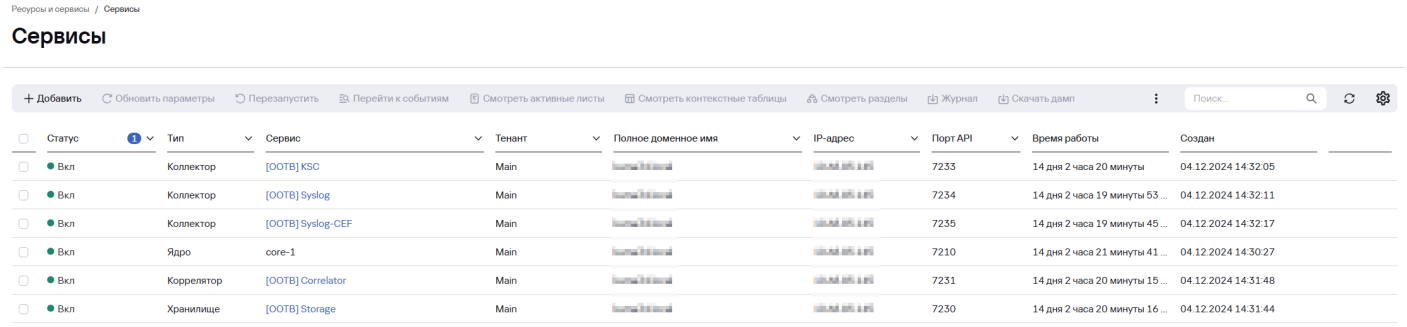
Базовая настройка

Проверка сервисов

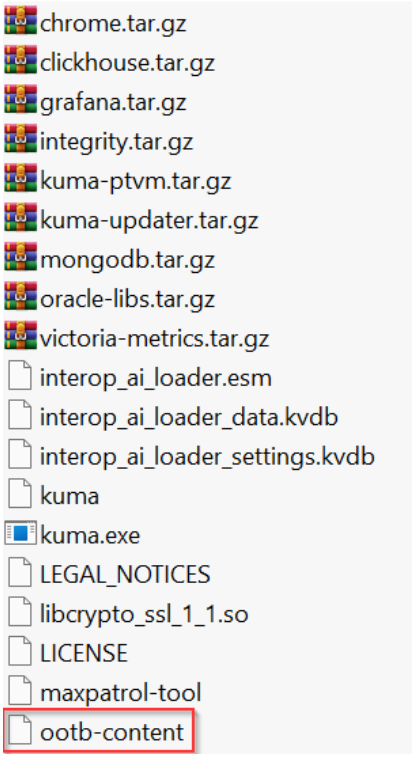
????? ????? ? ???-????????? KUMA ????????? ??????? ? ?????? ???????????????? ????????:

- ????????? ? ?????? **Ресурсы** ? **Активные сервисы**
- ????????? ? ??????? ???????? ? ????????? `[OOTB]` ? ??? ?????? ??????? ????????? ? ??????? **«Вкл»**.



??? ??????? ???????????????? ????????, ??? ?? ????????? ????, ????? ??????? ? ????????? ????? ??????? ?????????.

? ?????? ???? ???????????????? ??????? (?????????, ?????????? ? ??????????) ?? ???? ?????????? ????? ????????????? ????? ???????? ??? ???????? ???????? ?? ????? `ootb-content`, ??????? ???????? ?? ???? `/kuma-ansible-installer/roles/kuma/files/`.



??? ??????? ?????? ???????? ?? ????? ??. ?????? **Импорт ресурсов из файла**.

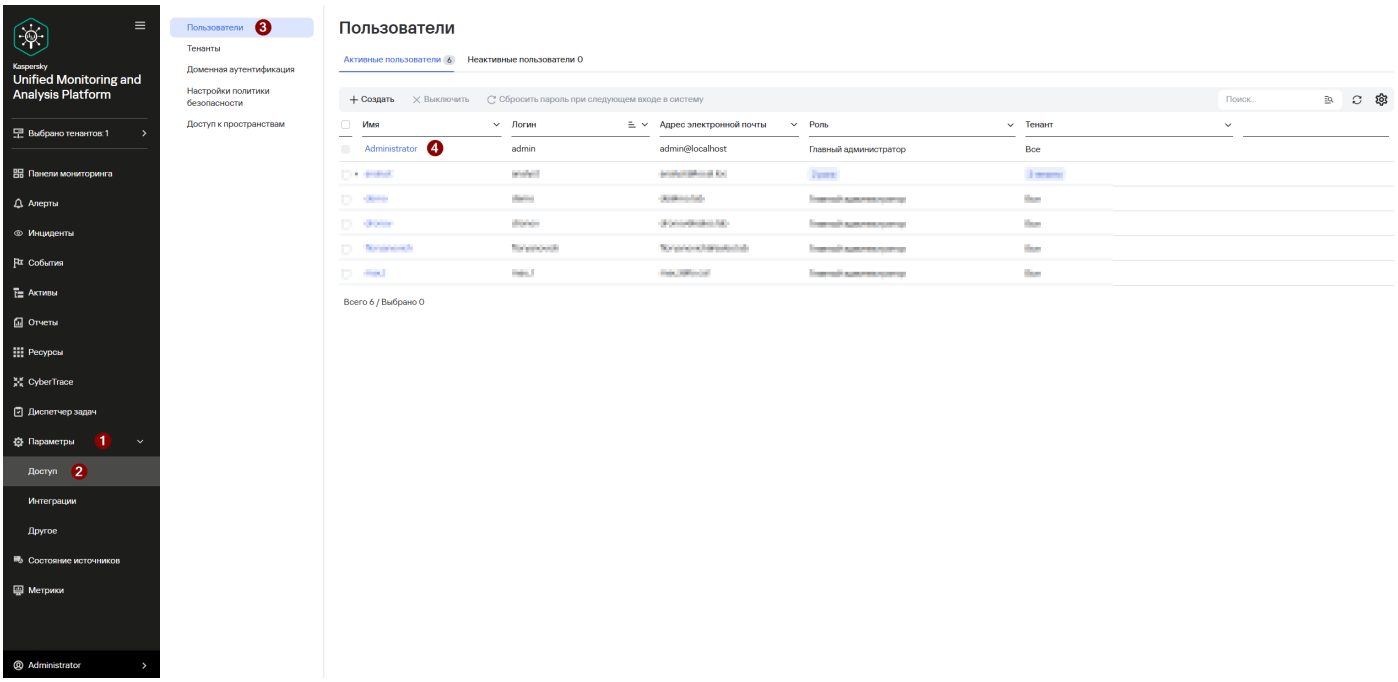
????? ????? ??????? ??????? ???????? ??????? (??. ?????? ???????? ? ????????? ????????).

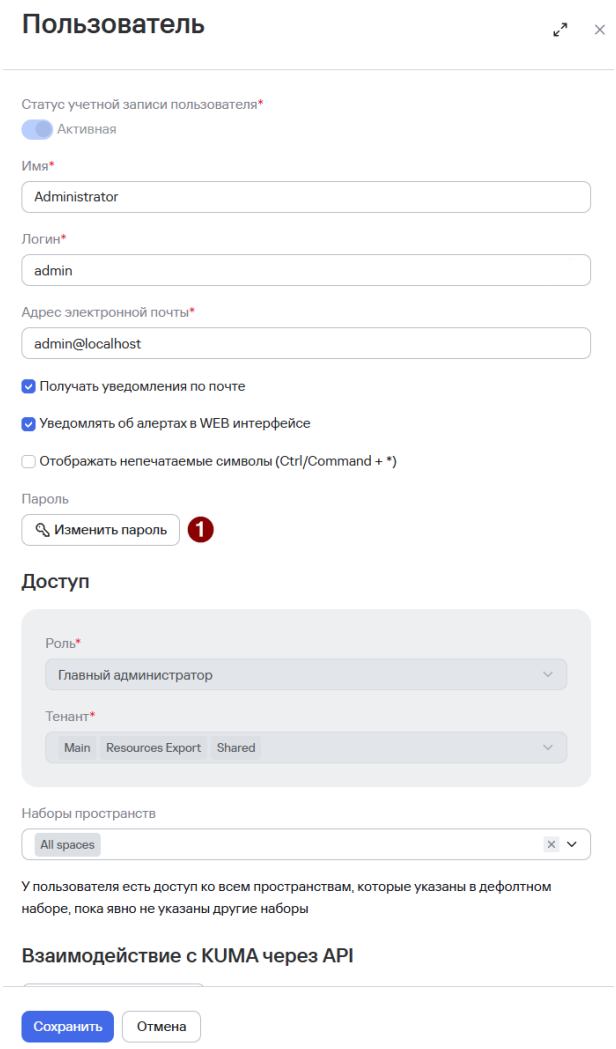
Создание пользователей

?? ????????? ? KUMA ????????????? ???? ??????? ?????? **admin** ? ????? ????????
????????????? ? ??????????? ??????? ??????????.

??????????? ????????????? ???????? ?????? ??? ??????? ?????? **admin** ????? ??????? ?????.
??? ?????:

- ????????? ? ?????? **Параметры** ? **Доступ** ? **Пользователи**.
- ??????? ?? ???????????? **admin**.
- ? ??????????? ???? **Пользователь** ??????? **Изменить пароль**.
- ? ???? **Изменить пароль** ??????? ??????????? ?????? ? ??????? ????? ??????.
- ??????? **OK**.
- ????? ??????? **Сохранить**.


Kaspersky
Unified Monitoring and Analysis Platform
Выбрано тенантов: 1
Панели мониторинга
Алерты
Инциденты
События
Активы
Отчеты
Ресурсы
CyberTrace
Диспетчер задач
Параметры
1
Доступ
2
Интеграции
Другое
Состояние источников
Метрики
Administrator
Пользователи
3
Тенанты
Доменная аутентификация
Настройки политики безопасности
Доступ к пространствам
Пользователи
Активные пользователи 6
Неактивные пользователи 0
+ Создать
Выключить
Сбросить пароль при следующем входе в систему
Поиск...
Имя
Логин
Адрес электронной почты
Роль
Тенант
Administrator
4
admin
admin@localhost
Главный администратор
Все
Всего 6 / Выбрано 0


Пользователь
Статус учетной записи пользователя*
Активная
Имя*
Administrator
Логин*
admin
Адрес электронной почты*
admin@localhost
Получать уведомления по почте
Уведомлять об алертах в WEB интерфейсе
Отображать непечатаемые символы (Ctrl/Command + *)
Пароль
Изменить пароль
1
Доступ
Роль*
Главный администратор
Тенант*
Main
Resources Export
Shared
Наборы пространств
All spaces
У пользователя есть доступ ко всем пространствам, которые указаны в дефолтном наборе, пока явно не указаны другие наборы
Взаимодействие с KUMA через API
Сохранить
Отмена

?????? ? KUMA ????? ????? ????????? ?????????????. ????????????? ????????????? ???? ?????????????, ??????? ?????? ??, ????? ??????? ?????????? ????? ???????? ????????????? ? ????? ??????? ??? ?????? ?????????.

?????? ??????-??????? «???? ?????????????»: https://support.kaspersky.ru/kuma/4.0/218031

????? ??????? ??????? ?????? ????????????:

- ????????? ? ?????? **Параметры** ? **Доступ** ? **Пользователи**.
- ??????? **Создать**.
- ? ??????????? ???? **Пользователь** ??????? ????????? ?????? ????????????:
  - **Статус учетной записи пользователя** – ???????.
  - **Имя** – ??????? ??? ????????????.
  - **Логин** – ??????? ?????????? ????? ??????? ?????? ????????????. ????? ?????? ???? ?? 3 ?? 64 ???????? (??????????? ????????????? ?????? ???????? a–z, A–Z, 0–9, . \ - _).
  - **Адрес электронной почты** – ??????? ?????????? ????? ?????????? ????? ????????????. ????? ??????????? ????? ?????? ???? ?????????????.

