KEDR: API ??? ?????????? ?????????? ?? ????????????? ?? ??????/ Response_api

API для управления действиями по реагированию на угрозы/ Response_api

KATA предоставляет интерфейс API для осуществления действий по реагированию на угрозы. Команды на выполнение операций поступают на сервер Central Node, после чего приложение передает их компоненту Endpoint Agent.

С помощью внешних систем вы можете выполнить следующие операции на хостах с компонентом Endpoint Agent:

- Управлять сетевой изоляцией хостов.
- Управлять правилами запрета.
- Запускать приложения.

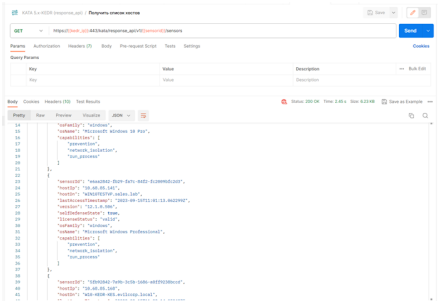
Все перечисленные операции доступны на хостах, на которых в роли компонента Endpoint Agent используются приложения Kaspersky Endpoint Agent для Windows и Kaspersky Endpoint Security для Windows. На хостах с Kaspersky Endpoint Agent для Linux и Kaspersky Endpoint Security для Linux доступна только функция запуска приложения.

Запрос на получение списка хостов с компонентом Endpoint Agent

Выберите «**Получить список хостов**».
В строке запроса, вы можете добавить параметры filter, max_timeout, max_events, continuation_token.

Нажмите **Send**.
При корректном выводе запроса вы получите статус 200 OK. Так же, при успешной обработке запроса отобразится весь список хостов с компонентом Endpoint Agent.

Вы можете сохранить информацию о хостах в файл. Перейдите в меню вывода информации. Нажмите на значек расширенного меню, выберите пункт меню «Save response to file ». Вывод сохранится в виде *.json файла.



Синтаксис команды

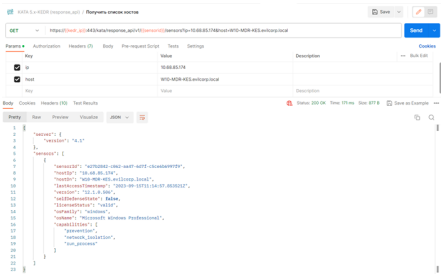
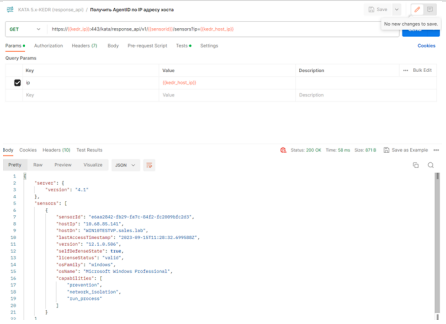
```
GET https://{{kedr_ip}}:443/kata/response_api/v1/{{sensorid}}/sensors
```

Вы можете создать запрос на вывод информации о хостах с фильтрами по IP-адресу, имени или идентификатору хоста. Вы можете указать один, несколько или все перечисленные фильтры.

При указании имени хоста вам нужно учитывать, что фильтр чувствителен к регистру символов.

Перечень параметров доступен ниже в таблице:

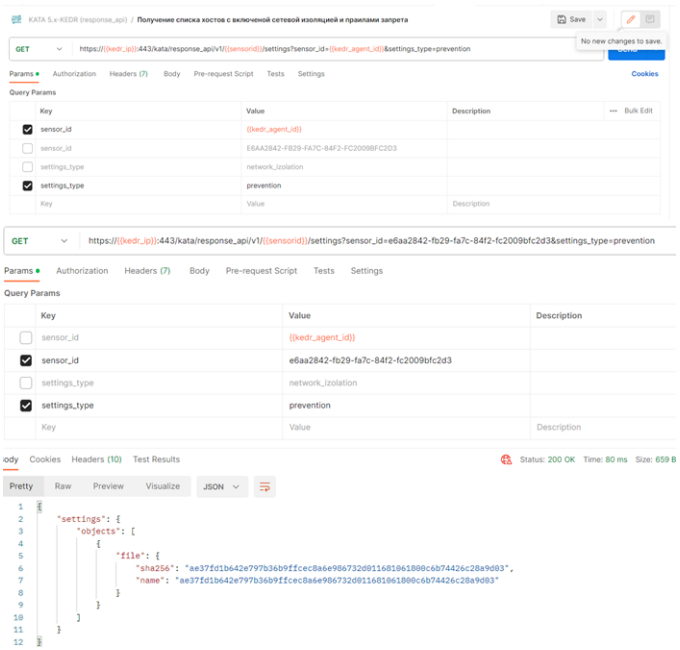
Параметр	**Тип**	**Описание**
`external_system_id`	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`sensor_id`	UUID	Уникальный идентификатор хоста с компонентом Endpoint Agent.
`ip`	string	IP-адрес хоста с компонентом Endpoint Agent.

