

Cisco FMC

Cisco Firepower Management Center (Cisco FMC) - централизованная платформа управления и администрирования решений Cisco Firepower. Cisco FMC используется для настройки, мониторинга и сопровождения устройств Firepower Threat Defense (FTD), включая управление политиками безопасности, обновлениями, лицензированием и интеграциями.

В рамках задач информационной безопасности Cisco FMC является источником событий технического и административного аудита. События FMC позволяют отслеживать действия администраторов, изменения конфигурации, операции управления устройствами и системные события, что используется для контроля доступа, расследования инцидентов и формирования технического аудита в системах класса SIEM.

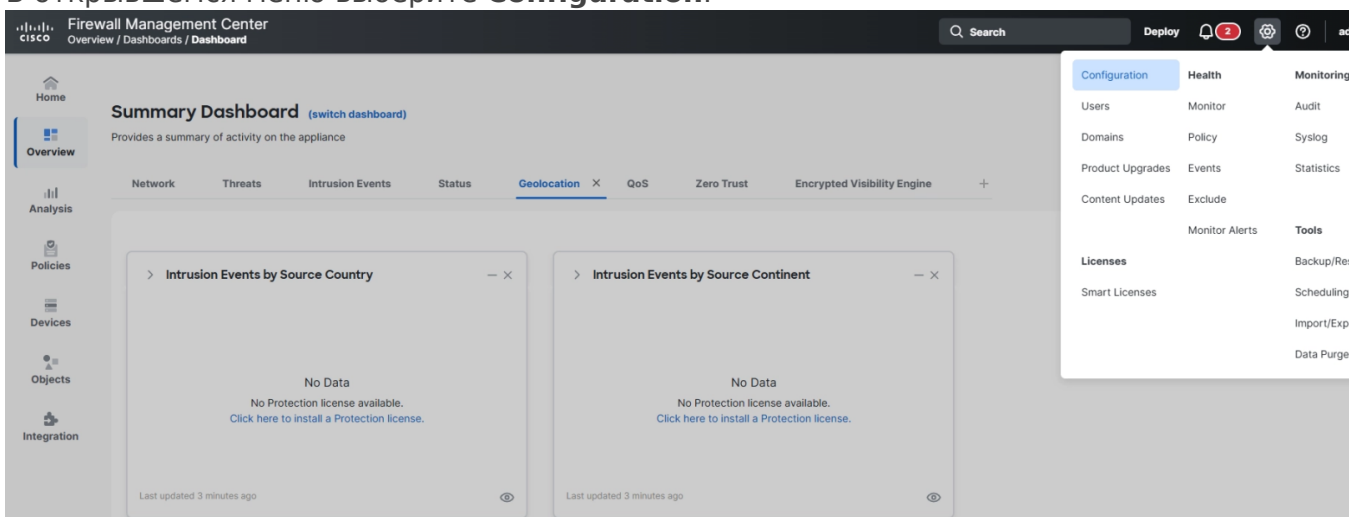
- Документация: <https://www.cisco.com/c/en/us/support/security/defense-center/series.html>

Типы собираемых событий:

- Аутентификация и завершение сессий администраторов
- Административные действия и выполнение команд
- Изменения конфигурации и объектов управления
- Операции управления устройствами (добавление, удаление, изменение параметров)
- Системные и сервисные события управления
- События, связанные с применением и обновлением конфигураций

Настройка отправки Audit log:

1. Войдите в веб-консоль **Cisco Firepower Management Center** под учетной записью, обладающей административными правами.
2. В правом верхнем углу интерфейса нажмите на значок **System** (шестерёнка).
3. В открывшемся меню выберите **Configuration**.



4. В левой части окна перейдите в раздел **Audit Log**.
5. В параметре **Send Audit Log to Syslog** выберите значение **Enabled**.
6. В параметре **Send Configuration Changes** выберите формат отправки событий (**Send as JSON**).
7. В поле **Hosts (Up to 5)** укажите адрес сервера приёма syslog.
8. В параметре **Facility** выберите используемую facility в соответствии с принятой схемой.
9. В параметре **Severity** укажите уровень важности собираемых событий, рекомендуется **INFO**
10. В поле **Tag** укажите произвольную метку для идентификации источника в SIEM, например **FMC**
11. Нажмите кнопку **Test Syslog Server**
12. Убедитесь, что отображается сообщение об успешной доступности syslog-сервера (*Syslog server has been reached*).

The screenshot shows the Cisco Firewall Management Center (FMC) interface. The top header displays the Cisco logo and the text "Firewall Management Center System / Configuration". On the left, a navigation sidebar includes icons and labels for Home, Overview, Analysis, Policies, Devices, Objects, and Integration. A secondary menu lists various configuration areas, with "Audit Log" highlighted. The main content area shows the configuration for the Audit Log, with the following settings:

- Send Audit Log to Syslog: Enabled
- Send Configuration Changes: Send as JSON
- Hosts (Up to 5): 172.20.3.102
- Facility: SYSLOG
- Severity: INFO
- Tag (optional): FMC
- Send Audit Log to HTTP Server: Disabled
- URL to Post Audit: https://kuma.local.lab:4514

At the bottom of the configuration area, a status message reads "Syslog server has been reached." with a green checkmark and the IP address "172.20.3.102". A blue button labeled "Test Syslog Server" is positioned to the right of the message.

Revision #2

Created 2026-05-20 12:46:38 UTC by lerat

Updated 2026-05-20 12:57:38 UTC by lerat