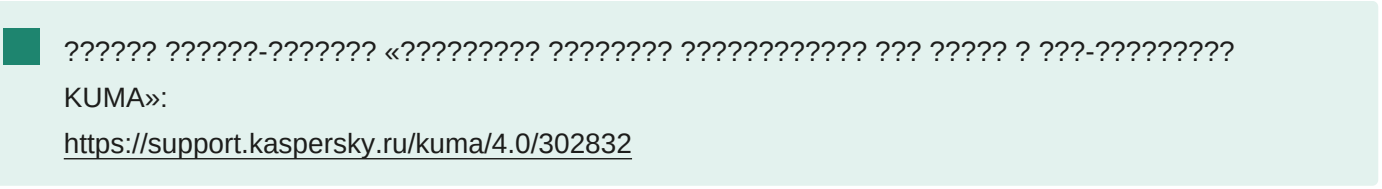
???? ???????? ??????????? ?? ????? ?? ?????????????, ?? ????? ??????? ????? ?????, ???????? test@abc.local

  - **Часовой пояс** - ???????? ??????? ????, ? ??????? ????? ???????????? ????????? ????? ??? ?????? ? KUMA. ?????? ??????????? ?? ?????? ?????????? ???????????? ??????? ???????????? ? ????????? ??????? ?? ?????? ? ?????? ?????. ?? ????????? ???????????? ??????? ???? ???????? ????????????.
  - **Использовать формат ISO 8601** – ?????????? ???? ??????, ????? ????????? ????? ???????????? ? ??????? ISO 8601 (????????, 2026-02-08T17:35:27+03:00). ?????? ??????????? ? ??? ???????? ???-?????????? KUMA, ??? ???????????? ??????????? ??? ?????? ??????????? ???? ? ???????, ? ????????? ?? ???? ??????? KUMA. ??????????? ?????? ??????????? ? ?????????? ???? KUMA.
  - **Получать уведомления по почте** - ?????????? ???? ??????, ????? ???????????? ??????? ???????? ??????????? ?? KUMA.
  - **Уведомлять об алертах в WEB интерфейсе** - ?????????? ???? ??????, ????? ? ???-?????????? KUMA ???????????? ??????????? ?? ???????. ??????? ??????, ???? ?????? ????????? ??????????? ???????????. ?? ????????? ?????? ??????????.
  - **Отображать непечатаемые символы (Ctrl/Command + *)** - ?????????? ???? ??????, ????? ? ???-?????????? KUMA ???????????? ???????????? ???????: ???????, ????? ?????????, ??????? ?? ????? ??????. ???? ??????

Отображать непечатаемые символы ??????????, ???????????
???????????? ???????? ????? ???????? ? ????????? ? ??????? ??????

Ctrl/Command+*.

- **Новый пароль** – ??????? ?????? ??? ??????? ?????? ????????????. ?? ??????
???? ?????? ?????? ???????, ???? ?????? ?? ?????? ????????????? ??????. ??????
?????? ?????????????? ????????? ???????????:
  - ????? ????????????? ???????? ????????????;
  - ??? ??????? ???? ?????? ? ?????? ????????;
  - ??? ??????? ???? ?????? ? ??????? ????????;
  - ??? ??????? ???? ?????;
  - ??? ??????? ???? ?????????? ?????? ?? ?????? ?????????? ???????? ?
???????? ????????????;
  - ?? ????? ???? ?????????? ???????? ??????;
  - ?????? ?? ???????? ?????.



?????? ??????-??????? «????????? ???????? ???????????? ??? ????? ? ???-?????????
KUMA»:
https://support.kaspersky.ru/kuma/4.0/302832

- **Подтверждение пароля** – ????????? ??????.
- **Пользователь должен сменить пароль при следующем входе в систему** - ?????????? ???? ??????, ????? ??? ????????? ??????? ????? ? ???-
????????? KUMA ???????????? ?????? ?????? ?????? ? ????? ????? ??????. ?????
????? ???????????? ????? ???????? ???? ? ???-????????? KUMA ? ????? ???????.
?? ????????? ???? ?????? ??????????.

????????, ?? ?????? ???????????? ???? ???????? ??? ???????? ?????? ????????????.
???????????? ????? ????????? ????????? ?????? ? ?????????? ???? ??????. ????? ????? ?
????????? ??????? KUMA ????????? ???????????? ??????? ??????.

- **Неограниченный срок действия пароля** - ?????????? ???? ??????, ?????
?? ??????? ?????? ???????????? ?? ?????????? ???????? ????? ????? ??????.

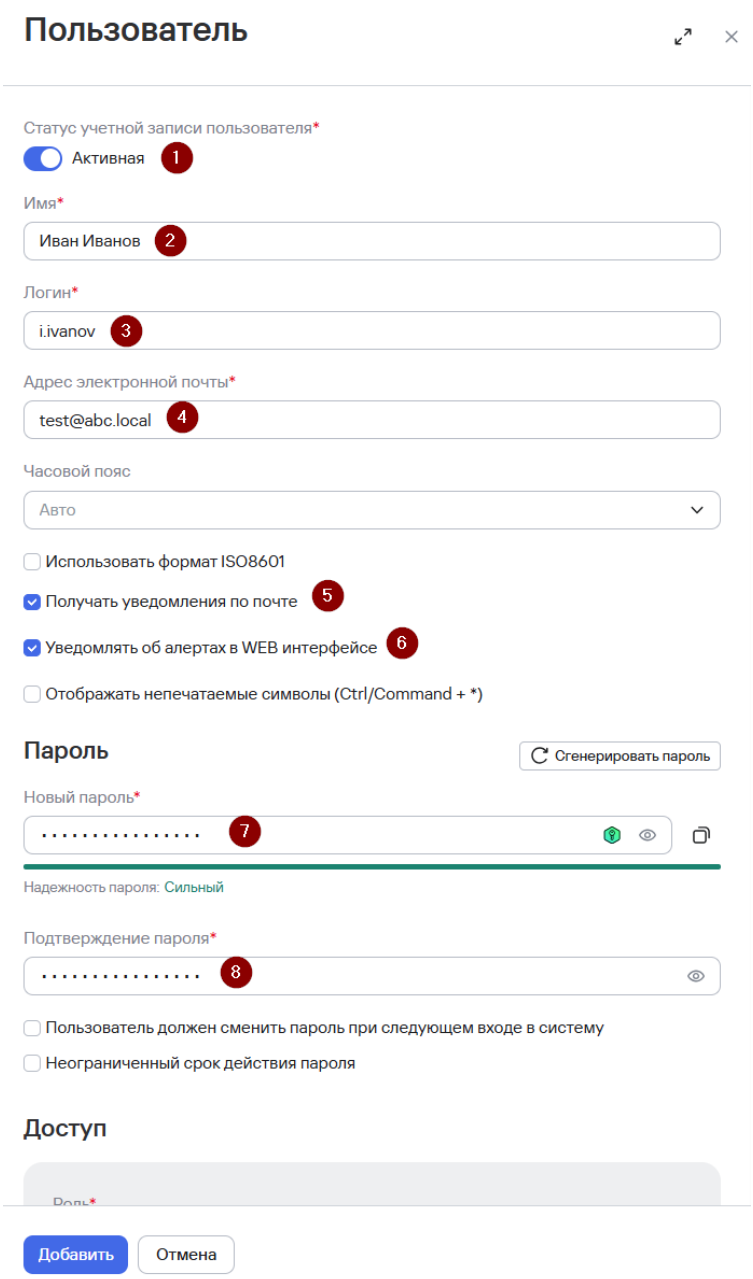
????????????? ???????? ???? ???????? ??? ????????? ??????? ??????, ?????????? ?????
??????? ?????? ????? ? ?????????? ?????? ???????????? ?????????. ?????? ???????
?????? ? ?????????????? ???????? ????? ?????? ???????????? ??? ???????????.

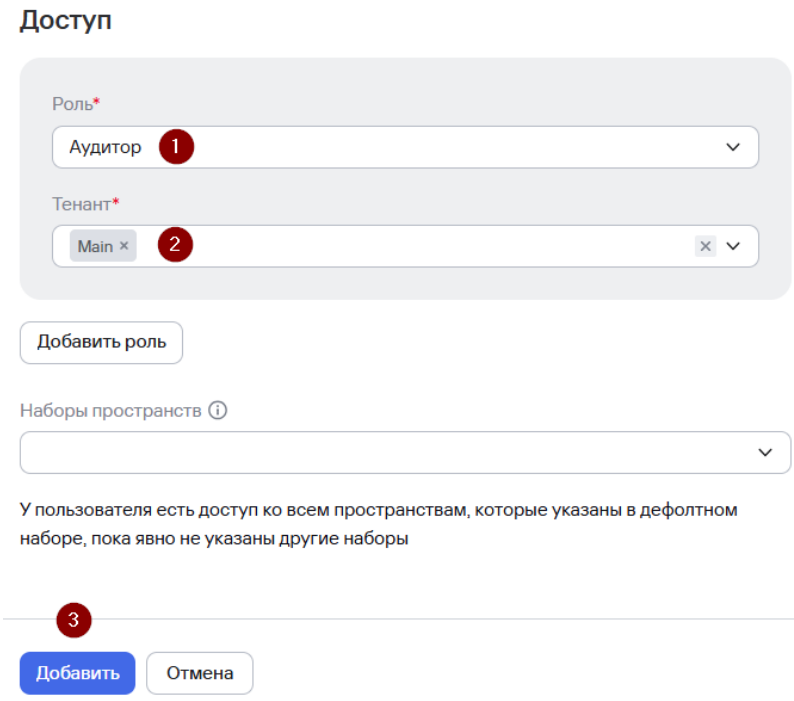
- **Роль** – ???????? ???? ????????????.

- **Тенант** - ???????? ??????, ? ???????? ????? ???????????? ????????????. ???????????? ????? ????????? ?????? ???? ? ?????? ????????, ? ????? ??????? ????? ????????? ????????? ?????.

?????? ??????-??????? «? ????????»: https://support.kaspersky.ru/kuma/4.0/221264

- **Наборы пространств** – ? ?????????????? ?????? ???????? ???? ??? ????????? ??????? ???????????, ? ??????? ?? ?????? ???????????? ??????, ????????? ????? ??????. ???? ? ???????????? ??? ????????? ??????? ???????????, ????? ???????????? ?????? ? ?????? ???????????? ?? ?????????.
- ??????? **Добавить**.


Пользователь
Статус учетной записи пользователя*
Активная
1
Имя*
Иван Иванов
2
Логин*
i.ivanov
3
Адрес электронной почты*
test@abc.local
4
Часовой пояс
Авто
Использовать формат ISO8601
Получать уведомления по почте
5
Уведомлять об алертах в WEB интерфейсе
6
Отображать непечатаемые символы (Ctrl/Command + *)
Пароль
Сгенерировать пароль
Новый пароль*
7
Надежность пароля: Сильный
Подтверждение пароля*
8
Пользователь должен сменить пароль при следующем входе в систему
Неограниченный срок действия пароля
Доступ
Роль*
Добавить
Отмена



??????? ?????? ???????????? ??????? ? ???????????? ? ??????? **Пользователи**.

Пользователь

Статус учетной записи пользователя*

Активная 1

Имя*

Петр Петров 2

Логин*

p.petrov 3

Адрес электронной почты*

ppetrov@truecompany.local 4

Получать уведомления по почте

Уведомлять об алертах в WEB интерфейсе 5

Отображать непечатаемые символы (Ctrl/Command + *)

Пароль

Сгенерировать пароль

Новый пароль* 6

Надежность пароля: Сильный

Подтверждение пароля*

Пользователь должен сменить пароль при следующем входе в систему 7

Неограниченный срок действия пароля

Доступ

Роль*

Младший аналитик 8

Тенант*

Main × 9

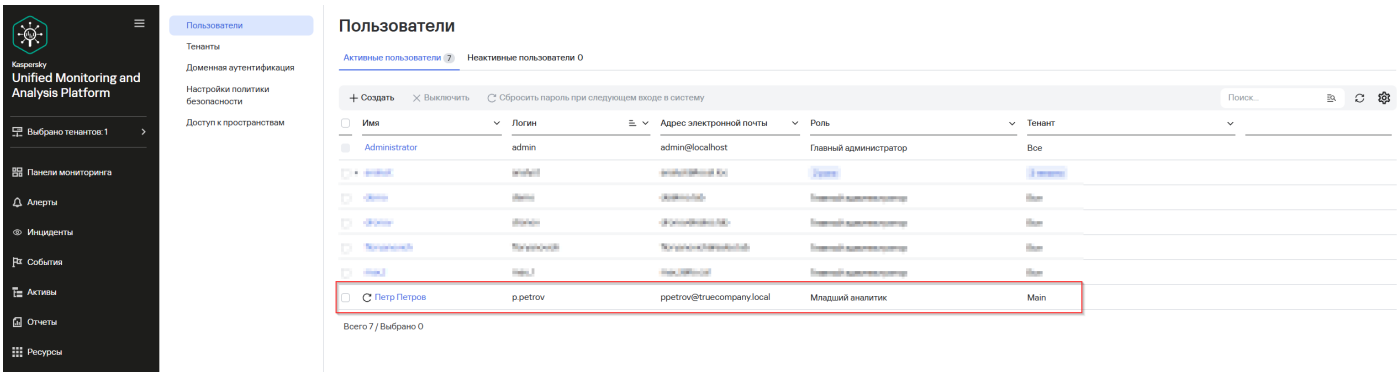
Добавить роль

Наборы пространств

All spaces 10

У пользователя есть доступ ко всем пространствам, которые указаны в дефолтном наб 11 пока явно не указаны другие наборы

Добавить Отмена



> ?????? ??????-??????? «?????????? ??????????????»: https://support.kaspersky.ru/kuma/4.0/217937
>
> ?????? ??????-??????? «?????????????? ? ??????? ???????? ??????? ???????»: https://support.kaspersky.ru/kuma/4.0/221427
>
> ????? ?? ????????? «?????????????? ? ??????? ???????? ??????? ??????? Active Directory»: https://rutube.ru/video/8cabd9b4a160f875fa2ef1abbd286e5d/

[4.2+] Создание пользовательской роли

??????? ? ?????? 4.2 ? ?????????? ? ???????????????? ?????, ? KUMA ????????? ??????????? ????????? ???????????????? ????. ??? ???????????????? ????? ????? ??????????? ?????????? ?????? ???? ? ?????????? ? ????????? ??????????? ???????????? ????????????? ????????. ?????? ????????????? ??????? – ?????? ??????.

