

Базовая настройка

Проверка сервисов

После входа в веб-интерфейс KUMA проверьте наличие и статус демонстрационных сервисов:

- Перейдите в раздел **Ресурсы** → **Активные сервисы**
- Убедитесь в наличии сервисов с префиксом `[OOTB]` и что данные сервисы находятся в статусе «Вкл».

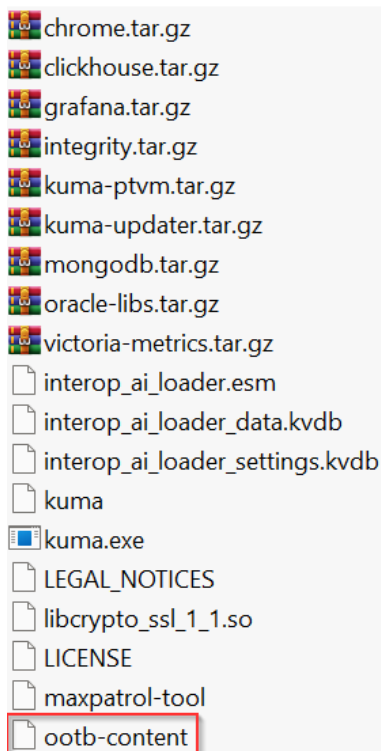
Ресурсы и сервисы / Сервисы

Сервисы

+ Добавить	Обновить параметры	Перезапустить	Перейти к событиям	Смотреть активные листы	Смотреть контекстные таблицы	Смотреть разделы	Журнал	Скачать дамп	Поиск	↺	⚙
☐	Статус	Тип	Сервис	Тенант	Полное доменное имя	IP-адрес	Порт API	Время работы	Создан		
☐	Вкл	Коллектор	[OOTB] KSC	Main	kuma-ansible-installer.kuma	10.10.10.10	7233	14 дня 2 часа 20 минуты	04.12.2024 14:32:05		
☐	Вкл	Коллектор	[OOTB] Syslog	Main	kuma-ansible-installer.kuma	10.10.10.10	7234	14 дня 2 часа 19 минуты 53 ...	04.12.2024 14:32:11		
☐	Вкл	Коллектор	[OOTB] Syslog-CEF	Main	kuma-ansible-installer.kuma	10.10.10.10	7235	14 дня 2 часа 19 минуты 45 ...	04.12.2024 14:32:17		
☐	Вкл	Ядро	core-1	Main	kuma-ansible-installer.kuma	10.10.10.10	7210	14 дня 2 часа 21 минуты 41 ...	04.12.2024 14:30:27		
☐	Вкл	Коррелятор	[OOTB] Correlator	Main	kuma-ansible-installer.kuma	10.10.10.10	7231	14 дня 2 часа 20 минуты 15 ...	04.12.2024 14:31:48		
☐	Вкл	Хранилище	[OOTB] Storage	Main	kuma-ansible-installer.kuma	10.10.10.10	7230	14 дня 2 часа 20 минуты 16 ...	04.12.2024 14:31:44		

При наличии демонстрационных сервисов, как на скриншоте выше, можно перейти к следующим шагам базовой настройки.

В случае если демонстрационные сервисы (Хранилище, Коррелятор и Коллекторы) не были установлены можно импортировать набор ресурсов для создания сервисов из файла `ootb-content`, который доступен по пути `/kuma-ansible-installer/roles/kuma/files/`.



Для импорта набора ресурсов из файла см. Раздел **Импорт ресурсов из файла**.

Также можно создать ресурсы сервисов вручную (см. статью [Создание и установка сервисов](#)).

Создание пользователей

По умолчанию в KUMA преднастроена одна учетная запись **admin** с ролью главного администратора с максимальным набором привилегий.

