GeoIP-обогащение (Геоданными)

- ??????????, ??????????? ?? ?????? ????????, ???????? ??????????? ??????? pre-sales ?/??? community KUMA ? **НЕ** ???????? ??????????? ????????????? ???????.

- ??????????? ???????????? ?? ??????? ??????? ????????? ? ??????-??????? ?? ???????: https://support.kaspersky.com/KUMA/3.2/ru-RU/233257.htm

- ????????? ? ???????????????? ???? (IP2Location) - https://box.kaspersky.com/d/c77609e6f5bd463b8f56/

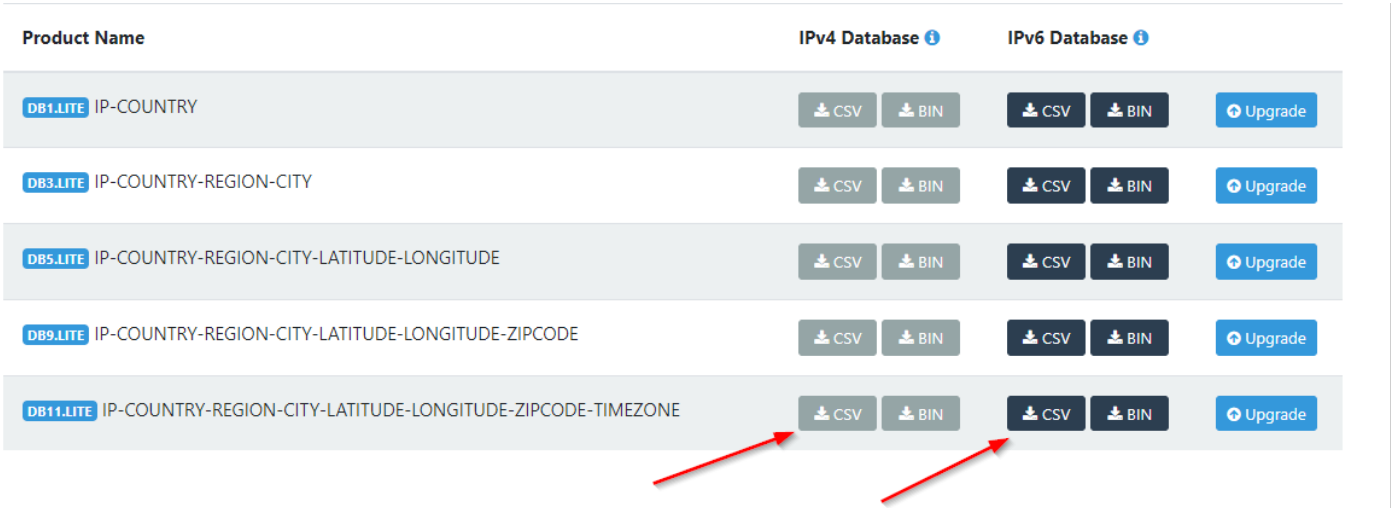
- ??????????? mmdb ????? ???? ? CSV ??? KUMA - https://github.com/KUMA-Community/mmdb2kuma

- ?????????? ???? (????????? ???????????) - https://geoip.noc.gov.ru/

Скачивание БД

IP2Location

????? ??????? ???? ?????????? ??????????????????. ????? ??????????? ? ????? ?? ???? ????????? ?? ??????: https://lite.ip2location.com/database-download
? ???????? ?????? ??? ?? (???? ??? ipv4 ? ipv6) ? ?????????.



MAXMIND

?????????? ?? ????? ???????? ????? ???????????. ????? ??? ??????????? ???????????? ???????????? ????????? ??????? ? ip, ? ???????? ?? ???????????????. ??? ???? ??? ?????? ?????? ??????????? ??????. ???????? ???????? ????? ?????? ????? VPN.

