Eltex Distribution Manager (EDM)

Руководство по эксплуатации

Версия ПО 1.2

Содержание

1 Введение

1.1 Аннотация

EDM (Eltex Distribution Manager) реализует механизм распространения правил (сигнатур) на устройства ESR для подсистемы обнаружения и предотвращения сетевых угроз в режиме реального времени (IDS/IPS).

Управление системой осуществляется при помощи CLI- и web-интерфейсов, которые предоставляют удобные и точные инструменты для настройки системы и контроля над распространением контента.

В данном руководстве по эксплуатации изложены назначение, описание возможностей, порядок установки и описание основных сценариев эксплуатации системы.

1.2 Целевая аудитория

Данное руководство пользователя предназначено для технического персонала, выполняющего установку, настройку и предоставление доступа к распространяемому контенту для устройств компании "ЭЛТЕКС". Для развертывания и поддержки системы администратору системы требуется знать основы развертывания ПО в Docker. Для обслуживания и настройки системы администраторам и операторам системы требуется знать основы работы с web-интерфейсами и интерфейсами командной строки.

1.3 Условные обозначения

[ ]	В квадратных скобках в командной строке указываются необязательные параметры, но их ввод предоставляет определенные дополнительные опции.
{ }	В фигурных скобках в командной строке указываются возможные обязательные параметры. Необходимо выбрать один из параметров.
«,» **«-»**	Данные знаки в описании команды используются для указания диапазонов.
«|»	Данный знак в описании команды обозначает «или».
Полужирный курсив	Полужирным шрифтом выделены примечания, предупреждения или информация.
<Полужирный курсив>	Полужирным курсивом в угловых скобках указываются названия клавиш на клавиатуре.
`Текст в рамке`	В рамках с текстом указаны примеры и результаты выполнения команд.

1.4 Примечания и предупреждения

Примечания содержат важную информацию, советы или рекомендации по использованию и настройке системы.

Предупреждения информируют пользователя о ситуациях, которые могут нанести вред системе, привести к некорректной работе системы или потере данных.

Информация содержит справочные данные об использовании системы.

2 Описание системы

2.1 Назначение системы

Eltex Distribution Manager (далее EDM) – это централизованная система передачи лицензируемого контента на устройства производства компании "ЭЛТЕКС".

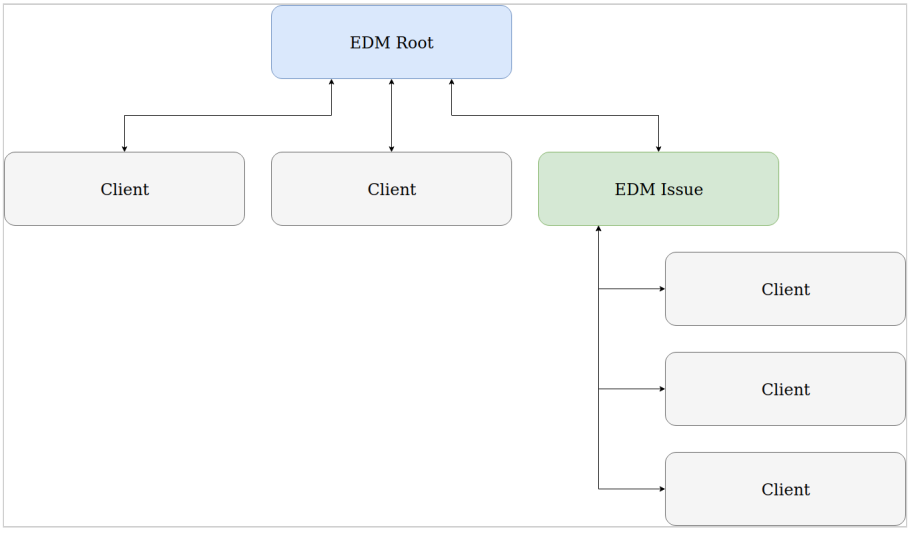
На данный момент EDM распространяет правила анализа трафика для системы IDS/IPS, функционирующей на маршрутизаторах ESR. Предоставляются правила от следующих источников:

- правила "Kaspersky SafeStream II" от компании "Лаборатория Касперского";
- правила "PT Expert Security Center" от компании "Positive Technologies".

2.2 Состав компонентов системы

EDM состоит из нескольких компонентов, взаимодействующих между собой:

- EDM Root – корневой сервис EDM, работающий на стороне компании "ЭЛТЕКС". В его задачи входят взаимодействие с клиентскими устройствами и пользовательскими сервисами EDM и передача на них запрошенного в рамках лицензий контента.
- EDM Issue – пользовательский сервис EDM, работающий на стороне клиента. В его задачи входят взаимодействие с EDM Root, кэширование распространяемого с EDM Root контента и обслуживание подключающихся к нему устройств на сети клиента.
- Клиентское устройство – устройство, которое является потребителем распространяемого EDM-контента. На данный момент к таким устройствам относится семейство сервисных маршрутизаторов ESR.



2.3 Лицензирование системы

Доступ к контенту осуществляется на основании лицензии, приобретаемой в коммерческим отделе компании "ЭЛТЕКС". Лицензии могут быть следующих типов:

- Индивидуальная лицензия – лицензия, привязанная к конкретному устройству. Устройство, для которого выписана данная лицензия, должно обращаться за лицензируемым контентом непосредственно на EDM Root.
- Групповая лицензия – лицензия, в которой разрешены определенные модели устройств компании "ЭЛТЕКС" в определенных количествах. В этом случае на стороне клиента должен быть развернут EDM Issue, который будет обращаться на EDM Root и получать разрешенный согласно лицензии контент, чтобы затем отдавать его на конечные устройства.

⚠ Настройка подключения сервисных маршрутизаторов ESR к EDM Root и EDM Issue однотипная и описана в соответствующем разделе документации ESR.

2.4 Функциональные возможности

Данная система дает возможность осуществлять:

- Распространение лицензируемого контента на устройства компании "ЭЛТЕКС" по защищенному протоколу;
- Администрирование EDM Issue на основе ролей пользователей;
- Создание на EDM Issue пользовательских категорий распространяемых правил подсистемы IDS/IPS, функционирующей на маршрутизаторах ESR;
- Ограничение доступа клиентских устройств к EDM Issue по IP-адресам.

Управление EDM Issue может осуществляться с помощью web-интерфейса и интерфейса командной строки. Более развернуто данные интерфейсы описаны в соответствующем разделе документации.

2.5 Требования к оборудованию

2.5.1 Требования к клиентским устройствам

Для подключения к системе EDM клиентские устройства должны отвечать следующим требованиям:

- Сервисные маршрутизаторы ESR:
  - версия ПО: 1.13.0 и выше;
  - сетевая связанность с EDM Root/EDM Issue по протоколу IPv4.

2.5.2 Требования к серверной части для запуска EDM Issue

Минимальная конфигурация сервера для запуска, стабильной работы системы и обслуживания около 100 клиентских устройств:

- операционная система Linux с поддержкой Docker (рекомендуется Ubuntu Server 18.04 и выше);
- объем оперативной памяти от 8 ГБ;
- процессор, поддерживающий виртуализацию и имеющий от 4 ядер;
- от 40 ГБ свободного места на жестком диске;
- наличие сетевого интерфейса 1 Гбит/с.

Требования к ресурсам нелинейно зависят от количества устройств. Система может быть запущена в различных конфигурациях. Также система имеет возможности горизонтального масштабирования, поэтому параметры должны рассчитываться, исходя из индивидуального проекта.

2.5.3 Требования к рабочему месту оператора EDM Issue

Оператор взаимодействует с системой через web-интерфейс или интерфейс командной строки, поэтому для работы ему потребуется компьютер, отвечающий следующим требованиям:

- объем оперативной памяти от 4 ГБ;
- процессор, имеющий от 2 ядер;
- операционная система Windows, Linux или MacOS;
- актуальная версия браузера Google Chrome, Mozilla Firefox (корректная работа с другими браузерами не гарантируется);
- монитор с разрешением FullHD, клавиатура, мышь.

2.6 Требования к персоналу

При запуске и эксплуатации EDM Issue администратор должен обладать навыками развертывания, мониторинга и поддержки работы сервисов, запущенных в Docker. При подключении устройств ESR к EDM Root и EDM Issue оператор должен обладать знаниями и навыками по работе с настраиваемыми устройствами.

2.6.1 Требования к администраторам EDM Issue

Для администрирования EDM Issue достаточно знать и уметь работать со следующими технологиями:

- Linux:
  - уверенное пользование терминалом;
  - понимание работы сети;
  - установка и администрирование сервисов в Docker;
- Docker:
  - понимание принципов работы технологии;
  - навыки работы с контейнерами (запуск, остановка, мониторинг);
  - использование Docker Compose.

2.6.2 Требования к операторам EDM Issue

Все операции в EDM Issue выполняются через web-интерфейс или интерфейс командной строки. От оператора EDM Issue требуется:

- понимание принципов распространения контента в системе EDM;
- понимание особенностей работы клиентских устройств ESR, подключающихся к EDM Issue;
- изучение инструкций по работе с пользовательскими интерфейсами EDM Issue.

3 Инструкция по установке EDM Issue

3.1 Предварительная установка дополнительного ПО на сервере

Для запуска EDM Issue на сервере требуется произвести установку дополнительного ПО:

1. Установить последнюю стабильную версию Docker (ссылка на инструкцию на официальном сайте).
2. Установить последнюю стабильную версию Docker Compose (ссылка на инструкцию на официальном сайте).

> Дальнейшие инструкции предполагают, что пользователь обладает правами взаимодействия с Docker и запуска Docker Compose без повышения привилегий командой sudo. Для формирования таких прав у текущего пользователя рекомендуется изучить следующий раздел официальной документации Docker.

3.2 Получение файлов, необходимых для запуска EDM Issue

Набор файлов, необходимых для запуска EDM Issue, находится в архиве: edm-issue.zip.

Структура архива

```
.
├── .env
├── data
│   ├── edmi-db
│   │   ├── init-db
│   │   │   └── init-db.sql
│   │   └── postgresql.conf
│   └── edmi-web-ui
│       └── ssl
│           ├── autocreated-cert.crt
│           └── autocreated-cert.key
├── docker-compose-cli.yml
├── docker-compose.yml
└── monitoring
    ├── .env
    ├── docker-compose.yml
    ├── grafana
    │   └── provisioning
    │       ├── dashboards
    │       │   ├── dashboard.yml
    │       │   ├── edm_alert_metrics.json
    │       │   └── edm_monitor.json
    │       ├── datasources
    │       │   └── datasource.yml
    │       └── notifiers
    │           ├── email.yml
    │           └── telegram.yml
    ├── influxdb
    │   └── influx_init.iql
    ├── prometheus
    │   └── prometheus.yml
    └── telegraf
        └── telegraf.conf
```

Архив должен быть загружен на целевой сервер и распакован в любой удобной для дальнейшей эксплуатации директории.

ⓘ У администраторов EDM Issue для запуска, остановки и редактирования конфигурации EDM Issue должны быть права на чтение и запись распакованных файлов.

3.3 Запуск EDM Issue

Для запуска EDM Issue требуется произвести следующие шаги:

1. Перейти в директорию с содержимым распакованного архива.
2. Убедиться, что в файле .env прописан "EDM_TAG" версии 1.2.

Заполнение файла .env

```
# EDM version
EDM_TAG=1.2
```

Прочие переменные окружения, которые можно описать в .env файле, описаны в разделе Управление настройками EDM Issue.

3. Запустить EDM Issue командой:

Команда запуска EDM Issue

```
docker compose up -d
```

Пример вывода команды при первом запуске EDM Issue на хосте

```
edm@edm:~/issue$ docker compose up -d
[+] Running 48/48
 ⠿ edmi-server Pulled
22.1s
   ⠿ fb7197b7a03c Pull complete
19.4s
   ⠿ a9ceb4e633c7 Pull complete
20.2s
   ⠿ fd80b0cb7230 Pull complete
20.3s
   ⠿ 8d120444f8b8 Pull complete
20.6s
   ⠿ 228d7167f27f Pull complete
21.0s
   ⠿ c71d47816735 Pull complete
21.3s
 ⠿ edmi-web-ui Pulled
19.5s
   ⠿ 9aae54b2144e Pull complete
15.0s
   ⠿ deb02d0f047e Pull complete
17.1s
   ⠿ faa46c06ae12 Pull complete
17.2s
   ⠿ 8bbe2a6a37c5 Pull complete
17.3s
   ⠿ f9b897942de0 Pull complete
17.4s
   ⠿ 7141e8eb7387 Pull complete
17.6s
   ⠿ c0ccde5fa165 Pull complete
17.7s
   ⠿ 8203d153ddc8 Pull complete
17.8s
   ⠿ ef58636d9683 Pull complete
18.0s
   ⠿ 45133997f00b Pull complete
18.1s
   ⠿ 0db6c69958e5 Pull complete
18.2s
   ⠿ b01475f50325 Pull complete
18.4s
 ⠿ edmi-init Pulled
21.9s
   ⠿ e7c96db7181b Pull complete
1.0s
   ⠿ f910a506b6cb Pull complete
1.0s
   ⠿ c2274a1a0e27 Pull complete
19.1s
   ⠿ b9df22590b50 Pull complete
19.5s
   ⠿ 2a68cad3fe5b Pull complete
20.0s
```

```
   ⠿ 980ec4e4c502 Pull complete
20.2s
   ⠿ 5b4b8f5271d4 Pull complete
20.4s
   ⠿ 19bd75f7d7d1 Pull complete
20.7s
   ⠿ 3c16d3d230bc Pull complete
21.0s
 ⠿ edmi-loader Pulled
22.4s
   ⠿ 927ebe035398 Pull complete
20.6s
   ⠿ c3e94fb116ad Pull complete
21.2s
 ⠿ edmi-db Pulled
26.1s
   ⠿ 45b42c59be33 Pull complete
10.2s
   ⠿ 40adec129f1a Pull complete
10.5s
   ⠿ b4c431d00c78 Pull complete
10.6s
   ⠿ 2696974e2815 Pull complete
10.9s
   ⠿ 564b77596399 Pull complete
13.1s
   ⠿ 5044045cf6f2 Pull complete
13.2s
   ⠿ d736e67e6ac3 Pull complete
13.3s
   ⠿ 390c1c9a5ae4 Pull complete
13.5s
   ⠿ fbb0dc403c2f Pull complete
24.6s
   ⠿ 1b9ba7c0986e Pull complete
24.7s
   ⠿ b6c9d2fab5c1 Pull complete
24.8s
   ⠿ 19f04f19f5bb Pull complete
24.9s
   ⠿ 0a195310fe0b Pull complete
25.1s
   ⠿ 1a99568d6863 Pull complete
25.2s
[+] Running 7/7
 ⠿ Network edmi-network             Created
0.0s
 ⠿ Network edmi-monitoring-network  Created
0.0s
 ⠿ Container edmi-db                Started
11.5s
 ⠿ Container edmi-init              Started
3.8s
 ⠿ Container edmi-server            Started
4.3s
 ⠿ Container edmi-loader            Started
4.3s
 ⠿ Container edmi-web-ui            Started
6.1s
```

```
edm@edm:~/issue$
```

4. Убедиться, что все контейнеры EDM Issue успешно запустились, используя команду:

Команда проверки статуса контейнеров EDM Issue

```
docker compose ps
```

Пример вывода команды при успешном запуске всех контейнеров EDM Issue

```
edm@edm:~/issue$ docker compose ps
NAME                COMMAND                  SERVICE             STATUS              PORTS
edmi-db             "docker-entrypoint.s…"   edmi-db             running (healthy)   5432/
tcp
edmi-init           "/bin/sh -c '/usr/lo…"   edmi-init           running (healthy)
edmi-loader         "/bin/sh -e /usr/loc…"   edmi-loader         running (healthy)   8098/
tcp
edmi-server         "/bin/sh -e /usr/loc…"   edmi-server         running (healthy)   0.0.
0.0:8098->8098/tcp, :::8098->8098/tcp
edmi-web-ui         "/usr/local/bin/entr…"   edmi-web-ui         running (healthy)   0.0.
0.0:8091->80/tcp, :::8091->80/tcp
edm@edm:~/issue$
```

Теперь с EDM Issue можно взаимодействовать через web-интерфейс и через интерфейс командной строки.

После первого запуска EDM Issue в текущем каталоге появятся три новых директории:

- db – содержит файлы базы данных, используемой в EDM Issue;
- config – содержит файлы конфигурации для сервисов EDM Issue;
- logs – содержит логи сервисов EDM Issue.

3.4 Остановка EDM Issue

Для остановки EDM Issue требуется произвести следующие шаги:

1. Перейти в директорию с файлами работающего EDM Issue.
2. Выполнить команду:

Команда остановки EDM Issue

```
docker compose down
```

Пример вывода команды при успешной остановке всех контейнеров EDM Issue

```
edm@edm:~/issue$ docker compose down
[+] Running 7/7
 ⠿ Container edmi-loader            Removed
10.9s
 ⠿ Container edmi-web-ui            Removed
1.2s
 ⠿ Container edmi-server            Removed
11.1s
 ⠿ Container edmi-init              Removed
10.8s
 ⠿ Container edmi-db                Removed
0.9s
 ⠿ Network edmi-network             Removed
0.1s
 ⠿ Network edmi-monitoring-network  Removed
edm@edm:~/issue$
```

EDM Issue теперь остановлен. Для повторного запуска остановленного EDM Issue нужно выполнить команду "docker compose up -d".

3.5 Удаление EDM Issue

Для удаления EDM Issue требуется произвести следующие шаги:

1. Перейти в директорию с файлами работающего EDM Issue.
2. Выполнить команду:

Команда для удаления EDM Issue с хоста

```
docker compose down --remove-orphans --rmi all --volumes
```

Пример вывода команды при успешной остановке EDM с удалением данных в Docker

```
edm@edm:~/issue$docker compose down --remove-orphans --rmi all --volumes
[+] Running 6/6
 ⠿ Volume issue_edmi-healthcheck              Removed
0.0s
 ⠿ Image lab3.eltex.loc:5000/edmi-web-ui:1.2  Removed
0.1s
 ⠿ Image lab3.eltex.loc:5000/postgres:12.5    Removed
0.6s
 ⠿ Image lab3.eltex.loc:5000/edmi-server:1.2  Removed
0.2s
 ⠿ Image lab3.eltex.loc:5000/edmi-init:1.2    Removed
0.4s
 ⠿ Image lab3.eltex.loc:5000/edmi-loader:1.2  Removed
edm@edm:~/issue$
```

В результате выполнения команды EDM Issue будет остановлен. В случае если на момент выполнения команды он еще функционировал, будут удалены служебные сети, хранилища и образы в Docker.

3. Удалить оставшиеся от EDM Issue каталоги и служебные файлы:

Удаление оставшихся служебных файлов

```
sudo rm -rf .env config  data  db  docker-compose-cli.yml  docker-compose.yml  log
monitoring
```

Теперь EDM Issue полностью удален с хоста.

4 Управление лицензией EDM

EDM Issue функционирует на базе групповой лицензии EDM, ориентированной на предоставление доступа к распространяемому контенту для большого количества устройств разных моделей. Администратор EDM Issue со своей стороны может:

- просматривать информацию о лицензии EDM;
- запустить процесс синхронизации информации о лицензии EDM с EDM Root вручную.

4.1 Указание ключа лицензии EDM

После запуска EDM Issue администратор обязан указать ключ лицензии EDM, полученный от коммерческого отдела компании "ЭЛТЕКС", в настройках EDM:

Указание ключа лицензии в .env файле

```
edmi-settings> set --param licenseKey --value TEST-KEY
OK
edmi-settings>
```

Для установки ключа лицензии через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Настройки".
3. Прописать ключ лицензии в параметре "Ключ лицензии EDM".

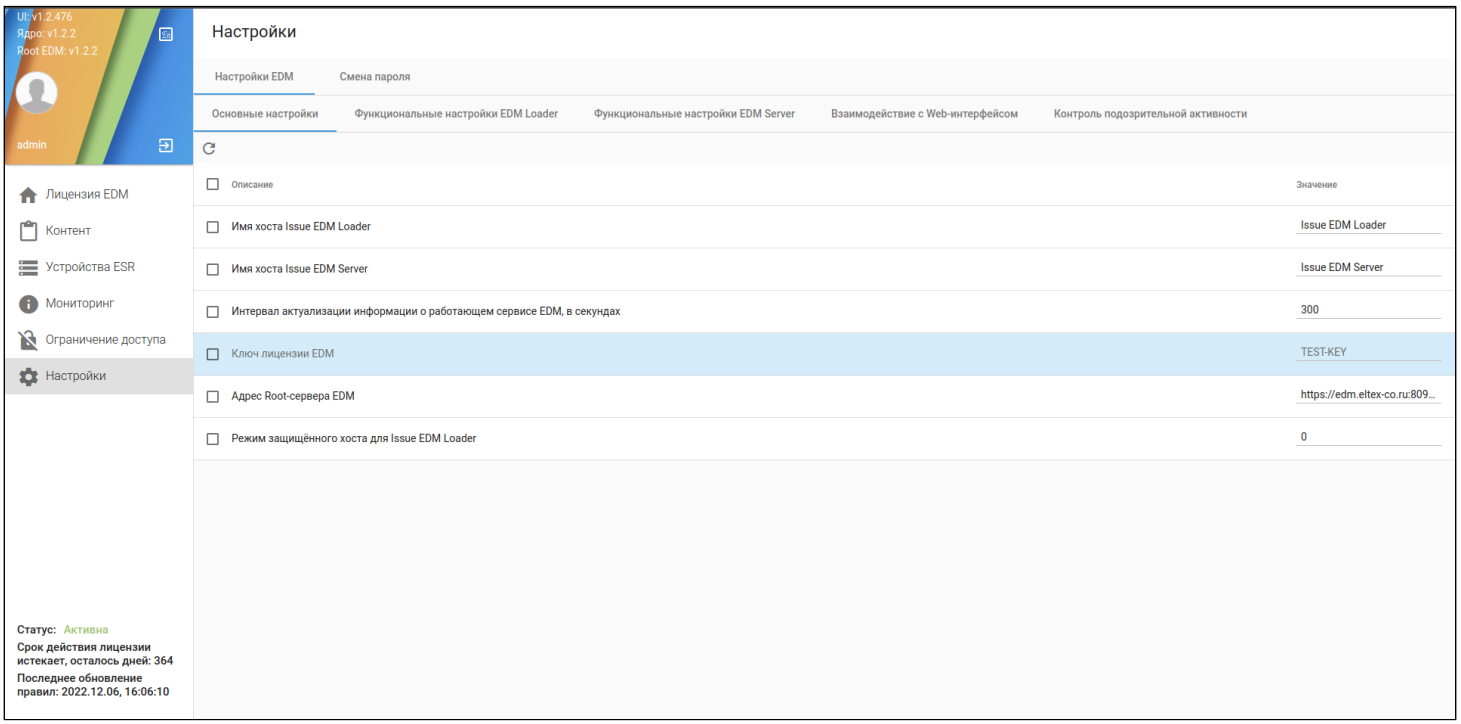


Рисунок 1 – Установка ключа лицензии через web-интерфейс

После установки данного параметра EDM Issue будет обращаться на EDM Root именно по этому ключу. Смену ключа лицензии EDM можно осуществить через EDM CLI или web-интерфейс.

Смена ключа лицензии через EDM CLI:

1. Запустить EDM CLI.
2. Перейти в раздел "settings".
3. Установить в качестве значения параметра licenseKey новый ключ.

Смена ключа лицензии через web-интерфейс:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Настройки".
3. Прописать новый ключ лицензии в параметре "Ключ лицензии EDM".

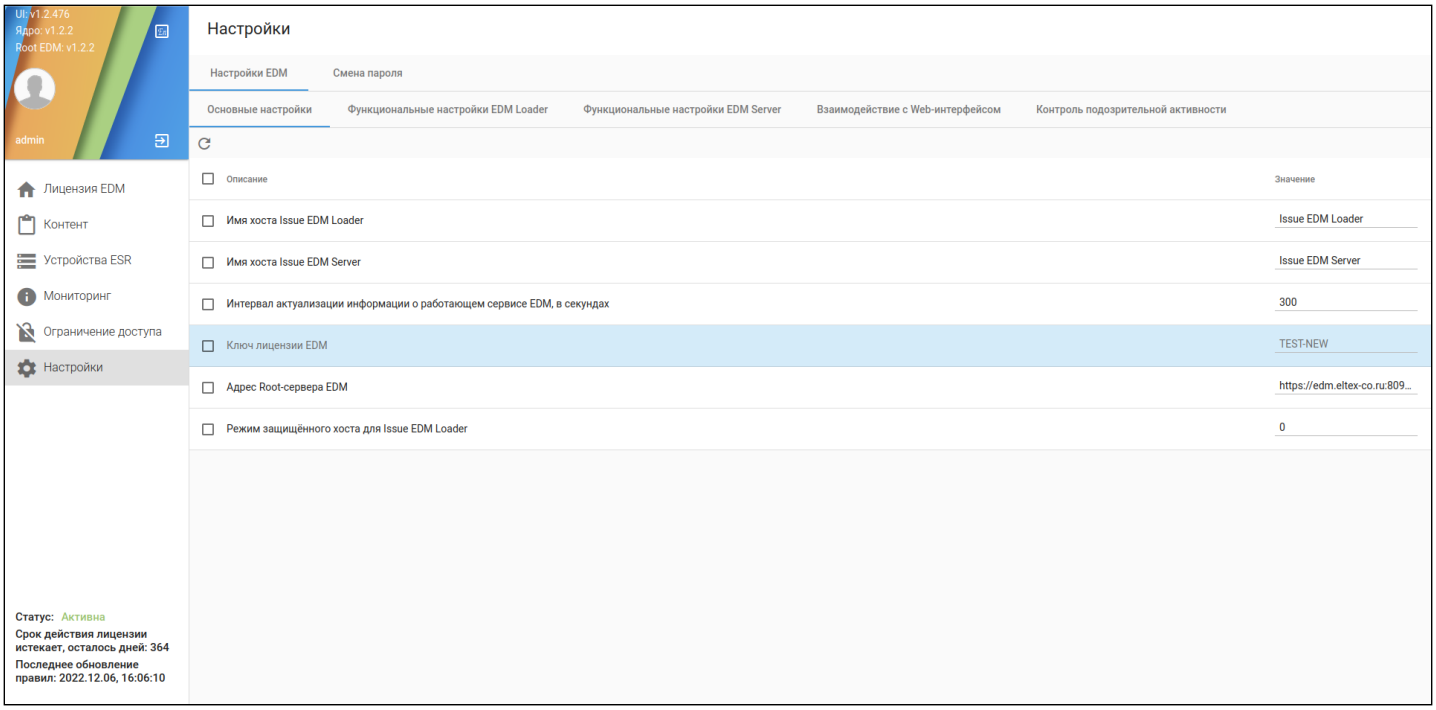


Рисунок 2 – Смена ключа лицензии через web-интерфейс

4.2 Просмотр информации о лицензии EDM

Для просмотра информации о лицензии EDM через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "license".
3. Ввести команду "show license".