Пример запроса информации по определенному хосту или IP адресу	 Пример: GET https://{{kedr_ip}}:443/kata/response_api/v1/{{sensorid}}/sensors?ip=10.68.85.174&host=W10-MDR-KES.evilcorp.local GET https://{{kedr_ip}}:443/kata/response_api/v1/{{sensorid}}/sensors?ip=10.68.85.174&host=W10-MDR-KES.evilcorp.local&sensor_id=e27b2842-c062-aa47-6d7f-c5ce6b6997f9 Синтаксис: GET "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию 443>/kata/response_api/v1/<идентификатор external_system_id>/sensors?ip=<IP-адрес хоста>&host=<имя хоста>&sensor_id=<идентификатор sensor_id>" При успешной обработке запроса отобразится информация о выбранном хосте с компонентом Endpoint Agent.
Запрос получения AgentID по IP адресу хоста	 Пример запроса: GET https://{{kedr_ip}}:443/kata/response_api/v1/{{sensorid}}/sensors?ip={{kedr_host_ip}}
Для удобства работы вы можете описать глобальные переменные в разделе переменные, либо работать с параметрами запросов, для таких параметров как sensor_id, settings_type, ip, host,	

Запрос на получение информации о сетевой изоляции и наличии правил запрета для хостов с компонентом Endpoint Agent

Выберите запрос «**Получение списка хостов с включеной сетевой изоляцией и праилами запрета** ».
В строке запроса необходимо обязательно указать параметры sensor_id, settings_type.

Нажмите **Send**.
При корректном выводе запроса вы получите статус 200 OK. Так же, при успешной обработке запроса отобразится весь список хостов с компонентом Endpoint Agent.



Пример запроса:
https://{{kedr_ip}}:443/kata/response_api/v1/{{sensorid}}/settings?sensor_id={{kedr_agent_id}}&settings_type=prevention
https://{{kedr_ip}}:443/kata/response_api/v1/{{sensorid}}/settings?sensor_id=e6aa2842-fb29-fa7c-84f2-fc2009bfc2d3&settings_type=prevention

Информация о запросах:

https://support.kaspersky.com/help/KATA/7.1/ru-RU/227597.htm

Синтаксис команды:
GET "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию 443>/kata/response_api/v1/<идентификатор external_system_id>/settings?sensor_id=<идентификатор sensor_id>&settings_type=<network_izolation или prevention>"

Управление сетевой изоляцией хостов

Для изоляции хоста с компонентом Endpoint Agent с помощью интерфейса API рекомендуется использовать следующий сценарий взаимодействия с Kaspersky Anti Targeted Attack Platform:

1. Создание запроса на получение списка хостов с компонентом Endpoint Agent
2. Создание запроса на получение информации о хостах, для которых уже включена сетевая изоляция
3. Создание запроса на одну из следующих операций с хостами с компонентом Endpoint Agent:

· включение сетевой изоляции;
· отключение сетевой изоляции;
· добавление исключения в уже существующее правило сетевой изоляции.

Вы можете управлять созданными правилами сетевой изоляции в веб-интерфейсе приложения.

