

Резервное копирование и восстановление Ядра KUMA

Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Официальная документация по данному разделу приведена в онлайн-справке на продукт: <https://support.kaspersky.com/help/KUMA/4.0/ru-RU/222208.htm>

Статья онлайн-справки «REST API»:
<https://support.kaspersky.ru/kuma/4.0/217973>

Статья онлайн-справки «Создание резервной копии Ядра KUMA»:
<https://support.kaspersky.ru/kuma/4.2/316014>

KUMA позволяет выполнять резервное копирование базы данных Ядра KUMA и сертификатов.

Функция резервного копирования предназначена для восстановления KUMA – для переноса или копирования ресурсов следует использовать функции экспорта и импорта ресурсов.

Доступны следующие возможности создания резервной копии и восстановления из резервной копии:

- С помощью REST API.
- Через веб-интерфейс (начиная с версии 4.2)

С помощью REST API [KUMA 3.4+]

Создание резервной копии

KUMA поддерживает API-интерфейс, который работает через HTTP и представляет набор методов запрос/ответ.

Для создания резервной копии ядра используется метод `GET /system/backup`.

Для восстановления из резервной копии метод `POST /system/restore`.

KUMA Public API (v. 3):

https://support.kaspersky.com/help/KUMA/4.0/common/RestAPI/3/swagger_dist/dist/index.html

Чтобы создать резервную копию Ядра необходимо создать пользователя и предоставить ему права доступа к методам API `GET /system/backup` и `POST /system/restore` (для восстановления):

- Перейдите в раздел **Параметры** → **Доступ** → **Пользователи** и нажмите **Создать**.
 - В появившемся окне **Пользователь** задайте параметры нового пользователя:
 - **Статус учетной записи пользователя** – Активна.
 - **Имя** – введите имя пользователя.
 - **Логин** – введите уникальный логин учетной записи пользователя.
Длина должна быть от 3 до 64 символов (допускается использование только символов a-z, A-Z, 0-9, . \ - _).
 - **Адрес электронной почты** – введите уникальный адрес электронной почты пользователя. Адрес электронной почты должен быть действительным.

Если отправка уведомлений на почту не предполагается, то можно указать любую почту, например test@abc.local

- **Новый пароль** – введите пароль для учетной записи пользователя. Вы можете либо задать пароль вручную, либо нажать на кнопку **Сгенерировать пароль**. Пароль должен соответствовать следующим требованиям:
 - длина соответствует политике безопасности;

- как минимум один символ в нижнем регистре;
- как минимум один символ в верхнем регистре;
- как минимум одна цифра;
- как минимум один специальный символ из списка специальных символов в политике безопасности;
- не более двух одинаковых символов подряд;
- пароль не содержит логин.

Статья онлайн-справки «Настройка политики безопасности при входе в веб-интерфейс KUMA»:

<https://support.kaspersky.ru/kuma/4.0/302832>

- **Подтверждение пароля** – повторите пароль.
- **Пользователь должен сменить пароль при следующем входе в систему** - уберите флажок, так как для служебной учетной записи это не требуется.
- **Неограниченный срок действия пароля** - установите этот флажок, чтобы на учетную запись пользователя не действовал параметр **Время жизни пароля**. Рекомендуется включать этот параметр для служебной учетной записи, ограничить такой учетной записи права и установить пароль максимальной сложности.
- **Роль** – выберите роли пользователя. В текущем примере достаточно минимальных прав – **Младший аналитик**.
- **Тенант** - выберите тенант **Main**.

Статья онлайн-справки «О тенантах»:

<https://support.kaspersky.ru/kuma/4.0/221264>

- **Наборы пространств** – в раскрывающемся списке выберите один или несколько наборов пространств, к которым вы хотите предоставить доступ, установив рядом флажок. Если у пользователя нет выбранных наборов пространств, будет предоставлен доступ к набору пространств по умолчанию.
- Нажмите **Добавить**.

Пользователь



Статус учетной записи пользователя*

☒ Активная **1**

Имя*

backup **2**

Логин*

backup **3**

Адрес электронной почты*

backup@truecompany.local **4**

Часовой пояс

Авто

☐ Использовать формат ISO8601

☐ Получать уведомления по почте

☐ Уведомлять об алертах в WEB интерфейсе

☐ Отображать непечатаемые символы (Ctrl/Command + *)

Пароль

Сгенерировать пароль

Новый пароль*

..... **5**



Надежность пароля: Сильный

Подтверждение пароля*

..... **6**



☐ Пользователь должен сменить пароль при следующем входе в систему

☒ Неограниченный срок действия пароля **7**

Доступ

Доп.*

Добавить

Отмена

Доступ

Роль*

Младший аналитик 1

Тенант*

Main x 2

Добавить роль

Наборы пространств ⓘ

All spaces 3

У пользователя есть доступ ко всем пространствам, которые указаны в дефолтном наборе, пока явно не указаны другие наборы

4

Добавить

Отмена

Учетная запись пользователя создана и отображается в таблице **Пользователи**.