Пример вывода информации о лицензии EDM в EDM CLI

```
edmi-license> show license
License key: TEST-KEY
Contract: Eltex
Organization: Eltex
Registered: 2022-11-23 13:16:03
Updated: 2022-11-23 13:16:33
Devices changed: 2022-11-25 17:20:30
Valid from: 2022-11-23 13:16:03
Expiry: 2023-11-23 13:16:03
Status: active
IPS access:

    Supported vendors:


            Vendor: kaspersky

            Supported files:


                    Name: MobileBotnetCAndCDF
                    EN description: set of URLs with context that cover mobile botnet C&C
servers
                    RU description: набор URL-адресов с контекстной информацией для
выявления командных серверов ботнетов, использующих мобильные устройства
                    Item count: 11327



                    Name: BotnetCAndCURLsDF
                    EN description: a set of URLs with context that cover desktop botnet
C&C servers and related malicious objects
                    RU description: набор URL-адресов командных серверов ботнетов и
связанных с ними вредоносных объектов
                    Item count: 10800



                    Name: RansomwareURLsDF
                    EN description: a set of URLs, domains, and hosts with context that
cover ransomware links and websites
                    RU description: набор URL-адресов, доменов и хостов, используемых для
распространения шифровальщиков
                    Item count: 8000



                    Name: IoTURLsDF
                    EN description: a set of URLs with context covering malware that
infects IoT (Internet of Things) devices
                    RU description: набор URL-адресов веб-сайтов, используемых для
размещения вредоносных программ, заражающих устройства IoT (Internet of Things)
                    Item count: 8000
```

```
                    Name: PhishingURLsDF
                    EN description: a set of URLs with context that cover phishing
websites and web pages
                    RU description: набор URL-адресов фишинговых сайтов и веб-страниц
                    Item count: 10213



                    Name: MaliciousHashDF
                    EN description: a set of hashes of malicious objects
                    RU description: набор файловых хэшей, охватывающий наиболее опасные и
распространенные, а также самые новые вредоносные программы
                    Item count: 1



                    Name: IPReputationDF
                    EN description: set of IP addresses with context that cover different
categories of suspicious and malicious hosts
                    RU description: набор IP-адресов с контекстной информацией о
подозрительных и вредоносных узлах
                    Item count: 8000



                    Name: MaliciousURLsDF
                    EN description: set of URLs with context that cover malicious websites
and web pages
                    RU description: набор URL-адресов, соответствующих опасным ссылкам и
веб-сайтам
                    Item count: 11530



                    Name: MobileMaliciousHashDF
                    EN description: a set of hashes of malicious objects for mobile
platforms
                    RU description: набор файловых хэшей для обнаружения вредоносных
объектов, заражающих мобильные устройства
                    Item count: 1




    Unsupported vendors:


            Vendor: ptsecurity

            Unsupported files:


                    Name: malware
                    EN description: a set of signatures for detection of malware related
activities
                    RU description: набор сигнатур для обнаружения активности вредоносного
программного обеспечения
```

```
                    Item count: 2921



                    Name: attack
                    EN description: a set of signatures for detection of attacks related
activities
                    RU description: набор сигнатур для обнаружения активности, проявляемой
во время различных атак
                    Item count: 1020



                    Name: remote
                    EN description: a set of signatures for detection of remote control
activities (which may be potentially malicious)
                    RU description: набор сигнатур для обнаружения активности программного
обеспечения для удаленного управления (возможно вредоносного)
                    Item count: 667



                    Name: tools
                    EN description: a set of signatures for detection of software used by
adversaries
                    RU description: набор сигнатур для обнаружения активности программного
обеспечения, применяемого злоумышленниками
                    Item count: 827



                    Name: info
                    EN description: a set of signatures informing about suspicious network
activity, which may indirectly relate to adversary operations
                    RU description: набор сигнатур, информирующий о подозрительной
активности в сети, которая может быть косвенно связана с действиями злоумышленника
                    Item count: 1150




Devices limits:

    Supported models:


            Model: ESR-200
            Limit: 2
            Used: 1
            Free: 1



            Model: ESR-100
            Limit: 40
            Used: 1
            Free: 39
```

```
edmi-license>
```

Для просмотра информации о лицензии EDM через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Лицензия EDM".
   a. В подразделе "Информация" отображаются основные данные о текущей лицензии (рисунок 3).
   b. В подразделе "Устройства" показан список поддерживаемых ESR по каждой модели в рамках текущей лицензии (рисунок 4).
   c. В подразделе "Подписки" содержится информация о распространяемом контенте (рисунок 5).

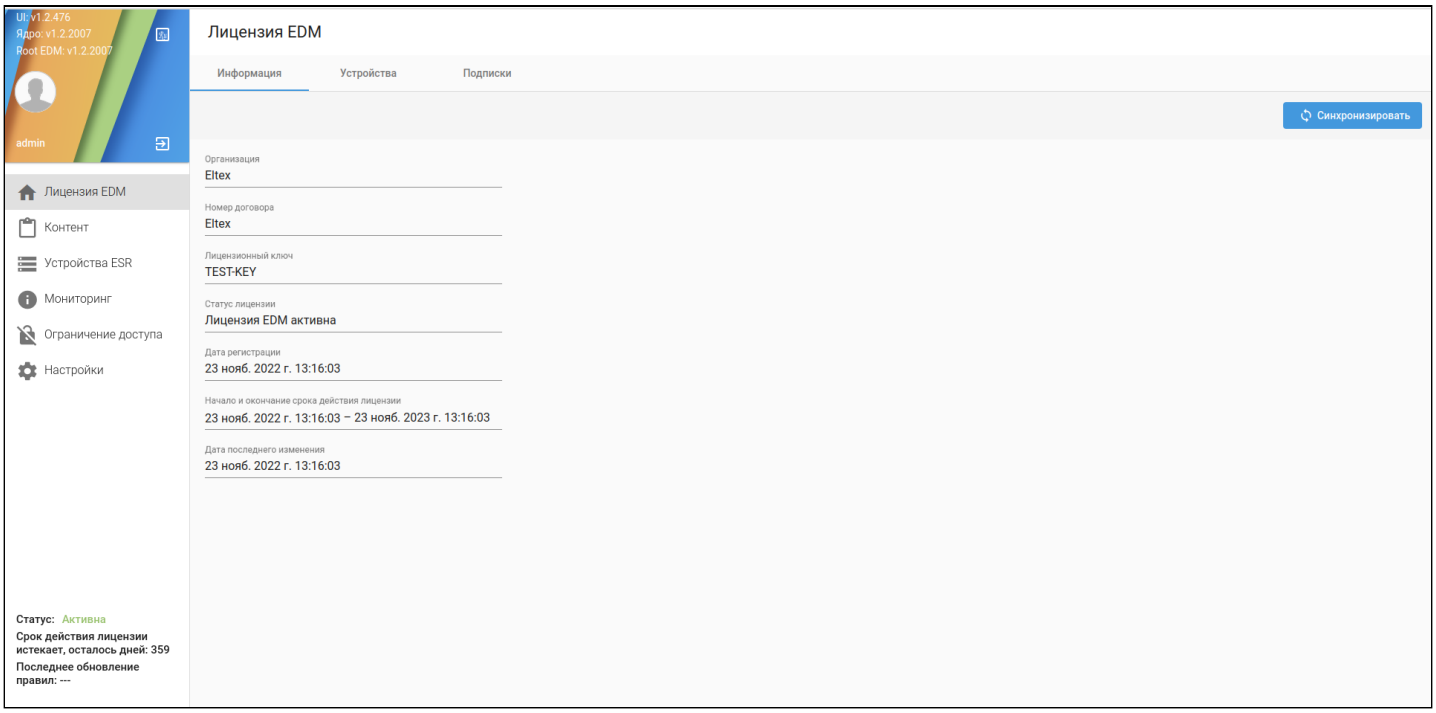


Рисунок 3 – Получение основной информации о лицензии EDM в подразделе "Информация" раздела "Лицензия EDM"

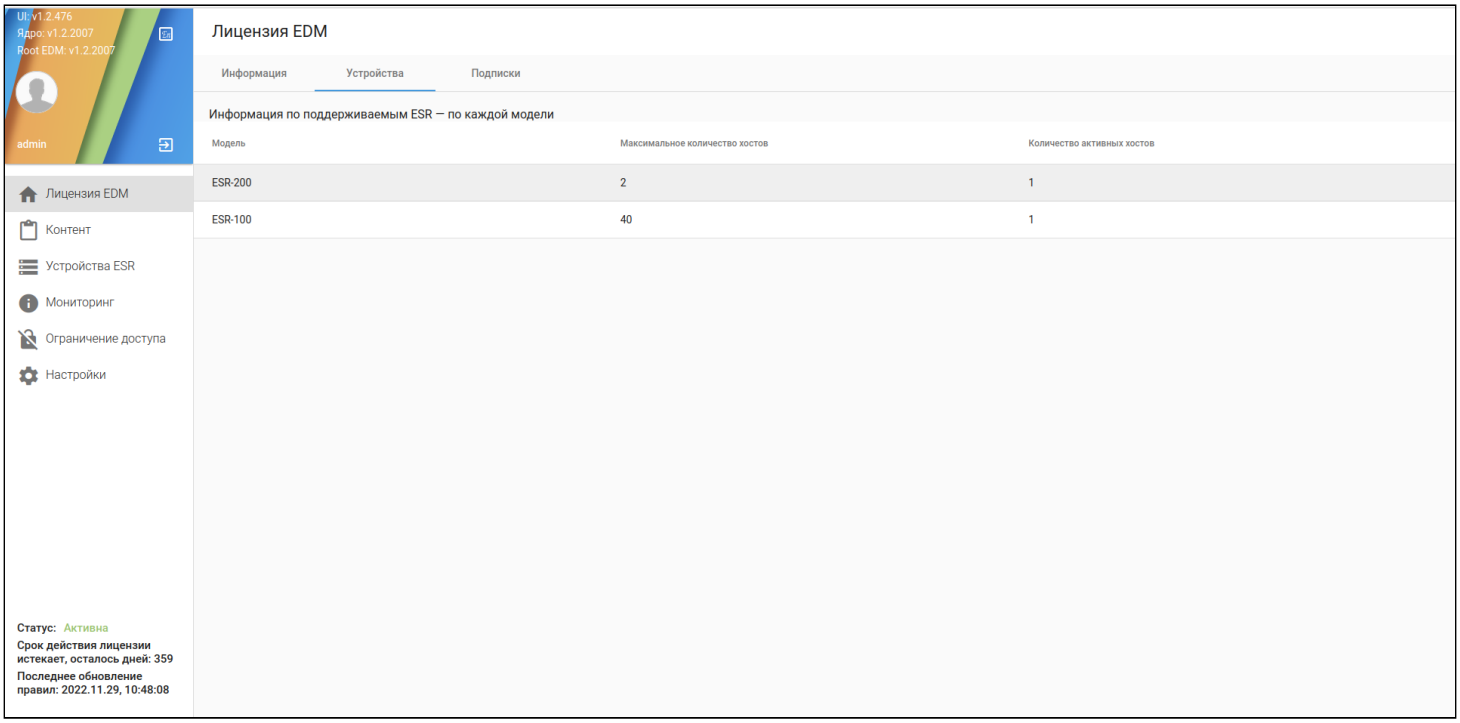


Рисунок 4 – Получение информации о списке поддерживаемых ESR в подразделе "Устройства" раздела "Лицензия EDM"

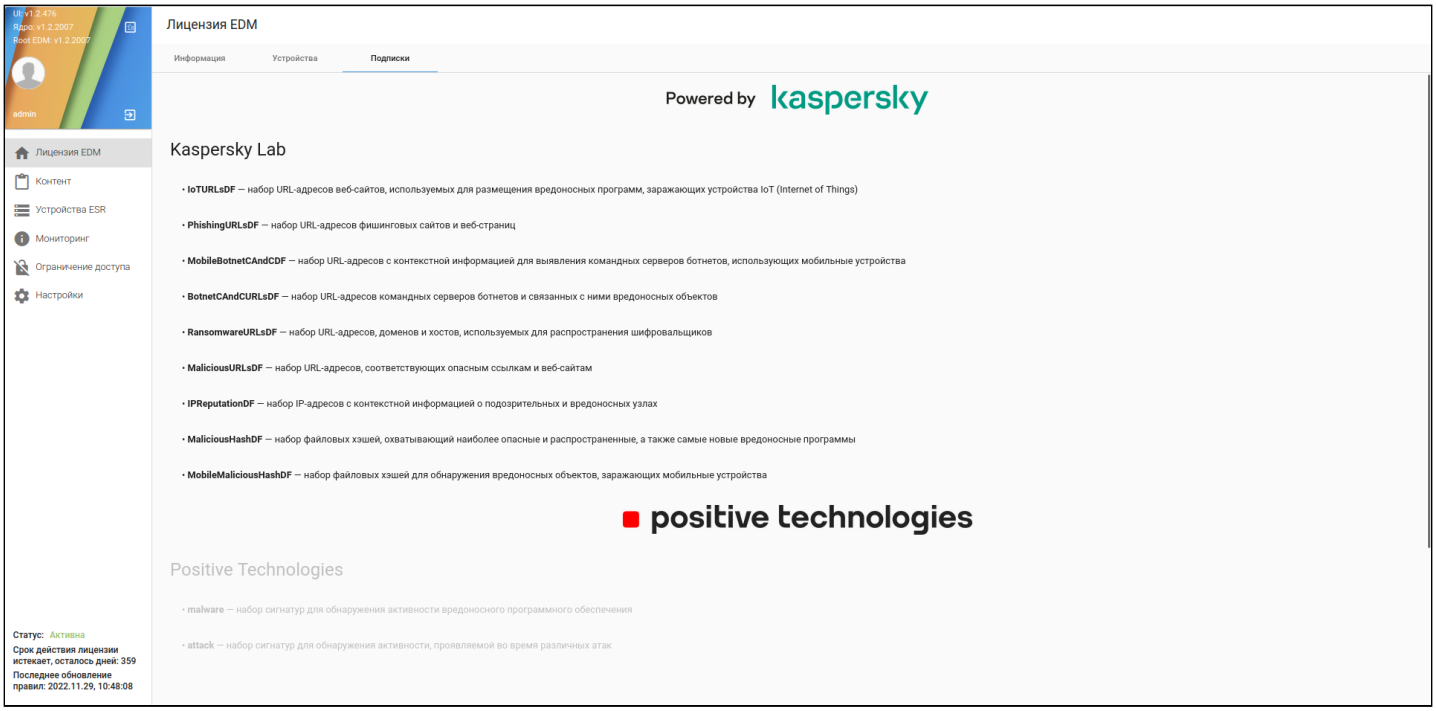


Рисунок 5 – Получение информации о распространяемом контенте в подразделе "Подписки" раздела "Лицензия EDM"

4.3 Запуск процесса синхронизации информации о лицензии EDM с EDM Root вручную

EDM Issue синхронизирует информацию о лицензии EDM с EDM Root раз в минуту. Однако запустить синхронизацию можно и вручную.

Для запуска ручной синхронизации информации о лицензии EDM в EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "license".
3. Ввести команду "load license".

Пример запуска ручной синхронизации информации о лицензии EDM в EDM CLI

```
edmi-license> load license
Upload license data command 1 is created. Please wait...
edmi-license> Upload license data command 1 is done!

edmi-license>
```

Для запуска ручной синхронизации информации о лицензии EDM в web-интерфейсе требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Лицензия EDM".
3. Нажать кнопку "Синхронизировать" в правой верхней части web-интерфейса. После нажатия кнопка станет неактивной на время процесса синхронизации, а по окончании – в правом верхнем углу появится всплывающее оповещение о результатах процесса синхронизации.

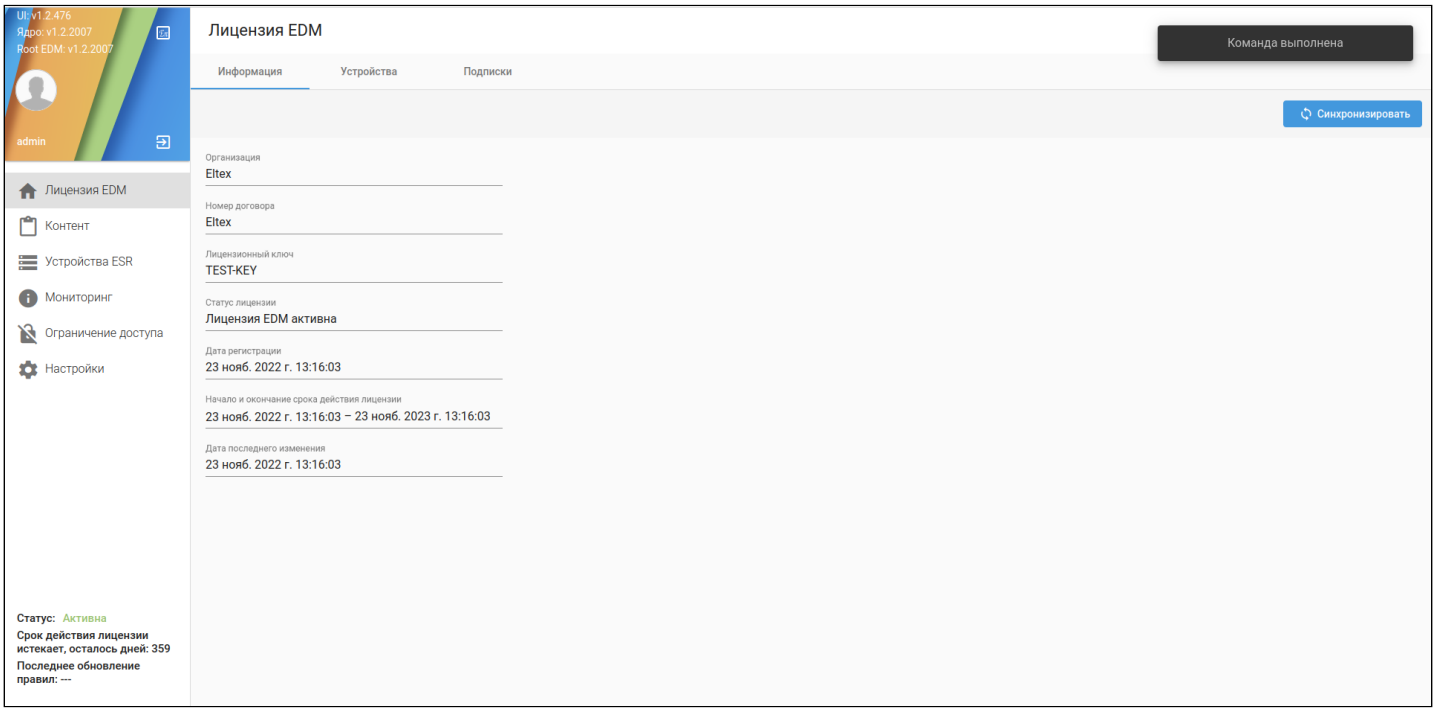


Рисунок 6 – Успешно завершенная синхронизация информации о лицензии EDM через web-интерфейс EDM Issue

5 Управление загружаемыми IDS/IPS-правилами

EDM Issue предоставляет возможность загружать и раздавать на клиентские устройства различный контент: как загружаемый с EDM Root согласно лицензии EDM, так и настроенный пользователем. На данный момент EDM Issue позволяет распространять только правила анализа трафика для системы IDS/IPS, функционирующей на маршрутизаторах ESR.

Администратор EDM Issue со своей стороны может:

- просматривать информацию о поддерживаемых лицензируемых и пользовательских поставщиках IDS/IPS-правил;
- просматривать информацию о поддерживаемых в поставщиках IDS/IPS-правил категориях IDS/IPS-правил;
- создавать пользовательских поставщиков IDS/IPS-правил и категории правил внутри них;
- редактировать пользовательских поставщиков IDS/IPS-правил;
- редактировать категории IDS/IPS-правил внутри пользовательских поставщиков IDS/IPS-правил;
- удалять категории IDS/IPS-правил внутри пользовательских поставщиков IDS/IPS-правил;
- удалять пользовательских поставщиков IDS/IPS-правил;
- настраивать интервал автоматической загрузки актуальных лицензируемых и пользовательских IDS/IPS-правил;
- запускать процесс загрузки актуальных лицензируемых IDS/IPS-правил с EDM Root вручную;
- запускать процесс загрузки актуальных пользовательских IDS/IPS-правил с внешних источников вручную.

5.1 Просмотр информации о поставщиках IDS/IPS-правил

Для просмотра информации о поставщиках IDS/IPS-правил через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "ips".
3. Ввести команду "show vendors".

Пример вывода информации о поставщиках IDS/IPS-правил в EDM CLI

```
edmi-ips> show vendors
Licensed vendors:

1. Name: kaspersky
Title: Kaspersky Lab
Licensed: true
gid: 11

Other sources:

1. Name: suricata
Title: suricata
Licensed: false
URL: https://rules.emergingthreats.net/open/suricata-4.0/rules/
gid: 101

edmi-ips>
```

Для просмотра информации о поставщиках IDS/IPS-правил через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Контент".
3. Под названием раздела располагаются подразделы в виде списка правил для каждого доступного поставщика (рисунок 7). Порядок отображения поставщиков следующий: сначала полужирным шрифтом отображается список лицензируемых поставщиков, после идет список пользовательских поставщиков без выделения.

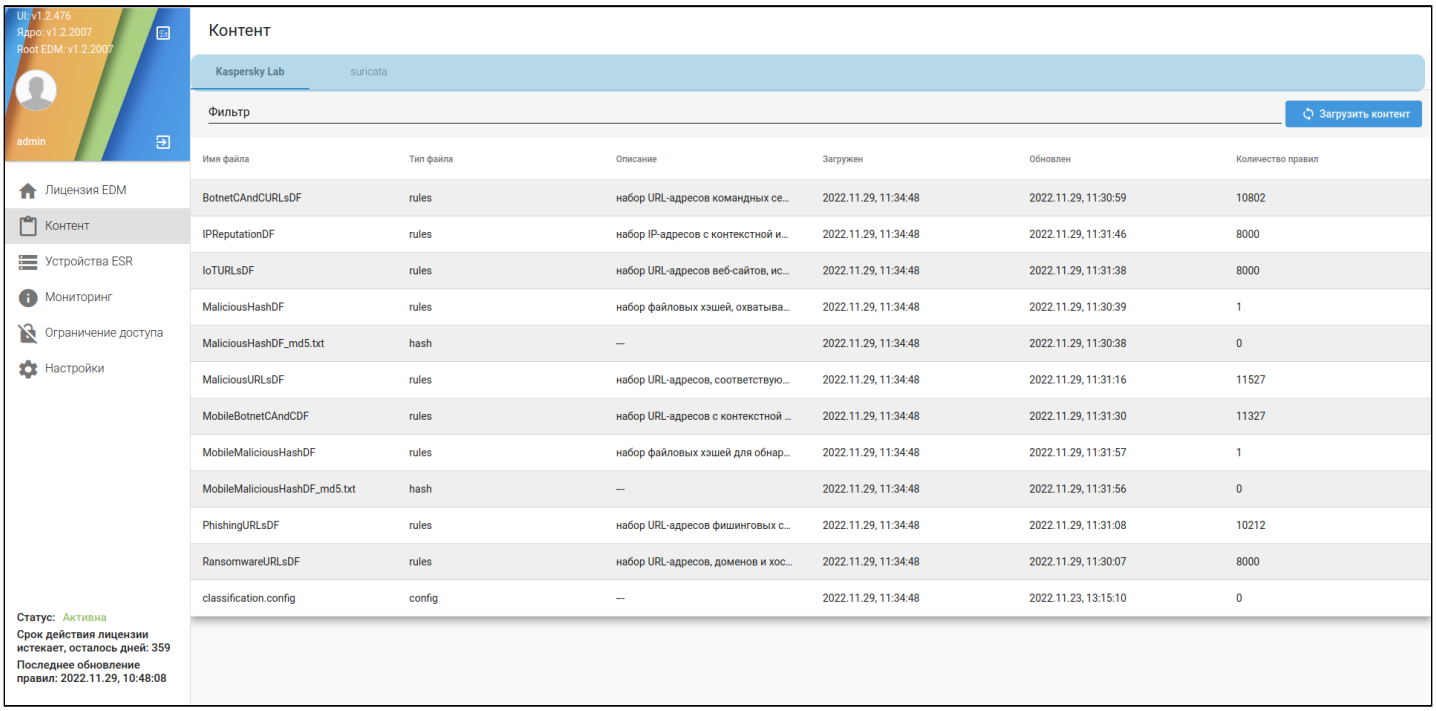


Рисунок 7 – Просмотр информации о поставщиках IDS/IPS-правил через web-интерфейс EDM Issue

5.2 Просмотр информации о поддерживаемых в поставщиках IDS/IPS-правил категориях IDS/IPS-правил

При просмотре информации о поддерживаемых категориях IDS/IPS-правил у каждого загруженного файла или категории есть дата обновления и дата загрузки (updated/loaded time). Дата загрузки – это всегда дата обновления IDS/IPS-правил на EDM Issue. Дата обновления для лицензируемых поставщиков IDS/IPS-правил – это дата обновления правил на EDM Root, а для пользовательских поставщиков IDS/IPS-правил эта дата совпадет с датой обновления IDS/IPS-правил на EDM Issue.

Каждая категория IDS/IPS-правил может содержать файлы нескольких типов:

- Файл с правилами для системы IDS/IPS;
- Файл с хешами, которые используются при анализе и обнаружении подозрительного трафика системой IDS/IPS;
- Файл с классификацией правил для классификации правил в системе IDS/IPS.

ⓘ В текущей версии EDM существует небольшая неточность. EDM Issue CLI в выводе команды "show files" в разделе "ips" оперирует не категориями правил, а именами скачиваемых и затем распространяемых файлов.

Для просмотра информации о поддерживаемых категориях IDS/IPS-правил для определенного поставщика IDS/IPS-правил через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "ips".
3. Ввести команду "show files --vendor <Имя поставщика IDS/IPS-правил>".