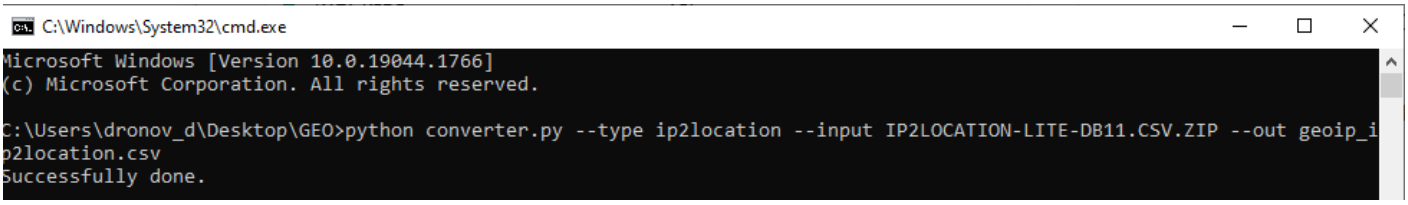
Конвертация БД

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

? ?????????? ?????? ??????? ??????? ???????? ???:

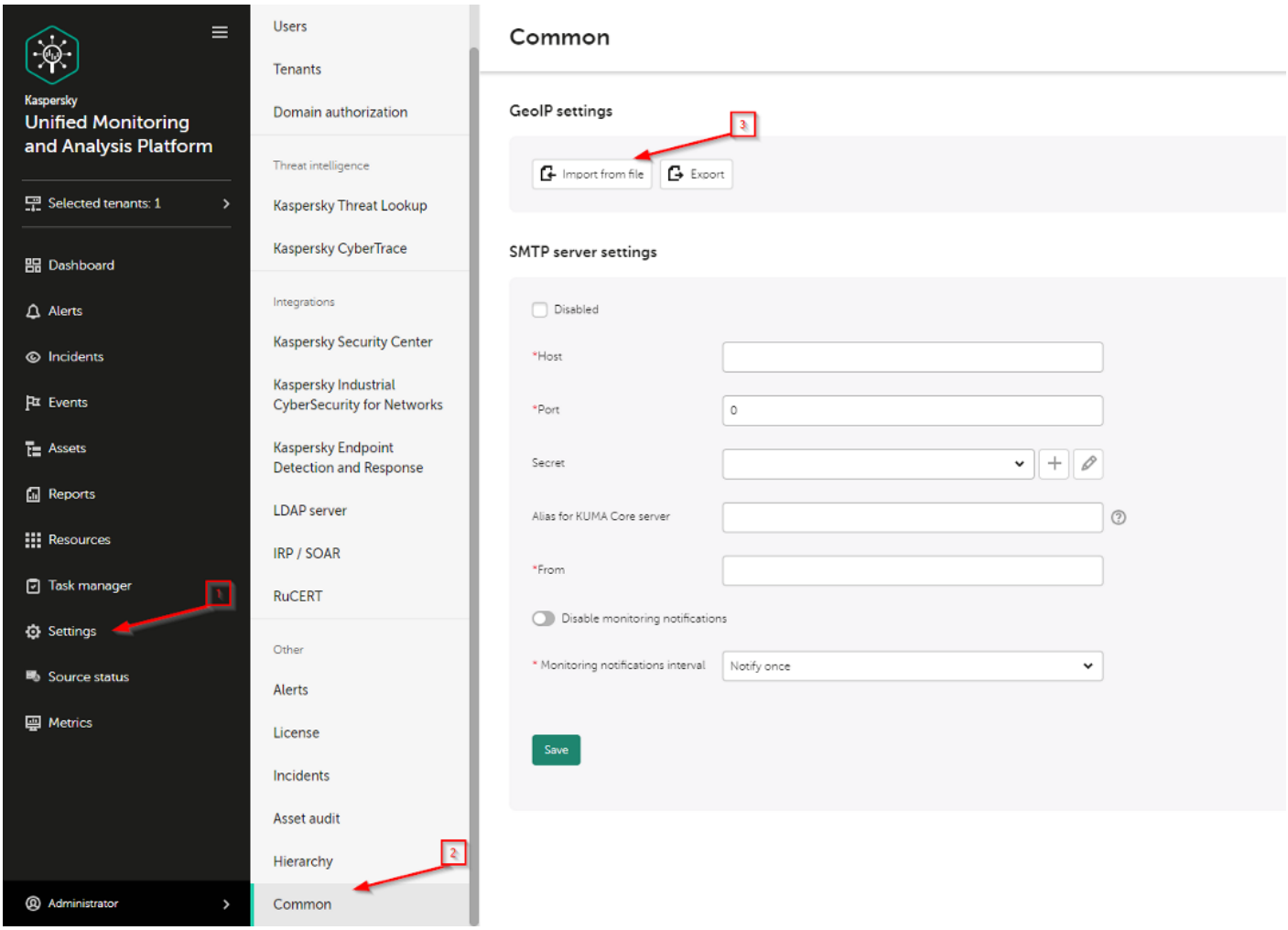
```
python converter.py --type ip2location --input IP2LOCATION-LITE-DB11.CSV.ZIP --out geoip_ip2location.csv
```