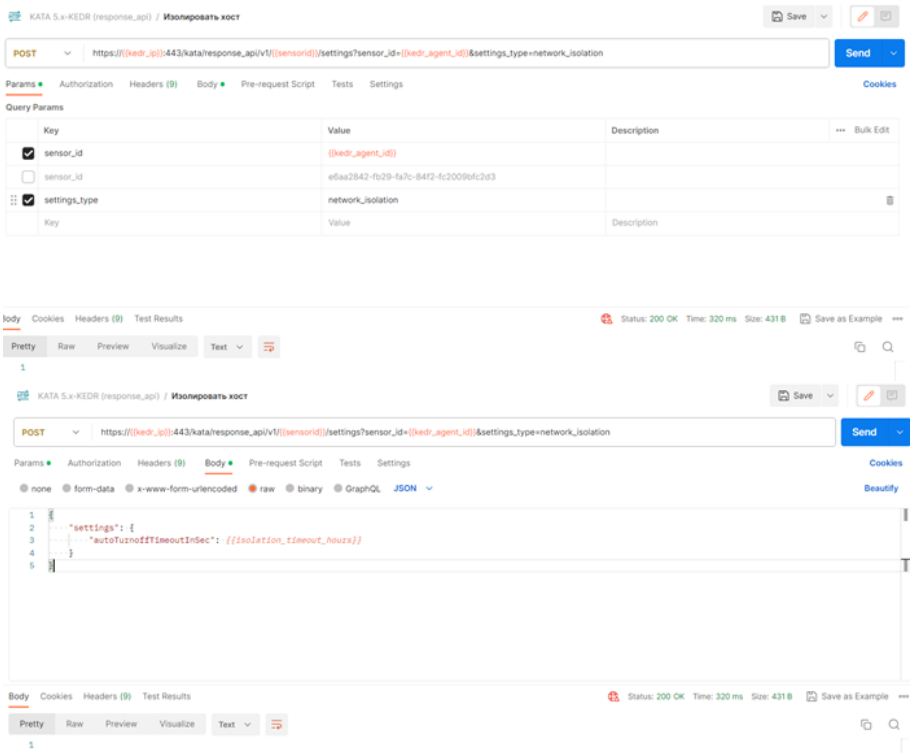
Запрос на включение сетевой изоляции

Выберите запрос «**Изолировать хост**».
В строке запроса необходимо обязательно указать параметры sensor_id, autoTurnoffTimeoutInSec.

Нажмите **Send**.

При корректном выводе запроса вы получите статус 200 OK, и результат выполнения.

В Postman переменная **isolation_timeout_hours** параметра autoTurnoffTimeoutInSec определена в резделе переменных «Variables». Используется POST запрос, поэтому в разделе BODY в параметре передаваемых значений выбран тип RAW, формат JSON.



Пример:

POST
https://{{kedr_ip}}:443/kata/response_api/v1/{{sensorid}}/settings?sensor_id={{kedr_agent_id}}&settings_type=network_isolation
{
"settings": {
"autoTurnoffTimeoutInSec": {{isolation_timeout_hours}}
}
}

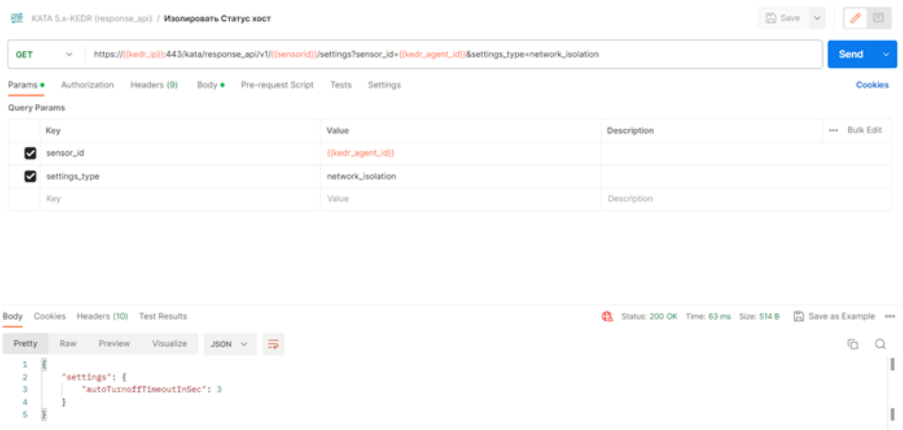
Синтаксис команды

POST "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию 443>/kata/response_api/v1/<идентификатор external_system_id>/settings?sensor_id=<идентификатор sensor_id>&settings_type=network_izolation" -H 'Content-Type: application/json' -d '
{
"settings": {
"autoTurnoffTimeoutInSec": <время действия сетевой изоляции>}
}

Выберите запрос «**Изолировать Статус хост**» для проверки статуса задачи.
В строке запроса необходимо обязательно указать параметры sensor_id, autoTurnoffTimeoutInSec.

Нажмите **Send**.

При корректном выводе запроса вы получите статус 200 OK, и результат выполнения.



Пример Postman:
GET
https://{{kedr_ip}}:443/kata/response_api/v1/{{sensorid}}/settings?sensor_id={{kedr_agent_id}}&settings_type=network_isolation {
"settings": {
"autoTurnoffTimeoutInSec": *{{isolation_timeout_hours}}*
}
}

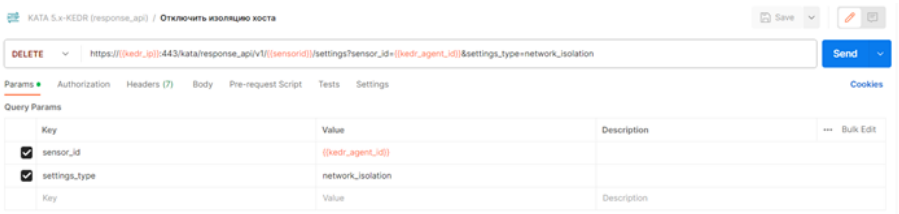
Запрос на отключение сетевой изоляции

Выберите запрос «**Отключить изоляцию хоста**».
В строке запроса необходимо обязательно указать параметр sensor_id.