Пример вывода информации о категориях IDS/IPS-правил в EDM CLI

```
edmi-ips> show files --vendor kaspersky
Supported rules files:

1. File: PhishingURLsDF (10215 items)
File type: rules
EN description: a set of URLs with context that cover phishing websites and web pages
RU description: набор URL-адресов фишинговых сайтов и веб-страниц
Updated: 2022-11-29 12:16:15
Loaded: 2022-11-29 12:19:57

2. File: MobileBotnetCAndCDF (11327 items)
File type: rules
EN description: set of URLs with context that cover mobile botnet C&C servers
RU description: набор URL-адресов с контекстной информацией для выявления командных серверов
ботнетов, использующих мобильные устройства
Updated: 2022-11-29 12:16:37
Loaded: 2022-11-29 12:19:57

3. File: BotnetCAndCURLsDF (10802 items)
File type: rules
EN description: a set of URLs with context that cover desktop botnet C&C servers and related
malicious objects
RU description: набор URL-адресов командных серверов ботнетов и связанных с ними вредоносных
объектов
Updated: 2022-11-29 12:16:06
Loaded: 2022-11-29 12:19:57

4. File: RansomwareURLsDF (8000 items)
File type: rules
EN description: a set of URLs, domains, and hosts with context that cover ransomware links and
websites
RU description: набор URL-адресов, доменов и хостов, используемых для распространения
шифровальщиков
Updated: 2022-11-29 12:15:09
Loaded: 2022-11-29 12:19:57

5. File: MaliciousURLsDF (11529 items)
File type: rules
EN description: set of URLs with context that cover malicious websites and web pages
RU description: набор URL-адресов, соответствующих опасным ссылкам и веб-сайтам
Updated: 2022-11-29 12:16:24
Loaded: 2022-11-29 12:19:57

6. File: IPReputationDF (8000 items)
File type: rules
EN description: set of IP addresses with context that cover different categories of suspicious
and malicious hosts
RU description: набор IP-адресов с контекстной информацией о подозрительных и вредоносных узлах
Updated: 2022-11-29 12:16:54
Loaded: 2022-11-29 12:19:57

7. File: MaliciousHashDF (1 items)
File type: rules
EN description: a set of hashes of malicious objects
RU description: набор файловых хэшей, охватывающий наиболее опасные и распространенные, а также
самые новые вредоносные программы
```

```
Updated: 2022-11-29 12:15:32
Loaded: 2022-11-29 12:19:57

8. File: IoTURLsDF (8000 items)
File type: rules
EN description: a set of URLs with context covering malware that infects IoT (Internet of
Things) devices
RU description: набор URL-адресов веб-сайтов, используемых для размещения вредоносных программ,
заражающих устройства IoT (Internet of Things)
Updated: 2022-11-29 12:16:46
Loaded: 2022-11-29 12:19:57

9. File: MobileMaliciousHashDF (1 items)
File type: rules
EN description: a set of hashes of malicious objects for mobile platforms
RU description: набор файловых хэшей для обнаружения вредоносных объектов, заражающих мобильные
устройства
Updated: 2022-11-29 12:17:08
Loaded: 2022-11-29 12:19:57

Supported hash files:

1. File: MobileMaliciousHashDF_md5.txt
File type: hash
Updated: 2022-11-29 12:17:07
Loaded: 2022-11-29 12:19:57

2. File: MaliciousHashDF_md5.txt
File type: hash
Updated: 2022-11-29 12:15:31
Loaded: 2022-11-29 12:19:57

Supported config files:

1. File: classification.config
File type: config
Updated: 2022-11-23 13:15:10
Loaded: 2022-11-29 12:19:57

edmi-ips>
```

ⓘ В текущей версии EDM существует небольшая неточность. EDM Issue в web-интерфейсе отображает не категории правил, а имена загруженных файлов.

Для просмотра информации о поставщиках файлов и доступных в них категориях через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в раздел "Контент".
3. Перейти в подраздел поставщика, информацию о категориях которого необходимо получить.

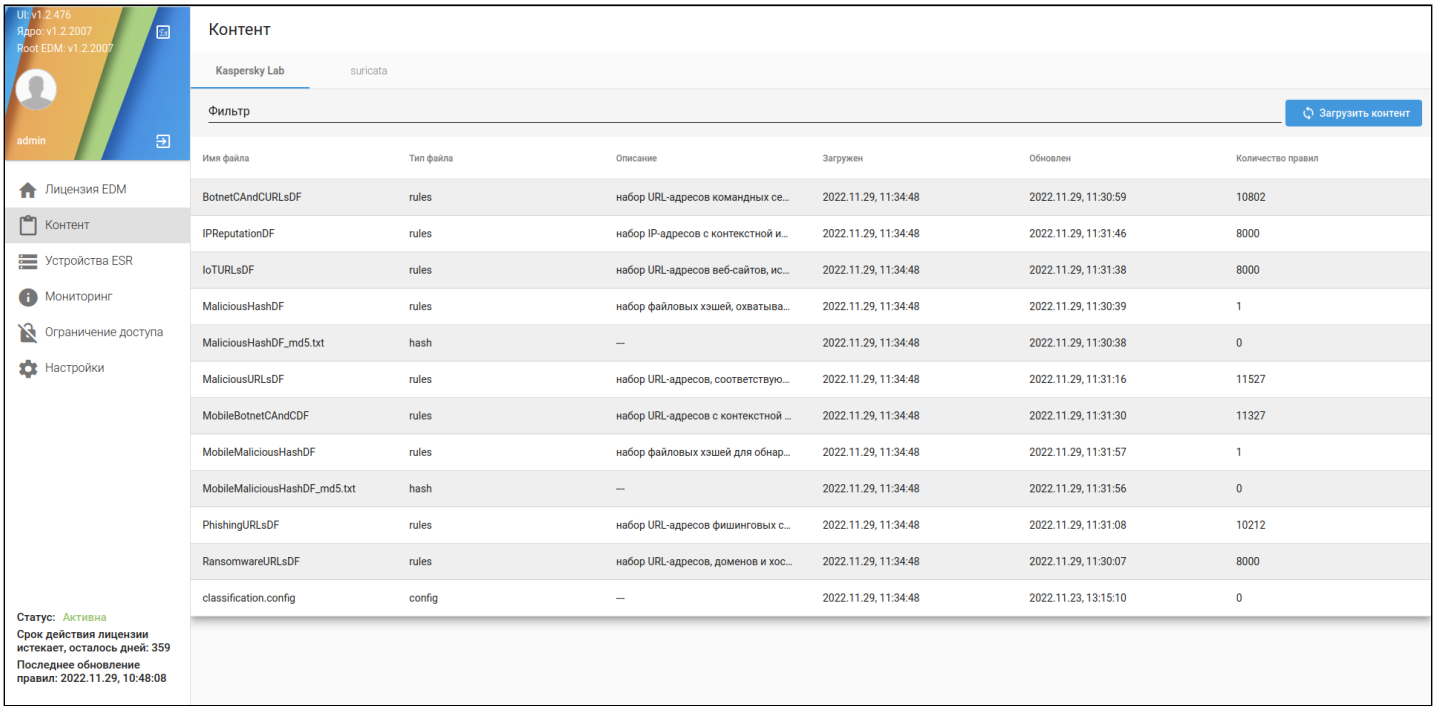


Рисунок 8 – Информация о доступных поставщиках IDS/IPS-правил и категорий IDS/IPS-правил в web-интерфейсе EDM Issue

5.3 Создание пользовательских поставщиков IDS/IPS-правил и категорий IDS/IPS-правил внутри них

EDM Issue позволяет создавать и распространять пользовательские IDS/IPS-правила, скачиваемые с внешних источников по протоколам HTTP и HTTPS, и отдавать их на клиентские устройства, сохраняя структуру отдачи IDS/IPS-правил как для лицензируемых поставщиков IDS/IPS-правил. Для того чтобы EDM Issue смог скачивать и раздавать такие правила, требуется создать пользовательского поставщика IDS/IPS-правил, а затем добавить в него требуемое количество категорий распространяемых правил.

Правила пользовательских поставщиков IDS/IPS-правил скачиваются по протоколам HTTP либо HTTPS, поэтому для каждой категории IDS/IPS-правил в пользовательском поставщике правил должна быть сформирована URL-ссылка на скачиваемый файл с правилами.

URL-ссылка формируется из двух частей:

1. Base URL – задается в параметре "–url" в команде "add vendor" при создании пользовательского поставщика IDS/IPS-правил.
2. Category path – задается в параметре "–path" в команде "add feed" при создании пользовательской категории IDS/IPS-правил.

В результате этого при запуске процесса обновления правил пользовательских поставщиков IDS/IPS-правил:

1. Будет произведена попытка загрузки файла с классификацией правил по пути <Base URL>classification.conf. Если файл не будет найден по указанному пути, то EDM будет считать, что для указанного пользовательского поставщика IDS/IPS-правил файл с классификацией правил отсутствует.
2. Для каждой категории IDS/IPS-правил будет произведена попытка загрузки файла с правилами по пути <Base URL><Category path>. Если такой файл не будет найден, то EDM будет считать, что для указанной категории IDS/IPS-правил правила не заданы.

Для создания пользовательского поставщика IDS/IPS-правил с категорией распространяемых IDS/IPS-правил через EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "ips".
3. Добавить нового поставщика IDS/IPS-правил командой "add vendor".
4. Добавить к созданному поставщику IDS/IPS-правил категорию IDS/IPS командой "add feed".

Пример создания пользовательского поставщика IDS/IPS-правил и категории IDS/IPS-правил в нем в EDM CLI

```
edmi-ips> add vendor --vendor suricata --url https://rules.emergingthreats.net/open/
suricata-4.0/rules/ --title Suricata rules
OK
edmi-ips> add feed --feed drop --path drop.rules --vendor suricata --en Rules to block
Spamhaus DROP listed networks --ru Правила блокировки сетей из списка Spamhaus DROP
OK
edmi-ips> show vendors
Licensed vendors:

1. Name: kaspersky
Title: Kaspersky Lab
Licensed: true
gid: 11

Other sources:

1. Name: suricata
Title: suricata
Licensed: false
URL: https://rules.emergingthreats.net/open/suricata-4.0/rules/
gid: 101

edmi-ips>
```

5.4 Редактирование пользовательских поставщиков IDS/IPS-правил

Для редактирования пользовательского поставщика IDS/IPS-правил через EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "ips".
3. Изменить параметры пользовательского поставщика IDS/IPS правил командой "edit vendor", указав имя изменяемого поставщика правил в параметре "--vendor".

Пример редактирования пользовательского поставщика IDS/IPS-правил в EDM CLI

```
edmi-ips> show vendors
Licensed vendors:

1. Name: kaspersky
Title: Kaspersky Lab
Licensed: true
gid: 11

Other sources:

1. Name: suricata
Title: suricata
Licensed: false
URL: https://rules.emergingthreats.net/open/suricata-4.0/rules/
gid: 101

edmi-ips> edit vendor --vendor suricata --title Suricata Rules
OK
edmi-ips> show vendors
Licensed vendors:

1. Name: kaspersky
Title: Kaspersky Lab
Licensed: true
gid: 11

Other sources:

1. Name: suricata
Title: Suricata Rules
Licensed: false
URL: https://rules.emergingthreats.net/open/suricata-4.0/rules/
gid: 101

edmi-ips>
```

5.5 Редактирование категорий IDS/IPS-правил в пользовательских поставщиках IDS/IPS-правил

Для редактирования категории IDS/IPS-правил в пользовательском поставщике IDS/IPS-правил через EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "ips".
3. Изменить параметры категории IDS/IPS-правил командой "edit feed", указав имя изменяемой категории IDS/IPS-правил в параметре "–feed" и имя поставщика IDS/IPS-правил, к которому относится категория, в параметре "--vendor".

Пример редактирования категории IDS/IPS-правил в пользовательском поставщике IDS/IPS-правил в EDM CLI

```
edmi-ips> show files --vendor suricata
Supported rules files:

1. File: drop (36 items)
File type: rules
Path: drop.rules
EN description: Rules to block Spamhaus DROP listed networks
RU description: Правила блокировки сетей из списка
Updated: 2022-11-29 14:36:53
Loaded: 2022-11-29 14:36:53

Supported config files:

1. File: classification.config
File type: config
Updated: 2022-11-29 14:36:54
Loaded: 2022-11-29 14:36:54

edmi-ips> edit feed --feed drop --vendor suricata --en Drop rule
OK
edmi-ips> show files --vendor suricata
Supported rules files:

1. File: drop (36 items)
File type: rules
Path: drop.rules
EN description: Drop rule
RU description: Правила блокировки сетей из списка
Updated: 2022-11-29 14:36:53
Loaded: 2022-11-29 14:36:53

Supported config files:

1. File: classification.config
File type: config
Updated: 2022-11-29 14:36:54
Loaded: 2022-11-29 14:36:54

edmi-ips>
```

5.6 Удаление категорий IDS/IPS-правил в пользовательских поставщиках IDS/IPS-правил

Для удаления категории IDS/IPS-правил из пользовательского поставщика IDS/IPS-правил через EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "ips".
3. Удалить категорию IDS/IPS-правил командой "delete feed".

Пример удаления категории IDS/IPS-правил из пользовательского поставщика IDS/IPS-правил в EDM CLI

```
edmi-ips> delete feed --feed drop --vendor suricata
You will delete file drop for vendor Suricata Rules. Are you sure? (y/N) y
OK
edmi-ips>
```

Также из поставщика правил можно удалить все категории IDS/IPS-правил командой "delete feeds".

```
edmi-ips> delete feeds --vendor suricata
You will delete all files for vendor Suricata Rules. Are you sure? (y/N) y
OK
edmi-ips>
```

5.7 Удаление пользовательских поставщиков IDS/IPS-правил

Для удаления пользовательского поставщика IDS/IPS-правил через EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "ips".
3. Удалить пользовательского поставщика IDS/IPS-правил командой "delete vendor". При удалении пользовательского поставщика IDS/IPS-правил будут также удалены все указанные в нем категории правил.

Пример удаления пользовательского поставщика IDS/IPS-правил в EDM CLI

```
edmi-ips> delete vendor --vendor suricata
You will delete vendor suricata and all its files. Are you sure? (y/N) y
OK
edmi-ips>
```

5.8 Настройка интервала автоматической загрузки актуальных IDS/IPS-правил

За интервал автоматической загрузки актуальных IDS/IPS-правил отвечает параметр "ipsLoadIntervalMinutes" в настройках EDM Issue.

Для изменения интервала автоматической загрузки актуальных IDS/IPS-правил через EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "settings".
3. Установить новое значение параметра "ipsLoadIntervalMinutes" командой "set".

Пример изменения интервала загрузки актуальных IDS/IPS-правил в EDM CLI

```
edmi-settings> show --param ipsLoadIntervalMinutes
Load IPS data from Root-server interval in minutes
ipsLoadIntervalMinutes = 15 [default]

edmi-settings> set --param ipsLoadIntervalMinutes --value 60
OK
edmi-settings> show --param ipsLoadIntervalMinutes
Load IPS data from Root-server interval in minutes
ipsLoadIntervalMinutes = 60

edmi-settings>
```

Для изменения интервала автоматической загрузки актуальных IDS/IPS-правил через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Настройки".
3. Перейти к категории настроек "Функциональные настройки EDM Loader".
4. Установить новое значение параметра "Интервал загрузки контента с Root-сервера".

5.9 Запуск процесса загрузки актуальных IDS/IPS-правил лицензируемых поставщиков с EDM Root вручную

Для запуска ручной загрузки актуальных лицензируемых IDS/IPS-правил в EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "ips".
3. Ввести команду "load content –vendor <VENDOR>", где <VENDOR> - имя лицензионного поставщика, для которого необходимо выполнить загрузку IDS/IPS-правил.

Пример запуска ручной загрузки актуальных лицензируемых IDS/IPS-правил в EDM CLI

```
edmi-ips> load content --vendor kaspersky
Upload IPS content for vendor 'kaspersky' command 98 is created. Please wait...
edmi-ips> Upload IPS content for vendor 'kaspersky' command 98 is done!

edmi-ips>
```

Для запуска ручной загрузки актуальных лицензируемых IDS/IPS-правил в web-интерфейсе требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Контент".
3. Перейти в подраздел поставщика, правила которого необходимо загрузить.
4. Нажать кнопку "Загрузить контент" в правой верхней части web-интерфейса. После нажатия кнопка станет неактивной на время процесса загрузки IDS/IPS-правил, а по его окончании в правом верхнем углу появится всплывающее оповещение о результатах процесса синхронизации.

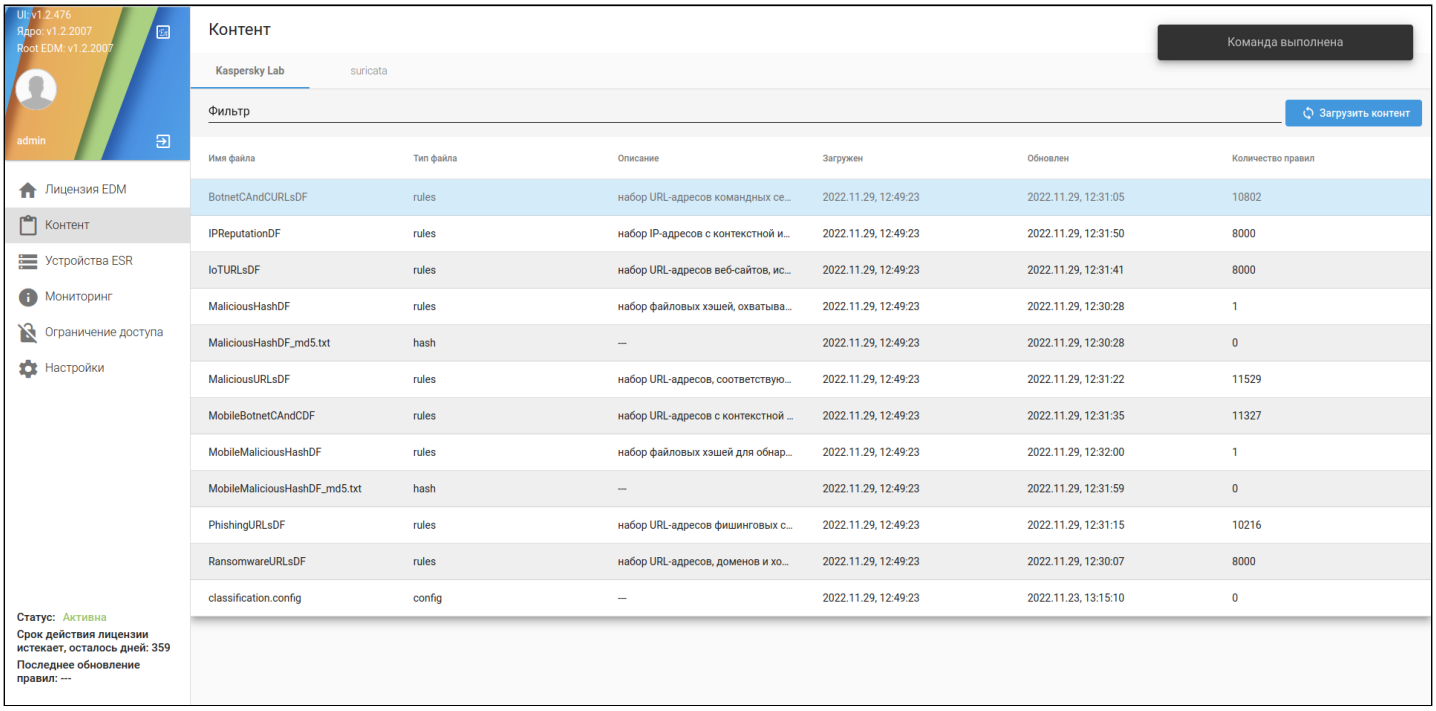


Рисунок 9 – Успешно завершенная загрузка актуальных лицензируемых IDS/IPS-правил через web-интерфейс EDM Issue

5.10 Запуск процесса загрузки актуальных пользовательских IDS/IPS-правил с внешних источников вручную

Для запуска ручной загрузки актуальных пользовательских IDS/IPS-правил в EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "ips".
3. Ввести команду "load ips-rules --vendor<VENDOR>", где <VENDOR> – имя поставщика, созданного пользователем, для которого необходимо выполнить загрузку IDS/IPS-правил.

Пример запуска ручной загрузки актуальных пользовательских IDS/IPS-правил в EDM CLI

```
edmi-ips> load ips-rules --vendor suricata
Upload IPS rules for vendor 'suricata' command 99 is created. Please wait...
edmi-ips> Upload IPS rules for vendor 'suricata' command 99 is done!

edmi-ips>
```

В web-интерфейсе EDM Issue можно загрузить IDS/IPS-правила пользовательских поставщиков в разделе "Контент" в подразделе нужного поставщика. При нажатии кнопки "Загрузить контент" начнется процесс загрузки правил, в случае успешного завершения процесса появится всплывающее сообщение, сообщающее о завершении команды.

6 Управление подключенными к EDM Issue устройствами

EDM Issue предоставляет доступ к распространяемому контенту для клиентских устройств, которыми на данный момент являются только сервисные маршрутизаторы ESR.

Администратор EDM Issue со своей стороны может:

- просматривать информацию о подключенных к EDM Issue устройствах ESR;
- просматривать подробную информацию по конкретному устройству ESR;
- настраивать параметры автоматической синхронизации списка подключенных к EDM Issue устройств с EDM Root;
- запускать процесс синхронизации списка подключенных к EDM Issue устройств с EDM Root вручную;
- отозвать сертификат устройства ESR.

6.1 Просмотр информации о подключенных к EDM Issue устройствах ESR

Для просмотра информации о подключенных к EDM Issue устройствах ESR через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "license".
3. Ввести команду "show devices".

Пример вывода информации о подключенных к EDM Issue устройствах ESR в EDM CLI

```
edmi-license> show devices
1. Serial: NP02003364
Mac: A8:F9:4B:AD:A5:2C
Model: ESR-200
Hardware: 1v8
Hostname: esr-200
Source IP: 192.168.35.81
Status: valid

2. Serial: NP03004647
Mac: A8:F9:4B:AB:97:F4
Model: ESR-100
Hardware: 1v6
Hostname: esr-100
Source IP: 192.168.35.82
Status: valid

End of list
edmi-license>
```

> При первом запуске EDM Issue или после изменения списка устройств, чтобы не ждать автоматического обновления данных, для отображения актуальной информации в web-интерфейсе необходимо вручную обновить данные лицензии (кнопка "Синхронизировать" в разделе "Лицензия EDM"), после чего нажать "Синхронизировать" в разделе "Устройства ESR".

Для просмотра информации о подключенных к EDM Issue устройствах ESR через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Устройства ESR".

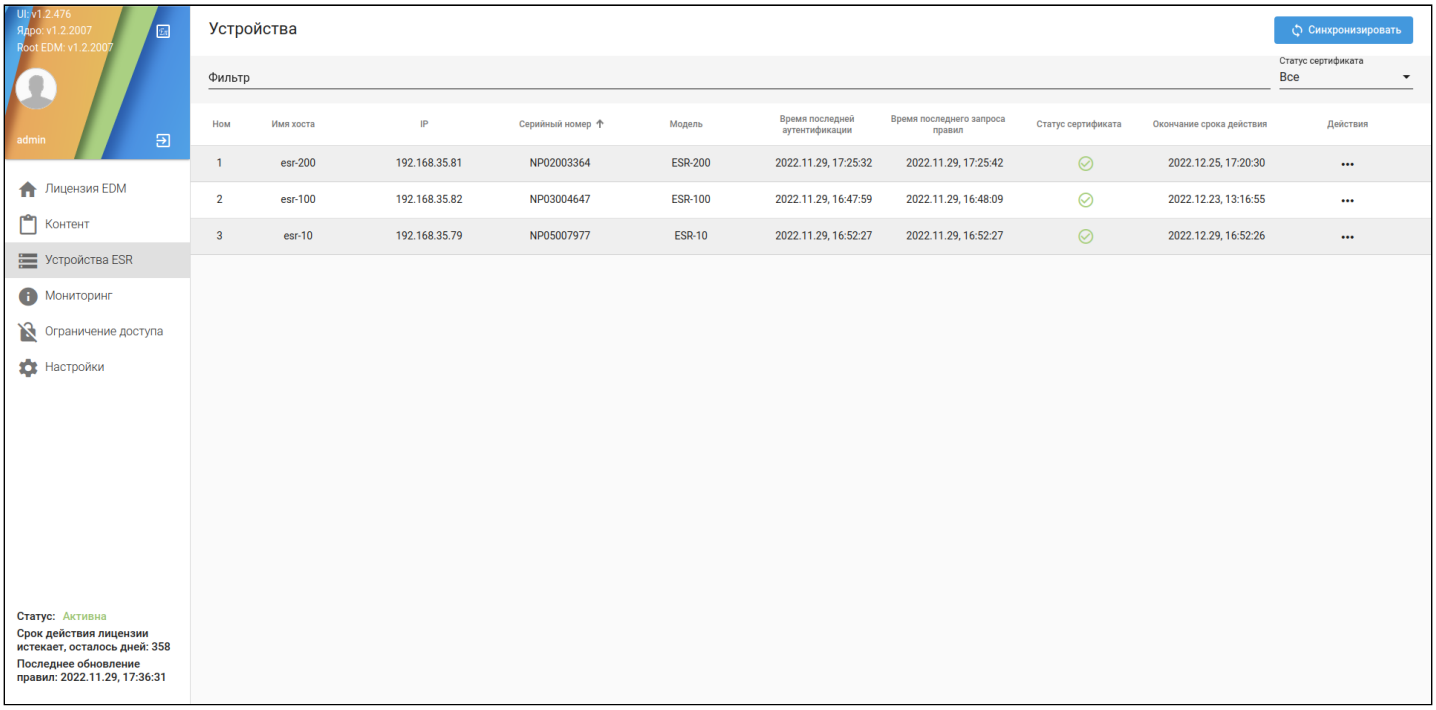


Рисунок 10 – Получение информации о подключенных к EDM Issue устройствах ESR в web-интерфейсе EDM Issue

6.2 Просмотр подробной информации о конкретном устройстве ESR, подключенном к EDM Issue

Для просмотра подробной информации о конкретном устройстве ESR, подключенном к EDM Issue через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "license".
3. Ввести команду "show device" с указанием в параметрах команды серийного номера устройства или заводского MAC-адреса.

Пример вывода подробной информации о конкретном устройстве ESR, подключенному к EDM Issue в EDM CLI

```
edmi-license> show device --serial NP02003364
Serial: NP02003364
Mac: A8:F9:4B:AD:A5:2C
Model: ESR-200
Hardware: 1v8
Hostname: esr-200
Source IP: 192.168.35.81
Registered: 2022-11-23 13:17:28
Last auth: 2022-11-29 17:25:32
Last request: 2022-11-29 17:25:32
Last rules given: 2022-11-29 17:25:42
Certificate:

    Last changed: 2022-11-25 17:20:31
    Status: valid
    Expiry: 2022-12-25 17:20:30


edmi-license> show device --mac A8:F9:4B:AD:A5:2C
Serial: NP02003364
Mac: A8:F9:4B:AD:A5:2C
Model: ESR-200
Hardware: 1v8
Hostname: esr-200
Source IP: 192.168.35.81
Registered: 2022-11-23 13:17:28
Last auth: 2022-11-29 17:25:32
Last request: 2022-11-29 17:25:32
Last rules given: 2022-11-29 17:25:42
Certificate:

    Last changed: 2022-11-25 17:20:31
    Status: valid
    Expiry: 2022-12-25 17:20:30


edmi-license>
```

Для просмотра подробной информации о конкретном устройстве ESR, подключенном к EDM Issue через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Устройства ESR".
3. В крайней правой колонке для требуемого устройства вызвать контекстное меню и выбрать в нем пункт "Информация".