> ?????? ??????-??????? «?????????????? ??????? ? ????????? ?? ?????? ??????????»: https://support.kaspersky.ru/kuma/4.2/316073

????????, ????? ??????? ???????????????? ???? «???????» (???? ????? ????? ?????? ?? ???? ????????????? ???????? ?????? ??? ??????):

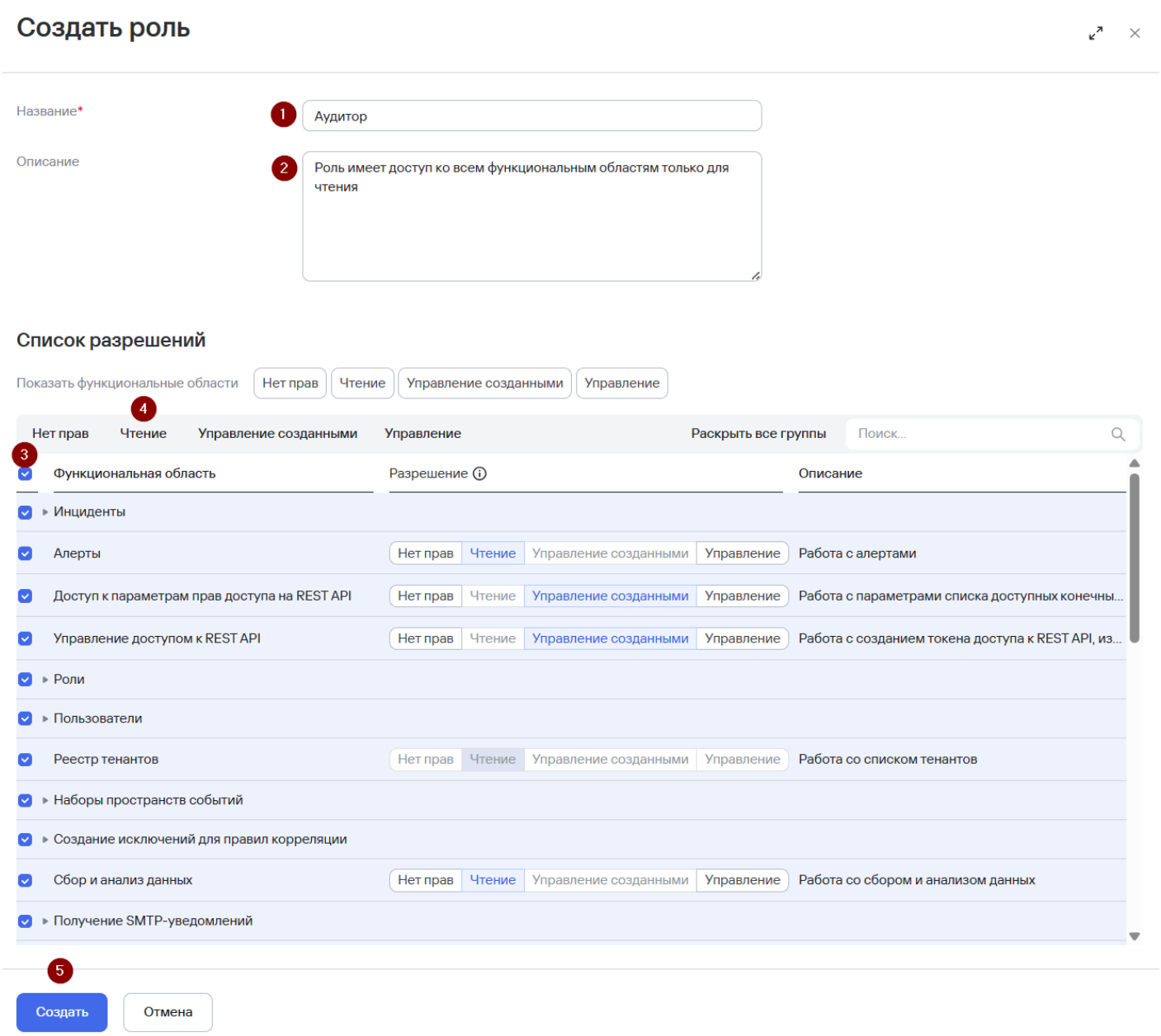
- ????????? ? ?????? **Параметры → Доступ → Роли.**
- ??????? **Создать**.
- ? ??????????? ???? **Создать** ???? ??????? ????????? ????? ????:
  - **Название** – ??????? ??? ???? (? ????? ??????? «???????»).
  - **Описание** – ??????????? ???????? ???????? ????.
  - ? ?????? **Список разрешений** ???????? ??? ????????????? ??????? ? ??????? **Чтение**.

? ?????? ????????? ??? ?????? ????????????? ???????? ????????? ????????? ????????????? ??????? ? ?????? ????????????? ????????. ????????, ?????? ksc ???????? ? ???? ????????? ????????????? ???????: ????? (???????? ??????? ????? KSC) ? ????????? (?????? ????????? KSC). ?? ?????? ??????? ?????? ????????????? ???????? ????????? ??? ??????? ????????? ????????????? ??????? ? ??????? ??????.

??? ????????? ????????????? ???????? ????? ??????? ??????? ??????????. ? KUMA ???????? ????????? ?????? ??????????:

- **Управление (англ. Manage)** – ?????? ????? ?? ?????? ? ????????????? ??????? (??????, ????????, ?????????????, ????????).
- **Управление созданными (англ. Manage created)** – ?????? ????? ?? ??? ? ????????????? ??????? (?????? ? ???????????? ???? ????????, ????????????? ? ???????? ????? ????????) ? ????????? ????????? ????????????? ????????.
- **Чтение (англ. Read)** – ????? ?? ??????.
- **Нет прав (англ. No rights)** – ?????????? ???? ?? ?????? ? ?????????.

- ??????? **Создать**.



?????????????? ???? ??????? ??????? ???????.

> ?? ????? ?????? ??????? ?????????????? ????, ?????????? ????????? ??? ???????????? ???? (? ??? ????? ?????????????? ????????? ????).

????? ????????? ????????? ?????????????? ???? ??????? ?????? ????????????:

- ????????? ? ?????? **Параметры** ? **Доступ** ? **Пользователи**.
- ???????? ????? ??????? ?????? ???????????? ??? ???????? ??? ???????????? ??????? ?????? (? ?????? ??????? ????? ??????? ????? ??????? ??????).
- ??????? **Создать**.
- ? ???????????? ???? **Пользователь** ??????? ????????? ?????? ????????????:

- **Статус учетной записи пользователя** – ???????.
- **Имя** – ??????? ??? ???????????.
- **Логин** – ??????? ?????????? ????? ??????? ?????? ???????????. ????? ?????? ???? ?? 3 ?? 64 ???????? (??????????? ????????????? ?????? ???????? a–z, A–Z, 0–9, . \ - _).
- **Адрес электронной почты** – ??????? ?????????? ????? ?????????? ????? ???????????. ????? ??????????? ????? ?????? ???? ?????????????.

???? ???????? ??????????? ?? ????? ?? ?????????????, ?? ????? ??????? ????? ?????, ???????? test@abc.local

- **Часовой пояс** - ???????? ??????? ????, ? ??????? ????? ???????????? ????????? ????? ??? ?????? ? KUMA. ?????? ??????????? ?? ?????? ?????????? ???????????? ??????? ???????????? ? ????????? ??????? ?? ?????? ? ?????? ?????. ?? ????????? ???????????? ??????? ???? ???????? ????????????.
- **Использовать формат ISO 8601** – ?????????? ???? ??????, ????? ????????? ????? ???????????? ? ??????? ISO 8601 (????????, 2026-02-08T17:35:27+03:00). ?????? ??????????? ? ??? ???????? ???-?????????? KUMA, ??? ???????????? ??????????? ??? ?????? ??????????? ???? ? ???????, ? ????????? ?? ???? ??????? KUMA. ??????????? ?????? ??????????? ? ?????????? ???? KUMA.
- **Получать уведомления по почте** - ?????????? ???? ??????, ????? ???????????? ??????? ???????? ??????????? ?? KUMA.
- **Уведомлять об алертах в WEB интерфейсе** - ?????????? ???? ??????, ????? ? ???-?????????? KUMA ???????????? ??????????? ?? ???????. ??????? ??????, ???? ?????? ????????? ??????????? ???????????. ?? ????????? ?????? ??????????.
- **Отображать непечатаемые символы (Ctrl/Command + *)** - ?????????? ???? ??????, ????? ? ???-?????????? KUMA ???????????? ???????????? ???????: ???????, ????? ?????????, ??????? ?? ????? ??????. ???? ?????? **Отображать непечатаемые символы** ??????????, ??????????? ???????????? ???????? ????? ???????? ? ????????? ? ??????? ?????? **Ctrl/Command+***.
- **Новый пароль** – ??????? ?????? ??? ??????? ?????? ????????????. ?? ?????? ???? ?????? ?????? ???????, ???? ?????? ?? ?????? ????????????? ??????. ?????? ?????? ?????????????? ????????? ???????????:
  - ????? ????????????? ???????? ????????????;
  - ??? ??????? ???? ?????? ? ?????? ????????;

- ??? ??????? ???? ?????? ? ??????? ????????;
- ??? ??????? ???? ?????;
- ??? ??????? ???? ??????????? ?????? ?? ?????? ??????????? ???????? ? ???????? ????????????;
- ?? ????? ???? ?????????? ???????? ??????;
- ?????? ?? ???????? ?????.

?????? ??????-??????? «????????? ???????? ???????????? ??? ????? ? ???-????????? KUMA»: https://support.kaspersky.ru/kuma/4.2/302832

- **Подтверждение пароля** – ????????? ??????.
- **Пользователь должен сменить пароль при следующем входе в систему** - ?????????? ???? ??????, ????? ??? ????????? ??????? ????? ? ???-????????? KUMA ???????????? ?????? ?????? ?????? ? ????? ????? ??????. ????? ????? ???????????? ????? ???????? ???? ? ???-????????? KUMA ? ????? ???????. ?? ????????? ???? ?????? ??????????.

???????, ?? ?????? ???????????? ???? ???????? ??? ???????? ?????? ????????????. ???????????? ????? ????????? ????????? ?????? ? ?????????? ???? ??????. ????? ????? ? ????????? ??????? KUMA ????????? ???????????? ??????? ??????.