Нажмите **Send**.

При корректном выводе запроса вы получите статус 200 OK, и результат выполнения.

Чтобы отключить сетевую изоляцию для выбранного хоста, вам требуется создать запрос на отключение правила сетевой изоляции. Для создания запроса используется HTTP-метод DELETE.



Пример:
DELETE
https://{{kedr_ip}}:443/kata/response_api/v1/{{sensorid}}/settings?sensor_id={{kedr_agent_id}}&settings_type=network_isolation

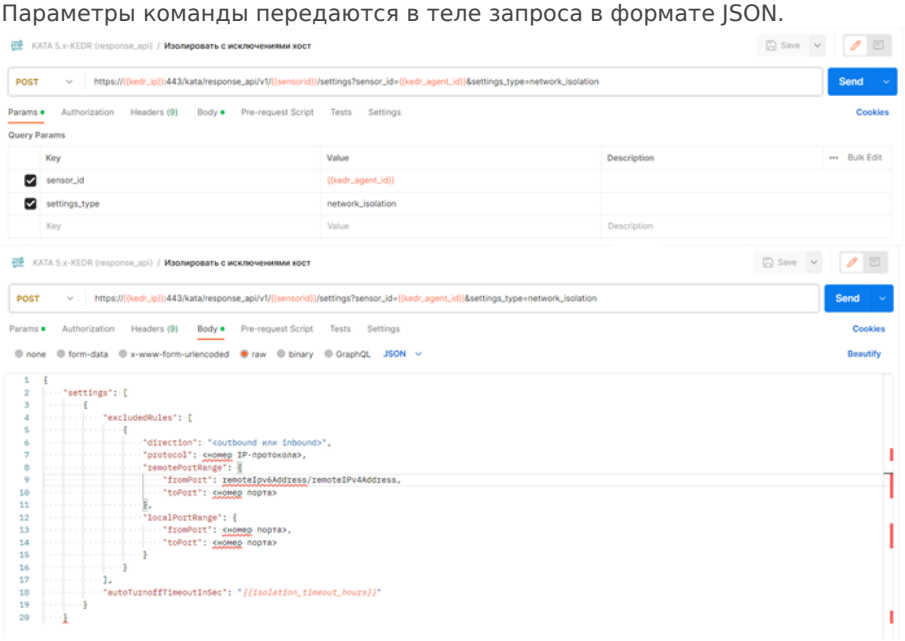
Запрос на добавление исключения в правило сетевой изоляции

Выберите запрос «**Изолировать с исключениями хост**».
В строке запроса необходимо обязательно указать параметр sensor_id и параметры указанные в таблице ниже.

Нажмите **Send**.

При корректном выводе запроса вы получите статус 200 OK, и результат выполнения.

Чтобы добавить исключение для ранее созданного правила сетевой изоляции, вам требуется создать запрос на добавление исключения. Для создания запроса используется HTTP-метод POST.
Параметры команды передаются в теле запроса в формате JSON.



Пример в Postman:
https://{{kedr_ip}}:443/kata/response_api/v1/{{sensorid}}
/settings?sensor_id={{kedr_agent_id}}&settings_type=network_isolation

```
{
  "settings": [
    {
      "excludedRules": [
        {
          "direction": "<outbound или inbound>",
          "protocol": <номер IP-протокола>,
          "remoteIpv6Address/remoteIPv4Address": <IP-
адрес хоста с компонентом Endpoint Agent>,
          "remotePortRange": {
            "fromPort": <номер порта>,
            "toPort": <номер порта>
          },
          "localPortRange": {
            "fromPort": <номер порта>,
            "toPort": <номер порта>
          }
        }
      ],
      "autoTurnoffTimeoutInSec": "{{isolation_timeout_hours}}"
    }
  ]
  }
```

Синтаксис команды
POST "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию 443>/kata/response_api/v1/<идентификатор external_system_id>/settings?sensor_id=<идентификатор sensor_id>&settings_type=network_izolation" -H 'Content-Type: application/json' -d '
{
"settings": [
{
"excludedRules": [
{
"direction": "<outbound или inbound>",
"protocol": <номер IP-протокола>,

Описание параметров добавляемого исключения в правило сетевой изоляции

Подробное описание приведено в документации по адресу: https://support.kaspersky.com/help/KATA/7.1/ru-RU/227499.htm