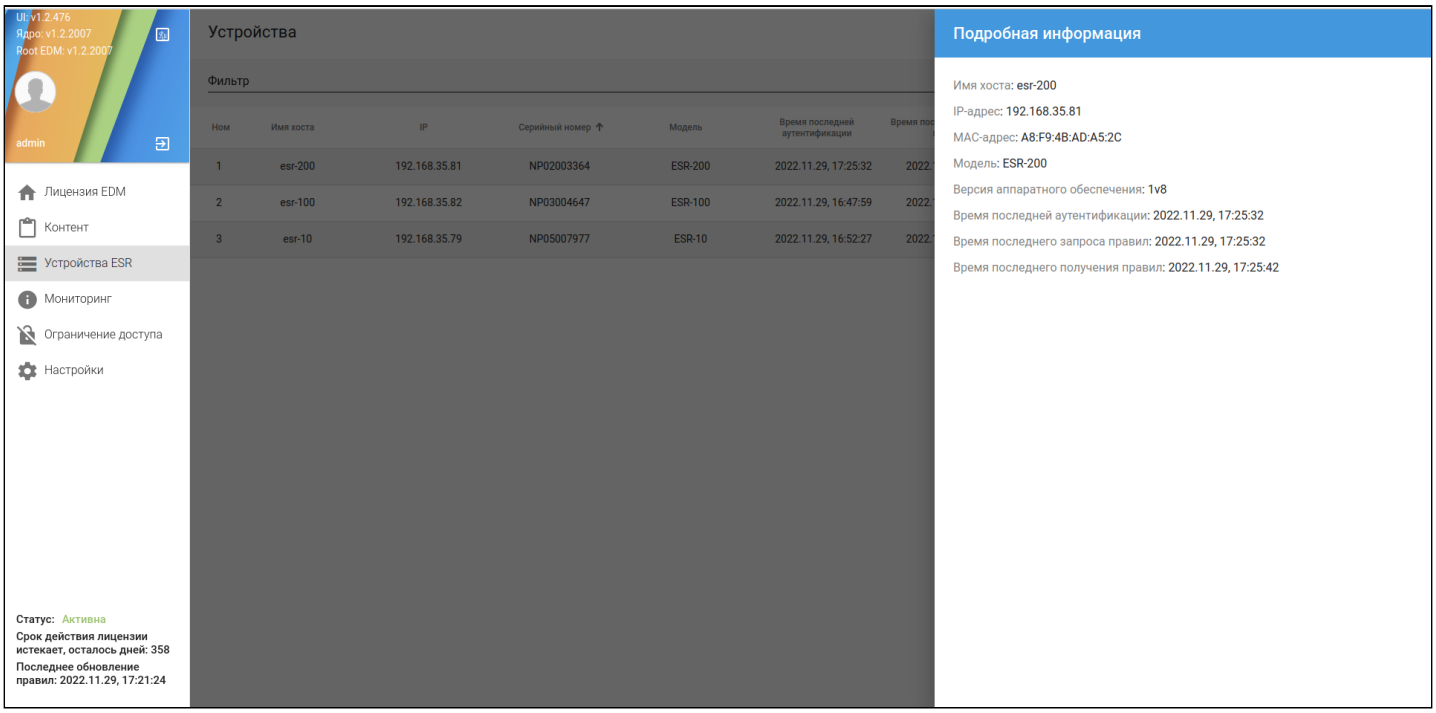


Рисунок 11 – Получение подробной информации о конкретном устройстве ESR, подключенном к EDM Issue в web-интерфейсе EDM Issue

6.3 Настройка параметров автоматической синхронизации списка подключенных к EDM Issue устройств с EDM Root

При регистрации новых устройств ESR на EDM Issue для каждого устройства на EDM Root создается уникальный сертификат, используя который, устройство ESR может подключаться к EDM Issue и запрашивать с него требуемые устройством IDS/IPS-правила. Поскольку сертификаты формируются на EDM Root, то он хранит информацию о каждом зарегистрированном на EDM Issue устройстве. Информация, которая хранится на EDM Root считается более достоверной, по этой причине EDM Issue синхронизирует информацию о зарегистрированных устройствах ESR с определенной периодичностью. При синхронизации EDM Issue запрашивает данные об устройствах с EDM Root определенное количество раз. Запросов делается столько, чтобы выгрузить информацию о всех имеющихся на EDM Root устройствах ESR.

За интервал автоматической синхронизации списка подключенных к EDM Issue устройств с EDM Root отвечает параметр "deviceSyncIntervalHours" в настройках EDM Issue. Для изменения интервала автоматической синхронизации списка подключенных к EDM Issue устройств с EDM Root через EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "settings".
3. Установить новое значение параметра "deviceSyncIntervalHours" командой "set".

Пример изменения интервала автоматической синхронизации списка подключенных к EDM Issue устройств с EDM Root в EDM CLI

```
edmi-settings> show --param deviceSyncIntervalHours
Synchronization of devices from Root-server interval in hours
deviceSyncIntervalHours = 720 [default]

edmi-settings> set --param deviceSyncIntervalHours --value 300
OK
edmi-settings> show --param deviceSyncIntervalHours
Synchronization of devices from Root-server interval in hours
deviceSyncIntervalHours = 300

edmi-settings>
```

Для изменения интервала автоматической синхронизации списка подключенных к EDM Issue устройств с EDM Root через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Настройки".
3. Перейти к категории настроек "Функциональные настройки EDM Loader".
4. Установить новое значение параметра "Интервал синхронизации списка устройств по данным с Root-сервера".

За количество устройств в запросе синхронизации списка подключенных к EDM Issue устройств с EDM Root отвечает параметр "deviceSyncAmount" в настройках EDM Issue. Для изменения количества устройств в запросе синхронизации списка подключенных к EDM Issue устройств с EDM Root через EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "settings".
3. Установить новое значение параметра "deviceSyncAmount" командой "set".

Пример изменения количества устройств в запросе синхронизации списка подключенных к EDM Issue устройств с EDM Root в EDM CLI

```
edmi-settings> show --param deviceSyncAmount
Devices amount per request on synchronization from Root-server
deviceSyncAmount = 200

edmi-settings> set --param deviceSyncAmount --value 400
OK
edmi-settings> show --param deviceSyncAmount
Devices amount per request on synchronization from Root-server
deviceSyncAmount = 400

edmi-settings>
```

Для изменения количества устройств в запросе синхронизации списка подключенных к EDM Issue устройств с EDM Rootчерез web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Настройки".
3. Перейти к категории настроек "Функциональные настройки EDM Loader".
4. Установить новое значение параметра "Количество устройств, запрашиваемое в одном запросе при синхронизации списка по данным с Root-сервера".

6.4 Запуск процесса синхронизации списка подключенных к EDM Issue устройств с EDM Root вручную

Для запуска ручной синхронизации списка подключенных к EDM Issue устройств с EDM Root в EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "license".
3. Ввести команду "load devices".

Пример запуска ручной синхронизации информации о лицензии EDM в EDM CLI

```
edmi-license> load devices
Synchronize device list command 1 is created. Please wait...
edmi-license> Synchronize device list command 1 is done! Issue devices is synchronized
 from Root server

edmi-license>
```

Для запуска ручной синхронизации списка подключенных к EDM Issue устройств с EDM Root в web-интерфейсе требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Устройства ESR".
3. Нажать кнопку "Синхронизировать" в правой верхней части web-интерфейса. После нажатия кнопка станет неактивной на время процесса синхронизации списка подключенных к EDM Issue устройств с EDM Root, а по его окончании в правом верхнем углу появится всплывающее оповещение о результатах процесса синхронизации.

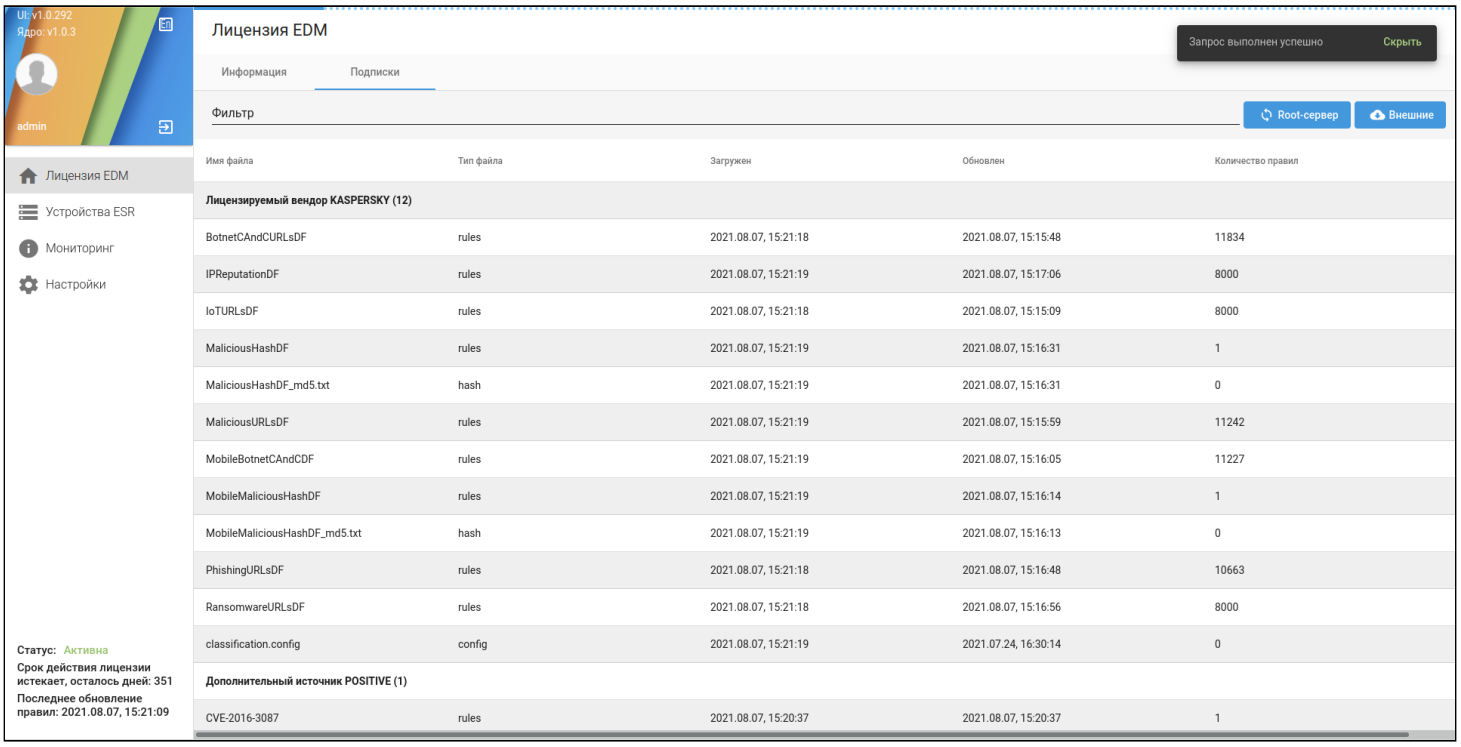


Рисунок 12 – Успешно завершенная синхронизация списка подключенных к EDM Issue устройств с EDM Root через web-интерфейс EDM Issue

6.5 Отзыв сертификата клиентского устройства ESR

Любое клиентское устройство, прошедшее процедуру сертификации на EDM Issue, получает сертификат, благодаря которому оно может взаимодействовать с EDM Issue согласно списку разрешенных моделей устройств в групповой лицензии. При этом устройство, которое однажды было сертифицировано в рамках групповой лицензии на EDM Issue, "забирает" из пула разрешенных моделей ESR одну единицу:

Вывод блока "Devices limit" команды "show license" EDM CLI после сертификации нового устройства ESR

```
Devices limits:

    Supported models:


            Model: ESR-1500
            Limit: 25
            Used: 10
            Free: 15

########################################################################


Devices limits:

    Supported models:


            Model: ESR-1500
            Limit: 25
            Used: 11
            Free: 14
```

Таким образом может возникнуть ситуация, когда:

- в лицензии EDM не будет возможности подключить новое устройство ESR, поскольку все текущие квоты по лицензии заняты;
- одно из устройств ESR в эксплуатации, которое было подключено к EDM Issue, требуется заменить другим устройством такой же модели.

В этом случае можно дождаться штатного окончания срока действия клиентского сертификата или произвести процедуру отзыва сертификата.

⚠ При отзыве клиентского устройства ESR оно больше не сможет подключиться к системе EDM ни в рамках текущей групповой лицензии EDM, ни в рамках какой-либо другой лицензии EDM до окончания срока действия отозванного сертификата. Таким образом быстро вернуть устройство с отозванным сертификатом в эксплуатацию будет нельзя. Для ускоренного возвращения доступа устройства с отозванным сертификатом к системе EDM требуется обратиться в Сервисный центр компании "ЭЛТЕКС".

Для запуска процедуры отзыва сертификата устройства ESR в EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "license".
3. Ввести команду "revoke" с указанием серийного номера или заводского MAC-адреса устройства, чей сертификат будет отозван.

Пример запуска ручной синхронизации информации о лицензии EDM в EDM CLI

```
edmi-license> revoke --serial NP05007977
Certificate revoke command 143 is created. Please wait...
edmi-license> Certificate revoke command 143 is done!

edmi-license> show device --serial NP05007977
Serial: NP05007977
Mac: A8:F9:4B:AE:A8:AA
Model: ESR-10
Hardware: 2v1
Hostname: esr-10
Source IP: 192.168.35.79
Registered: 2022-11-29 16:52:25
Last auth: 2022-11-29 16:52:27
Last request: 2022-11-29 16:52:27
Last rules given: 2022-11-29 16:52:27
Certificate:

    Last changed: 2022-11-29 17:41:48
    Status: revoked
    Expiry: 2022-12-29 16:52:26


edmi-license>
```

Для запуска процедуры отзыва сертификата устройства ESR в web-интерфейсе требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Устройства ESR".
3. В крайней правой колонке для требуемого устройства вызвать контекстное меню и в нем выбрать пункт "Отозвать сертификат".
4. В открывшемся окне подтвердить отзыв сертификата.

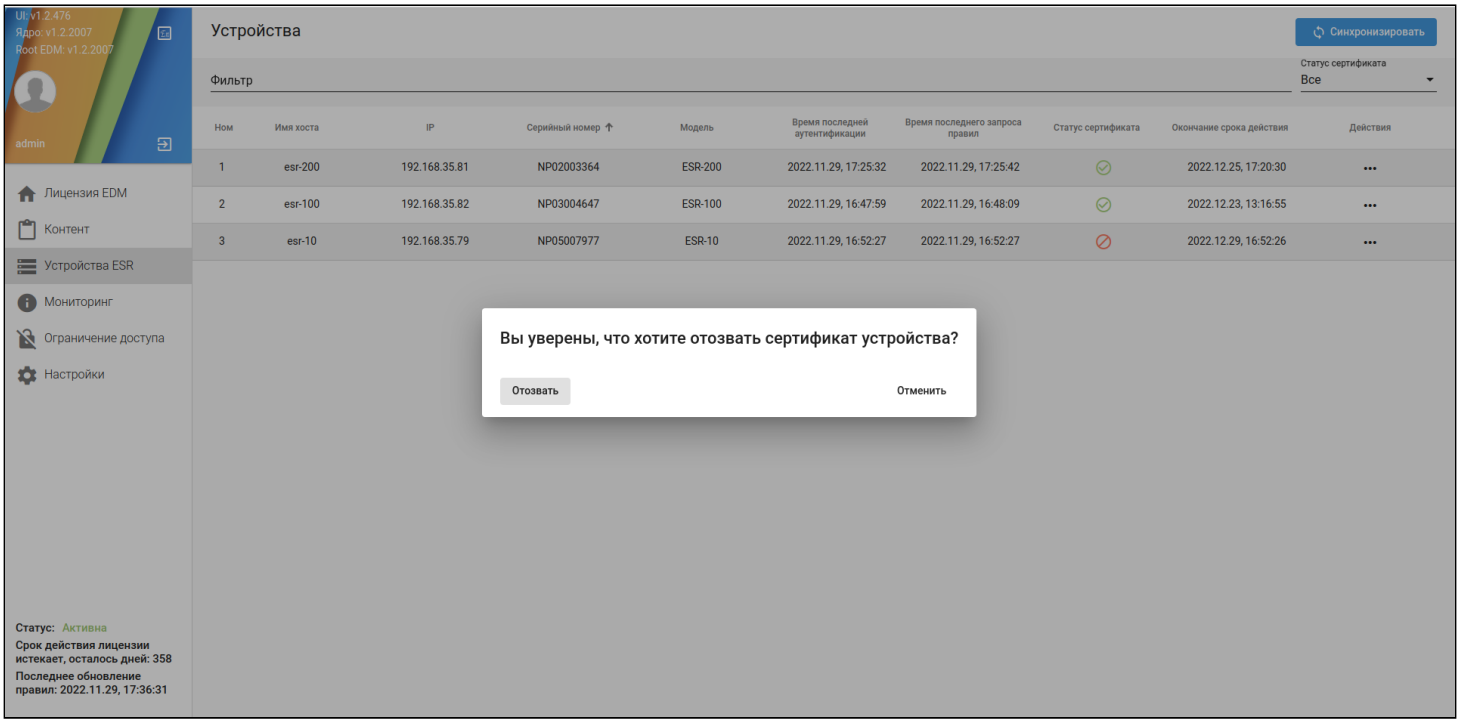


Рисунок 13 – Окно подтверждения отзыва сертификата устройства ESR через web-интерфейс EDM Issue

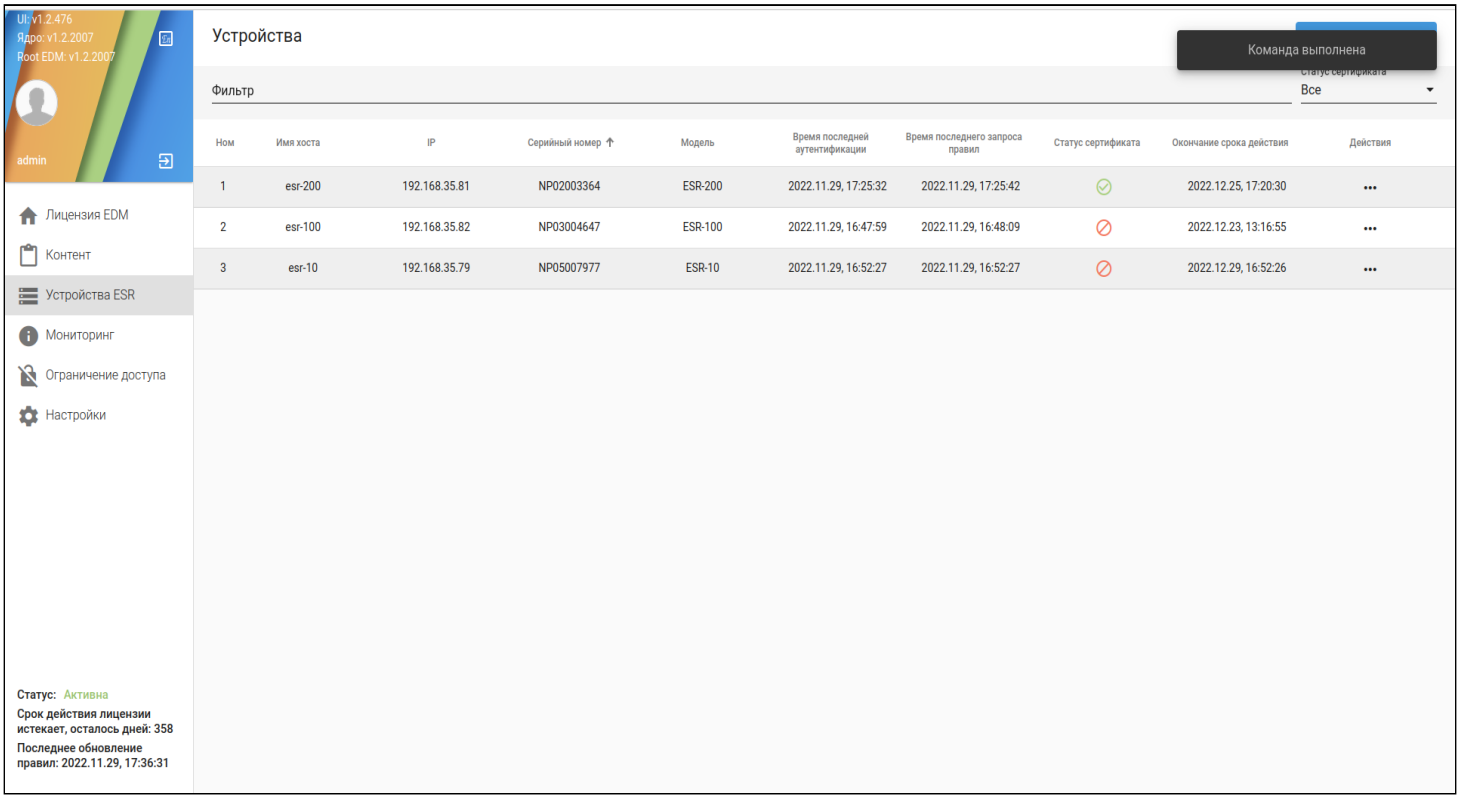


Рисунок 14 – Успешно завершенная процедура отзыва сертификата устройства ESR через web-интерфейс EDM Issue

7 Просмотр информации о компонентах сервиса EDM Issue

EDM Issue помимо интерфейсов управления – CLI- и web-интерфейса – содержит два компонента, на основании которых работает вся логика EDM Issue:

- server – обработка запросов от клиентских устройств;
- loader – синхронизация информации от EDM Root.

Эти компоненты периодически сохраняют информацию о себе в базу данных, что позволяет контролировать их работу.

Администратор EDM Issue со своей стороны может:

- просматривать информацию о компонентах EDM Issue;
- настраивать интервал сохранения компонентами EDM Issue информации о себе в базе данных.

7.1 Просмотр информации о компонентах EDM Issue

Для просмотра информации о компонентах EDM Issue через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "main".
3. Ввести команду "show edm".

Пример вывода информации о компонентах EDM Issue в EDM CLI

```
edmi> show edm
EDM Loader Host:
1. IP: 192.168.0.2
Hostname: Issue EDM Loader
Build version: Version 1.2, build 2007, date 17-11-2022 13:29:55
Status: work
Info: Root server connection state: ok
Last approved: 2022-11-23 13:15:53
Last updated: 2022-11-30 15:10:43
Next update: 2022-11-30 15:13:14

EDM Server Host:
1. IP: 192.168.0.2
Hostname: Issue EDM Server
Build version: Version 1.2, build 2007, date 17-11-2022 13:29:48
Status: work
Info: Root server connection state: ok
Last approved: 2022-11-23 13:15:53
Last updated: 2022-11-30 15:08:02
Next update: 2022-11-30 15:13:02

edmi>
```

Для просмотра информации о компонентах EDM Issue через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Мониторинг".

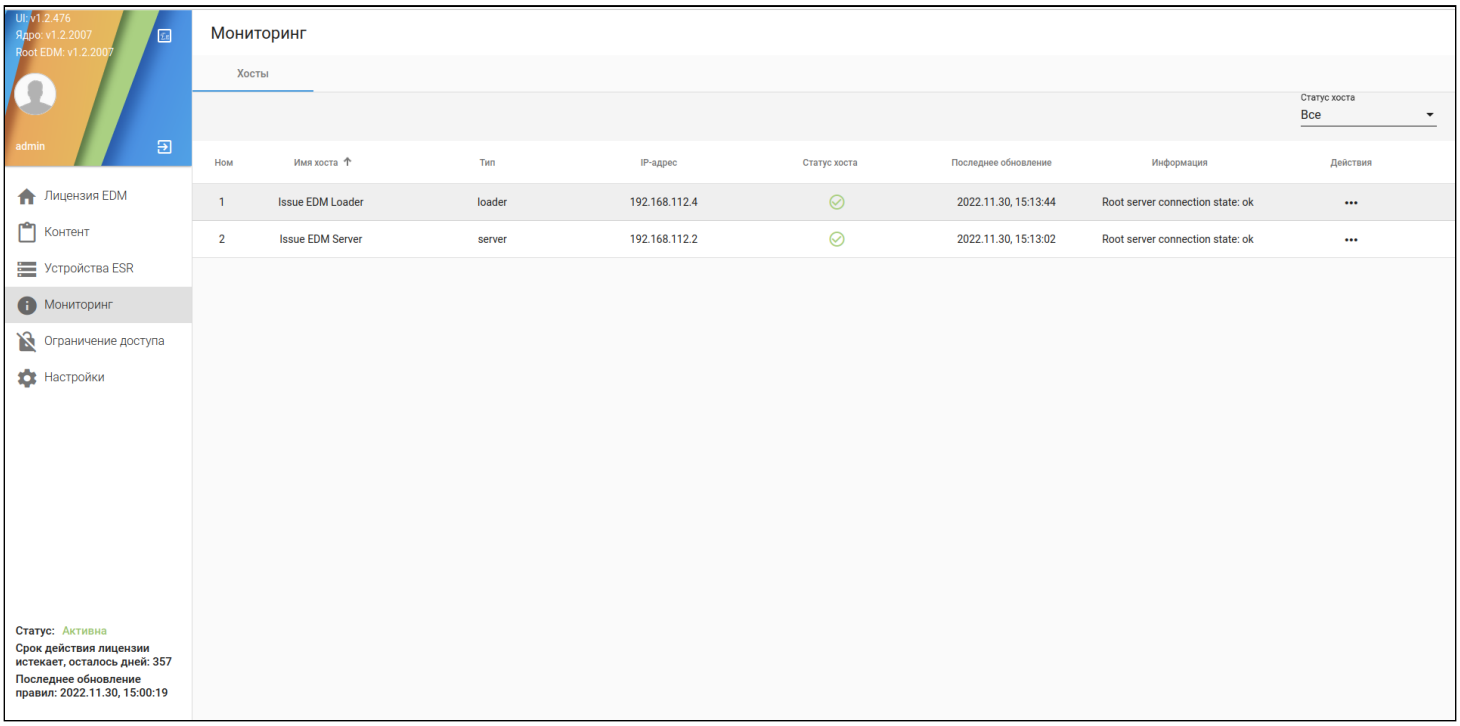


Рисунок 15 – Получение информации о компонентах EDM Issue в web-интерфейсе EDM Issue

Для просмотра подробной информации о компоненте EDM Issue через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Мониторинг".
3. В крайней правой колонке для требуемого компонента вызвать контекстное меню и в нем выбрать пункт "Информация".

