Cisco FMC

Cisco Firepower Management Center (Cisco FMC) - ???????????????? ????????? ?????????? ? ???????????????? ??????? Cisco Firepower. Cisco FMC ???????????? ??? ?????????, ???????????? ? ????????????? ????????? Firepower Threat Defense (FTD), ??????? ?????????? ?????????? ????????????, ????????????, ????????????????? ? ????????????.

? ?????? ????? ????????????? ???????????? Cisco FMC ???????? ?????????? ??????? ???????????? ? ???????????????? ??????. ??????? FMC ????????? ?????????? ???????? ????????????????, ????????? ????????????, ???????? ?????????? ???????????? ? ????????? ???????, ??? ???????????? ??? ???????? ???????, ????????????? ?????????? ? ???????????? ???????????? ?????? ? ???????? ?????? SIEM.

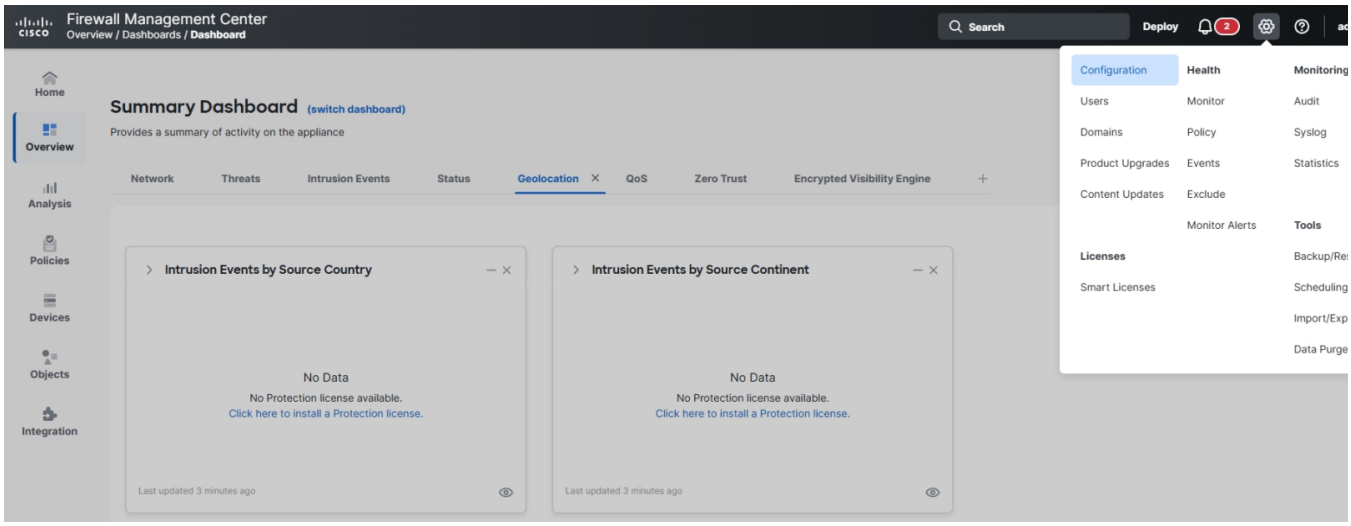
- ????????????: https://www.cisco.com/c/en/us/support/security/defense-center/series.html

Типы собираемых событий:

