SourceRegion | California |

---

# Формат файла CSV:

```
Network,Country,Region,City,Latitude,Longitude
10.0.0.0/8,Russia,Moscow,Butovo,,
192.168.0.0/16,Russia,SPB,Zelenograd,,
```

Revision #10
Created 11 August 2023 14:43:47 by Boris Rzr
Updated 5 November 2024 10:25:55 by Boris Rzr