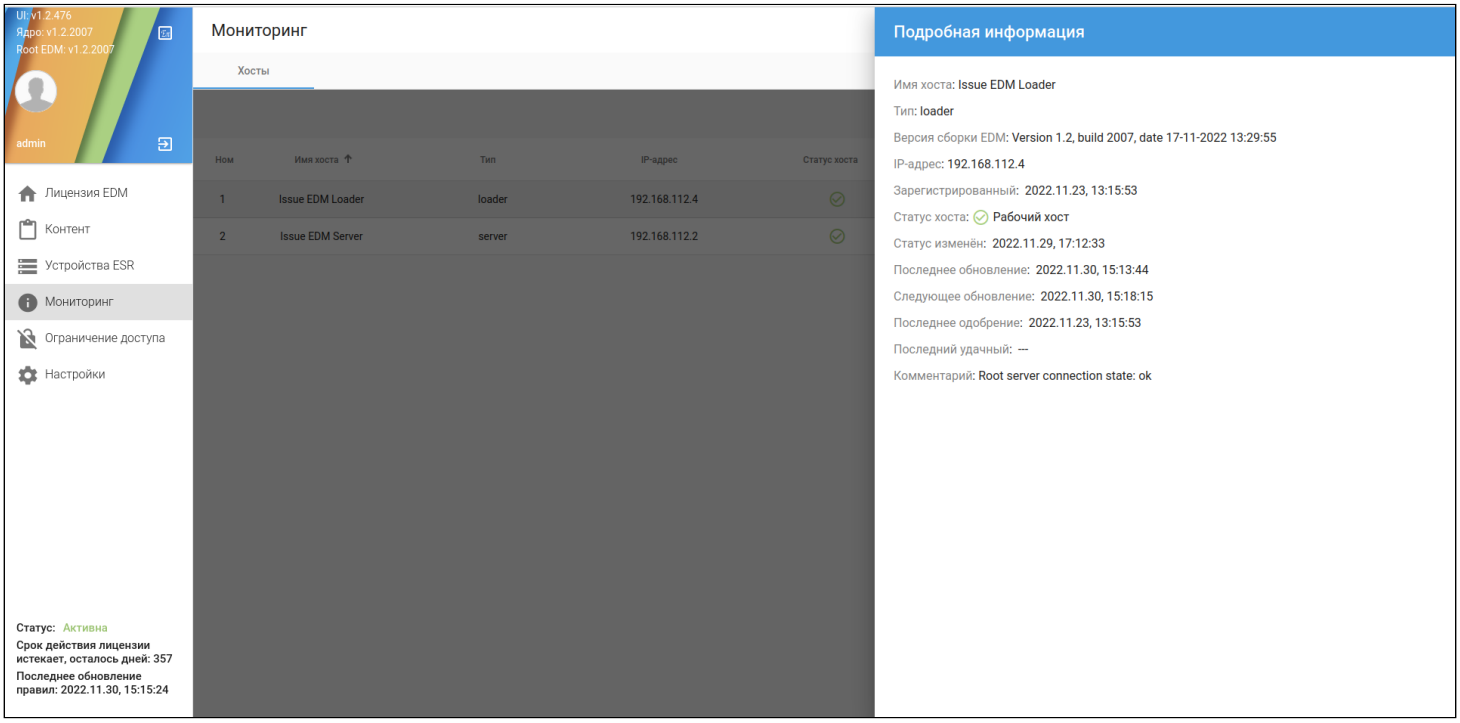


Рисунок 16 – Получение подробной информации о компоненте EDM Issue в web-интерфейсе EDM Issue

7.2 Настройка интервала сохранения компонентами EDM Issue информации о себе в базе данных

За интервал сохранения компонентами EDM Issue информации о себе в базе данных отвечает параметр "selfInfoSaveIntervalSeconds" в настройках EDM Issue. Для изменения интервала сохранения компонентами EDM Issue информации о себе в базе данных через EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "settings".
3. Установить новое значение параметра "selfInfoSaveIntervalSeconds" командой "set".

Пример изменения интервала автоматической синхронизации списка подключенных к EDM Issue устройств с EDM Root в EDM CLI

```
edmi-settings> show --param selfInfoSaveIntervalSeconds
EDM self-info saving interval, in seconds
selfInfoSaveIntervalSeconds = 300 [default]

edmi-settings> set --param selfInfoSaveIntervalSeconds --value 150
OK
edmi-settings> show --param selfInfoSaveIntervalSeconds
EDM self-info saving interval, in seconds
selfInfoSaveIntervalSeconds = 150

edmi-settings>
```

Для изменения интервала сохранения компонентами EDM Issue информации о себе в базе данных через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Настройки".
3. Перейти к категории настроек "Основные настройки".
4. Установить новое значение параметра "Интервал актуализации информации о работающем сервисе EDM, в секундах".

8 Управление доступом к EDM Issue

Клиентские устройства ESR получают информацию и загружаемый контент от EDM Issue. Для того чтобы контролировать подключающиеся клиентские устройства, в EDM Issue существуют несколько механизмов:

- IP-правила – списки доступа, ограничивающие доступ клиентских устройств по IP-адресу;
- Очередь запросов к EDM Issue – ограничение на обработку запросов нескольких клиентов и очередь запросов при перегрузке EDM Issue параллельными запросами;
- Защита от DOS-атаки на EDM Issue – ограничение на количество запросов и задержки при обмене сообщениями с одного IP-адреса в секунду, превышение любого из параметров приведет к обрыву сессии со стороны EDM Root;
- Защита от превышения попыток некорректной аутентификации – ограничение на максимальное количество попыток некорректной аутентификации с одного IP-адреса за отведенный интервал времени, превышение которого приведет к созданию IP-правила, ограничивающего доступ с данного IP-адреса на EDM Root, с определенным сроком действия. По истечению срока действия ограничивающее IP-правило перестанет действовать и будет автоматически удалено.

Таким образом, администратор EDM Issue со своей стороны может:

- просматривать информацию о группах IP-правил;
- просматривать информацию о существующих IP-правилах в группе IP-правил;
- создавать IP-правило;
- редактировать IP-правило;
- удалять IP-правило;
- очищать счетчик для ограничивающего IP-правила;
- переводить временное ограничивающее IP-правило в бессрочное;
- ограничить очереди запросов от клиентских устройств к EDM Issue;
- ограничить число запросов к EDM Issue с одного IP-адреса;
- настроить параметры автоматической блокировки клиентских устройств при нарушении процедуры аутентификации.

8.1 Просмотр информации о группах IP-правил

В EDM Issue существует две служебных группы IP-правил:

- edm – группа IP-правил для подключающихся к EDM Issue клиентских устройств;
- web – группа IP-правил для web-интерфейса.

> IP-правила в группе "web" заполняются автоматически и доступны для просмотра и редактирования в CLI исключительно в целях диагностики возможных ошибок. При обычной эксплуатации администратор EDM Issue должен работать только с IP-правилами группы "edm".

Также у групп IP-правил есть два режима работы:

1. trust – режим белого списка, при котором по умолчанию все запросы с любых IP-адресов запрещены. IP-правила в таком режиме используются для обозначения IP-адресов, которым разрешен доступ к EDM Issue.
2. deny – режим черного списка, при котором по умолчанию все запросы с любых IP-адресов разрешены. IP-правила в таком режиме используются для обозначения IP-адресов, которым запрещен доступ к EDM Issue.

Служебная группа IP-правил "web" работает в режиме "trust" без возможности смены режима. Служебная группа IP-правил "edm" работает по умолчанию в режиме "deny", при этом режим работы можно сменить в настройках EDM.

Для просмотра информации о группах IP-правил через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "iprules".
3. Ввести команду "show groups".

Пример вывода информации о группах IP-правил в EDM CLI

```
edmi-iprules> show groups
1. IP group: edm
Mode: deny

2. IP group: web
Mode: trust

edmi-iprules>
```

8.2 Просмотр существующих IP-правил в группе IP-правил

Для просмотра информации об IP-правилах в группе IP-правил через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "iprules".
3. Ввести команду "show iprules" с указанием группы IP-правил, IP-правила из которой требуется отобразить.

Пример вывода информации об IP-правилах в группе IP-правил в EDM CLI

```
edmi-iprules> show iprules --group edm
IP group: edm
Mode: deny


1. Group: edm
IP: 97.38.145.32/29
Status: block
Info: "08/06/2022 API DDoS"
Counter: 0
Registered: 2022-11-30 15:24:34
Updated: 2022-11-30 15:24:34

2. Group: edm
IP: 97.38.145.36
Status: allow
Info: "10/10/2022 Whitelisted from rule 97.38.145.32/29"
Registered: 2022-11-30 15:25:32
Updated: 2022-11-30 15:25:32

End of list
edmi-iprules>
```

Для просмотра информации об IP-правилах через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Ограничение доступа".

ⓘ В web-интерфейсе EDM Issue все взаимодействие с IP-правилами представлено только для служебной группы IP-правил "edm".

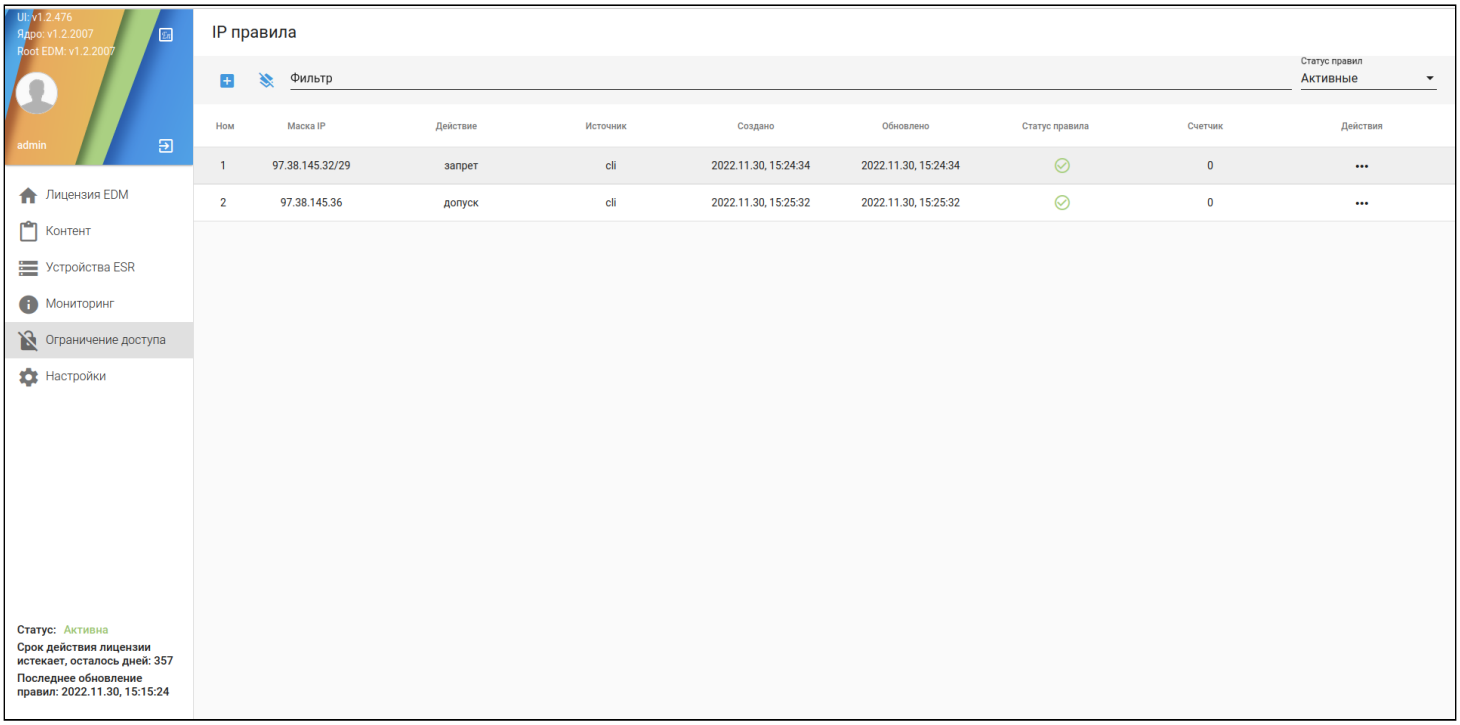


Рисунок 17 – Получение информации об IP-правилах в web-интерфейсе EDM Issue

Для просмотра более подробной информации об IP-правиле через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Ограничение доступа".
3. В крайней правой колонке для требуемого IP-правила вызвать контекстное меню и в нем выбрать пункт "Информация".

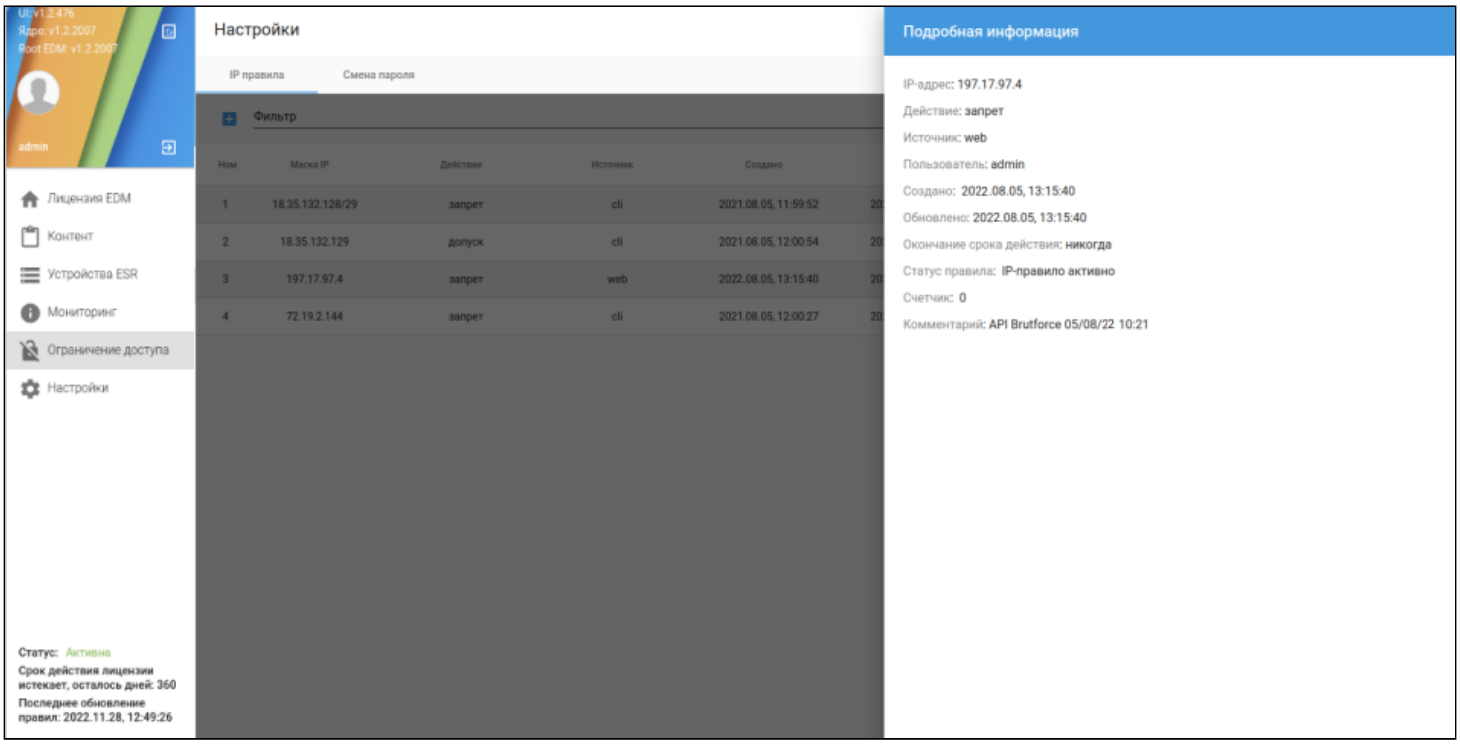


Рисунок 18 – Получение подробной информации об IP-правиле в web-интерфейсе EDM Issue

8.3 Создание IP-правила

IP-правила в EDM Issue бывают двух видов:

- allow – правила, разрешающие доступ к EDM Issue;
- block – правила, ограничивающие доступ к EDM Issue.

Соответственно при создании IP-правила нужно в параметре --action указать вид правила: для разрешающего IP-правила – "allow", а для ограничивающего IP-правила – "block".

Таким образом для создания IP-правила через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "iprules".
3. Ввести команду "add iprule".

Пример создания IP-правила в EDM CLI

```
edmi-iprules> add iprule --group edm --action block --ip 97.38.145.32/29 --info "08/06/2022 API
DDoS"
OK
edmi-iprules>

edmi-iprules> add iprule --action allow --group edm --ip 97.38.145.36/32 --info "10/10/2022
Whitelisted from rule 97.38.145.32/29"
OK
edmi-iprules>
```

Для создания IP-правила через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Ограничение доступа".
3. Нажать на кнопку  слева от поля фильтрации таблицы с IP-правилами.
4. Заполнить в появившемся окне информацию о новом IP-правиле, после чего нажать кнопку "Создать".

ⓘ В web-интерфейсе EDM Issue все взаимодействие с IP-правилами представленного только для служебной группы IP-правил "edm".

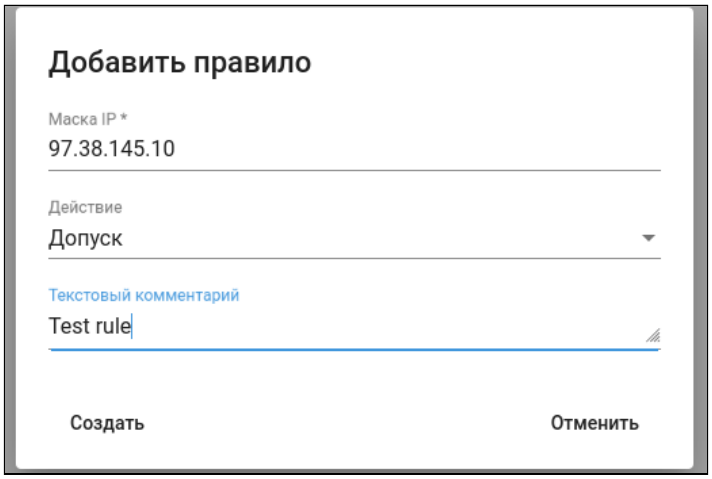


Рисунок 19 – Заполнение формы создания IP-правила в web-интерфейсе EDM Issue

8.4 Редактирование IP-правила

Для редактирования IP-правила через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "iprules".
3. Ввести команду "edit iprule" для редактирования IP-правила.

Пример редактирования IP-правила в EDM CLI

```
edmi-iprules> edit iprule --group edm --ip 97.38.145.32/29 --info "02/07/2021 API DDoS"
OK
edmi-iprules>
```

Для редактирования IP-правила через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Ограничение доступа".
3. В крайней правой колонке для требуемого IP-правила вызвать контекстное меню и в нем выбрать пункт "Редактировать".
4. В открывшемся окне произвести требуемые изменения IP-правила и нажать кнопку "Редактировать".

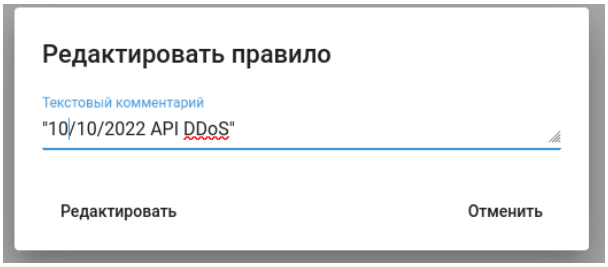


Рисунок 20 – Заполнение формы редактирования IP-правила в web-интерфейсе EDM Issue

8.5 Удаление IP-правила

Для удаления IP-правила через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "iprules".
3. Ввести команду "delete iprule" для удаления IP-правила.

Пример удаления IP-правила в EDM CLI

```
edmi-iprules> delete iprule  --group edm --ip 97.38.145.32/29
You will delete rule for IP 97.38.145.32/29. Are you sure? (y/N) y
OK
edmi-iprules>
```

Для удаления IP-правила через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Ограничение доступа".
3. В крайней правой колонке для требуемого IP-правила вызвать контекстное меню и в нем выбрать пункт "Удалить".

4. В открывшемся окне подтвердить удаление IP-правила нажатием кнопки "Удалить".

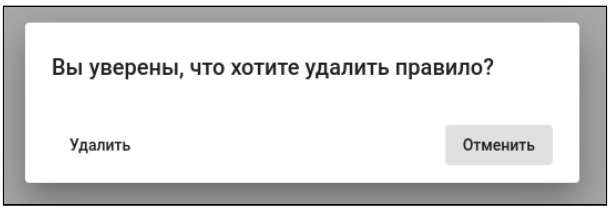


Рисунок 21 – Удаление IP-правила в web-интерфейсе EDM Issue

8.6 Очистка счетчика ограничивающего IP-правила

Для ограничивающих IP-правил на EDM Issue реализован счетчик срабатываний. Его значение можно посмотреть при выводе информации об IP-правилах как в CLI, так и в web. Помимо просмотра значения счетчика, его можно очистить.

Для очистки счетчика ограничивающего IP-правила через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "iprules".
3. Ввести команду "reset counter".

Пример очистки счетчика ограничивающего IP-правила в EDM CLI

```
edmi-iprules> show iprules --group edm
IP group: edm
Mode: deny


1. Group: edm
IP: 192.168.35.82
Status: block
Info: Block rule
Counter: 2
Registered: 2022-11-30 15:40:47
Updated: 2022-11-30 15:40:47

End of list
edmi-iprules> reset counter --group edm --ip 192.168.35.82
OK: Reset counter for rule with IP: 192.168.35.82
edmi-iprules> show iprules --group edm
IP group: edm
Mode: deny


1. Group: edm
IP: 192.168.35.82
Status: block
Info: Block rule
Counter: 0
Registered: 2022-11-30 15:40:47
Updated: 2022-11-30 15:40:47

End of list
edmi-iprules>
```

Если не указать параметр --ip, счетчики будут сброшены у всех правил в данной группе.

Для очистки счетчика ограничивающего IP-правила через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Ограничение доступа".
3. В крайней правой колонке для требуемого IP-правила вызвать контекстное меню и в нем выбрать пункт "Обнулить все счетчики".
4. В открывшемся окне подтвердить обнуление счетчиков нажатием кнопки "OK".

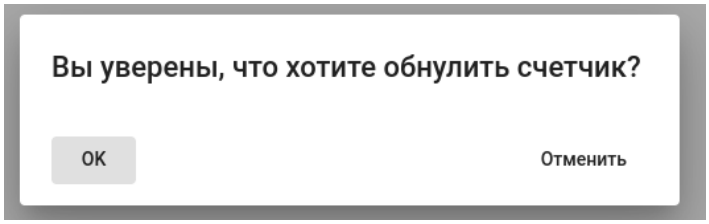


Рисунок 22 – Очистка счетчика ограничивающего IP-правила в web-интерфейсе EDM Issue

Для очистки всех счетчиков в группе edm ограничивающих IP-правил через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Ограничение доступа".
3. Нажать на кнопку  слева от поля фильтрации таблицы с IP-правилами.
4. В открывшемся окне подтвердить обнуление счетчиков нажатием кнопки "OK".

8.7 Перевод временного ограничивающего IP-правила в бессрочное

Системы ограничения доступа могут автоматически создавать ограничивающие IP-правила с определенным сроком действия. Администратор EDM Issue может переводить такие правила в бессрочный режим вручную.

Для перевода временного ограничивающего IP-правила в бессрочное через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "iprules".
3. Ввести команду "edit iprule" для требуемого правила с флагом "--unexpired".

Пример перевода временного ограничивающего IP-правила в бессрочное в EDM CLI

```
edmi-iprules> show iprules --group edm
IP group: edm
Mode: deny


1. IP: 109.88.52.0/25
Status: block
Info: 12/08/2022 Test Blocked Rule
Tool: web
Author: admin
Counter: 34
Registered: 2022-08-12 06:48:56
Updated: 2022-08-12 06:48:56
Expiry: 2022-08-15 20:55:36

End of list
edmi-iprules> edit iprule --group edm --ip 109.88.52.0/25 --unexpired
OK
edmi-iprules> show iprules --group edm
IP group: edm
Mode: deny


1. IP: 109.88.52.0/25
Status: block
Info: 12/08/2022 Test Blocked Rule
Tool: cli
Counter: 34
Registered: 2022-08-12 06:48:56
Updated: 2022-08-12 08:09:33

End of list
edmi-iprules>
```

8.8 Ограничение очереди запросов от клиентских устройств к EDM Issue

EDM Issue позволяет обрабатывать запросы нескольких клиентских устройств параллельно, обеспечивая высокую производительность системы и своевременное обслуживание запросов со стороны клиентских устройств. Однако при количестве одновременных запросов большем, чем EDM Issue может обработать параллельно, предусмотрен механизм постановки клиентских запросов в очередь. Это позволит не отказывать в обслуживании клиентам сразу, а взять их в работу позже, в момент, когда одна из текущих активных сессий будет завершена.

Администратор EDM Issue может управлять размером очереди и максимальным количеством одновременно обрабатываемых сессий через конфигурацию EDM Issue.

Для изменения максимального количества одновременно обрабатываемых клиентских сессий требуется:

1. Остановить EDM Issue командой "docker compose down", если он запущен.
2. В файле ".env" задать (или изменить при его наличии) параметр "EDM_THREAD_LIMIT".
3. Запустить EDM Issue командой "docker compose up -d". После запуска EDM Issue новое значение параметра вступит в силу.

Для изменения размера очереди клиентских запросов, ожидающих обработки, требуется:

1. Остановить EDM Issue командой "docker compose down", если он запущен.
2. В файле ".env" задать (или изменить при его наличии) параметр "EDM_QUEUE_LIMIT".
3. Запустить EDM Issue командой "docker compose up -d". После запуска EDM Issue новое значение параметра вступит в силу.

8.9 Ограничение числа запросов к EDM Issue с одного IP-адреса

На EDM Issue существует возможность установить максимальную частоту запросов от одного клиентского устройства в секунду и максимальную задержку при обмене данными между клиентским устройством и EDM Issue. При превышении любого из этих показателей клиентская сессия будет оборвана со стороны EDM Issue.

Администратор EDM Issue может управлять максимальной частотой запросов от одного клиентского устройства в секунду и максимальной задержкой при обмене данными между клиентским устройством и EDM Issue через конфигурацию EDM Issue.

Для изменения максимальной частоты запросов от одного клиентского устройства в секунду требуется:

1. Остановить EDM Issue командой "docker compose down", если он запущен.
2. В файле ".env" задать (или изменить при его наличии) параметр "EDM_DOS_FILTER_MAX_REQUESTS_PER_SECOND".
3. Запустить EDM Issue командой "docker compose up -d". После запуска EDM Issue новое значение параметра вступит в силу.

Для изменения максимальной задержки при обмене данными между клиентским устройством и EDM Issue требуется:

1. Остановить EDM Issue командой "docker compose down", если он запущен.
2. В файле ".env" задать (или изменить при его наличии) параметр "EDM_DOS_FILTER_DELAY_MS".
3. Запустить EDM Issue командой "docker compose up -d". После запуска EDM Issue новое значение параметра вступит в силу.

8.10 Настройка параметров автоматической блокировки клиентских устройств при нарушении процедуры аутентификации

На EDM Issue IP-адрес автоматически блокируется в случае фиксации с этого IP-адреса большого количества обращений за отведённый интервал времени, в которых:

- указаны неизвестные параметры клиентского устройства;
- нарушен порядок процедуры аутентификации.

Администратор EDM Issue может управлять как лимитами на некорректные обращения клиентских устройств на EDM Issue обоих типов, так и интервалом времени отслеживания некорректных обращений (т.е. будут считаться некорректные обращения за последние N часов).

Для изменения интервала отслеживания некорректных обращений через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "settings".
3. Установить новое значение параметра "securityCheckPeriodHours" командой "set".

```
edmi-settings> set --param securityCheckPeriodHours --value 2
OK
edmi-settings>
```

Для изменения интервала отслеживания некорректных обращений через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Настройки".
3. Перейти к категории настроек "Контроль подозрительной активности".
4. Установить новое значение параметра "Период учёта подозрительных событий".