????? ??????? ????? ????????? 20-30 ??? ? ? ?????? ???????? ??????????? ??????? ???? CSV:

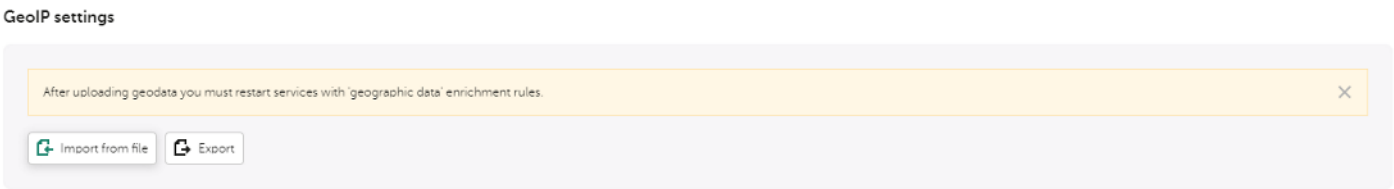


Загрузка БД в KUMA

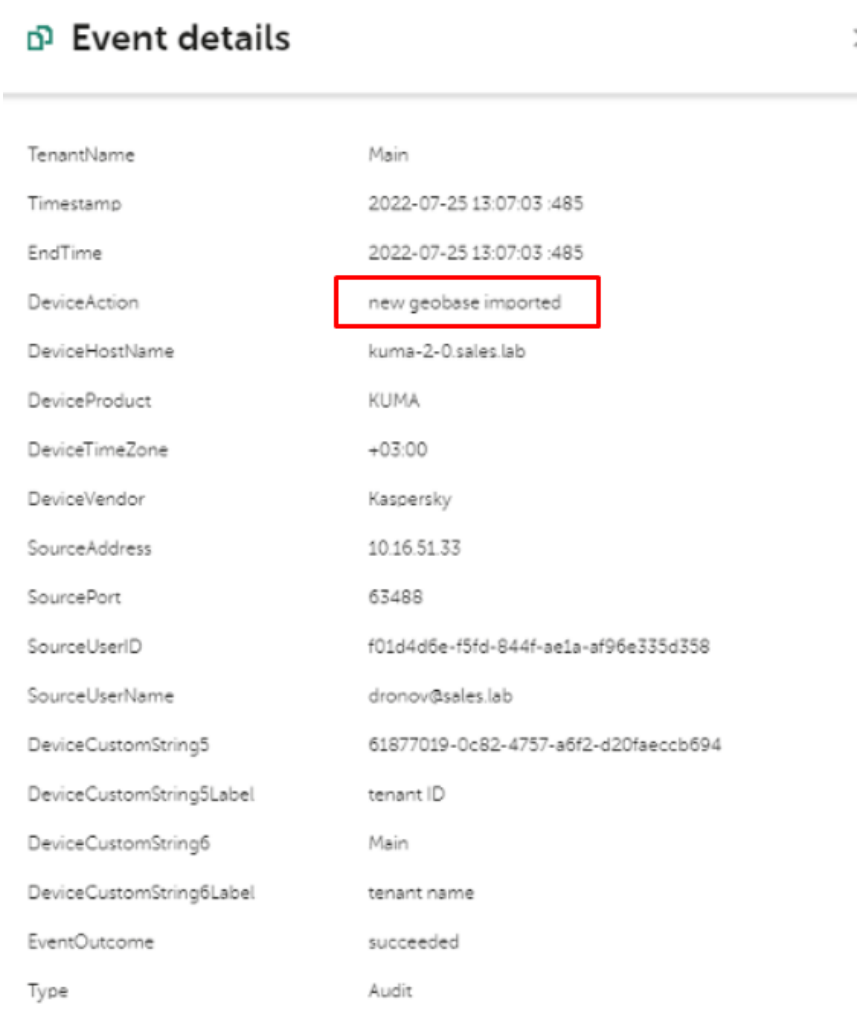
???????? ?? (?????????????? ???????????????? ????????!) ?????????????? ?? ????: **Settings - Common - GeoIP settings - Import from file**