Параметр	Тип	Описание
`external_system_id`	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`sensor_id`	UUID	Уникальный идентификатор хоста с компонентом Endpoint Agent.
`protocol`	integer	Номер IP-протокола, назначенный Internet Assigned Numbers Authority (IANA).
`remoteIpv4Address/remoteIpv6Address`	string	IP-адрес хоста с компонентом Endpoint Agent, сетевой трафик которого не должен быть заблокирован.
`remotePortRange`	string	Порт назначения. Вы можете указать порт, только если вы выбрали входящее или исходящее направление сетевого трафика. Для двунаправленного трафика нельзя задавать диапазон портов.
`localPortRange`	string	Порт, с которого устанавливается соединение. Вы можете указать порт, только если вы выбрали входящее или исходящее направление сетевого трафика. Для двунаправленного трафика нельзя задавать диапазон портов.
`autoTurnoffTimeoutInSec`	integer	Время, в течение которого будет действовать сетевая изоляция хоста. Допустимый диапазон – от 1 до 9999 часов. Время сетевой изоляции указывается в секундах. Например, если вы хотите включить сетевую изоляцию хоста на два часа, вам требуется указать 7200 секунд.

Управление правилами запрета

Важная информация по работе с правилами запрета, пожалуйста ознаккомьтесь внимательно с информацией.

Информация взята из справки. https://support.kaspersky.com/help/KATA/7.1/ru-RU/227294.htm

С помощью правил запрета вы можете заблокировать запуск файлов или процессов на выбранном хосте или всех хостах с компонентом Endpoint Agent. Например, вы можете запретить запуск приложений, использование которых считаете небезопасным. Приложение **идентифицирует файлы по их хешу** с помощью алгоритмов хеширования **MD5** и **SHA256**. Правило запрета, созданное через внешние системы, может содержать несколько хешей файлов.

Через внешние системы вы можете управлять всеми правилами запрета, созданными для одного хоста или всех хостов, одновременно. При создании правила запрета для выбранного хоста через внешние системы Kaspersky Anti Targeted Attack Platform заменяет все правила запрета, назначенные на этот хост, правилом с новыми параметрами. Например, если ранее вы добавили несколько правил запрета для выбранного хоста через веб-интерфейс приложения, а потом добавили правило запрета через внешние системы, все правила запрета, добавленные в веб-интерфейсе, будут заменены добавленным через внешние системы правилом.

При изменении параметров правила запрета, созданного через внешние системы, приложение сохраняет только новые параметры. Например, если вы создали правило запрета, которое содержит хеши для нескольких файлов, и хотите добавить в это правило еще один хеш, вам требуется создать запрос на добавление правила запрета и указать в нем все хеши, для которых вы создавали запрет ранее, и новый хеш.

Описанный сценарий также актуален для правил запрета, назначенных на все хосты.

Для создания правила запрета с помощью интерфейса API рекомендуется использовать следующий сценарий взаимодействия с Kaspersky Anti Targeted Attack Platform:

1. Создание запроса на получение списка хостов с компонентом Endpoint Agent
2. Создание запроса на получение информации о хостах, для которых существуют правила запрета
3. Создание запроса на одну из следующих операций с правилами запрета:

· создание правила;

· удаление правила.

Добавленные правила запрета отображаются в веб-интерфейсе приложения в разделе **Политики**, подразделе **Правила запрета**.

Если вы создаете через внешнюю систему правило запрета для всех хостов, вам требуется предварительно убедиться, что на сервере отсутствует и не применяется к одному или нескольким хостам правило запрета для этого же файла. Это условие также справедливо, если вы хотите создать через внешнюю систему правило запрета для выбранного хоста: вам требуется убедиться, что на сервере отсутствует и не применяется ко всем хостам правило запрета для этого же файла. В противном случае сервер вернет внешней системе ошибку со списком хостов, к которым уже применяется правило запрета.

Если правило запрета, создаваемое через внешнюю систему, содержит несколько хешей файлов, в информации об ошибке указывается только первый файл, вызвавший ошибку. Сведения о других дублирующихся правилах запрета не отображаются.

Для изменения уже созданного через веб-интерфейс или внешние системы правила запрета вам нужно создать запрос на добавление правила запрета с обновленными параметрами.

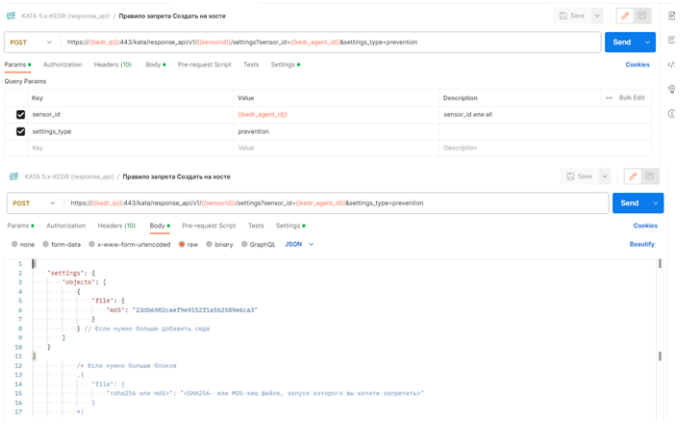
Запрос на создание правила запрета

Выберите запрос «**Правило запрета Создать на хосте**».
В строке запроса необходимо обязательно указать параметры sensor_id, objects, sha256 или md5 и парамерты, в виде json.