Для изменения лимита обращений клиентского устройства на EDM Issue с неизвестными параметрами устройства через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "settings".
3. Установить новое значение параметра "sourceUnknownRequestLimit" командой "set".

```
edmi-settings> set --param sourceUnknownRequestLimit --value 15
OK
edmi-settings>
```

Для изменения интервала отслеживания некорректных обращений через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Настройки".
3. Перейти к категории настроек "Контроль подозрительной активности".
4. Установить новое значение параметра "Лимит запросов с неизвестными параметрами от одного и того же IP-адреса за период".

Для лимита обращений клиентского устройства на EDM Issue с некорректной процедурой аутентификации через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "settings".
3. Установить новое значение параметра "badAuthLimit" командой "set".

```
edmi-settings> set --param badAuthLimit --value 15
OK
edmi-settings>
```

Для изменения интервала отслеживания некорректных обращений через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Настройки".
3. Перейти к категории настроек "Контроль подозрительной активности".
4. Установить новое значение параметра "Лимит неуспешных аутентификаций с одного и того же IP-адреса за период".

9 Управление пользователями EDM Issue

В EDM Issue реализована поддержка пользователей с предоставлением доступа к различным функциям EDM Issue на основе системы разрешений. В EDM Issue представлены следующие виды разрешений:

- license-view — возможность просмотра информации о лицензии EDM, подключенных к EDM Issue клиентских устройствах и их сертификатах;
- license-manage — возможность управления лицензией EDM, подключенными к EDM Issue клиентскими устройствами и их сертификатами;
- ips-view — возможность просмотра информации о поставщиках IDS/IPS-правил и распространяемых в них категориях IDS/IPS-правил;
- ips-manage — возможность управления поставщиками IDS/IPS-правил и распространяемыми в них категориями IDS/IPS-правил;
- users-view — возможность просмотра информации о пользователях EDM Issue;
- users-manage — возможность управления пользователями EDM Issue;
- hosts-view — возможность просмотра информации о компонентах EDM Issue и настроенных IP-правилах;
- hosts-manage — возможность управления IP-правилами;
- settings-view — возможность просмотра текущих настроек EDM Issue;
- settings-manage — возможность управления текущими настройками EDM Issue.

Все разрешения для пользователей EDM Issue для удобства сгруппированы в три роли, которые задаются при создании или изменении пользователя:

1. watcher — наблюдатель, в его права заложен только просмотр общей информации о функционировании EDM Issue без каких-либо прав управления. Поддержанные разрешения:
    a. license-view
    b. ips-view
    c. users-view
    d. hosts-view
2. manager — менеджер, его права позволяют осуществлять просмотр и управление всем функционалом EDM Issue за исключением управления другими пользователями и настройками EDM Issue. Поддержанные разрешения:
    a. license-view
    b. license-manage
    c. ips-view
    d. ips-manage
    e. users-view
    f. hosts-view
    g. hosts-manage
    h. settings-view
3. admin — администратор, его права позволяют осуществлять просмотр и управление всем функционалом EDM Issue. Поддержанные разрешения:
    a. license-view
    b. license-manage

c. ips-view
d. ips-manage
e. users-view
f. users-manage
g. hosts-view
h. hosts-manage
i. settings-view
j. settings-manage

Также у пользователей EDM Issue существует установка и смена статуса пользователя. Поддержанные статусы:

- valid — активный, неограниченный пользователь;
- suspect — активный пользователь, который длительное время не менял пароль, после успешной авторизации ему будет рекомендована смена пароля без принуждения к этому;
- initialize — активный пользователь, который длительное время не менял пароль, после успешной авторизации для него будут доступны не все функции EDM Issue, пока пользователь не сменит пароль;
- blocked — заблокированный пользователь, для которого запрещены авторизация и любое взаимодействие с EDM Issue. В отличие от первых трех статусов данный статус может иметь срок действия, по истечению которого статус пользователя сменится на "valid".

В системе при первом запуске существует предустановленный пользователь admin со следующими характеристиками:

- Логин: admin
- Пароль: password
- Статус: initialize

Администратор EDM Issue со своей стороны может:

- просматривать информацию о пользователях;
- просматривать подробную информацию по конкретному пользователю;
- создавать нового пользователя;
- редактировать существующего пользователя;
- удалять существующего пользователя;
- менять пароль существующего пользователя;
- устанавливать время жизни пользовательской сессии в web-интерфейсе EDM Issue;
- управлять политикой устаревания паролей пользователей;
- управлять политикой блокировки пользователя за превышение количества попыток некорректной авторизации.

9.1 Просмотр информации о пользователях

Для просмотра информации о пользователях EDM Issue через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "users".
3. Ввести команду "show users".

Пример вывода информации о пользователях EDM Issue в EDM CLI

```
edmi-users> show users
1. Login: admin
Permissions: admin
Status: valid

2. Login: blocked_user
Name: Blocked
Surname: Test
Registered: 2022-11-30 17:06:53
Permissions: LV/LM/IV/IM/UV/UM/HV/HM/SV/SM
Status: blocked

3. Login: manager
Name: Manager
Surname: Test
Registered: 2022-11-30 17:07:29
Permissions: LV/LM/IV/IM/UV/HV/HM/SV
Status: valid

4. Login: watcher
Name: Watcher
Surname: Test
Registered: 2022-11-30 17:07:50
Permissions: LV/IV/HV/UV
Status: valid

End of list
edmi-users>
```

9.2 Просмотр подробной информации по конкретному пользователю

Для просмотра подробной информации по конкретному пользователю EDM Issue через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "users".
3. Ввести команду "show user" с указанием имени нужного пользователя.

Пример вывода подробной информации по конкретному пользователю EDM Issue в EDM CLI

```
edmi-users> show user --login manager
Login: manager
Name: Manager
Surname: Test
Registered: 2022-11-30 17:07:29
Permissions:

    license-view
    license-manage
    ips-view
    ips-manage
    users-view
    hosts-view
    hosts-manage
    settings-view

Password changed: 2022-11-30 17:07:29
Status info:

    Status: valid
    Changed: 2022-11-30 17:07:29

Stats:

    Strikes: 0


edmi-users>
```

9.3 Создание нового пользователя

Для создания нового пользователя через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "users".
3. Ввести команду "add" с параметрами нового пользователя.

Пример создания нового пользователя в EDM CLI

```
edmi-users> add --login manager --name Manager --surname Test --role manager
Enter new password (Ctrl+C to cancel): ********
Repeat new password (Ctrl+C to cancel): ********
OK
edmi-users>
```

9.4 Редактирование существующего пользователя

Для редактирования существующего пользователя через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "users".
3. Ввести команду "edit" с параметрами, которые требуется изменить для указанного пользователя.

Пример редактирования существующего пользователя в EDM CLI

```
edmi-users> edit --login manager --status initialize --info "Need to change password"
OK
edmi-users>
```

9.5 Удаление существующего пользователя

Для удаления существующего пользователя через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "users".
3. Ввести команду "delete" с указанием удаляемого пользователя.

Пример удаления существующего пользователя в EDM CLI

```
edmi-users> delete --login blocked_user
You will delete user 'blocked_user'. Are you sure? (y/N) y
OK
edmi-users>
```

9.6 Смена пароля существующего пользователя

Для смены пароля существующего пользователя через CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "users".
3. Ввести команду "set password" с указанием пользователя, чей пароль будет изменен.

Пример смены пароля существующего пользователя в EDM CLI

```
edmi-users> set password --login admin
Enter new password (Ctrl+C to cancel): *********
Repeat new password (Ctrl+C to cancel): *********
Password has been successfully changed
OK
edmi-users>
```

Для смены пароля текущего пользователя через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в раздел меню "Настройки".
3. Перейти в подраздел "Смена пароля".

4. Заполнить форму смены пароля, указав текущий пароль учетной записи и новый пароль с повторным вводом пароля.
5. Нажать кнопку "Сохранить", чтобы изменить пароль учетной записи на новый.

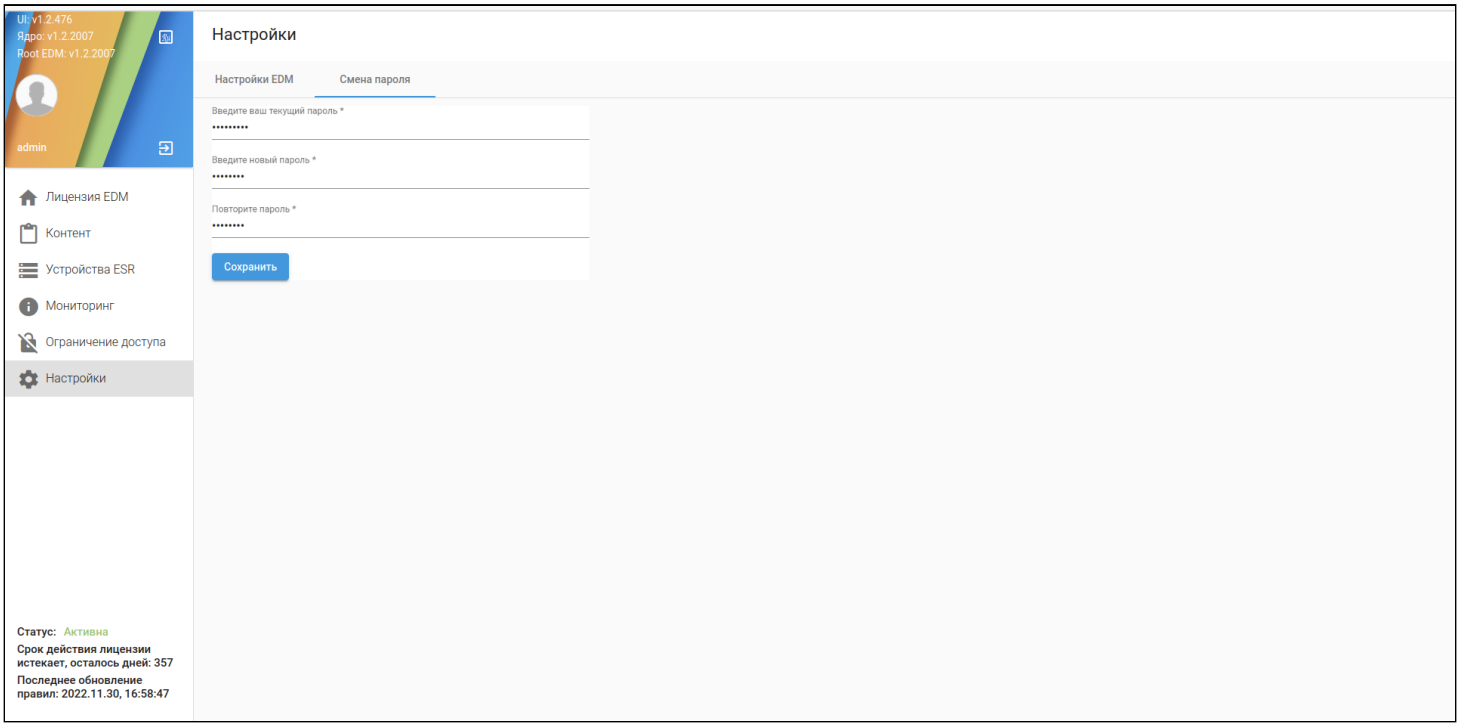


Рисунок 22 – Заполнение формы смены пароля пользователя в web-интерфейсе EDM Issue

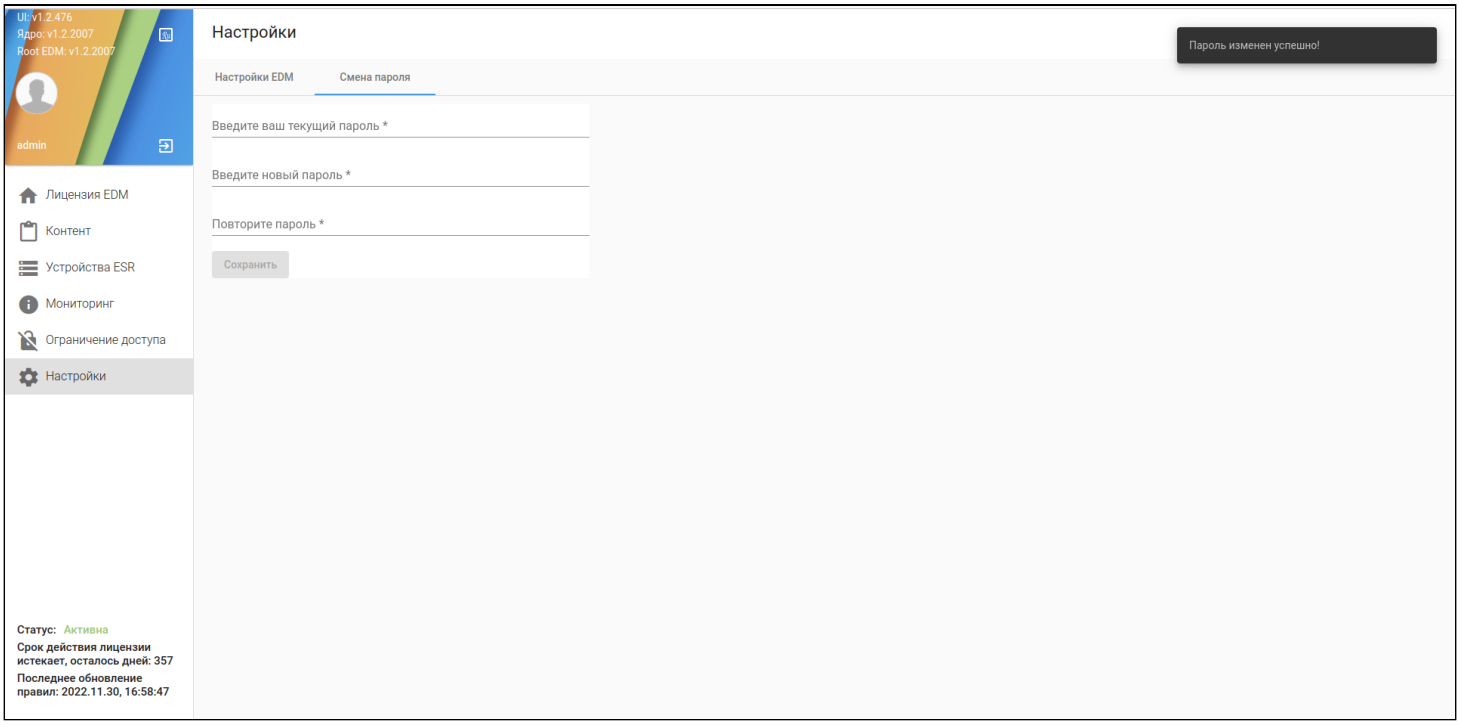


Рисунок 23 – Успешная смена пароля пользователя в web-интерфейсе EDM Issue

9.7 Установка времени жизни пользовательской сессии в web-интерфейсе EDM Issue

После успешной авторизации в web-интерфейсе EDM Issue пользовательская сессия существует некоторое время, а затем закрывается на стороне сервера. После этого пользователь выходит из учетной записи и вынужден произвести повторный вход в web-интерфейс EDM. Существует два настраиваемых таймаута для пользовательских сессий – короткий, работающий в том случае, если пользователь в форме авторизации не устанавливает флаг "Запомнить меня", и длинный – когда флаг "Запомнить меня" устанавливается.

За интервал жизни пользовательской сессии без установленного флага "Запомнить меня" отвечает параметр "webSessionMaxHours" в настройках EDM Issue. Для изменения интервала жизни пользовательской сессии без установленного флага "Запомнить меня" через EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "settings".
3. Установить новое значение параметра "webSessionMaxHours" командой "set".

Пример изменения интервала жизни пользовательской сессии без установленного флага "Запомнить меня" в EDM CLI

```
edmi-settings> show --param webSessionMaxHours
User web session timeout in hours
webSessionMaxHours = 24 [default]

edmi-settings> set --param webSessionMaxHours --value 12
OK
edmi-settings> show --param webSessionMaxHours
User web session timeout in hours
webSessionMaxHours = 12

edmi-settings>
```

Для изменения интервала жизни пользовательской сессии без установленного флага "Запомнить меня" через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Настройки".
3. Перейти к категории настроек "Взаимодействие с Web-интерфейсом".
4. Установить новое значение параметра "Период активности сессии авторизованного Web-пользователя".

За интервал жизни пользовательской сессии с установленным флагом "Запомнить меня" отвечает параметр "webSessionRememberedMaxHours" в настройках EDM Issue. Для изменения интервала жизни пользовательской сессии с установленным флагом "Запомнить меня" через EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "settings".
3. Установить новое значение параметра "webSessionRememberedMaxHours" командой "set".

Пример изменения интервала жизни пользовательской сессии с установленным флагом "Запомнить меня" в EDM CLI

```
edmi-settings> show --param webSessionRememberedMaxHours
User web session timeout with flag 'remember me' in hours
webSessionRememberedMaxHours = 168 [default]

edmi-settings> set --param webSessionRememberedMaxHours --value 120
OK
edmi-settings> show --param webSessionRememberedMaxHours
User web session timeout with flag 'remember me' in hours
webSessionRememberedMaxHours = 120

edmi-settings>
```

Для изменения интервала жизни пользовательской сессии с установленным флагом "Запомнить меня" через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Настройки".
3. Перейти к категории настроек "Взаимодействие с Web-интерфейсом".
4. Установить новое значение параметра "Период активности сессии авторизованного Web-пользователя с флагом 'Запомнить меня'".

9.8 Управление политикой устаревания паролей пользователей

Политика устаревания паролей создана с целью контроля за сроками жизни паролей пользователей и организации регулярных обновлений паролей учетных записей пользователей. В случае если эта функция включена, то после прохождения определенного времени с момента последней смены пароля пользователь будет предупрежден об устаревании своего пароля с предложением сменить его. Также при прохождении определенного интервала времени без смены пароля пользователь после авторизации не сможет продолжать работу с EDM Issue без смены пароля учетной записи.

За включение и отключение политики устаревания паролей отвечает параметр "userCheckPassValid" в настройках EDM Issue. Для включения или отключения политики устаревания паролей через EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "settings".
3. Установить новое значение параметра "userCheckPassValid" командой "set".

Пример отключения политики устаревания паролей в EDM CLI

```
edmi-settings> show --param userCheckPassValid
Check user passwords validity expiration
userCheckPassValid = 1 [default]

edmi-settings> set --param userCheckPassValid --value 0
OK
edmi-settings> show --param userCheckPassValid
Check user passwords validity expiration
userCheckPassValid = 0

edmi-settings>
```

Для включения или отключения политики устаревания паролей через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Настройки".
3. Перейти к категории настроек "Взаимодействие с Web-интерфейсом".
4. Установить новое значение параметра "Проверять устаревшие пароли пользователей".

За интервал времени, по прошествии которого пользователю будет предложено сменить пароль учетной записи, отвечает параметр "userPassValidDays" в настройках EDM Issue. Для изменения интервала времени, по прошествии которого пользователю будет предложено сменить пароль учетной записи, через EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "settings".
3. Установить новое значение параметра "userPassValidDays" командой "set".

Пример изменения интервала времени, по прошествии которого пользователю будет предложено сменить пароль учетной записи в EDM CLI

```
edmi-settings> show --param userPassValidDays
User password validity period in days (before suspect status)
userPassValidDays = 180 [default]

edmi-settings> set --param userPassValidDays --value 30
OK
edmi-settings> show --param userPassValidDays
User password validity period in days (before suspect status)
userPassValidDays = 30

edmi-settings>
```

Для включения или отключения политики устаревания паролей через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Настройки".
3. Перейти к категории настроек "Взаимодействие с Web-интерфейсом".
4. Установить новое значение параметра "Период использования пароля пользователя до уведомления о необходимости изменения".

За интервал времени, по прошествии которого пользователь будет обязан сменить пароль учетной записи, отвечает параметр "userAddPassValidDays" в настройках EDM Issue. Для изменения интервала времени, по прошествии которого пользователь будет обязан сменить пароль учетной записи, через EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "settings".
3. Установить новое значение параметра "userAddPassValidDays" командой "set".

Пример изменения интервала времени, по прошествии которого пользователь будет обязан сменить пароль учетной записи в EDM CLI

```
edmi-settings> show --param userAddPassValidDays
User password additional validity period in days (before initialize status)
userAddPassValidDays = 180 [default]

edmi-settings> set --param userAddPassValidDays --value 60
OK
edmi-settings> show --param userAddPassValidDays
User password additional validity period in days (before initialize status)
userAddPassValidDays = 60

edmi-settings>
```

Для изменения интервала времени, по прошествии которого пользователь будет обязан сменить пароль учетной записи, через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Настройки".
3. Перейти к категории настроек "Взаимодействие с Web-интерфейсом".
4. Установить новое значение параметра "Дополнительный период использования пароля пользователя до принудительного изменения".

9.9 Управление политикой блокировки пользователя за превышение количества попыток некорректной авторизации

В EDM Issue предусмотрена временная блокировка аккаунтов пользователей при превышении количества попыток некорректной авторизации. Количество таких попыток, необходимых для блокировки аккаунта, и срок блокировки могут быть настроены администратором EDM Issue.

За количество попыток некорректной авторизации, при достижении которых пользователь будет заблокирован, отвечает параметр "userBadAuthLimit" в настройках EDM Issue. Для настройки количества попыток некорректной авторизации, при достижении которых пользователь будет заблокирован, через EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "settings".
3. Установить новое значение параметра "userBadAuthLimit" командой "set".

Пример настройки количества попыток некорректной авторизации, при достижении которых пользователь будет заблокирован в EDM CLI

```
edmi-settings> show --param userBadAuthLimit
Limit on the number of unsuccessful authorization attempts before blocking a user
userBadAuthLimit = 6 [default]

edmi-settings> set --param userBadAuthLimit --value 10
OK
edmi-settings> show --param userBadAuthLimit
Limit on the number of unsuccessful authorization attempts before blocking a user
userBadAuthLimit = 10

edmi-settings>
```

Для настройки количества попыток некорректной авторизации, при достижении которых пользователь будет заблокирован, через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Настройки".
3. Перейти к категории настроек "Взаимодействие с Web-интерфейсом".
4. Установить новое значение параметра "Лимит неуспешных попыток авторизации перед автоматической блокировкой пользователя".

За время блокировки пользователя, для которого был превышен лимит некорректных попыток авторизации, отвечает параметр "userBlockMinutes" в настройках EDM Issue. Для настройки времени блокировки пользователя, для которого был превышен лимит некорректных попыток авторизации, через EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "settings".
3. Установить новое значение параметра "userBlockMinutes" командой "set".

Пример настройки времени блокировки пользователя, для которого был превышен лимит некорректных попыток авторизации в EDM CLI

```
edmi-settings> show --param userBlockMinutes
Duration of one user lock in minutes
userBlockMinutes = 5 [default]

edmi-settings> set --param userBlockMinutes --value 30
OK
edmi-settings> show --param userBlockMinutes
Duration of one user lock in minutes
userBlockMinutes = 30

edmi-settings>
```

Для настройки времени блокировки пользователя, для которого был превышен лимит некорректных попыток авторизации, через web-интерфейс требуется:

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Настройки".
3. Перейти к категории настроек "Взаимодействие с Web-интерфейсом".
4. Установить новое значение параметра "Длительность автоматической блокировки пользователя".

10 Управление настройками EDM Issue

- IP-адрес, на котором будут работать EDM-сервисы
- Максимальное количество одновременно поддерживаемых сессий
- Размер очереди для клиентских запросов
- Размер очереди для клиентских запросов
- Максимальное число запросов в секунду к EDM Issue с одного IP-адреса
- Максимальная задержка при взаимодействии клиентского устройства и EDM Issue
- Максимальный размер файла с логами для ротации
- Максимальное количество файлов с логами для ротации
- Интервал отслеживания некорректных обращений на EDM Issue
- Уровень логирования для событий ядра EDM Issue
- Уровень логирования для внутренних событий EDM Issue
- Уровень логирования для событий взаимодействия компонентов EDM Issue с базой данных EDM Issue
- Уровень логирования для событий сети EDM Issue
- Уровень логирования для событий безопасности EDM Issue
- Уровень логирования для событий, генерируемых компонентами EDM Issue
- Уровень логирования для событий ядра EDM Issue CLI
- Уровень логирования для внутренних событий EDM Issue CLI
- Уровень логирования для событий взаимодействия EDM Issue CLI с базой данных EDM Issue
- Уровень логирования для событий сети EDM Issue CLI
- Уровень логирования для событий безопасности EDM Issue CLI

За поведение EDM Issue отвечают настройки EDM Issue, которые глобально можно изменить в двух местах:

1. Настройки EDM Issue, хранящиеся в базе данных EDM Issue:
   a. Изменение настроек через EDM CLI;
   b. Изменение настроек через web-интерфейс.
2. Файл с переменными окружения .env.

10.1 Внесение изменений в настройки EDM Issue через EDM CLI

Для внесения изменений в настройки EDM Issue через EDM CLI требуется:

1. Запустить EDM CLI.
2. Перейти в раздел "settings".
3. Установить новое значение параметра командой "set", указав в параметре "--param" имя изменяемого параметра настроек EDM Issue, а в параметре "--value" новое значение параметра настроек EDM Issue.

Пример изменения настроек EDM Issue в EDM CLI

```
edmi-settings> show --param webSessionMaxHours
User web session timeout in hours
webSessionMaxHours = 24

edmi-settings> set --param webSessionMaxHours --value 12
OK
edmi-settings> show --param webSessionMaxHours
User web session timeout in hours
webSessionMaxHours = 12

edmi-settings>
```

10.2 Внесение изменений в настройки EDM Issue через web-интерфейс

1. Авторизоваться в web-интерфейсе EDM Issue.
2. Перейти в меню в раздел "Настройки".
3. Перейти к требуемой категории настроек.
4. Установить новое значение параметра необходимого параметра.

Изменить настройки можно, нажав по соответствующему параметру в колонке "Значение". После установки нового значения необходимо нажать кнопку ✓ для применения изменений.