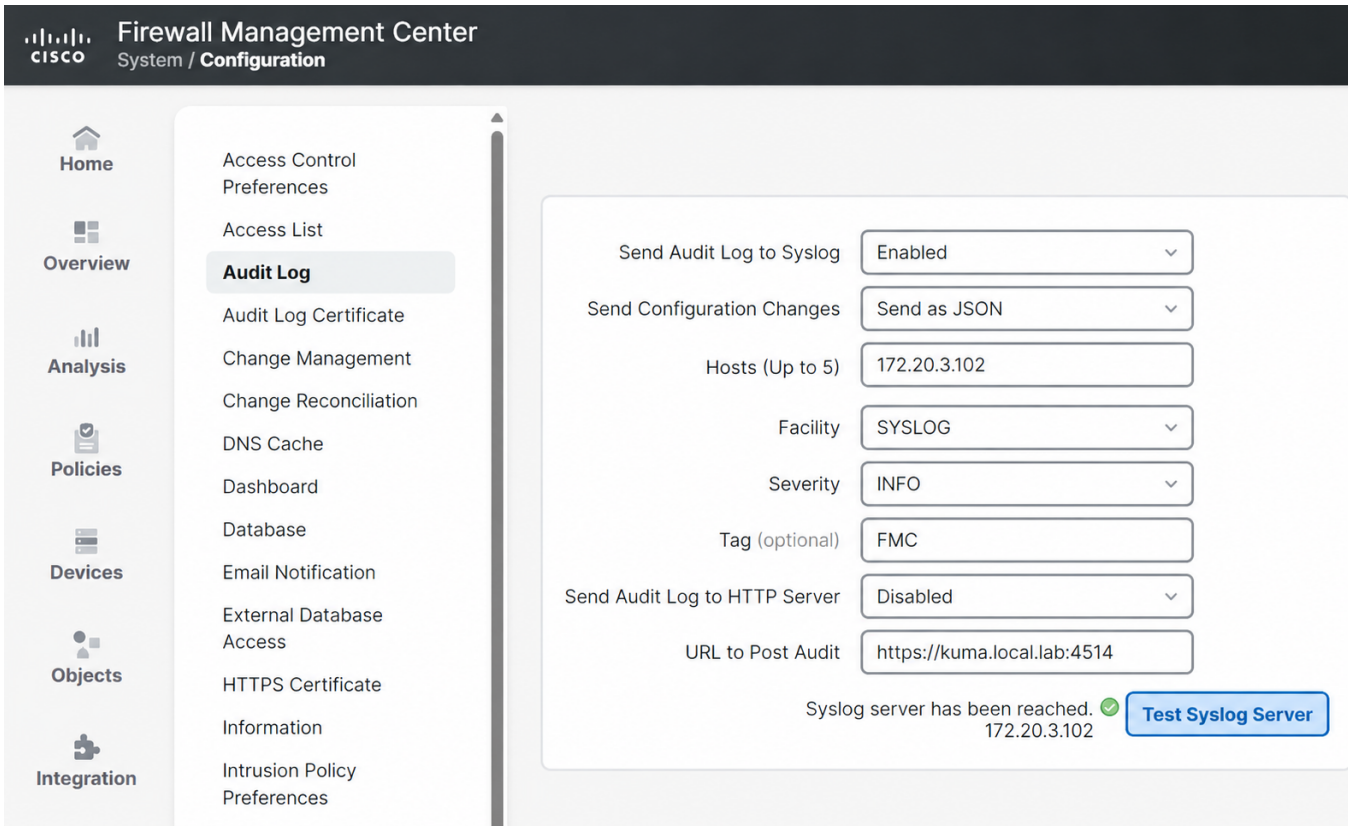
- ????????????? ? ?????????? ?????? ?????????????????
- ???????????????? ???????? ? ?????????? ??????
- ????????? ???????????? ? ???????? ??????????
- ???????? ?????????? ???????????? (??????????, ????????, ????????? ??????????)
- ????????? ? ????????? ??????? ??????????
- ???????, ????????? ? ???????????? ? ???????????? ????????????

Настройка отправки Audit log:

1. ??????? ? ???-??????? **Cisco Firepower Management Center** ??? ??????? ???????, ?????????? ???????????????? ???????.
2. ? ?????? ??????? ???? ?????????? ??????? ?? ?????? **System** (??????????).
3. ? ???????????? ???? ???????? **Configuration**.



4. ? ????? ????? ???? ????????? ? ?????? **Audit Log**.
5. ? ????????? **Send Audit Log to Syslog** ???????? ???????? **Enabled**.
6. ? ????????? **Send Configuration Changes** ???????? ?????? ???????? ??????? (**Send as JSON**).
7. ? ???? **Hosts (Up to 5)** ??????? ????? ??????? ?????? syslog.
8. ? ????????? **Facility** ???????? ???????????? facility ? ???????????? ? ???????? ??????.
9. ? ????????? **Severity** ??????? ??????? ???????? ?????????? ???????, ????????????? **INFO**
10. ? ???? **Tag** ??????? ???????????? ????? ??? ????????????? ????????? ? SIEM, ???????? **FMC**
11. ??????? ?????? **Test Syslog Server**
12. ?????????, ??? ???????????? ????????? ?? ???????? ??????????? syslog-??????? (S*yslog server has been reached*).



Revision #2
Created 2026-05-20 12:46:38 UTC by lerat
Updated 2026-05-20 12:57:38 UTC by lerat