Нажмите **Send**.

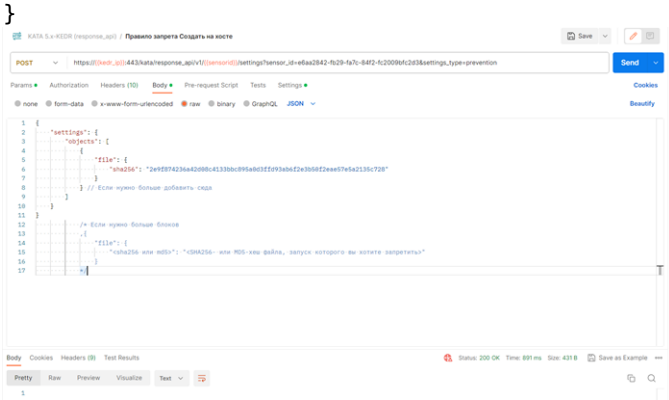
При корректном выводе запроса вы получите статус 200 OK, и результат выполнения.

Для создания запроса используется HTTP-метод POST. Параметры команды передаются в теле запроса в формате JSON.



Пример использования Postman:
POST
https://{{kedr_ip}}:443/kata/response_api/v1/{{sensorid}}/settings?sensor_id={{kedr_agent_id}}&settings_type=prevention

```
{
   "settings": {
      "objects": [
         {
            "file": {
               "sha256":
"2e9f874236a42d08c4133bbc895a0d3ffd93ab6f2e3b50f2eae57e5a2135c728"
            }
         } // Если нужно больше добавить сюда
      ]
   }
}
```



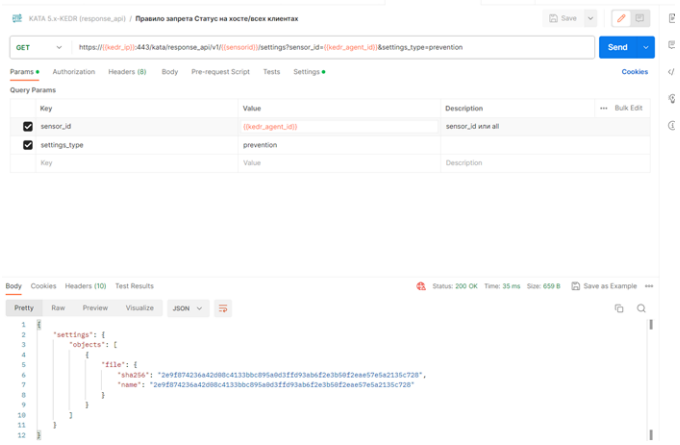
Отображение запроса в интерфейсе на CN:

Выберите запрос «**Правило запрета Статус на хосте/всех клиентах**».
В строке запроса необходимо обязательно указать параметры sensor_id, settings.

Нажмите **Send**.

При корректном выводе запроса вы получите статус 200 OK, и результат выполнения.

Для получения статуса правила запрета используется GET запрос



Пример в Postman:
https://{{kedr_ip}}:443/kata/response_api/v1/{{sensorid}}/settings?sensor_id={{kedr_agent_id}}&settings_type=prevention

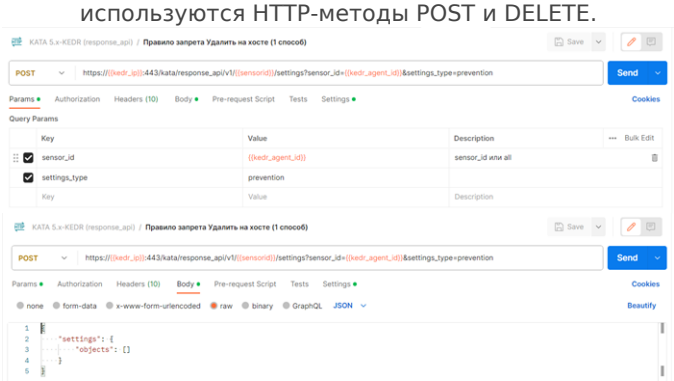
Запрос на удаление правила запрета (вариант 1 POST)

Выберите запрос «**Правило запрета Удалить на хосте (1 способ)**».
В строке запроса необходимо обязательно указать параметры sensor_id, settings.

Нажмите **Send**.

При корректном выводе запроса вы получите статус 200 OK, и результат выполнения.

Вы можете удалить правило запрета с помощью нового запроса с пустыми значениями или запроса с параметром DELETE. Для создания запросов используются HTTP-методы POST и DELETE.