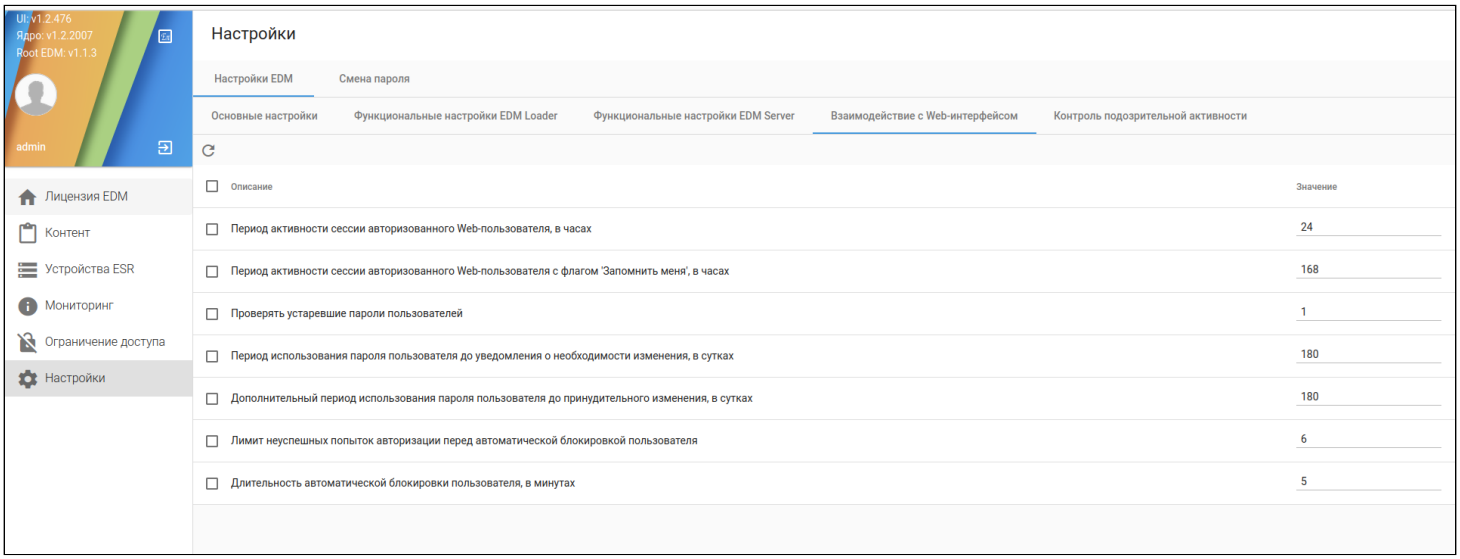


Рисунок 24 – Изменение настроек через web-интерфейс EDM Issue

10.3 Внесение изменений в настройки EDM Issue через переменные окружения

Для внесения изменений в настройки EDM Issue через переменные окружения требуется:

1. Остановить EDM Issue командой "docker-compose down", если он запущен.
2. В файле ".env" задать (или изменить при его наличии) требуемый параметр настроек EDM Issue.
3. Запустить EDM Issue командой "docker-compose up -d". После запуска EDM Issue новое значение параметра настроек EDM Issue вступит в силу.

Пример изменения настроек EDM Issue через переменные окружения

```
edm@edm-server:/opt/edm$ diff .env .env-changed
9c9
< EDM_DOS_FILTER_MAX_REQUESTS_PER_SECOND=5
---
> EDM_DOS_FILTER_MAX_REQUESTS_PER_SECOND=10
```

10.4 Настройка EDM Issue через EDM CLI и web-интерфейс

10.4.1 Имя хоста Issue EDM Loader

Описание параметра

Имя хоста Issue EDM Loader

Значение по умолчанию

Issue EDM Loader

Допустимые значения для параметра

не более 255 символов, допустимые символы — " _-."

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Имя хоста Issue EDM Loader

Именование параметра в разделе "settings" EDM CLI

loaderHostTitle

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param loaderHostTitle --value LoaderIssue
OK
edmi-settings>
```

10.4.2 Имя хоста Issue EDM Server

Описание параметра

Имя хоста Issue EDM Server

Значение по умолчанию

Issue EDM Server

Допустимые значения для параметра

не более 255 символов, допустимые символы — " _-."

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Имя хоста Issue EDM Server

Именование параметра в разделе "settings" EDM CLI

serverHostTitle

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param serverHostTitle --value ServerIssue
OK
edmi-settings>
```

10.4.3 Интервал сохранения данных EDM о самом себе

Описание параметра

Интервал сохранения данных EDM о самом себе

Значение по умолчанию

300 секунд

Допустимые значения для параметра

5–3600 секунд

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Интервал актуализации информации о работающем сервисе EDM

Именование параметра в разделе "settings" EDM CLI

selfInfoSaveIntervalSeconds

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param selfInfoSaveIntervalSeconds --value 500
OK
edmi-settings>
```

10.4.4 Ключ лицензии

Описание параметра

Ключ лицензии

Значение по умолчанию

Пустая строка

Допустимые значения для параметра

не более 128 символов

Обязательность указания значения для параметра

Параметр является обязательным

Именование параметра в web-интерфейсе EDM Issue

Ключ лицензии EDM

Именование параметра в разделе "settings" EDM CLI

licenseKey

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param licenseKey --value TEST-KEY
OK
edmi-settings>
```

10.4.5 Адрес Root-сервера

Описание параметра

Адрес Root-сервера

Значение по умолчанию

https://edm.eltex-co.ru:8098/

Допустимые значения для параметра

Формат URL

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Адрес Root-сервера EDM

Именование параметра в разделе "settings" EDM CLI

rootUrl

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param rootUrl --value https://192.168.10.10:8098
OK
edmi-settings>
```

10.4.6 Режим защищённого хоста для Issue EDM Loader

Описание параметра

Режим защищённого хоста для Issue EDM Loader

Значение по умолчанию

0

Допустимые значения для параметра

1 (вкл) или 0 (выкл)

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Режим защищённого хоста для Issue EDM Loader

Именование параметра в разделе "settings" EDM CLI

loaderHostProtectMode

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param loaderHostProtectMode --value 1
OK
edmi-settings>
```

10.4.7 Интервал автоматической загрузки актуальных IDS/IPS-правил

Описание параметра

Интервал времени, через который EDM Issue будет загружать актуальные IDS/IPS-правила с EDM Root в случае лицензируемых IDS/IPS поставщиков правил и с пользовательских серверов, указанных в пользовательских поставщиках IDS/IPS-правил

Значение по умолчанию

15 минут

Допустимые значения для параметра

1–720 минут

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Интервал загрузки контента с Root-сервера

Именование параметра в разделе "settings" EDM CLI

ipsLoadIntervalMinutes

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param ipsLoadIntervalMinutes --value 360
OK
edmi-settings>
```

10.4.8 Интервал автоматической синхронизации списка подключенных к EDM Issue устройств с EDM Root

Описание параметра

Интервал автоматической синхронизации списка подключенных к EDM Issue устройств с EDM Root

Значение по умолчанию

720 часов

Допустимые значения для параметра

72–8760 часов

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Интервал синхронизации списка устройств по данным с Root-сервера

Именование параметра в разделе "settings" EDM CLI

deviceSyncIntervalHours

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param deviceSyncIntervalHours --value 300
OK
edmi-settings>
```

10.4.9 Количество устройств в запросе синхронизации списка подключенных к EDM Issue устройств с EDM Root

Описание параметра

Количество устройств в запросе синхронизации списка подключенных к EDM Issue устройств с EDM Root.

Значение по умолчанию

200 устройств в запросе синхронизации

Допустимые значения для параметра

10–5000 устройств в запросе синхронизации

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Количество устройств, запрашиваемое в одном запросе при синхронизации списка по данным с Root-сервера

Именование параметра в разделе "settings" EDM CLI

deviceSyncAmount

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param deviceSyncAmount --value 100
OK
edmi-settings>
```

10.4.10 Режим работы IP-правил группы IP-правил "edm"

Описание параметра

Режим работы IP-правил группы IP-правил "edm"

Значение по умолчанию

deny

Допустимые значения для параметра

- deny
- trust

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Режим работы IP-правил для группы EDM

Именование параметра в разделе "settings" EDM CLI

edmIpRulesMode

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param edmIpRulesMode --value trust
OK
edmi-settings>
```

10.4.11 Таймаут неактивности сессий при взаимодействии с клиентскими устройствами

Описание параметра

Таймаут неактивности сессий с клиентскими устройствами. В случае если со стороны клиентского устройства в течение указанного таймаута не было принято ни одного запроса, сессия будет разорвана со стороны EDM Issue

Значение по умолчанию

300 секунд

Допустимые значения для параметра

30–600 секунд

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Таймаут неактивности сессии для устройств

Именование параметра в разделе "settings" EDM CLI

deviceSessionTimeout

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param deviceSessionTimeout --value 100
OK
edmi-settings>
```

10.4.12 Таймаут ожидания следующего запроса от клиентского устройства в рамках текущей сессии

Описание параметра

Таймаут, отвечающий за максимальное время ожидания следующего запроса от клиентского устройства в рамках текущей открытой сессии. В случае если со стороны клиентского устройства в течение указанного таймаута не было принято нового запроса, сессия будет разорвана со стороны EDM Issue

Значение по умолчанию

60 секунд

Допустимые значения для параметра

30–300 секунд

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Таймаут ожидания следующего запроса от устройства

Именование параметра в разделе "settings" EDM CLI

deviceRequestTimeout

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param deviceRequestTimeout --value 100
OK
edmi-settings>
```

10.4.13 Таймаут ожидания ответа от EDM Root при взаимодействии с клиентским устройством

Описание параметра

Таймаут, отвечающий за максимальное время ожидания ответа от EDM Root на запрос, выполненный в рамках текущей сессии с клиентским устройством. Если EDM Root не отвечает на запрос в течение указанного таймаута, то сессия с клиентским устройством будет разорвана со стороны EDM Issue

Значение по умолчанию

300 секунд

Допустимые значения для параметра

30–300 секунд

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Таймаут ожидания ответа от Root-сервера по запросу от устройства

Именование параметра в разделе "settings" EDM CLI

deviceRootAnswerTimeout

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param deviceRootAnswerTimeout --value 100
OK
edmi-settings>
```

10.4.14 Таймаут неактивности сессий при взаимодействии с web-сервисом EDM Issue

Описание параметра

Таймаут неактивности сессий с web-сервисом EDM Issue. В случае, если со стороны web-сервиса EDM Issue в течение указанного таймаута не было принято ни одного запроса, сессия будет разорвана со стороны EDM Issue

Значение по умолчанию

1800 секунд

Допустимые значения для параметра

300–86400 секунд

Обязательность указания значения для параметра

Параметр не является обязательным.

Именование параметра в web-интерфейсе EDM Issue

Таймаут неактивности сессии для web-интерфейса

Именование параметра в разделе "settings" EDM CLI

webSessionTimeout

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param webSessionTimeout --value 2400
OK
edmi-settings>
```

10.4.15 Таймаут выполнения команд

Описание параметра

Таймаут выполнения команд

Значение по умолчанию

2 минуты

Допустимые значения для параметра

1–30 минут

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Таймаут выполнения команд сервером EDM

Именование параметра в разделе "settings" EDM CLI

commandTimeoutMinutes

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param commandTimeoutMinutes --value 4
OK
edmi-settings>
```

10.4.16 Период хранения информации о неактивных компонентах EDM Issue

Описание параметра

Таймаут, отвечающий за максимальное время хранения EDM Issue информации о входящих в него компонентах. По истечении данного таймаута информация об устаревших компонентах EDM Issue будет удалена.

Значение по умолчанию

180 суток

Допустимые значения для параметра

1–1825 суток

Обязательность указания значения для параметра

Параметр не является обязательным.

Именование параметра в web-интерфейсе EDM Issue

Период хранения сведений о неактивных хостах EDM

Именование параметра в разделе "settings" EDM CLI

inactiveHostsKeepDays

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param inactiveHostsKeepDays --value 10
OK
edmi-settings>
```

10.4.17 Время жизни пользовательской сессии в web-интерфейсе EDM Issue без установленного флага "Запомнить меня"

Описание параметра

Время жизни пользовательской сессии web-интерфейса EDM Issue без установленного флага "Запомнить меня", по окончании которого сессия будет прервана и пользователю потребуется повторная авторизация

Значение по умолчанию

24 часов

Допустимые значения для параметра

1–168 часов

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Период активности сессии авторизованного web-пользователя

Именование параметра в разделе "settings" EDM CLI

webSessionMaxHours

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param webSessionMaxHours --value 48
OK
edmi-settings>
```

10.4.18 Время жизни пользовательской сессии в web-интерфейсе EDM Issue с установленным флагом "Запомнить меня"

Описание параметра

Время жизни пользовательской сессии web-интерфейса EDM Issue с установленным флагом "Запомнить меня", по окончании которого сессия будет прервана и пользователю потребуется повторная авторизация

Значение по умолчанию

168 часов

Допустимые значения для параметра

1–4320 часов

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Период активности сессии авторизованного web-пользователя с флагом "Запомнить меня"

Именование параметра в разделе "settings" EDM CLI

webSessionRememberedMaxHours

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param webSessionRememberedMaxHours --value 100
OK
edmi-settings>
```

10.4.19 Включение политики устаревания паролей пользователей

Описание параметра

Включение и отключение политики устаревания паролей пользователей. Включение этой опции запускает механизм контроля частоты смены паролей пользователей и своевременную смену статусов пользователей.

Значение по умолчанию

1

Допустимые значения для параметра

- 0 – политика выключена
- 1 – политика включена

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Проверять устаревшие пароли пользователей

Именование параметра в разделе "settings" EDM CLI

userCheckPassValid

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param userCheckPassValid --value 0
OK
edmi-settings>
```

10.4.20 Интервал времени, по прошествии которого пользователю будет предложено сменить пароль учетной записи

Описание параметра

Интервал времени, по прошествии которого пользователю будет предложено сменить пароль учетной записи

Значение по умолчанию

180 суток

Допустимые значения для параметра

3–365 суток

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Период использования пароля пользователя до уведомления о необходимости изменения

Именование параметра в разделе "settings" EDM CLI

userPassValidDays

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param userPassValidDays --value 220
OK
edmi-settings>
```

10.4.21 Интервал времени, по прошествии которого пользователь будет обязан сменить пароль учетной записи

Описание параметра

Интервал времени, по прошествии которого пользователь будет обязан сменить пароль учетной записи

Значение по умолчанию

180 суток

Допустимые значения для параметра

3–365 суток

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Дополнительный период использования пароля пользователя до принудительного изменения

Именование параметра в разделе "settings" EDM CLI

userAddPassValidDays

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param userAddPassValidDays --value 220
OK
edmi-settings>
```

10.4.22 Максимальное количество попыток некорректной авторизации пользователя до временной блокировки

Описание параметра

Максимальное количество попыток некорректной авторизации пользователя, при достижении которых аккаунт пользователя будет временно заблокирован

Значение по умолчанию

6 попыток некорректной авторизации до блокировки

Допустимые значения для параметра

3–20 попыток некорректной авторизации до блокировки

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Лимит неуспешных попыток авторизации перед автоматической блокировкой пользователя

Именование параметра в разделе "settings" EDM CLI

userBadAuthLimit

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param userBadAuthLimit --value 10
OK
edmi-settings>
```

10.4.23 Период временной блокировки пользователя, для которого было превышено количество попыток некорректной авторизации

Описание параметра

Период временной блокировки пользователя, для которого был превышен лимит некорректных попыток авторизации

Значение по умолчанию

5 минут

Допустимые значения для параметра

1–1440 минут

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Длительность автоматической блокировки пользователя

Именование параметра в разделе "settings" EDM CLI

userBlockMinutes

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param userBlockMinutes --value 10
OK
edmi-settings>
```

10.4.24 Период учёта подозрительных событий

Описание параметра

Период учёта подозрительных событий

Значение по умолчанию

1 час

Допустимые значения для параметра

1–72 часа

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Период учёта подозрительных событий

Именование параметра в разделе "settings" EDM CLI

securityCheckPeriodHours

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param securityCheckPeriodHours --value 14
OK
edmi-settings>
```

10.4.25 Лимит на запросы с неизвестными параметрами от одного и того же IP-адреса за период

Описание параметра

Лимит на запросы с неизвестными параметрами от одного и того же IP-адреса за период

Значение по умолчанию

10 событий

Допустимые значения для параметра

1–1000 событий

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Лимит запросов с неизвестными параметрами от одного и того же IP-адреса за период

Именование параметра в разделе "settings" EDM CLI

sourceUnknownRequestLimit

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param sourceUnknownRequestLimit --value 300
OK
edmi-settings>
```

10.4.26 Лимит на количество неуспешных аутентификаций с одного и того же IP-адреса за период

Описание параметра

Лимит на количество неуспешных аутентификаций с одного и того же IP-адреса за период

Значение по умолчанию

10 событий

Допустимые значения для параметра

1–1000 событий

Обязательность указания значения для параметра

Параметр не является обязательным

Именование параметра в web-интерфейсе EDM Issue

Лимит неуспешных аутентификаций с одного и того же IP-адреса за период

Именование параметра в разделе "settings" EDM CLI

badAuthLimit

Пример указания значения параметра через EDM CLI

```
edmi-settings> set --param badAuthLimit --value 300
OK
edmi-settings>
```

10.5 Настройки EDM Issue через .env файл

10.5.1 Версия EDM Issue

Описание параметра

Версия используемых EDM Issue Docker образов

Значение по умолчанию

Отсутствует

Допустимые значения для параметра

Текстовая строка длиной до 32 символов

Обязательность указания значения для параметра

Параметр является обязательным

Именование переменной окружения для указания значения параметра

EDM_TAG

Пример указания значения параметра через переменную окружения

```
EDM_TAG=1.2
```

10.5.2 Часовой пояс

Описание параметра

Имя часового пояса, которое будет использовано внутри контейнера

Значение по умолчанию

"UTC"

Допустимые значения для параметра

Название часового пояса в формате timezone database (официальный сайт)

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

COMMON_TZ

Пример указания значения параметра через переменную окружения

```
COMMON_TZ="Asia/Novosibirsk"
```

10.5.3 Порт для доступа клиентских устройств к EDM Issue

Описание параметра

Номер порта, на котором EDM Issue будет принимать подключения от клиентских устройств

Значение по умолчанию

8098

Допустимые значения для параметра

1–65535

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_SERVER_HOST_PORT

Пример указания значения параметра через переменную окружения

```
EDM_SERVER_HOST_PORT=9000
```

10.5.4 Порт для доступа web-интерфейсу EDM Issue

Описание параметра

Номер порта, на котором будет доступен web-интерфейс EDM Issue

Значение по умолчанию

8091

Допустимые значения для параметра

1–65535

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_web_UI_PORT

Пример указания значения параметра через переменную окружения

```
EDM_web_UI_PORT=8080
```

10.5.5 Имя файла сертификата для работы web-интерфейса EDM Issue

Описание параметра

Имя файла сертификата, который будет использоваться для поднятия HTTPS-сессий между браузерами пользователей EDM Issue и web-сервисом EDM Issue. Файл с указанным именем необходимо расположить в директории по пути "<расположение служебных файлов EDM Issue>/data/data/edmi-web-ui/ssl/". В случае, если параметр не будет задан, то будет использован файл "autocreated-cert.crt", расположенный в этой директории и входящий в комплект поставки EDM Issue

Значение по умолчанию

"autocreated-cert.crt"

Допустимые значения для параметра

Текстовая строка – имя файла с сертификатом, который должен быть размещен администратором EDM Issue в директории "<расположение служебных файлов EDM Issue>/data/data/edmi-web-ui/ssl/"

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_web_CERT

Пример указания значения параметра через переменную окружения

```
EDM_web_CERT="mycompany.crt"
```

10.5.6 Имя файла ключа для работы web-интерфейса EDM Issue

Описание параметра

Имя файла ключа, который будет использоваться для поднятия HTTPS-сессий между браузерами пользователей EDM Issue и web-сервисом EDM Issue. Файл с указанным именем необходимо расположить в директории по пути "<расположение служебных файлов EDM Issue>/data/data/edmi-web-ui/ssl/". В случае если параметр не будет задан, то будет использован файл "autocreated-cert.key", расположенный в этой директории и входящий в комплект поставки EDM Issue

Значение по умолчанию

"autocreated-cert.key"

Допустимые значения для параметра

Текстовая строка – имя файла с ключом, который должен быть размещен администратором EDM Issue в директории "<расположение служебных файлов EDM Issue>/data/data/edmi-web-ui/ssl/"

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_web_CERT_KEY

Пример указания значения параметра через переменную окружения

```
EDM_web_CERT_KEY="mycompany.key"
```

10.5.7 Адрес подключения к базе данных EDM Issue

Описание параметра

Адрес подключения компонентов EDM Issue к базе данных EDM Issue. В комплекте поставки база данных работает в отдельном Docker-контейнере, и по умолчанию все компоненты обращаются к базе данных в этом контейнере

Значение по умолчанию

edmi-db

Допустимые значения для параметра

Текстовая строка – адрес базы данных EDM Issue. Задается либо в формате IPv4-адреса, либо в виде имени хоста – строкой длиной до 254 символов

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_DB_HOST

Пример указания значения параметра через переменную окружения

```
EDM_DB_HOST=db.mycompany.loc
```

10.5.8 Порт подключения к базе данных EDM Issue

Описание параметра

Порт подключения компонентов EDM Issue к базе данных EDM Issue

Значение по умолчанию

5432

Допустимые значения для параметра

Текстовая строка – порт для подключения к базе данных EDM issue

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_DB_PORT

Пример указания значения параметра через переменную окружения

```
EDM_DB_PORT=4343
```

10.5.9 Имя базы данных EDM Issue

Описание параметра

Имя базы данных, которую будут использовать компоненты EDM Issue

Значение по умолчанию

edm

Допустимые значения для параметра

Текстовая строка – имя базы данных EDM Issue

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_DB

Пример указания значения параметра через переменную окружения

```
EDM_DB=edm-custom
```

10.5.10 Имя пользователя базы данных EDM Issue

Описание параметра

Имя пользователя базы данных, которое будут использовать компоненты EDM Issue для записи данных в базу данных EDM Issue

Значение по умолчанию

edm

Допустимые значения для параметра

Текстовая строка – имя пользователя базы данных EDM Issue

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_DB_USER

Пример указания значения параметра через переменную окружения

```
EDM_DB_USER=user
```

10.5.11 Пароль пользователя базы данных EDM Issue

Описание параметра

Пароль пользователя базы данных, который в связке с именем пользователя будет использовать компоненты EDM Issue для записи данных в базу данных EDM Issue

Значение по умолчанию

edm

Допустимые значения для параметра

Текстовая строка – пароль пользователя базы данных EDM Issue

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_DB_PASSWORD

Пример указания значения параметра через переменную окружения

```
EDM_DB_PASSWORD=password
```

10.5.12 Имя хоста или IP-адрес http/https прокси-сервера

Описание параметра

Имя хоста или IP-адрес http/https прокси-сервера, к которому будет подключаться EDM Issue. Данный параметр используется совместно с PROXY_PORT

Значение по умолчанию

Отсутствует

Допустимые значения для параметра

IPv4-адрес

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

PROXY_HOST

Пример указания значения параметра через переменную окружения

```
PROXY_HOST=10.11.12.13
```

10.5.13 Порт http/https прокси-сервера

Описание параметра

Порт http/https прокси-сервера. Данный параметр используется совместно с PROXY_HOST

Значение по умолчанию

Отсутствует

Допустимые значения для параметра

1–65535

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

PROXY_PORT

Пример указания значения параметра через переменную окружения

```
PROXY_PORT=3322
```

10.5.14 IP-адрес, на котором будут работать EDM-сервисы

Описание параметра

IP-адрес, на котором EDM Issue будет принимать подключения от клиентских устройств

Значение по умолчанию

0.0.0.0

Допустимые значения для параметра

IPv4-адрес

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_SERVER_HOST_IP

Пример указания значения параметра через переменную окружения

```
EDM_SERVER_HOST_IP=192.168.10.122
```

10.5.15 Максимальное количество одновременно поддерживаемых сессий

Описание параметра

Максимальное количество одновременно поддерживаемых сессий. Рекомендуется оставить значение данного параметра по умолчанию

Значение по умолчанию

10

Допустимые значения для параметра

1–1000

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_THREAD_LIMIT

Пример указания значения параметра через переменную окружения

```
EDM_THREAD_LIMIT=12
```

10.5.16 Размер очереди для клиентских запросов

Описание параметра

Размер очереди для клиентских запросов, которые EDM Issue не смог обработать сразу из-за превышения лимита одновременно обрабатываемых сессий. Запросы свыше размера очереди будут прерываться с ошибкой со стороны EDM Issue

Значение по умолчанию

100 запросов

Допустимые значения для параметра

50–300 запросов в очереди

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_QUEUE_LIMIT

Пример указания значения параметра через переменную окружения

```
EDM_QUEUE_LIMIT=75
```

10.5.17 Размер очереди для клиентских запросов

Описание параметра

Размер очереди для клиентских запросов, которые EDM Issue не смог обработать сразу из-за превышения лимита одновременно обрабатываемых сессий. Запросы свыше размера очереди будут прерываться с ошибкой со стороны EDM Issue

Значение по умолчанию

100 запросов

Допустимые значения для параметра

50–300 запросов в очереди

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_QUEUE_LIMIT

Пример указания значения параметра через переменную окружения

```
EDM_QUEUE_LIMIT=75
```

10.5.18 Максимальное число запросов в секунду к EDM Issue с одного IP-адреса

Описание параметра

Максимальное число запросов от одного IP-адреса к EDM Issue в секунду, запросы сверх этого числа не будут обрабатываться EDM Issue и будут отброшены

Значение по умолчанию

50 запросов в секунду

Допустимые значения для параметра

10–100 запросов в секунду

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_DOS_FILTER_MAX_REQUESTS_PER_SECOND

Пример указания значения параметра через переменную окружения

```
EDM_DOS_FILTER_MAX_REQUESTS_PER_SECOND=30
```

10.5.19 Максимальная задержка при взаимодействии клиентского устройства и EDM Issue

Описание параметра

Максимальная задержка при взаимодействии клиентского устройства и EDM Issue. Запросы с задержкой свыше указанной не будут обрабатываться EDM Issue и будут отброшены

Значение по умолчанию

200 мс

Допустимые значения для параметра

30–1000 мс

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_DOS_FILTER_DELAY_MS

Пример указания значения параметра через переменную окружения

```
EDM_DOS_FILTER_DELAY_MS=75
```

10.5.20 Максимальный размер файла с логами для ротации

Описание параметра

Максимальный размер файла с логами, при превышении которого произойдет ротация этого файла с логами

Значение по умолчанию

10 МБ

Допустимые значения для параметра

1–1024 МБ

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_LOG_FILE_MAX_SIZE

Пример указания значения параметра через переменную окружения

```
EDM_LOG_FILE_MAX_SIZE=5
```

10.5.21 Максимальное количество файлов с логами для ротации

Описание параметра

Максимальное количество файлов с логами, при превышении которого произойдет ротация этого файла с логами

Значение по умолчанию

4 файла

Допустимые значения для параметра

1–50 файлов

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_LOG_FILE_MAX_COUNT

Пример указания значения параметра через переменную окружения

```
EDM_LOG_FILE_MAX_COUNT=10
```

10.5.22 Интервал отслеживания некорректных обращений на EDM Issue

Описание параметра

Интервал времени, за который будет рассчитываться число некорректных обращений на EDM Issue

Значение по умолчанию

1 час

Допустимые значения для параметра

1–4 часа

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_SECURITY_CHECK_PERIOD_HOURS

Пример указания значения параметра через переменную окружения

```
EDM_SECURITY_CHECK_PERIOD_HOURS=2
```

10.5.23 Уровень логирования для событий ядра EDM Issue

Описание параметра

Указание уровня логирования для событий ядра EDM Issue

Значение по умолчанию

info

Допустимые значения для параметра

- off
- error
- info
- debug

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_KERNEL_LOG_LEVEL

Пример указания значения параметра через переменную окружения