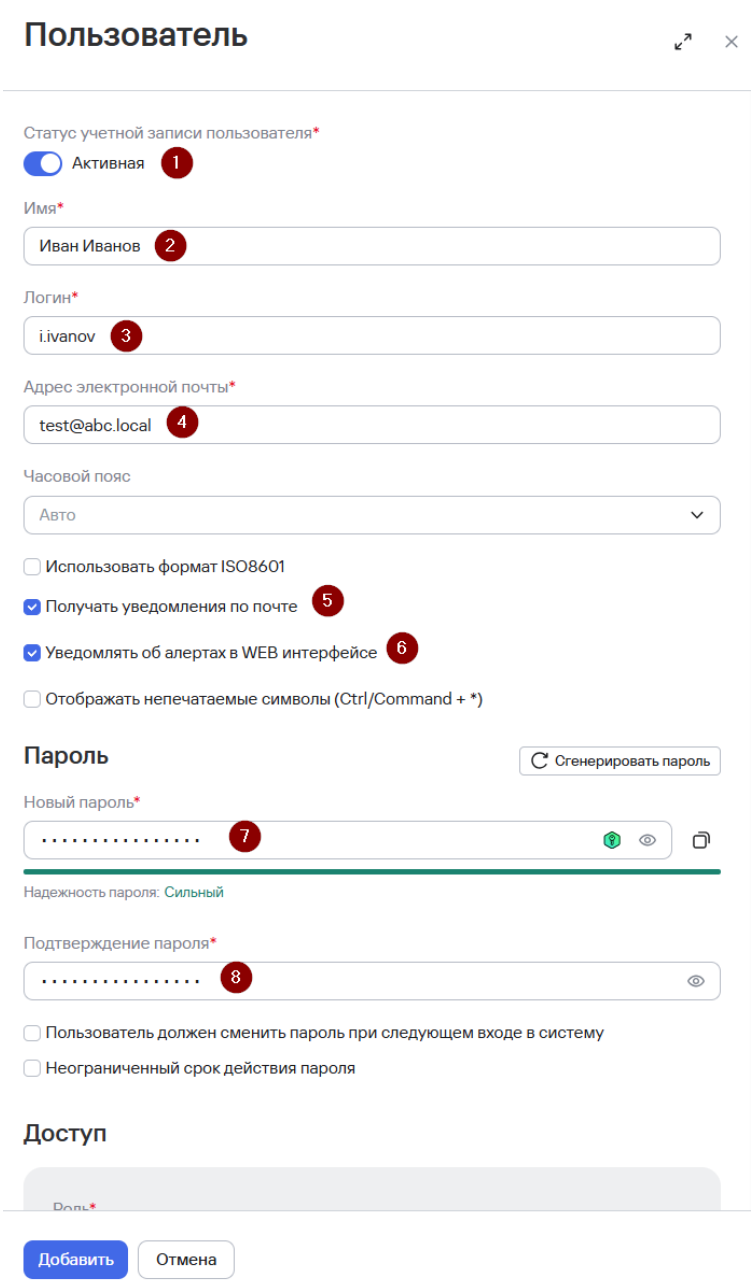
- **Неограниченный срок действия пароля** - ?????????? ???? ??????, ????? ?? ??????? ?????? ???????????? ?? ?????????? ???????? ????? ????? ??????.

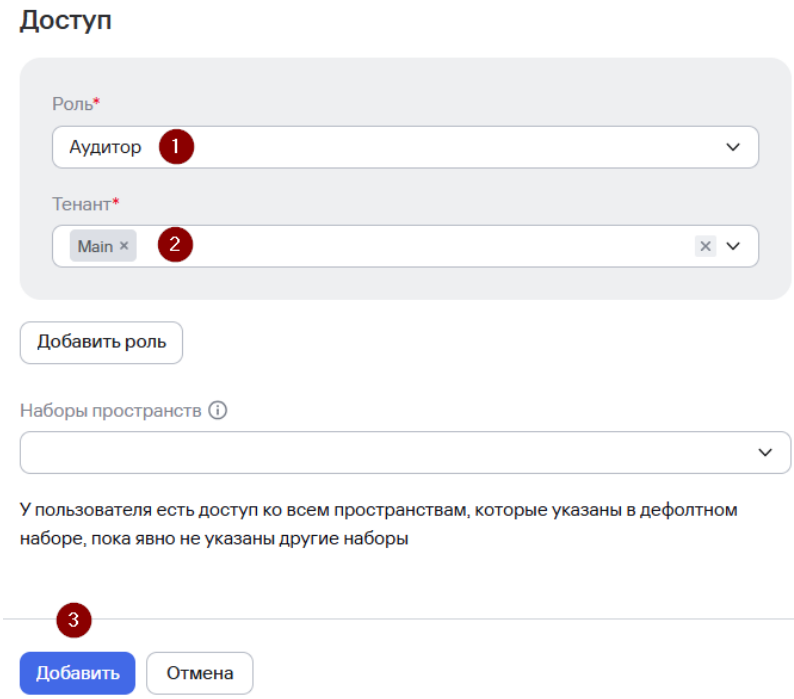
????????????? ???????? ???? ???????? ??? ????????? ??????? ??????, ?????????? ????? ??????? ?????? ????? ? ?????????? ?????? ???????????? ?????????. ?????? ??????? ?????? ? ????????????? ???????? ????? ?????? ???????????? ??? ??????????.

- **Роль** – ???????? ???? ????????????.
- **Тенант** - ???????? ??????, ? ???????? ????? ???????????? ????????????. ???????????? ????? ????????? ?????? ???? ? ?????? ????????, ? ????? ??????? ????? ????????? ????????? ?????.

?????? ??????-??????? «? ????????»: https://support.kaspersky.ru/kuma/4.0/221264

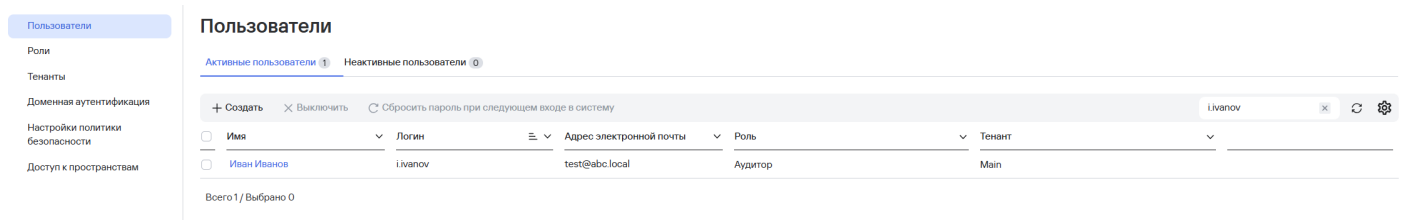
- **Наборы пространств** – ? ????????????? ?????? ???????? ???? ??? ????????? ??????? ???????????, ? ??????? ?? ?????? ???????????? ??????, ????????? ????? ??????. ???? ? ???????????? ??? ????????? ??????? ???????????, ????? ???????????? ?????? ? ?????? ???????????? ?? ?????????.
- ??????? **Сохранить**.





??????? ?????? ???????????? ? ????? ??????? ??????? ? ???????????? ? ???????

Пользователи.



?????? ??????-??????? «???????? ???????????????? ????»: https://support.kaspersky.ru/kuma/4.2/315754

Импорт ресурсов в KUMA

Ресурсы – ??? ?????????? KUMA, ??????? ???????? ????????? ??? ?????????? ????????? ???????: ????????, ???????????? ?????????? ? ?????????? ??????? (**коннекторы**) ??? ??????? ??? ?????????? ??????????? ??????? ? ???????, ????????????????? ? KUMA (**нормализаторы**) ? ?.?. ?? ???? ???????????, ??? ?? ?????? ????????????, ?????????? ?????? ???????? ??? ????????, ?? ?????? ??????? ? ???? ??????? ????????? ??????? KUMA.

?????? ??????-??????? «??????? KUMA»: https://support.kaspersky.ru/kuma/4.0/217687

KUMA ???????????? ? ??????? ???????????????? ????????, ?? ????? ?????????? ?? ???????? `[00TB]<????????_???????>`.

????????????? ??????? ??? ?????????? ???????????? ???????? ????? ????????????:

- ?? ??????????:
  - ???????? ? ???????? ?????????? ?????????? ??????????.
  - ? ??????? ???????????????? ????????? ??????????.
- ?? ?????.

???? ????????? ??????? ????????? ??????? ???????? ?? ?????????? ?????????? ?????????? ? ?? ?????.

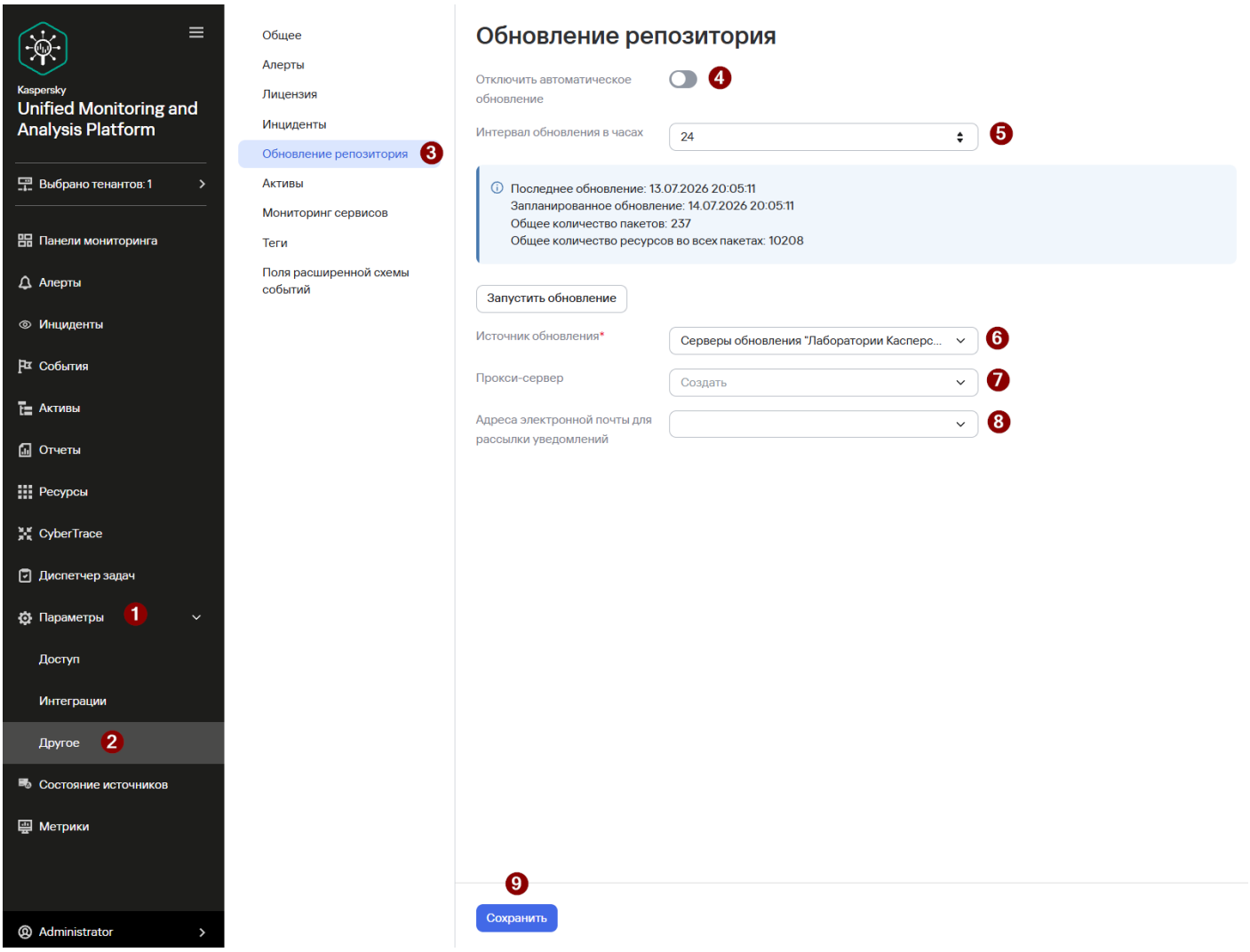
Импорт ресурсов из репозитория (серверы обновлений Лаборатории Касперского)

> ????????????? ????????? ?????? ?? ?????????? ?????????? ?????? ? ????????? URL (??? ????????????? ?????????? ???????? SSL/TLS-???????): https://support.kaspersky.ru/common/start/6105

????? ????????? ????????????? ?????? ???????? ?? ??????????, ????????? ??????? ?????????? ?????????? ??????????:

- ????????? ? ?????? **Параметры** ? **Другое** ? **Обновление репозитория**.
- ?????????, ??? ?????? **Отключить автоматическое обновление** ????.
- ??????? **Интервал обновления в часах**.
- ? ???? **Источник обновления** ???????? **Серверы обновления “Лаборатории Касперского”**.
- ??? ????????????? ? ???? **Прокси-сервер** ???????? ?? ?????? ???????????? ??????-??????, ??????? ?????? ????????????? ??? ??????? ?????? **Обновление репозитория**. ???? ??????-?????? ??? ?? ???????????? ? ???? **Прокси-сервер** ??????? ?? **Создать** ? ????????? ????????? ??????? ??????-??????? ???????? ??????.
- ?????????? ??????? ?????? ?????????? ????? ??? ???????? ??????????, ????? **Добавить.** ????? ??????? ?????????? ?????? ?????????? ?????????? KUMA ????? ?????????? ?? ????????? ?????? ?????????? ? ????????? ??? ?????????? ???????.
- ??????? ?????? **Сохранить** ??? ?????????? ?????????.