Настоятельно рекомендуется изменить пароль для учетной записи **admin** после первого входа. Для этого:

- Перейдите в раздел **Параметры** → **Доступ** → **Пользователи**.
- Нажмите на пользователя **admin**.
- В появившемся окне **Пользователь** нажмите **Изменить пароль**.
- В окне **Изменить пароль** укажите действующий пароль и введите новый пароль.
- Нажмите **ОК**.
- Далее нажмите **Сохранить**.

Корпоративный Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панели мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

CyberGate

Диспетчер задач

Параметры

Доступ

Интеграции

Другое

Состояние источников

Метрики

Administrator

Пользователи

Тенанты

Доменная аутентификация

Настройки политики безопасности

Доступ к пространствам

Пользователи

Активные пользователи

Неактивные пользователи

Создать

Выключить

Сбросить пароль при следующем входе в систему

Поиск...

Ва

Имя	Логин	Адрес электронной почты	Роль	Тенант
Administrator	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

Доступ

Роль*

Главный администратор

Тенант*

MainResources ExportShared

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

Доступ к KUMA может иметь несколько пользователей. Пользователям присваиваются роли пользователей, которые влияют то, какие разделы интерфейса будут доступны пользователям и какие функции они смогут выполнять.

Чтобы создать учетную запись пользователя:

- Перейдите в раздел **Параметры** → **Доступ** → **Пользователи**.
- 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

- **Часовой пояс** - выберите часовой пояс, в котором будут отображаться временные метки при работе в KUMA. Список формируется на основе параметров операционной системы пользователя и учитывает переход на летнее и зимнее время. По умолчанию используется часовой пояс браузера пользователя.
- **Использовать формат ISO 8601** - установите этот флажок, чтобы временные метки отображались в формате ISO 8601 (например, 2026-02-08T17:35:27+03:00). Формат применяется в тех разделах веб-интерфейса KUMA, где используется сокращенное или полное отображение даты и времени, и действует во всей системе KUMA. Настроенный формат сохраняется в параметрах Ядра KUMA.
- **Получать уведомления по почте** - установите этот флажок, чтобы пользователь получал почтовые уведомления от KUMA.
- **Уведомлять об алертах в WEB интерфейсе** - установите этот флажок, чтобы в веб-интерфейсе KUMA отображались уведомления об алертах. Снимите флажок, если хотите выключить отображение уведомлений. По умолчанию флажок установлен.
- **Отображать непечатаемые символы (Ctrl/Command + *)** - установите этот флажок, чтобы в веб-интерфейсе KUMA отображались непечатаемые символы: пробелы, знаки табуляции, перенос на новую строку. Если флажок **Отображать непечатаемые символы** установлен, отображение непечатаемых символов можно включать и выключать с помощью клавиш **Ctrl/Command+***.
- **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** - установите этот флажок, чтобы при следующей попытке входа в веб-интерфейс KUMA пользователь указал старый пароль и задал новый пароль. После этого пользователю будет разрешен вход в веб-интерфейс KUMA с новым паролем. По умолчанию этот флажок установлен.

Например, вы можете использовать этот параметр при создании нового пользователя. Пользователю можно назначить временный пароль и установить этот флажок. После входа с временным паролем KUMA предложит пользователю сменить пароль.

- **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. Обычно учетная запись с неограниченным временем жизни пароля используется для мониторинга.

- **Роль** – выберите роли пользователя.
- **Тенант** - выберите тенант, к которому будет принадлежать пользователь. Пользователю можно назначить разные роли в разных тенантах, в одном тенанте можно назначить несколько ролей.

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*

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

Доступ

Роль*

Аудитор 1

Тенант*

Main x 2

Добавить роль

Наборы пространств ⓘ

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

3

Добавить

Отмена

Учетная запись пользователя создана и отображается в таблице **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*

.....