```
EDM_KERNEL_LOG_LEVEL=debug
```

10.5.24 Уровень логирования для внутренних событий EDM Issue

Описание параметра

Указание уровня логирования для внутренних событий EDM Issue

Значение по умолчанию

info

Допустимые значения для параметра

- off
- error

- info
- debug

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_ENGINE_LOG_LEVEL

Пример указания значения параметра через переменную окружения

```
EDM_ENGINE_LOG_LEVEL=debug
```

10.5.25 Уровень логирования для событий взаимодействия компонентов EDM Issue с базой данных EDM Issue

Описание параметра

Указание уровня логирования для событий взаимодействия компонентов EDM Issue с базой данных EDM Issue

Значение по умолчанию

info

Допустимые значения для параметра

- off
- error
- info
- debug

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_DB_LOG_LEVEL

Пример указания значения параметра через переменную окружения

```
EDM_DB_LOG_LEVEL=debug
```

10.5.26 Уровень логирования для событий сети EDM Issue

Описание параметра

Указание уровня логирования для событий сети EDM Issue

Значение по умолчанию

info

Допустимые значения для параметра

- off
- error
- info
- debug

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_NETWORKING_LOG_LEVEL

Пример указания значения параметра через переменную окружения

```
EDM_NETWORKING_LOG_LEVEL=debug
```

10.5.27 Уровень логирования для событий безопасности EDM Issue

Описание параметра

Указание уровня логирования для событий безопасности EDM Issue.

Значение по умолчанию

info

Допустимые значения для параметра

- off
- error
- info
- debug

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_SECURITY_LOG_LEVEL

Пример указания значения параметра через переменную окружения

```
EDM_SECURITY_LOG_LEVEL=debug
```

10.5.28 Уровень логирования для событий, генерируемых компонентами EDM Issue

Описание параметра

Указание уровня логирования для событий, генерируемых компонентами EDM Issue

Значение по умолчанию

info

Допустимые значения для параметра

- off
- error
- info
- debug

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_HOSTS_LOG_LEVEL

Пример указания значения параметра через переменную окружения

```
EDM_HOSTS_LOG_LEVEL=debug
```

10.5.29 Уровень логирования для событий ядра EDM Issue CLI

Описание параметра

Указание уровня логирования для событий ядра EDM Issue CLI

Значение по умолчанию

info

Допустимые значения для параметра

- off
- error
- info
- debug

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_CLI_KERNEL_LOG_LEVEL

Пример указания значения параметра через переменную окружения

```
EDM_CLI_KERNEL_LOG_LEVEL=debug
```

10.5.30 Уровень логирования для внутренних событий EDM Issue CLI

Описание параметра

Указание уровня логирования для внутренних событий EDM Issue CLI

Значение по умолчанию

info

Допустимые значения для параметра

- off
- error
- info
- debug

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_CLI_ENGINE_LOG_LEVEL

Пример указания значения параметра через переменную окружения

```
EDM_CLI_ENGINE_LOG_LEVEL=debug
```

10.5.31 Уровень логирования для событий взаимодействия EDM Issue CLI с базой данных EDM Issue

Описание параметра

Указание уровня логирования для событий взаимодействия EDM Issue CLI с базой данных EDM Issue

Значение по умолчанию

info

Допустимые значения для параметра

- off
- error
- info
- debug

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_CLI_DB_LOG_LEVEL

Пример указания значения параметра через переменную окружения

```
EDM_CLI_DB_LOG_LEVEL=debug
```

10.5.32 Уровень логирования для событий сети EDM Issue CLI

Описание параметра

Указание уровня логирования для событий сети EDM Issue CLI

Значение по умолчанию

info

Допустимые значения для параметра

- off
- error
- info
- debug

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_CLI_NETWORKING_LOG_LEVEL

Пример указания значения параметра через переменную окружения

```
EDM_CLI_NETWORKING_LOG_LEVEL=debug
```

10.5.33 Уровень логирования для событий безопасности EDM Issue CLI

Описание параметра

Указание уровня логирования для событий безопасности EDM Issue CLI

Значение по умолчанию

info

Допустимые значения для параметра

- off
- error
- info
- debug

Обязательность указания значения для параметра

Параметр не является обязательным

Именование переменной окружения для указания значения параметра

EDM_CLI_SECURITY_LOG_LEVEL

Пример указания значения параметра через переменную окружения

```
EDM_CLI_SECURITY_LOG_LEVEL=debug
```

11 Мониторинг EDM Issue

EDM предоставляется клиентам как набор Docker-контейнеров с файлами для их запуска с определенными настройками. С учётом существующих практик мониторинга и контроля работы Docker-контейнеров был сформирован набор сервисов для мониторинга EDM Issue:

- Telegraf – получение данных о физическом хосте и Docker-контейнерах EDM Issue и сохранение этих данных в базе данных Influxdb;
- Influxdb – хранение данных, получаемых от сервиса Telegraf, и их предоставление сервису Grafana;
- Prometheus – получение данных о метриках EDM Issue и их предоставление сервису Grafana;
- Grafana – сбор данных системы мониторинга с сервисов Influxdb и Prometheus и предоставление этих данных в понятном пользователю системы мониторинга виде.

11.1 Запуск системы мониторинга EDM Issue

Пример файлов конфигурации сервисов мониторинга и пример файла Docker Compose для запуска сервисов мониторинга вместе с EDM Issue поставляется в архиве вместе с служебными файлами для запуска EDM Issue. Файлы системы мониторинга в этом архиве находятся в директории monitoring и имеют следующую структуру:

Структура файлов системы мониторинга EDM Issue

```
.
├── .env
├── docker-compose.yml
├── grafana
│   └── provisioning
│       ├── dashboards
│       │   ├── dashboard.yml
│       │   ├── edm_alert_metrics.json
│       │   └── edm_monitor.json
│       ├── datasources
│       │   └── datasource.yml
│       └── notifiers
│           ├── email.yml
│           └── telegram.yml
├── influxdb
│   └── influx_init.iql
├── prometheus
│   └── prometheus.yml
└── telegraf
    └── telegraf.conf
```

Для запуска системы мониторинга EDM Issue требуется произвести следующие шаги:

1. Перейти в директорию с служебными файлами EDM Issue.
2. Перейти в директорию "monitoring".
3. Запустить систему мониторинга EDM Issue командой:

Команда запуска EDM Issue

```
docker compose up -d
```

Пример вывода команды при первом запуске EDM Issue на хосту

```
edm@edm:~/issue/monitoring$ docker compose up -d
[+] Running 42/42
 ⠿ prometheus Pulled
47.0s
   ⠿ 76df9210b28c Pull complete
11.1s
   ⠿ 559be8e06c14 Pull complete
11.5s
   ⠿ 0f8c479799f2 Pull complete
25.5s
   ⠿ 18b600182fb7 Pull complete
30.0s
   ⠿ 7107ca4b8b6a Pull complete
38.3s
   ⠿ 6d4f7a6bf1de Pull complete
40.2s
   ⠿ 70791e712bf8 Pull complete
45.8s
   ⠿ 11ccf794006c Pull complete
46.1s
   ⠿ 44dc96c0af43 Pull complete
46.2s
   ⠿ ecdf06ab4b8d Pull complete
46.4s
   ⠿ 50e51d4c12aa Pull complete
46.5s
   ⠿ c37593abaed6 Pull complete
46.8s
 ⠿ grafana Pulled
46.1s
   ⠿ 188c0c94c7c5 Pull complete
8.0s
   ⠿ 63b9b7e38dd5 Pull complete
8.2s
   ⠿ a1b68a35c4eb Pull complete
8.6s
   ⠿ fb97c1057eb0 Pull complete
10.9s
   ⠿ 6ab60835f369 Pull complete
26.6s
   ⠿ 4f4fb700ef54 Pull complete
31.2s
   ⠿ 006fd685411a Pull complete
38.3s
   ⠿ c1801e3c15c0 Pull complete
41.0s
 ⠿ nginx-exporter Pulled
38.6s
   ⠿ 16fc7305de97 Pull complete
25.7s
   ⠿ 6da7d2f4f3c3 Pull complete
35.9s
 ⠿ influxdb Pulled
49.5s
```

```
   ⠿ 2587235a7635 Pull complete
38.2s
   ⠿ 953fe5c215cb Pull complete
41.2s
   ⠿ d4d3f270c7de Pull complete
46.0s
   ⠿ d81696497404 Pull complete
46.1s
   ⠿ febe82b40114 Pull complete
48.5s
   ⠿ 9a89692c7853 Pull complete
48.6s
   ⠿ 5b833af9a4dc Pull complete
48.7s
   ⠿ 69d297038fc8 Pull complete
48.9s
 ⠿ telegraf Pulled
42.7s
   ⠿ 0bc3020d05f1 Pull complete
15.8s
   ⠿ a110e5871660 Pull complete
18.2s
   ⠿ 83d3c0fa203a Pull complete
19.0s
   ⠿ bc0127a0f443 Pull complete
22.3s
   ⠿ c9d5466d920e Pull complete
26.8s
   ⠿ 5e68d2e1c8a4 Pull complete
38.2s
   ⠿ 2aaece7e10c3 Pull complete
38.5s
[+] Running 9/9
 ⠿ Volume "monitoring_influxdb"           Created
0.0s
 ⠿ Volume "monitoring_prometheus"         Created
0.0s
 ⠿ Volume "monitoring_grafana_config"     Created
0.0s
 ⠿ Volume "monitoring_grafana_data"       Created
0.0s
 ⠿ Container monitoring-prometheus-1      Started
5.0s
 ⠿ Container monitoring-grafana-1         Started
5.4s
 ⠿ Container monitoring-nginx-exporter-1  Started
5.4s
 ⠿ Container monitoring-influxdb-1        Started
5.2s
 ⠿ Container monitoring-telegraf-1        Started
5.1s
edm@edm:~/issue/monitoring$
```

4. Убедиться, что все контейнеры EDM Issue успешно запустились, используя команду:

Команда проверки статуса контейнеров EDM Issue

```
docker compose ps
```

Пример вывода команды при успешном запуске всех контейнеров EDM Issue

```
edm@edm:~/issue/monitoring$ docker compose ps
NAME                          COMMAND                  SERVICE             STATUS
PORTS
monitoring-grafana-1          "/run.sh"                grafana             running
0.0.0.0:3000->3000/tcp, :::3000->3000/tcp
monitoring-influxdb-1         "/entrypoint.sh infl…"   influxdb            running
8086/tcp
monitoring-nginx-exporter-1   "/usr/bin/nginx-prom…"   nginx-exporter      running
monitoring-prometheus-1       "/bin/prometheus --c…"   prometheus          running
0.0.0.0:9090->9090/tcp, :::9090->9090/tcp
monitoring-telegraf-1         "/entrypoint.sh tele…"   telegraf            running
8125/udp
edm@edm:~/issue/monitoring$
```

Теперь с системой мониторинга EDM Issue можно взаимодействовать через web-интерфейс Grafana.

11.2 Остановка системы мониторинга EDM Issue

Для остановки системы мониторинга EDM Issue требуется произвести следующие шаги:

1. Перейти в директорию с файлами работающего EDM Issue.
2. Перейти в директорию "monitoring".
3. Выполнить команду:

Команда остановки EDM Issue

```
docker compose down
```

Пример вывода команды при успешной остановке всех контейенров EDM Issue

```
edm@edm:~/issue/monitoring$ docker compose down
[+] Running 5/5
 ⠿ Container monitoring-telegraf-1         Removed
1.5s
 ⠿ Container monitoring-grafana-1          Removed
3.2s
 ⠿ Container monitoring-prometheus-1       Removed
3.9s
 ⠿ Container monitoring-nginx-exporter-1   Removed
3.8s
 ⠿ Container monitoring-influxdb-1         Removed
3.9s
edm@edm:~/issue/monitoring$
```

В результате этого сервис мониторинга EDM Issue будет остановлен. Ошибка, возникшая при остановке системы мониторинга, появляется в том случае, если работа системы мониторинга останавливается при работающем EDM Issue, т.е. эту ошибку можно игнорировать. Для повторного запуска остановленного сервиса мониторинга EDM Issue нужно выполнить команду "docker compose up -d".

11.3 Информация о доступных в системе мониторинга метриках EDM Issue

11.3.1 Авторизация

После запуска системы мониторинга EDM Issue администратору системы мониторинга становится доступен web-интерфейс Grafana по адресу **http://<EDM_ADDRESS>:3000/**,где **<EDM_ADDRESS>** — это адрес сервера EDM Issue в сети (это может быть IP-адрес или доменное имя, если для IP-адреса хоста, на котором запущен EDM Issue, создана DNS-запись). Авторизоваться в ней можно по умолчанию с логином **admin** и паролем **password**.

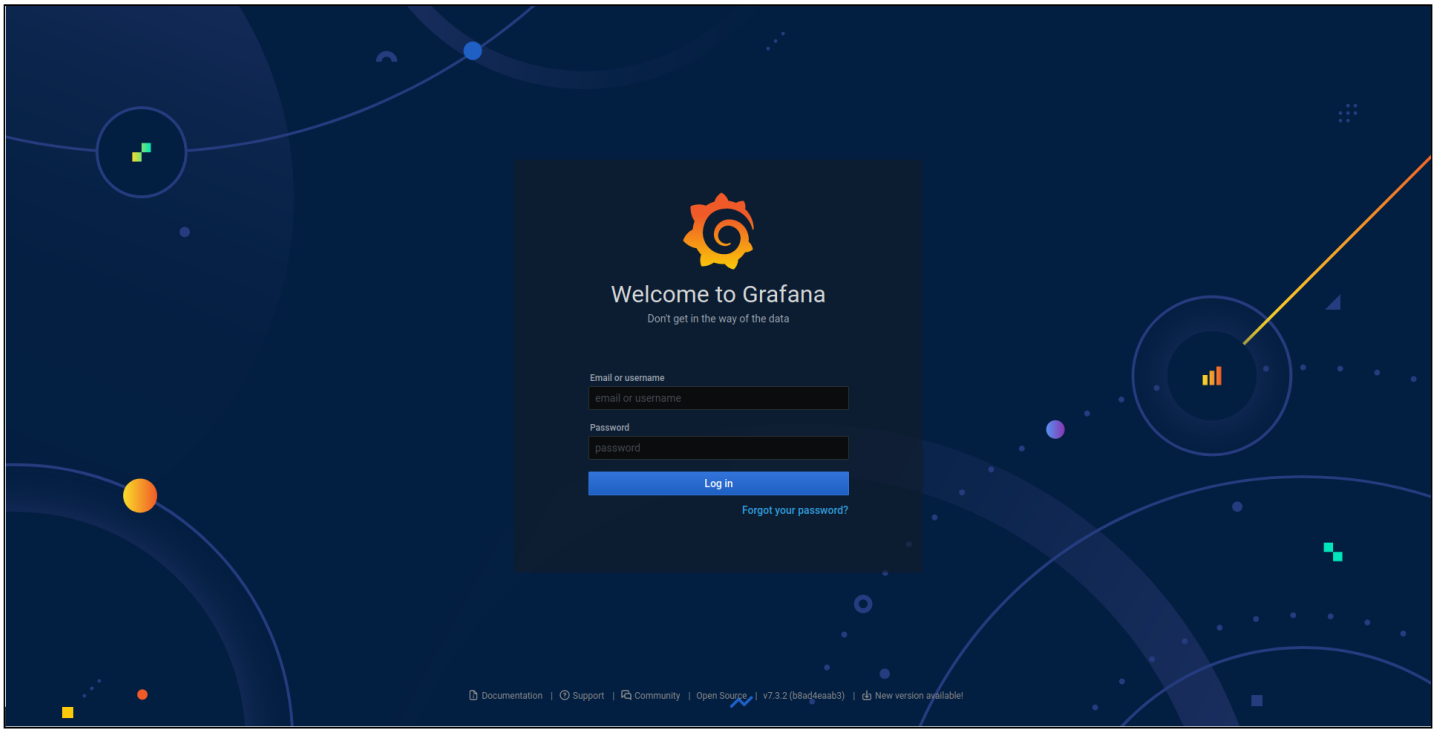


Рисунок 25 – Форма авторизации web-интерфейса Grafana

После авторизации в web-интерфейсе Grafana для доступа к данным мониторинга с EDM Issue требуется перейти в раздел "Dashboards" – "Manage". В этом разделе в директории "General" будет располагаться две панели мониторинга – "edm_alert_metrics" и "edm_monitor".

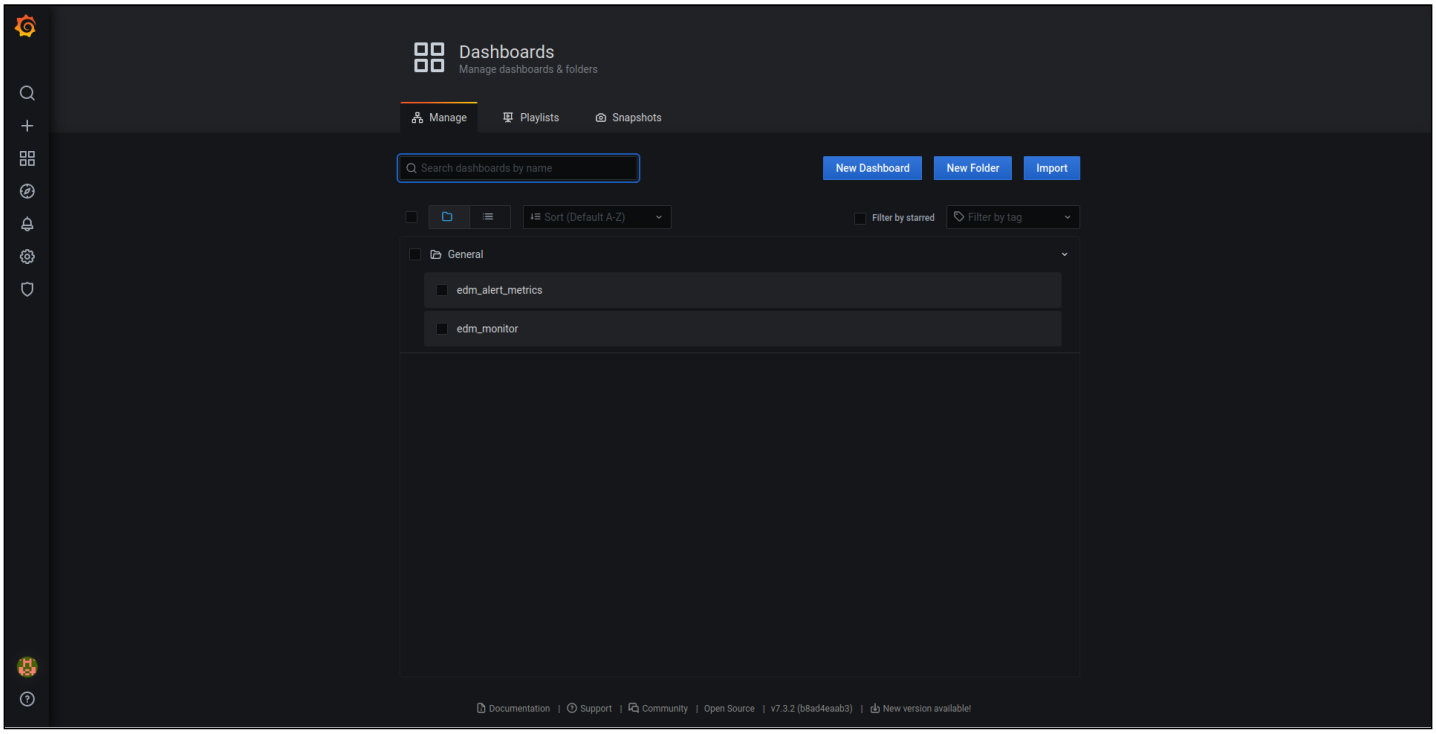


Рисунок 26 – Список панелей мониторинга EDM Issue

11.3.2 Панель мониторинга "edm_alert_metrics"

Панель мониторинга "edm_alert_metrics" предоставляет администратору EDM Issue информацию о состоянии внутренних метрик EDM Issue.

Рисунок 27 – Общий вид панели мониторинга "edm_alert_metrics"

Полный список представленных на панели метрик перечислен в таблице 1.

Таблица 1 — Список внутренних метрик EDM Issue, отображающийся в панели мониторинга "edm_alert_metrics" web-интерфейса Grafana

Имя счётчика	Описание	Примечание
Общие для контейнеров edmi-server и edmi-loader		
dbAccessError	Ошибки доступа к БД	
sqlError	Ошибки выполнения SQL-запроса	
rootAccessError	Ошибки подключения к Root-серверу	
Только для контейнера edmi-loader		
loadLicenseData	Время получения данных лицензии	С замером длительности и фиксацией успешности
loadIpsDataError	Ошибки, возникшие при обновлении загружаемого контента, не связанные с конкретным поставщиком IDS/IPS-правил	
kasperskyLoadRules	Время загрузки лицензируемых IDS/IPS-правил вендора Kaspersky Lab от EDM Root	С замером длительности и фиксацией успешности
ptsecurityLoadRules	Время загрузки лицензируемых IDS/IPS-правил вендора Positive Technologies от EDM Root	С замером длительности и фиксацией успешности
loadOpenRules	Время загрузки лицензируемых IDS/IPS-правил из открытых источников	С замером длительности и фиксацией успешности
loadOpenFileError	Ошибки получения отдельно взятого файла с IDS/IPS-правилами из открытого источника	
syncDevices	Время синхронизации списка устройств	С замером длительности и фиксацией успешности
Только для контейнера edmi-server		
esrRulesRequest	Количество запросов правил от ESR	С замером длительности и фиксацией успешности
esrCertificateRequest	Количество запросов сертификата от EDM Issue	С замером длительности и фиксацией успешности
revokeCertificate	Количество отзывов сертификата ESR	С замером длительности и фиксацией успешности
esrAuthFailed	Количество ошибок аутентификации от ESR	
getEsrLicenseError	Ошибки получения файла лицензии ESR от EDM Root	
ipAccessDenied	Количество заблокированных запросов к EDM Issue с помощью IP-правил	
blockIp	Количество автоматически заблокированных IP-адресов	

Имя счётчика	Описание	Примечание
serviceDenial	Количество зарегистрированных отказов в обслуживании (отклонение запросов из-за загруженности сервера)	
requestRejected	Количество зарегистрированных отказов в обработке запроса (переполнение очереди запросов)	

11.3.3 Панель мониторинга "edm_monitor"

Панель мониторинга "edm_monitor" предоставляет администратору EDM Issue общую информацию о хосте, в котором запущен EDM Issue, а также информацию о Docker-контейнерах EDM Issue.

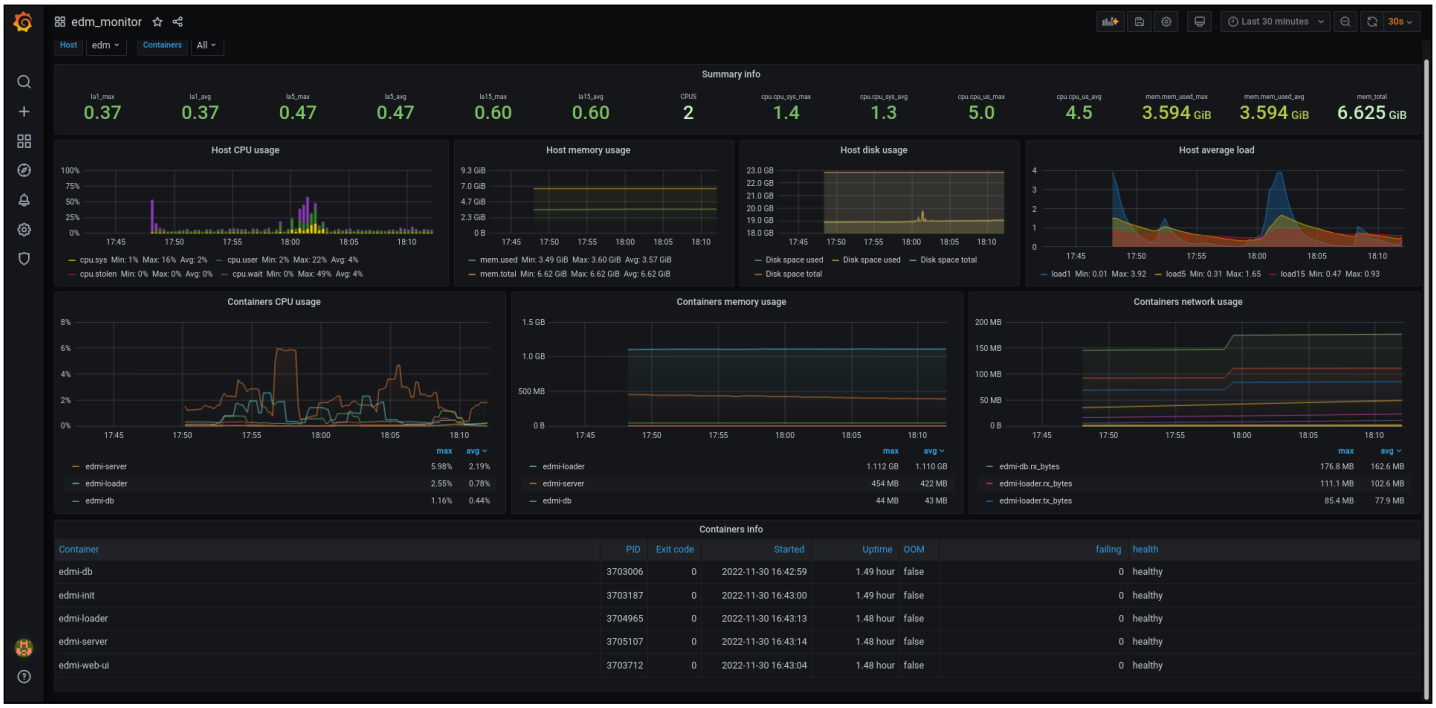


Рисунок 28 – Общий вид панели мониторинга "edm_monitor"

На данной панели мониторинга представлена следующая информация:

- Средняя загруженность системы (за 1/5/15 минут);
- Количество ядер процессора;
- Загруженность процессора (в процентах);
- Количество используемой/всего оперативной памяти;
- Загрузка процессора Docker-контейнерами EDM Issue;
- Использование памяти Docker-контейнерами EDM Issue;
- Информация о Docker-контейнерах EDM Issue:
  - имя сервиса;
  - идентификатор процесса;
  - код возврата (при работе контейнера – код 0);
  - время старта контейнера;
  - время работы контейнера;
  - флаг нехватки оперативной памяти.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ООО «Предприятие «ЭЛТЕКС» вы можете обратиться в Сервисный центр компании:

Форма обратной связи на сайте: https://eltex-co.ru/support/

Servicedesk: https://servicedesk.eltex-co.ru

На официальном сайте компании вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС», обратиться к базе знаний, оставить интерактивную заявку или проконсультироваться у инженеров Сервисного центра на техническом форуме:

Официальный сайт компании: https://eltex-co.ru

Технический форум: https://eltex-co.ru/forum

База знаний: https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base

Центр загрузок: https://eltex-co.ru/support/downloads