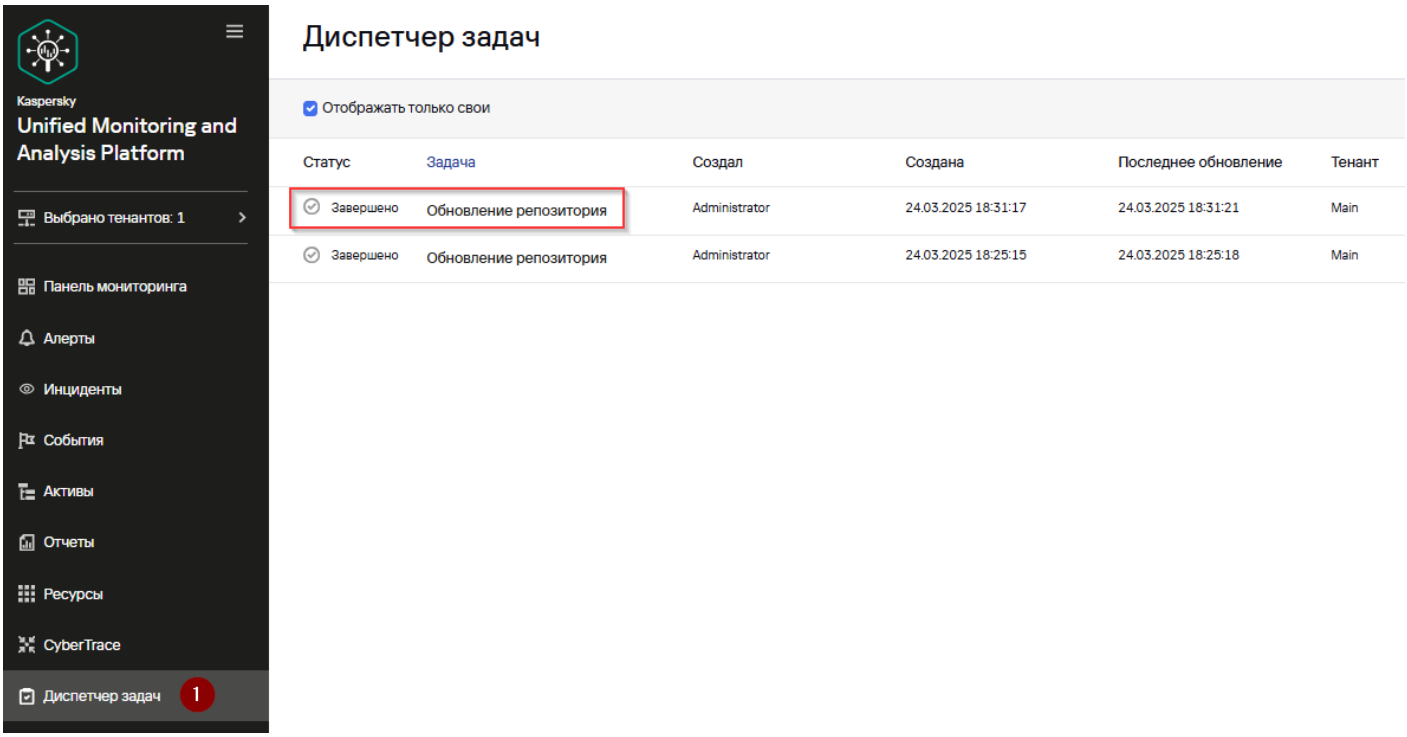
????????????? ?????? ???????? ?? ?????????? ?????????? ?????????? ????????.



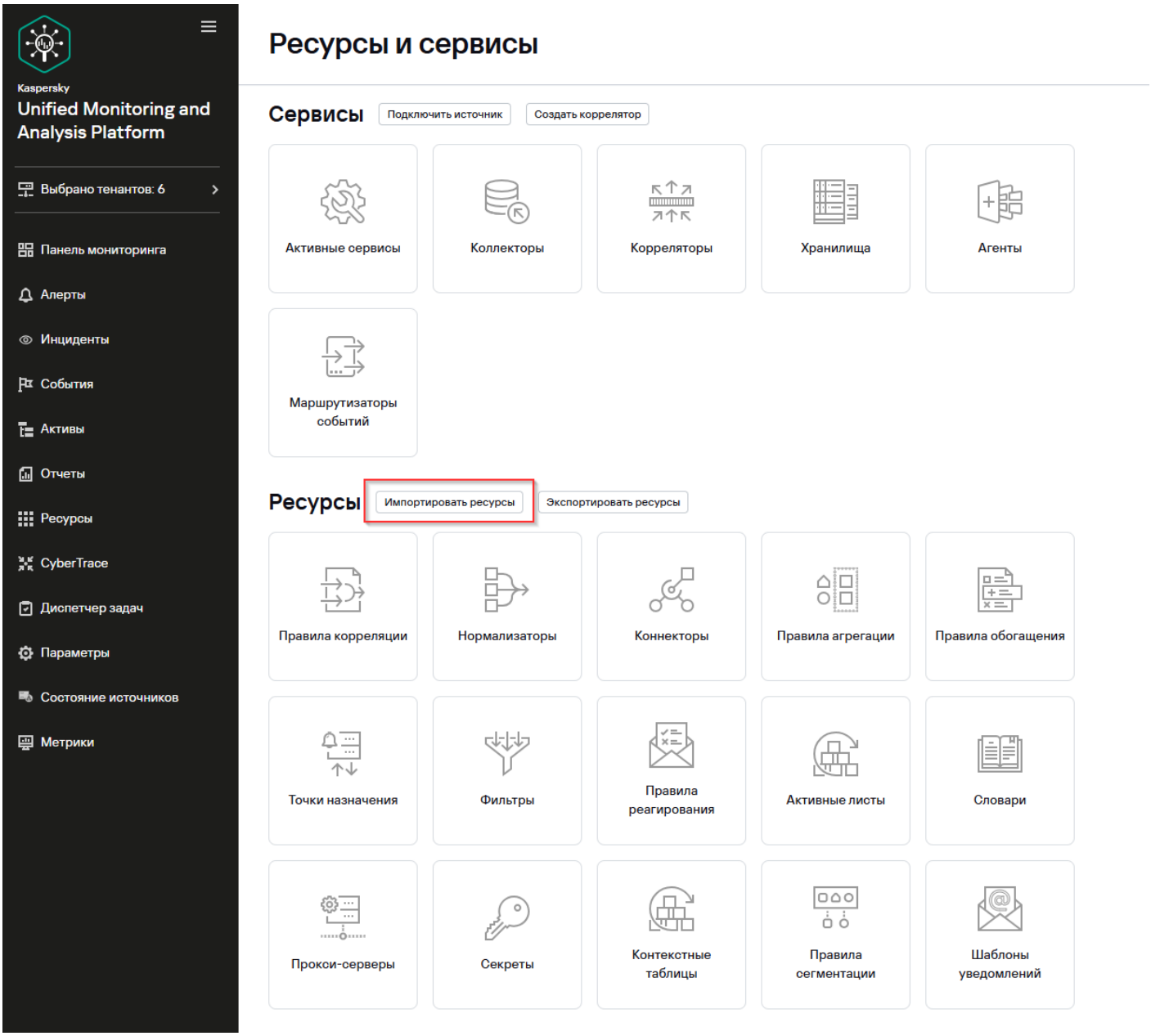
????? ????????? ?????????? ??????????? ???????. ??? ?????:

- ??????? **Запустить обновление**.
- ????????? ? ?????? **Диспетчер задач** ? ?????????, ??? ?????? ??????

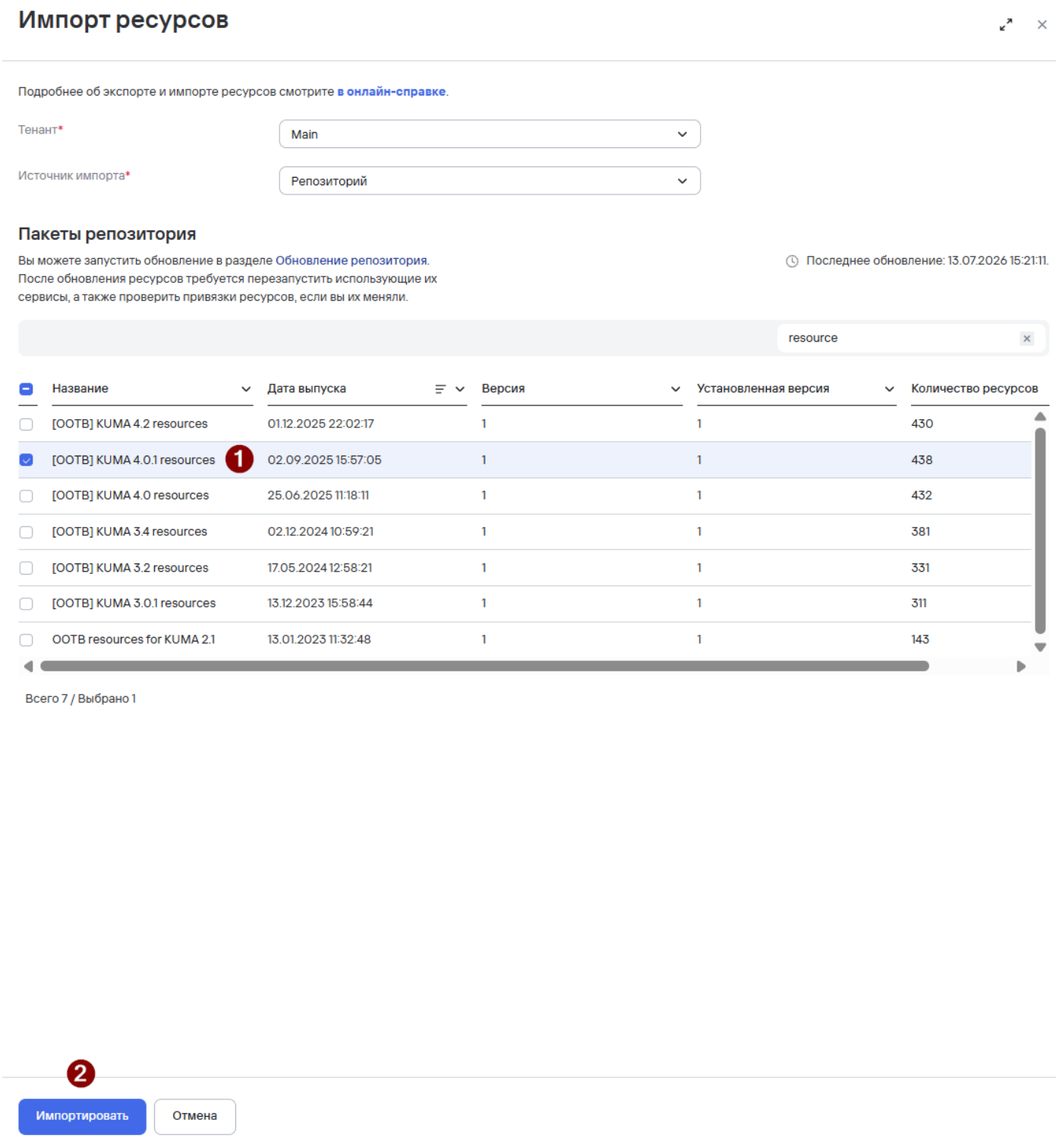
  Обновление репозитория ? ????????? **Завершено**.