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 x **9**

Добавить роль

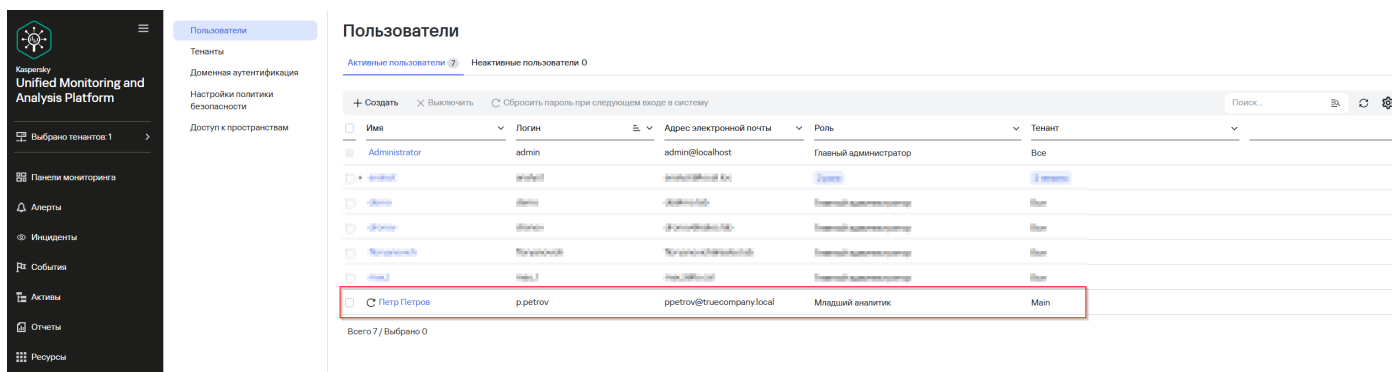
Наборы пространств ⓘ

All spaces **10**

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

Добавить

Отмена



Статья онлайн-справки «Управление пользователями»:

<https://support.kaspersky.ru/kuma/4.0/217937>

Статья онлайн-справки «Аутентификация с помощью доменных учетных записей»:

<https://support.kaspersky.ru/kuma/4.0/221427>

Видео по настройке «Аутентификации с помощью доменных учетных записей Active Directory»:

<https://rutube.ru/video/8cabd9b4a160f875fa2ef1abbd286e5d/>

[4.2+] Создание пользовательской роли

Начиная с версии 4.2 в дополнение к предустановленным ролям, в KUMA появилась возможность создавать пользовательские роли. Для пользовательских ролей можно формировать уникальные наборы прав и разрешений с указанием необходимых пользователю функциональных областей. Пример функциональной области – раздел Алерты.

Статья онлайн-справки «Функциональные области и доступные им уровни полномочий»:

<https://support.kaspersky.ru/kuma/4.2/316073>

Например, чтобы создать пользовательскую роль «Аудитор» (роль будет иметь доступ ко всем функциональным областям только для чтения):

- Перейдите в раздел **Параметры → Доступ → Роли**.
- Нажмите **Создать**.
- В появившемся окне **Создать** роль задайте параметры новой роли:
 - **Название** – введите имя роли (в нашем примере «Аудитор»).
 - **Описание** – опционально добавьте описание роли.

- В секции **Список разрешений** выберите все функциональные области и нажмите **Чтение**.

В списке доступных для выбора функциональных областей приводятся отдельные функциональные области и группы функциональных областей. Например, группа ksc включает в себя следующие функциональные области: Общее (просмотр статуса задач KSC) и Обновления (чтение обновлений KSC). Вы можете выбрать группу функциональных областей полностью или указать отдельные функциональные области в составе группы.

Для выбранных функциональных областей нужно указать уровень полномочий. В KUMA доступны следующие уровни полномочий:

- **Управление (англ. Manage)** – полные права на работу в функциональной области (чтение, создание, редактирование, удаление).
- **Управление созданными (англ. Manage created)** – полные права на тип в функциональной области (чтение и дублирование всех объектов, редактирование и удаление своих объектов) в отношении созданных пользователем объектов.
- **Чтение (англ. Read)** – права на чтение.
- **Нет прав (англ. No rights)** – отсутствие прав на работу с объектами.
- Нажмите **Создать**.