Синтаксис:
Параметры команды передаются в теле запроса в формате JSON.

POST
https://{{kedr_ip}}:443/kata/response_api/v1/{{sensorid}}/settings?sensor_id={{kedr_agent_id}}&settings_type=prevention -H 'Content-Type: application/json' -d '
{ "settings": {"objects": [] } }'

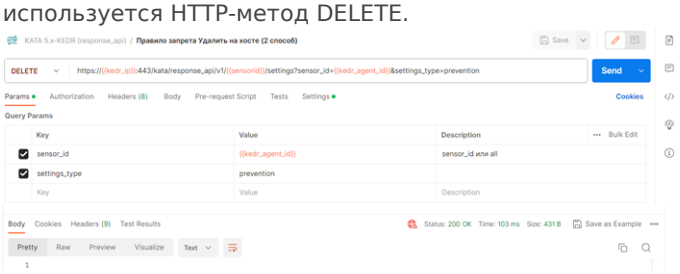
Запрос на удаление правила запрета (вариант 2 DELETE)

Выберите запрос «**Правило запрета Удалить на хосте (2 способ)**».
В строке запроса необходимо обязательно указать параметры sensor_id, settings.

Нажмите **Send**.

При корректном выводе запроса вы получите статус 200 OK, и результат выполнения.

Вы можете удалить правило запрета с помощью запроса с параметром DELETE. Для создания запроса используется HTTP-метод DELETE.



Синтаксис команды с параметром DELETE

DELETE https://{{kedr_ip}}:443/kata/response_api/v1/{{sensorid}}/settings?sensor_id={{kedr_agent_id}}&settings_type=prevention

Управление задачей запуска приложения

Для управления задачей запуска приложения с помощью интерфейса API рекомендуется использовать следующий сценарий взаимодействия с Kaspersky Anti Targeted Attack Platform:

1. Создание запроса на получение информации о параметрах, времени создания и статусе выполнения задачи
2. Создание запроса на одну из следующих операций с задачей:

· создание задачи;
· удаление задачи.

Добавленные задачи отображаются в веб-интерфейсе приложения в разделе **Задачи**.

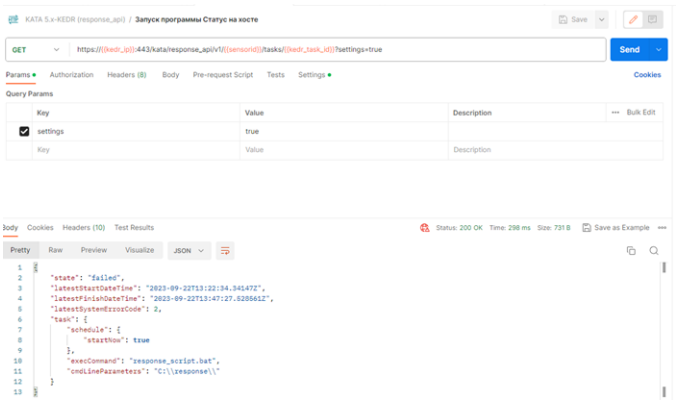
Получение информации о задаче

Выберите запрос «**Запуск программы Статус на хосте**».
В строке запроса необходимо обязательно указать параметры sensor_id, task_id и settings.

Нажмите **Send**.

При корректном выводе запроса вы получите статус 200 OK, и результат выполнения.

Для создания запроса на получение информации о задаче используется HTTP-метод GET.



Пример:
https://{{kedr_ip}}:443/kata/response_api/v1/{{sensorid}}/tasks/{{kedr_task_id}}?settings=true
где **task_id** из справки это переменная **{{kedr_task_id}}**, указываемая в разделе переменные.
Если будет генерироватья множество задач, то для генерации используется переменная {{$guid}}, которая генерирует случайный UUID для новой задачи. (Рассматривается далее в **Запрос на создание задачи**)