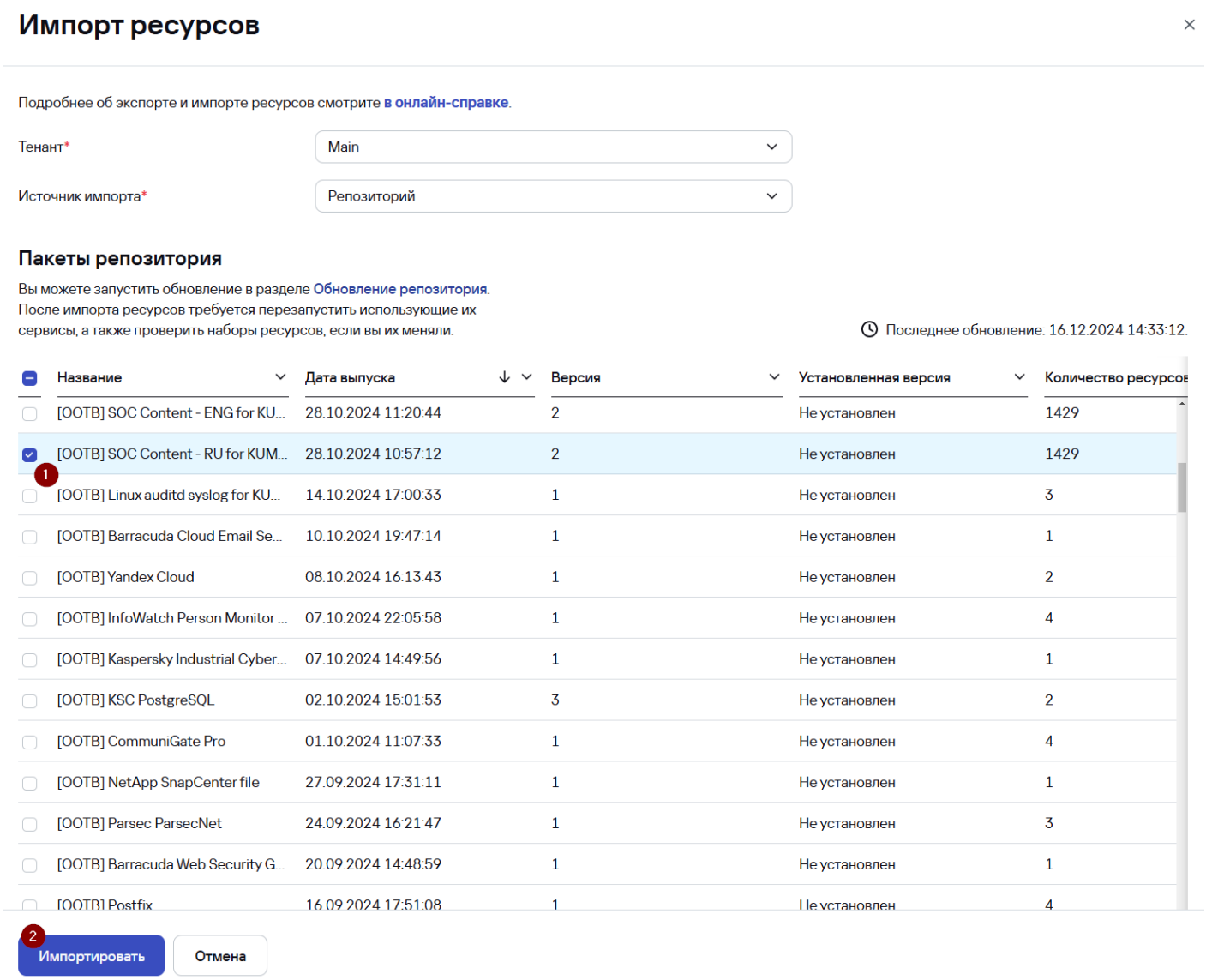
- ????????? ? ?????? **Ресурсы** ? ??????? **Импортировать ресурсы**.



- ? ??????????? ???? **Импорт ресурсов** ??????? **Тенант** (?? ????????, Main) ? ???????? **Источник импорта** – **Репозиторий**. .
- ? ?????? **Пакеты репозитория** ???????? ?????? ????????? ??????? ???????? ??? ????????.
- ??????? ? ???????? ????? **[OOTB] KUMA 4.0.1 resources** (??? ?????? KUMA 4.0) ??? **[OOTB] KUMA 4.2 resources** (??? ?????? KUMA 4.2).
- ??????? **Импортировать**. ?????? ?????? ???????? ??????? ??? KUMA 4.0 ??? 4.2 (?????????????, ??????????, ??????? ? ?.?.). ????????? ????????? ??????????? ??????????? **Ресурсы из пакета [OOTB] KUMA <версия> resources успешно импортированы**.



- ????????? ????????? ? ????????? ?????? ?????? **[OOTB] SOC Content - RU for KUMA 3.2** (??? ?????? KUMA 3.2+). ?????? ????? ???????? ????? ????????, ??????????????? ??? ????????? ??????????????? ????????? ? ???????????? ? ????????? ????????? ??????? MITRE ATT&CK.



?????? ??????? ? OOTB-????????? ??????? ????????. ??????????? ????? ????????????? ?????? ?????? ?? ??????????? ? ?????? ?????????????.

?????? ??????-??????? «??????????? ????????»: https://support.kaspersky.ru/kuma/4.0/242817

Импорт ресурсов из файла

???? ? ??????? KUMA ??????????? ?????? ? ???????? (??????? ???????????? ? ???????? ???????) ??? ?????????? ????????? ??????? ???????? ?? ?????? ??????????? KUMA ??????? ????? ????? ????????????? ?? ??????.

?????? KUMA, ? ??????? ????????????? ?????? ????????, ?????? ???? ????????? ??? ???? ?????? KUMA, ?? ??????? ??????? ???? ?????????????

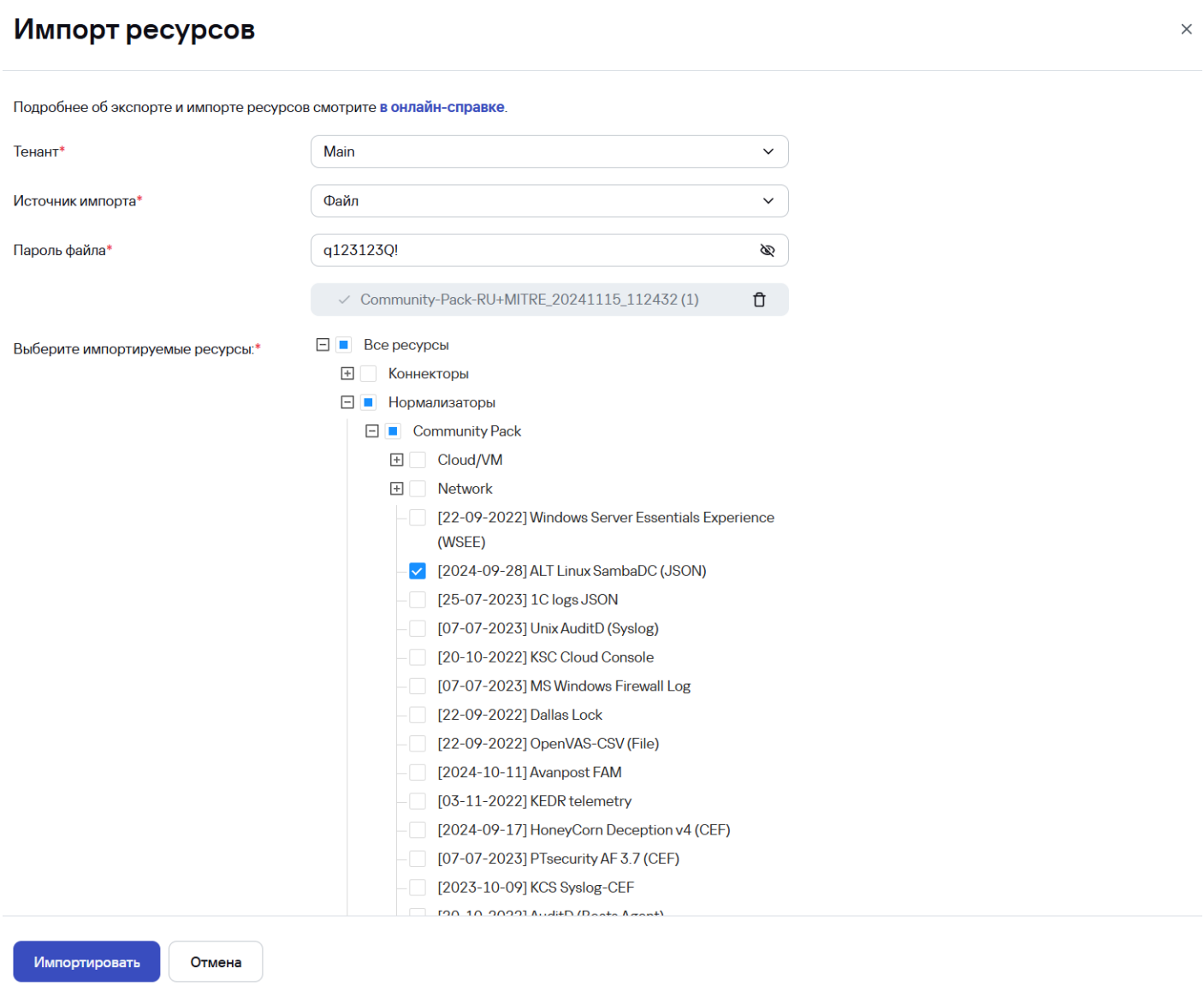
??? ???????? ???????? ?? ????? ??????? ?????? KUMA ? ????? ?????? ????? ???????????? ?????? ?? ??????????? KUMA Community

???? ?????????????? ?????? ??????? ???????? Community Pack (????? ???????? ?? ?????????? KUMA) ?? ?????. ??? ???????, ??? ??????????? ??????? ???????? ? ???????????, ?? ? ???????? ?????????????? ????????? ????? ??????????? ??????? ?????????? KUMA.

??????? ?????????? KUMA:
https://box.kaspersky.com/d/f630e3ab02b64405881a/?p=%2F&mode=list
https://github.com/KUMA-Community/kuma_content

????? ????????????? ??????? ?? ????? ?? ??????? Community Pack:

- ????????? **пакет ресурсов нормализаторов** Community-Pack-RU+MITRE_<????>_<?????>?? ?????? ??? **пакет ресурсов правил корреляции** Community-Pack-RU+MITRE_<????>_<?????>?? ??????.
- ? ???-?????????? KUMA ????????? ? **Ресурсы** ? ???????? **Импортировать ресурсы**.
- ? ??????????? ???? ??????? ???????? ???????? **Тенант** (?? ????????? Main), ? ???????? **Источника импорта** ??????? **Файл** ? ??????? ?????? (?????? ?? ???????? ?????????? `q123123Q!q123123Q!` ??? `q123123Q!KLaapt-M4`), ????? ???? ???????? ????? ??????????? ????. ?????? ?? ????? ? ????????? ?????????? ??????? ?? ???????? ?????? ?????.
- ????? ??????? ????? ????????? ?????? ???????? ? ???????? ??????????? ??????? ??? ??????? (????????????? ????????????? ?????? ????????????? ??????????? ??? ?????? ???????), ????? ???? ??????? ?????? **Импортировать**.