Создать роль



Название*

1 Аудитор

Описание

2 Роль имеет доступ ко всем функциональным областям только для чтения

Список разрешений

Показать функциональные области

Нет прав Чтение Управление созданными Управление

3	4	Нет прав	Чтение	Управление созданными	Управление	Раскрыть все группы	Поиск...	
	Функциональная область	Разрешение ⓘ				Описание		
✓	Инциденты							
✓	Алерты	Нет прав	Чтение	Управление созданными	Управление	Работа с алертами		
✓	Доступ к параметрам прав доступа на REST API	Нет прав	Чтение	Управление созданными	Управление	Работа с параметрами списка доступных конечны...		
✓	Управление доступом к REST API	Нет прав	Чтение	Управление созданными	Управление	Работа с созданием токена доступа к REST API, из...		
✓	Роли							
✓	Пользователи							
✓	Реестр тенантов	Нет прав	Чтение	Управление созданными	Управление	Работа со списком тенантов		
✓	Наборы пространств событий							
✓	Создание исключений для правил корреляции							
✓	Сбор и анализ данных	Нет прав	Чтение	Управление созданными	Управление	Работа со сбором и анализом данных		
✓	Получение SMTP-уведомлений							

5

Создать

Отмена

Пользовательская роль Аудитор успешно создана.

Вы также можете создать пользовательскую роль, скопировав параметры уже существующей роли (в том числе предустановленной системной роли).

Чтобы назначить созданную пользовательскую роль учетной записи пользователя:

- Перейдите в раздел **Параметры → Доступ → Пользователи**.
- Создайте новую учетную запись пользователя или выберите уже существующую учетную запись (в данном примере будет создана новая учетная запись).
- 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

- **Часовой пояс** - выберите часовой пояс, в котором будут отображаться временные метки при работе в KUMA. Список формируется на основе параметров операционной системы пользователя и учитывает переход на летнее и зимнее время. По умолчанию используется часовой пояс браузера пользователя.
- **Использовать формат ISO 8601** – установите этот флажок, чтобы временные метки отображались в формате ISO 8601 (например, 2026-02-08T17:35:27+03:00). Формат применяется в тех разделах веб-интерфейса KUMA, где используется сокращенное или полное отображение даты и времени, и действует во всей системе KUMA. Настроенный формат сохраняется в параметрах Ядра KUMA.
- **Получать уведомления по почте** - установите этот флажок, чтобы пользователь получал почтовые уведомления от KUMA.
- **Уведомлять об алертах в WEB интерфейсе** - установите этот флажок, чтобы в веб-интерфейсе KUMA отображались уведомления об алертах. Снимите флажок, если хотите выключить отображение уведомлений. По умолчанию флажок установлен.
- **Отображать непечатаемые символы (Ctrl/Command + *)** - установите этот флажок, чтобы в веб-интерфейсе KUMA отображались непечатаемые символы: пробелы, знаки табуляции, перенос на новую строку. Если флажок **Отображать непечатаемые символы** установлен, отображение непечатаемых символов можно включать и выключать с помощью клавиш **Ctrl/Command+***.
- **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/4.2/302832>

- **Подтверждение пароля** – повторите пароль.
- **Пользователь должен сменить пароль при следующем входе в систему** - установите этот флажок, чтобы при следующей попытке входа в веб-интерфейс KUMA пользователь указал старый пароль и задал новый пароль. После этого пользователю будет разрешен вход в веб-интерфейс KUMA с новым паролем. По умолчанию этот флажок установлен.

Например, вы можете использовать этот параметр при создании нового пользователя. Пользователю можно назначить временный пароль и установить этот флажок. После входа с временным паролем KUMA предложит пользователю сменить пароль.

- **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. Обычно учетная запись с неограниченным временем жизни пароля используется для мониторинга.