????? ?????????? ?? ?????????? ????????????? ??? ???????, ??? ????????? ?????????? ?? GeoIP (??? ?????????? ?????? ???? ?????????? ????????? reload, ? ?? restart)

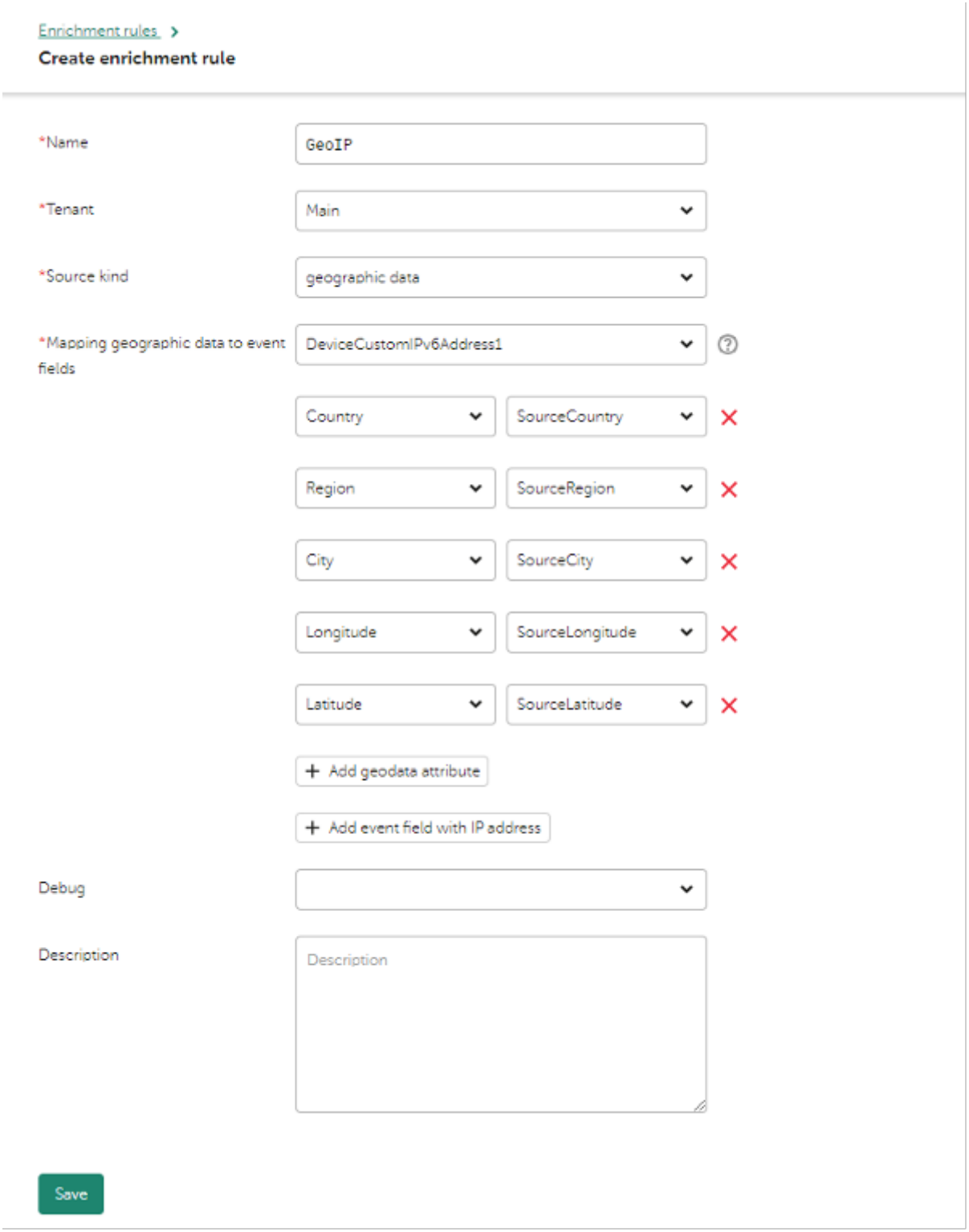


??? ??????? ?????? ????? ? ??????? GeoIP ????? ??????????? ?????? ????????????? (? ????????? ??????? ??????). ??????? ???? ????? ?????? ????????????? ????????? ??? ??????????? ????????????? ????????????? ??????? ??????? ?? ?? ?????????? KUMA, ????? ???? ?????? ???? ????????? ? ?????????? ???????.