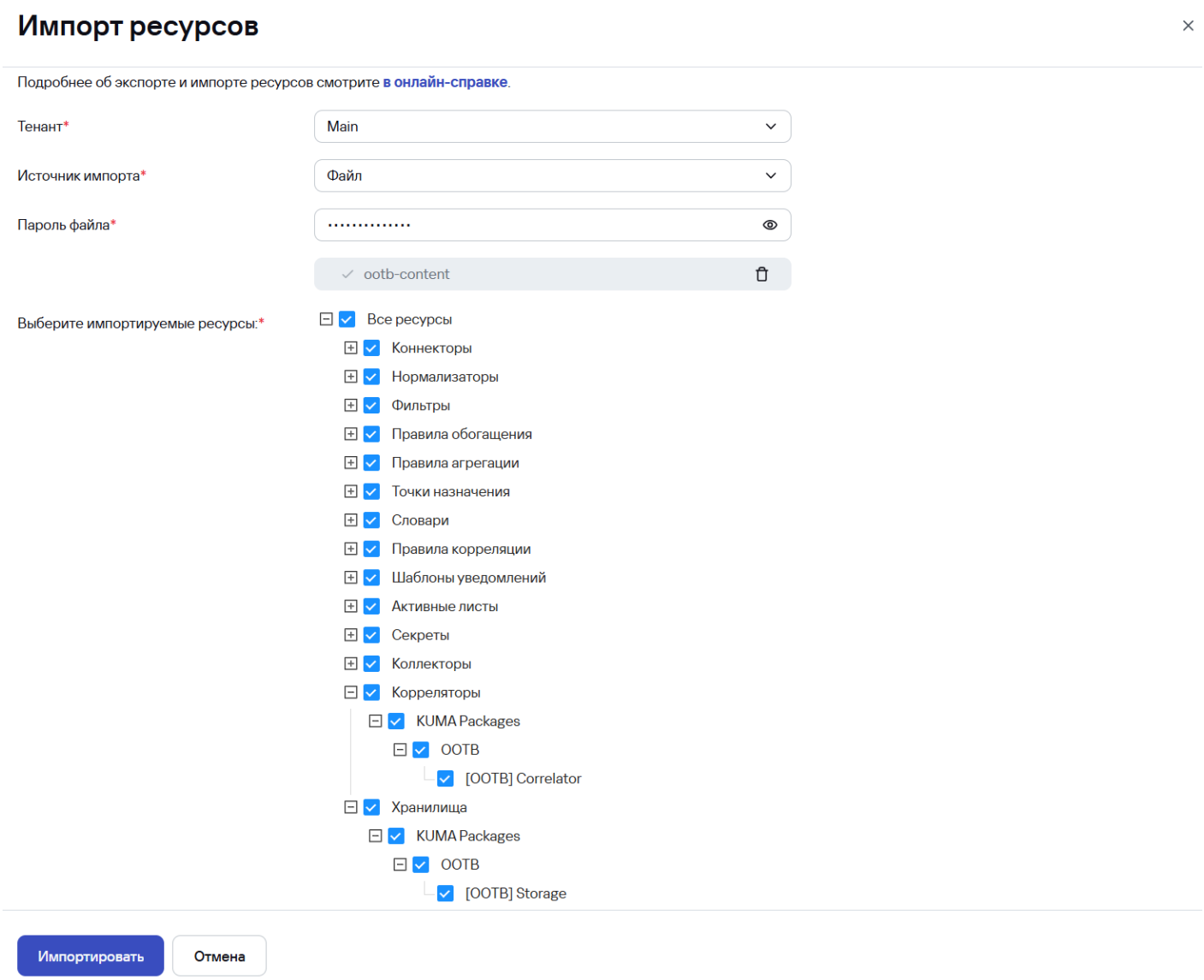
- ????????? ????????? ???????????? ??????????? **Ресурсы успешно импортированы**.

?????? ??????? ????????????.

????? ????????????? ????? ???????? ?? ????? ootb-content ("?????????? ???????", ???????????? ?????? ? ????????????? KUMA):

- ? ???-?????????? KUMA ????????? ? **Ресурсы** ? ???????? **Импортировать ресурсы**.
- ? ??????????? ???? ??????? ???????? ???????? **Тенант** (?? ????????? Main), ? ???????? **Источника импорта** ??????? **Файл** ? ??????? ?????? `mustB3Ch@ng3d!`, ????? ???? ???????? ???? ootb-content. ?????? ?? ????? ? ????????? ?????????? ??????? ?? ???????? ?????? ?????.

- ????? ??????? ????? ???????? ??? ??????? ? ??????? ?????? **Импортировать**.



? ?????????? ????? ????????? ????????? ???? OOTB-????????, ? ??? ????? ??????? ????????, ?????????? ??????? ????? ???????? ?????? ???????? ? ????????? ????????.

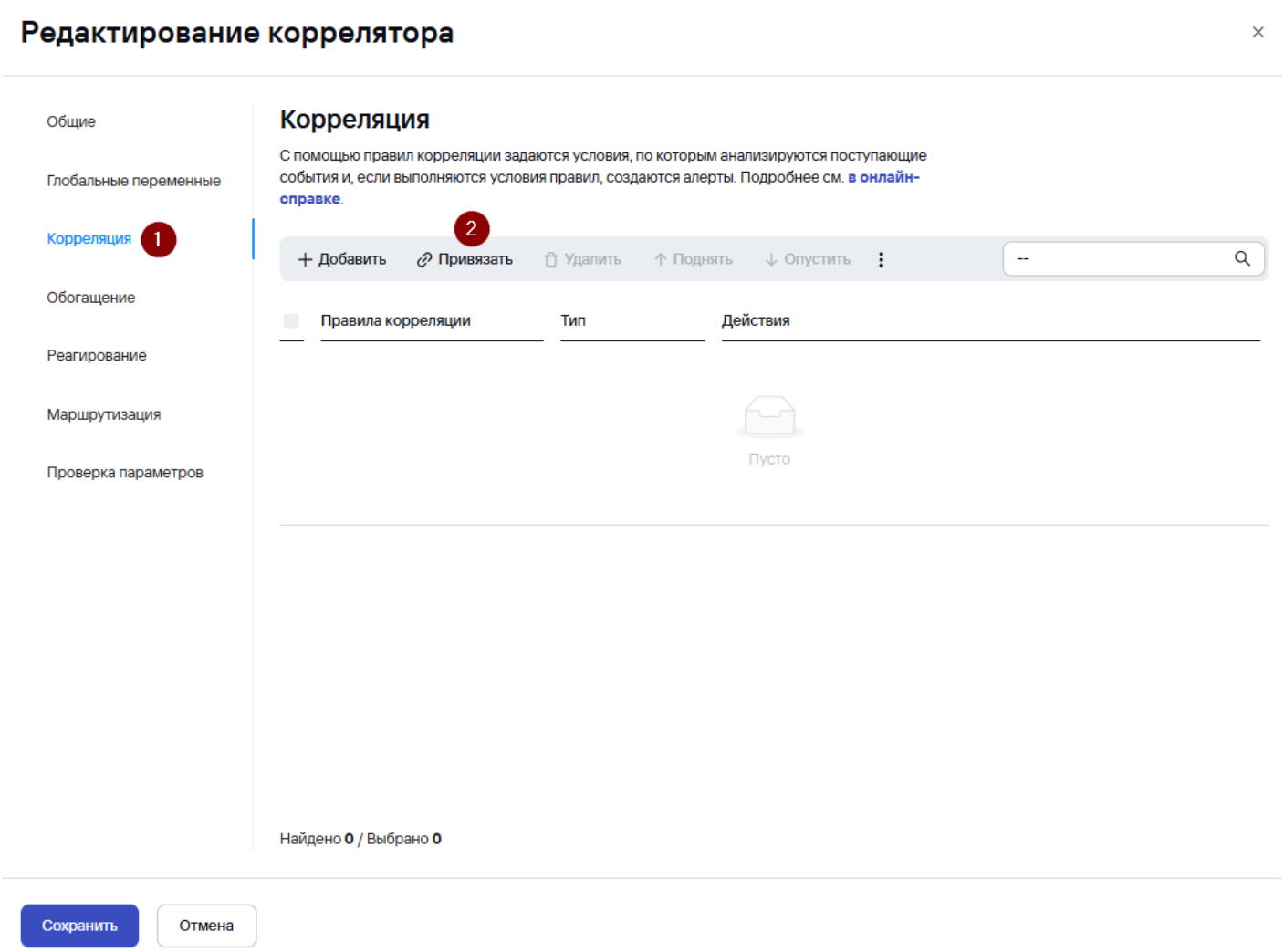
Привязка правил корреляции

????? ??????? ?????? ???????? **[OOTB] SOC Content - RU for KUMA 3.2** (??? ?????? KUMA 3.2+) ? ????????? ?????????? ?????????? ????????? ?????? ??????? ?????????? ? ???????????.

????? ????????? ??????? ?????????? ? ???????????:

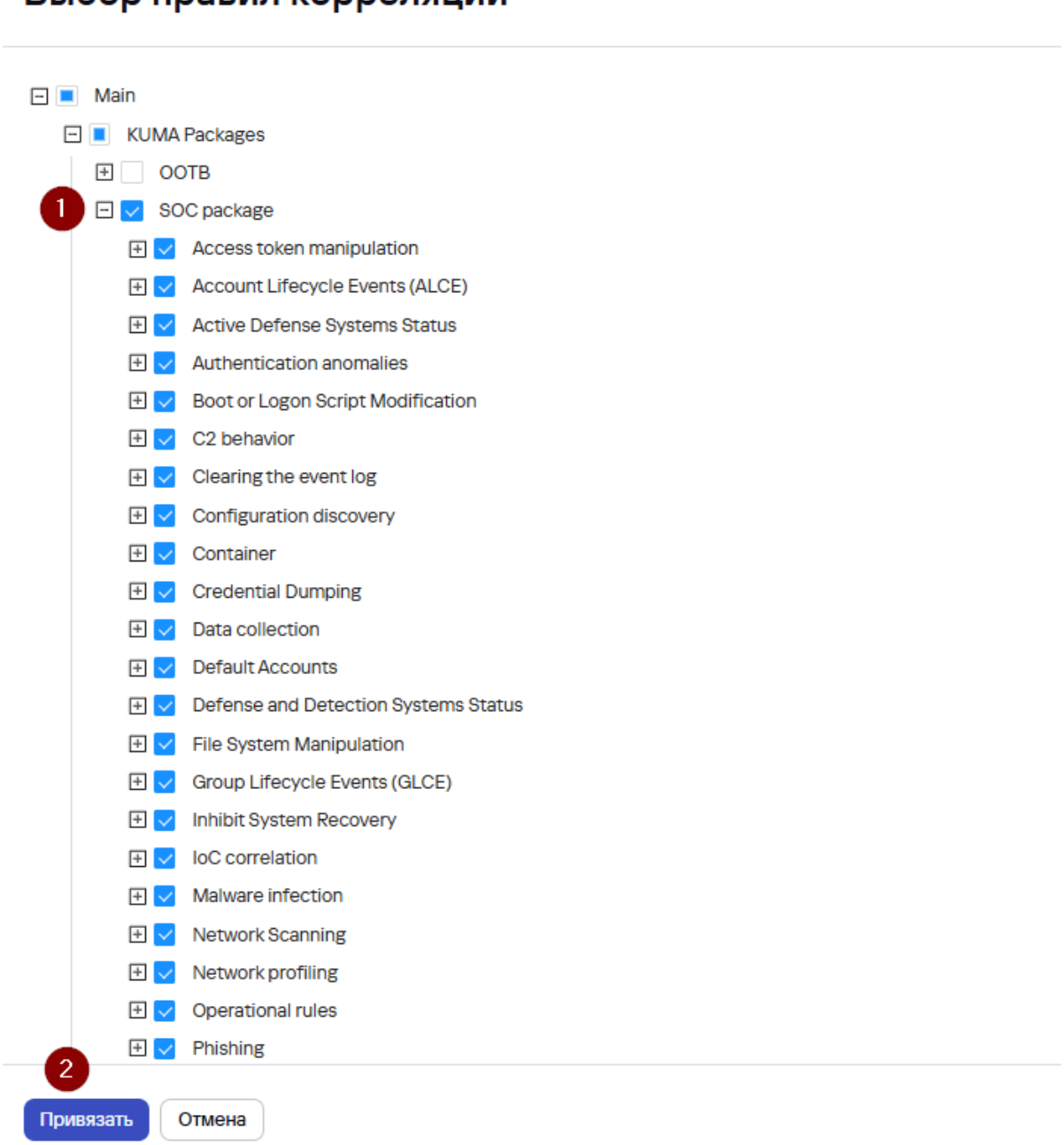
1. ????????? ? **Ресурсы** ? **Активные сервисы**.
2. ??????? ?? ???????? ??????? **Коррелятора**.
3. ? ??????????? ???? **Редактирование коррелятора** ????????? ?? ??? **Корреляция** ?

??????? **Привязать**.



4. ? ???? **Выбор правил корреляции** ???????? ????????? ?????? ?????????? ??? ???????????? ??????? ?????????? SOC Package ? ??????? **Привязать**.