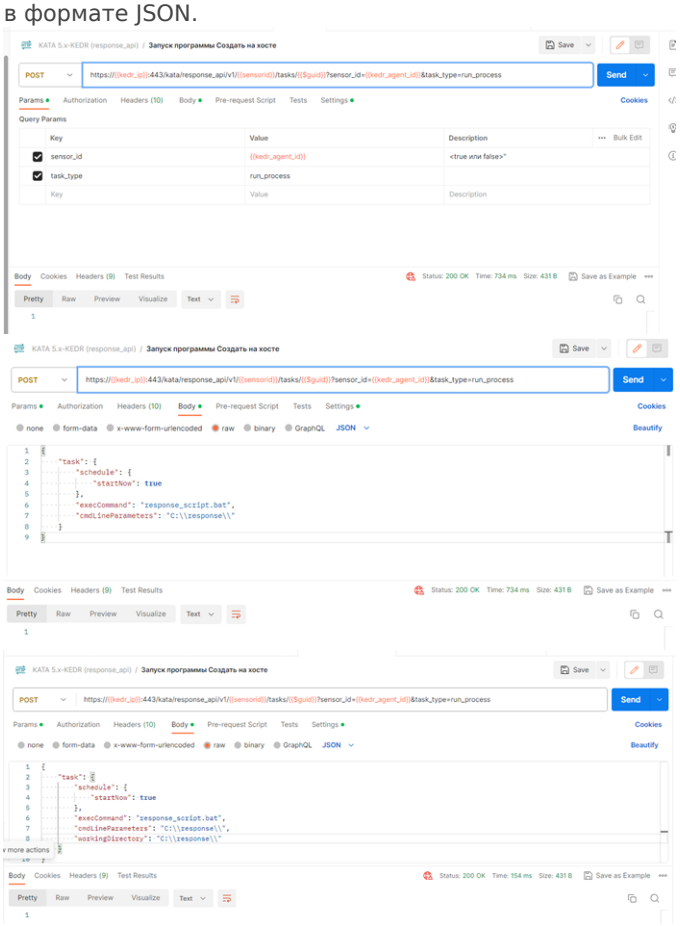
Запрос на создание задачи

Выберите запрос «**Запуск программы Создать на хосте**».
В строке запроса необходимо обязательно указать параметры sensor_id, task_id, settings и параметры запроса.

Нажмите **Send**.

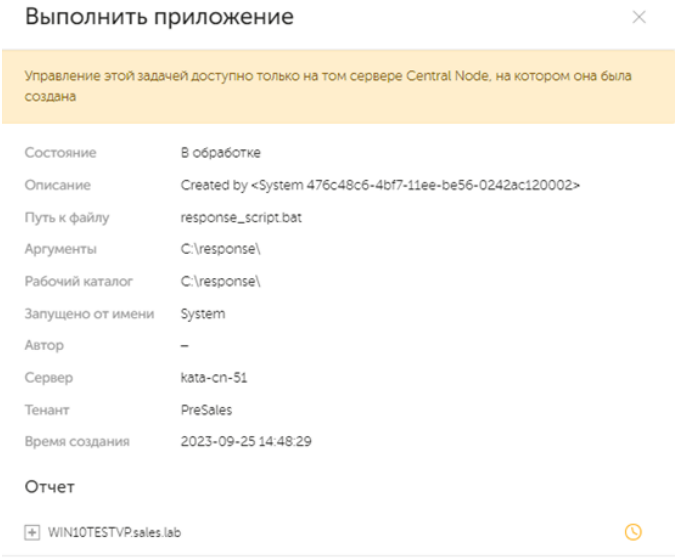
При корректном выводе запроса вы получите статус 200 OK, и результат выполнения.

Для создания запроса на запуск приложения Kaspersky Anti Targeted Attack Platform используется HTTP-метод POST. Параметры команды передаются в теле запроса в формате JSON.



При успешной обработке запроса задача на запуск приложения будет создана.
При генерации множества задач используется переменная (именно в Postman/Ansible) **{{$guid}}**, которая генерирует случайный **UUID** для **каждой** новой задачи.

В веб интерфейе Central Node, отобразится созданная задача:



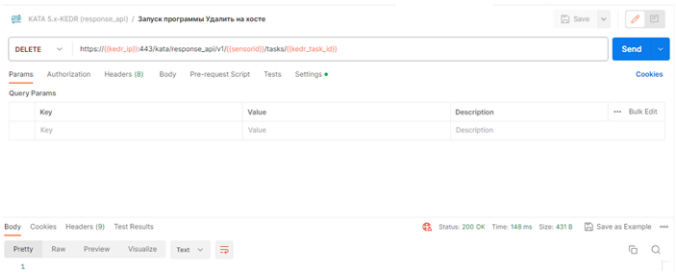
Запрос на удаление задачи

Выберите запрос «**Запуск программы Статус на хосте**».
В строке запроса необходимо обязательно указать параметры sensor_id, settings.

Нажмите **Send**.

При корректном выводе запроса вы получите статус 200 OK, и результат выполнения.

Для создания запроса на удаление задачи Kaspersky Anti Targeted Attack Platform используется HTTP-метод DELETE.



Пример:

DELETE https://{{kedr_ip}}:443/kata/response_api/v1/{{sensorid}}/tasks/{{kedr_task_id}}
Где, {{kedr_task_id}} - sensor_id – ID ранее созданной задачи.
При успешной обработке запроса задача на запуск приложения будет удалена.

Revision #10
Created 16 December 2025 21:28:35 by Владислав
Updated 6 February 2026 10:55:44 by Кирилл