Нажмите на созданного пользователя и в появившемся окне **Пользователь**:

- В секции Взаимодействие с KUMA через API нажмите **Сгенерировать токен**. В окне **Сгенерировать токен** укажите **Без окончания срока действия** (так как токен будет использоваться сервисной учетной записью backup для задач создания резервных копий) и поставьте флажок напротив методов `GET /system/backup` и `POST /system/restore`.
- Нажмите **Сгенерировать**.

Сгенерировать токен



Срок действия*

☒ Без окончания срока действия **1**

Права доступа через API

Выберите методы API, к которым необходимо разрешить доступ. Если у вашей учетной записи нет доступа к методу в приложении, токен не предоставит вам доступ к методу через API, даже если вы выберете этот метод в списке ниже.

☐ **Выбрать все**

- ☐ GET /activeLists
- ☐ GET /alerts
- ☐ GET /alerts/id/:id
- ☐ GET /assets
- ☐ GET /contextTables
- ☐ GET /contextTables/export
- ☐ GET /dictionaries
- ☐ GET /download/:id
- ☐ GET /events/clusters
- ☐ GET /folders
- ☐ GET /incidents
- ☐ GET /incidents/id/:id
- ☐ GET /reports
- ☐ GET /resources
- ☐ GET /resources/:kind/:id
- ☐ GET /resources/:kind/:id/history
- ☐ GET /resources/:kind/:id/history/:changeNumber
- ☐ GET /resources/download/:id
- ☐ GET /services
- ☐ GET /services/:id/activeLists/export/:list
- ☐ GET /services/:id/activeLists/scan/:list
- ☐ GET /settings/extendedFields/export
- ☐ GET /settings/id/:id
- ☒ GET /system/backup **2**
- ☐ GET /tenants
- ☐ GET /users

Сгенерировать

Отмена

☒ POST /system/restore **1**

- ☐ POST /tasks/create
- ☐ POST /tenants/create
- ☐ PUT /resources/:kind/:id

2

Сгенерировать

Отмена

- Скопируйте и сохраните полученный токен доступа к API.

×

Token

1

Чтобы создать резервную копию Ядра:

- ```
curl -k -H "Authorization: Bearer ТОКЕН_ПОЛЬЗОВАТЕЛЯ" -H "accept: binary" -o
/opt/backup.tar.gz https://<IP-адрес/FQDN-сервера KUMA>:7223/api/v3/system/backup
```

Автоматизировать процесс создания резервной копии можно с помощью утилиты `scp` и дальнейшей выгрузки файла резервной копии на файловый сервер/сторонний ресурс.

Если операция выполнена успешно, создается событие аудита со следующими параметрами:

SourceUserID = "<user-login>"

Чтобы создать резервную копию Ядра:

- Выполните подключение к CLI сервера KUMA (серверу с компонентом Ядро при распределенной установке).
- Выполните следующую команду для восстановления из резервной копии с помощью API:

```
curl -k --request POST 'https://<IP-адрес/FQDN-сервера KUMA>:7223/api/v3/system/restore' --header 'Authorization: Bearer <token>' -H 'accept: */*' -H 'Content-Type: binary' --data-binary '@/opt/backup.tar.gz'
```

Тело запроса должно содержать архив с резервной копией Ядра KUMA, полученный в результате выполнения API-запроса создания резервной копии.

После получения архива с резервной копией KUMA выполняет следующие действия:

- Распаковывает архив с резервной копией Ядра KUMA во временную директорию.
- Сравнивает версию текущей KUMA и с версией резервной копии KUMA.
- Если версии соответствуют друг другу, создается событие аудита со следующими параметрами:
  - DeviceAction = "Core restore scheduled"
  - SourceUserID = "<имя пользователя инициировавшего восстановление KUMA из резервной копии"
- Если версии не различаются, выполняет восстановление данных из резервной копии Ядра KUMA.
- Удаляет временную директорию и запускает в штатном режиме.
- В журнале Ядра KUMA появится запись "WARN: restored from backup".

## Через веб-интерфейс [KUMA 4.2+]

| Статус | Тип  | Сервис | Версия    | Тенант | Полное доменное имя           | IP-адрес      | Порт API | Время работы           | Создан              |
|--------|------|--------|-----------|--------|-------------------------------|---------------|----------|------------------------|---------------------|
| Вкл    | Ядро | core-1 | 4.2.0.259 | Main   | kaspsky-unified-analysis-head | 192.168.1.100 | 7210     | 30 дня 5 часа 16 ми... | 17.06.2024 13:04:03 |

## Полезные ссылки

- Создание резервной копии Ядра KUMA (Postman): <https://www.postman.com/kl-ru-presales/workspace/kaspersky-products-apis-ru/request/23340929-bd766c26-c34b-467e-a28a-4ff65ac05328>

- Восстановление Ядра KUMA из резервной копии (Postman):

<https://www.postman.com/kl-ru-presales/workspace/kaspersky-products-apis-ru/request/23340929-974b96b4-0876-449c-9001-9912783f6acc>

---

Revision #29

Created 2023-08-10 13:27:25 UTC by Boris RZR

Updated 2026-08-18 10:51:56 UTC by Dmitry Borisov