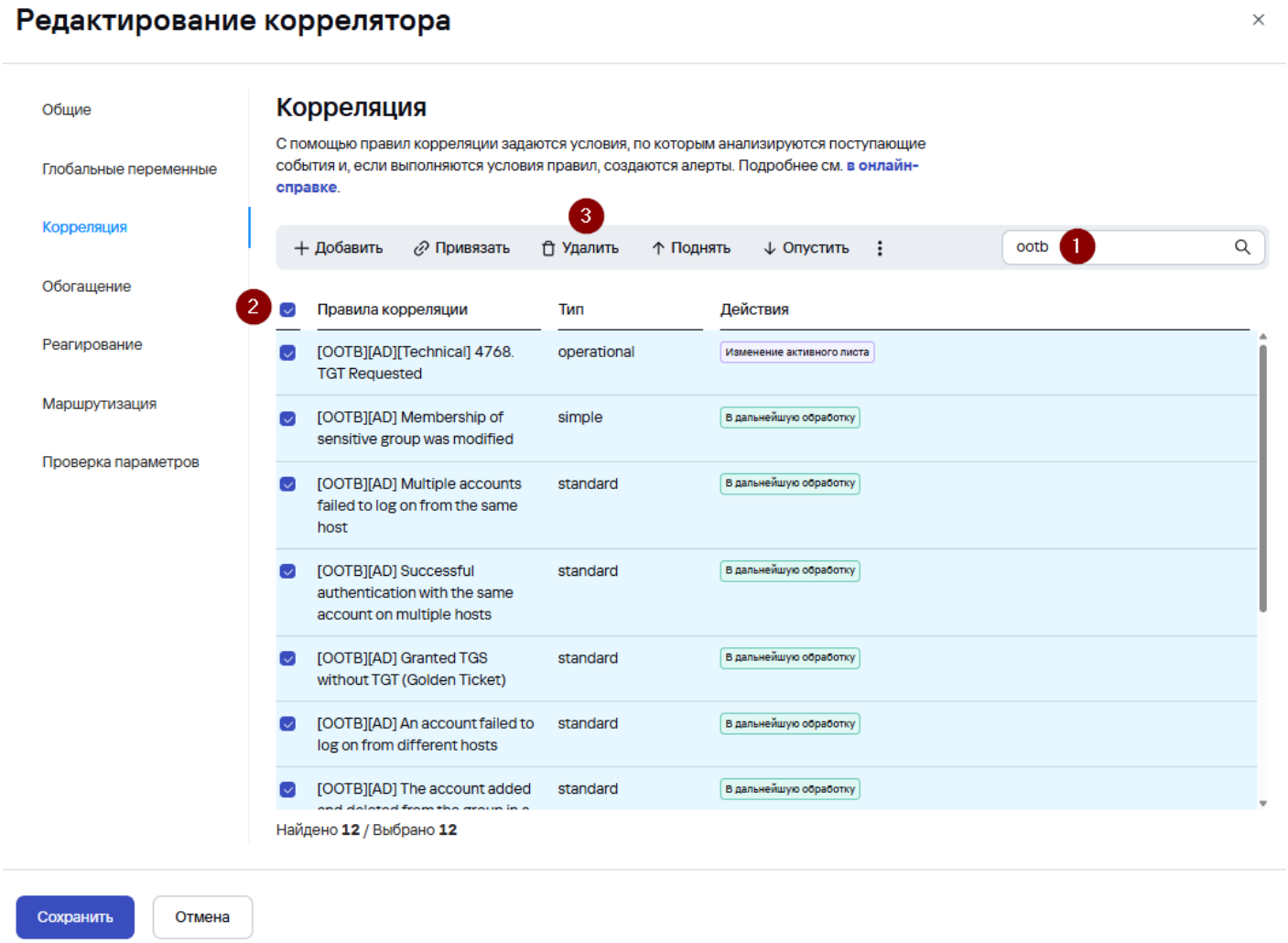
> ?????? ??????? ?????????? ???????????? ??? ??????? ??????? ???????????? ?????????, ??????? ????????????? ????????? ????? ????????? ??????? ?????????? ? KUMA ? ?????????? ?????? ?? ??????? ??????????, ??????? ???????????? ??? ???? ??????????. ?????????? ??? ??????? ?????? ????????? ???????????? ??????? ?????????? ????? ? ????????? «???????? ?????? ??????????, ???????????? ? SOC_package.xlsx»: https://support.kaspersky.ru/kuma/4.0/250594



5. ????????? ??????? ?????????? ????????? ? ???????????.

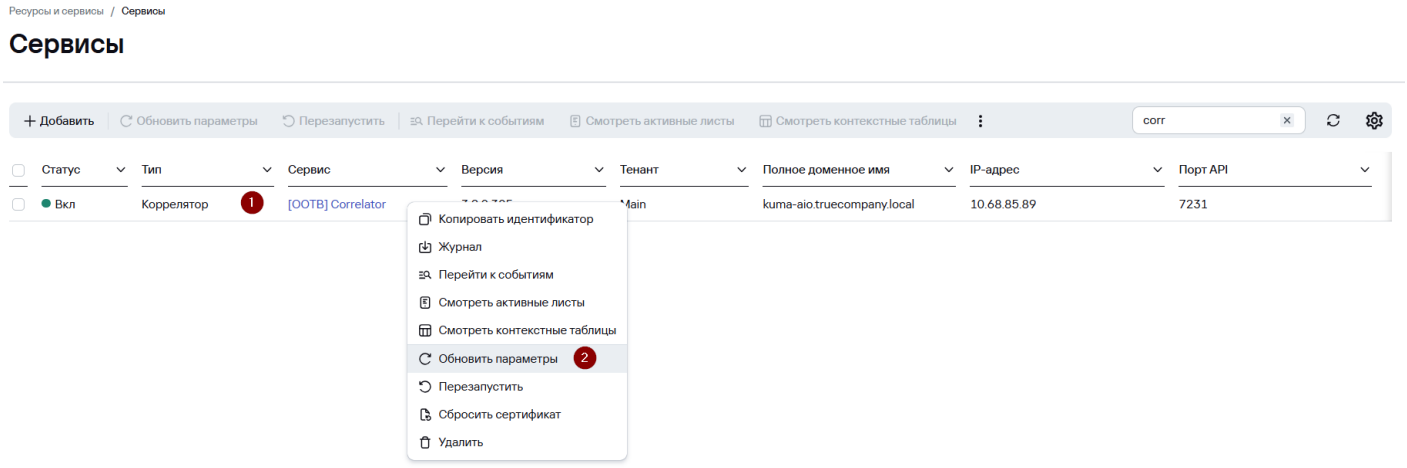
> ????????????? ??????? ???????????????? ????????????? ??????? ? ????????? [OOTB]. ?????? ??????? ???????? ????????? ??? ???????? ?????????? ?????? ??????????. ??? ???????? ?????? ? ????????? [OOTB] ??????? «ootb» ? ???? ??????, ???????? ??? ??????? ? ??????? **Удалить**.

6. ??????? **Сохранить**.



????? ?????????? ???????? ????????? ???????????? ?????????? ???????? ????????? ???????:

- ????????? ? **Ресурсы** ? **Активные сервисы**.
- ??????? ??? ?? ?????? **Коррелятора** ? ???????? **Обновить параметры**.



????? «????????????? OOTB (Out-Of-The-Box) ??????»: https://rutube.ru/video/ff4e4e2890023379682874042952 3e1f/?playlist=891489

Настройка параметров наполнения алертов

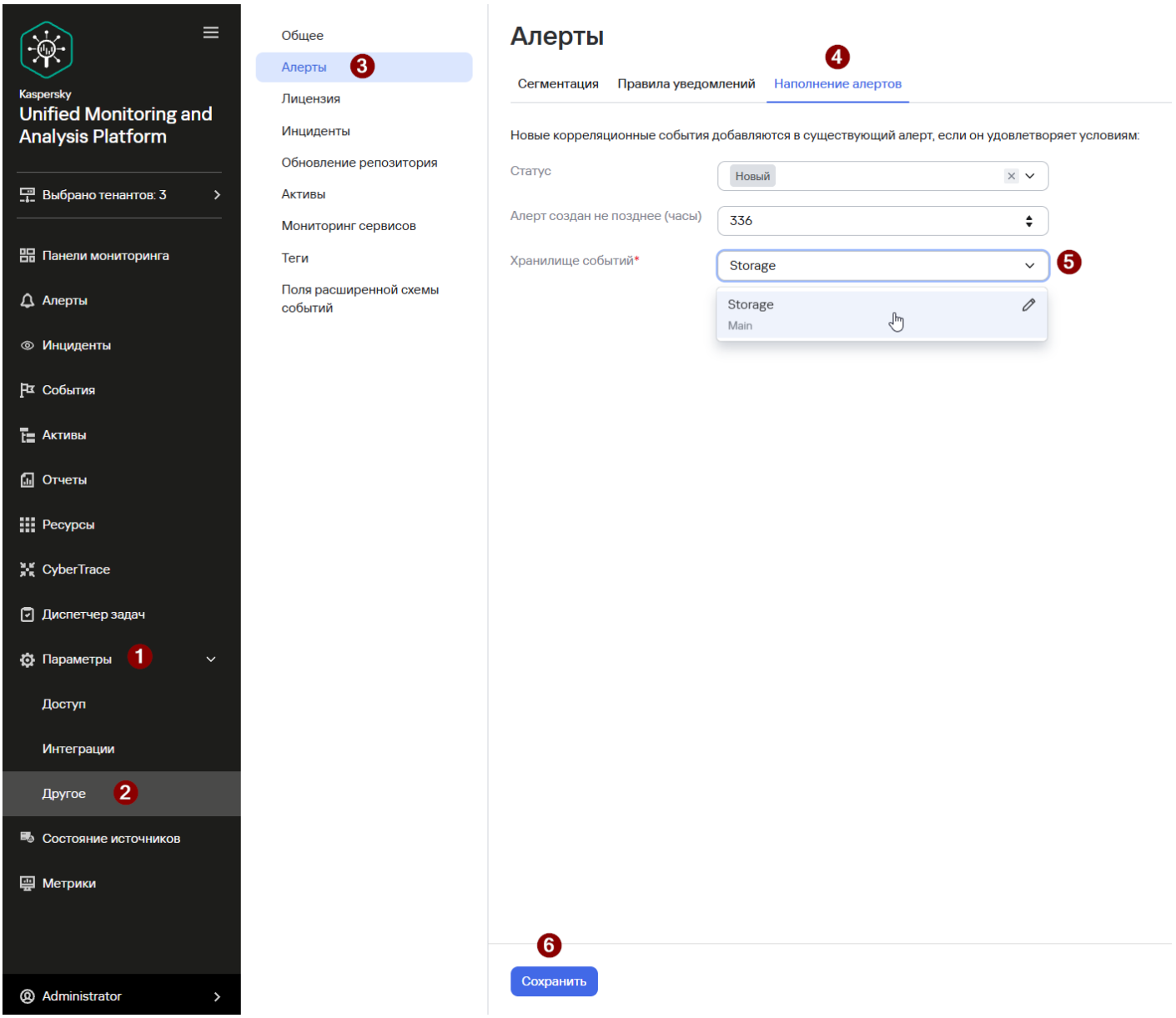
??????? ? ?????? 4.0 ??????? ??????? KUMA ???????? ? ClickHouse ?????? MongoDB, ??????? ????? ????????? KUMA ??? ?????????? ? ?????????? ??????, ?????????? ????????? ????????? ?????????? ?????????? ??????? ? ??????? ????????? ??? ??????? ???????.

??? ???????? ????????? ????? ?????? ????? ?????????? ??? ???????.

????? ????????? ????????? ?????????? ???????:

- ? ???-?????????? KUMA ????????? ? ?????? **Параметры** ? **Другое** ? **Алерты**.
- ? ?????????? ???? **Алерты** ????????? ?? ??????? **Наполнение алертов** ? ??????? ???????? ????????? ??????????:
  - ? ????????????? ?????? **Статус** ???????? ????????, ??? ??????? ????? ????? ?????????? ?????????. ????????????? ???????? ?? ?????????: **Новый**.
- ? ???? **Алерт создан не позднее (часы)** ??????? ?????, ? ??????? ???????? ????? ????? ?????????? ?????????. ???????? ????????? ?????? ???? ????? ??????. ?????? ??????? ????????????? ?? ??????? ???????? ??????. ???????? ?? ?????????: 336 ????? (2 ??????). ?????????? ????????: 1 ???.
- ? ????????????? ?????? **Хранилище событий** ???????? ?????????, ? ??????? ????? ???????? ??????? ??????. ????? ??????? ?????? ???? ?????????. ? ?????? ??????????? ??????? ?????????, ? ?? ?????????? ???????. ??? ???? ????? ?????? ?????????? ?????????, ?????? ????????? ?????? ???? ???????.

????????? ?????????? ??????? ?????????.



?????? ??????-??????? «????????? ?????????? ?????????? ???????»:
https://support.kaspersky.ru/kuma/4.0/304498

Revision #6
Created 2026-07-13 15:33:22 UTC by Dmitry Borisov
Updated 2026-08-18 15:07:59 UTC by Dmitry Borisov