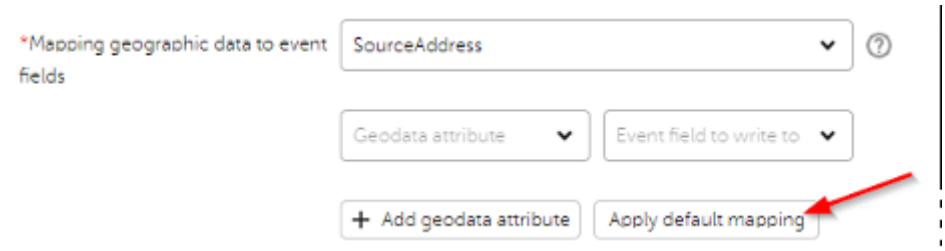


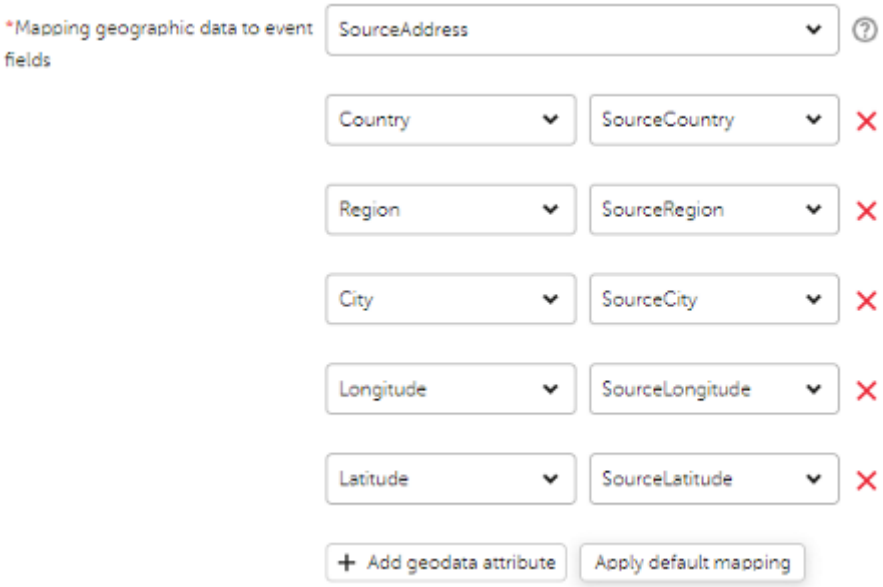
Обогащение GeoIP

- ? ??????? **Ресурсы - Правила Обогащения** ??????? ????? ???????
- ? ???? Source kind ???????? geographic data
- ? ???? Mapping geographic data to event fields ???????? ???? ??????? KUMA, ? ??????? ???????????? ?????? ??? ?????????? ip-?????
- ????? ?? ???????? Geodata attribute ? ?????????????? ???? ??????? KUMA Event field to write to
- ??? GeoIP ????????? ????? ???? ???????, ?? ????? ???????????? ?????



????????????? ?? ????????? ????????, ???? ? ???????? ????????? IP ??????? ???? ?? ????? ??????? SourceAddress, DestinationAddress ? DeviceAddress.
??? ?????? ?????? ????? ? ???????? ????????? ????????????? ?? ????????? ?? ????????.





????? ????? ????????? ??????? ???? ????????? ? ?????????? ? ????? ??????????. ?????? ????, ??? ???????? ??????????? ???????:

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 #12
Created 2023-08-11 14:43:47 UTC by Boris Rzr
Updated 2025-07-07 20:19:46 UTC by Boris Rzr