- **Роль** – выберите роли пользователя.
- **Тенант** - выберите тенант, к которому будет принадлежать пользователь. Пользователю можно назначить разные роли в разных тенантах, в одном тенанте можно назначить несколько ролей.

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 **Сохранить**.

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

Доступ

Роль*

Аудитор 1

Тенант*

Main x 2

Добавить роль

Наборы пространств ⓘ

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

3

Добавить

Отмена

Учетная запись пользователя с ролью Аудитор создана и отображается в таблице **Пользователи**.

Пользователи	Пользователи
Роли	Активные пользователи ⓘ Неактивные пользователи ⓘ
Тенанты	
Доменная аутентификация	
Настройки политики безопасности	
Доступ к пространствам	

+ Создать ✕ Выключить ⚙ Сбросить пароль при следующем входе в систему

Ivanov x ↺ ⚙

☐	Имя	Логин	Адрес электронной почты	Роль	Тенант
☐	Иван Иванович	i.ivanov	test@abc.local	Аудитор	Main

Всего 1 / Выбрано 0

Статья онлайн-справки «Создание пользовательской роли»:
<https://support.kaspersky.ru/kuma/4.2/315754>

Импорт ресурсов в KUMA

Ресурсы – это компоненты KUMA, которые содержат параметры для реализации различных функций: например, установления соединений с источниками событий (**коннекторы**) или правила для приведения поступающих событий к формату, поддерживаемому в KUMA (**нормализаторы**) и т.д. Из этих компонентов, как из частей конструктора, собираются наборы ресурсов для сервисов, на основе которых в свою очередь создаются сервисы KUMA.

Статья онлайн-справки «Ресурсы KUMA»:
<https://support.kaspersky.ru/kuma/4.0/217687>

KUMA поставляется с набором предустановленных ресурсов, их можно определить по названию `[00ТВ]<название_ресурса>`.

Дополнительные ресурсы или обновления существующих ресурсов можно импортировать:

- из репозитория:
 - напрямую с серверов обновлений Лаборатории Касперского.
 - с помощью пользовательского источника обновлений.
- из файла.

Ниже приведены примеры настройки импорта ресурсов из репозитория Лаборатории Касперского и из файла.

Импорт ресурсов из репозитория (серверы обновлений Лаборатории Касперского)

Предварительно разрешите доступ на пограничном межсетевом экране к следующим URL (без использования механизмов вскрытия SSL/TLS-трафика):

<https://support.kaspersky.ru/common/start/6105>

Чтобы настроить автоматический импорт ресурсов из репозитория, используя серверы обновлений Лаборатории Касперского:

- Перейдите в раздел **Параметры → Другое → Обновление репозитория**.
- Убедитесь, что флажок **Отключить автоматическое обновление** снят.
- Задайте **Интервал обновления в часах**.
- В поле **Источник обновления** выберите **Серверы обновления “Лаборатории Касперского”**.
- При необходимости в поле **Прокси-сервер** выберите из списка существующий прокси-сервер, который должен использоваться при запуске задачи **Обновление репозитория**. Если прокси-сервер еще не настраивался в поле **Прокси-сервер** нажмите на **Создать** и выполните настройку ресурса прокси-сервера согласно [статье](#).
- Опционально укажите адреса электронной почты для рассылки уведомлений, нажав **Добавить**. После первого выполнения задачи обновления репозитория KUMA будет отправлять на указанные адреса уведомления о доступных для обновления пакетах.
- Нажмите кнопку **Сохранить** для применения изменений.

Автоматический импорт ресурсов из репозитория Лаборатории Касперского настроен.

The screenshot displays the Kaspersky Unified Monitoring and Analysis Platform interface. On the left is a dark sidebar with navigation options: Выбрано тенантов: 1, Панели мониторинга, Алерты, Инциденты, События, Активы, Отчеты, Ресурсы, CyberTrace, Диспетчер задач, Параметры (marked with a red circle 1), Доступ, Интеграции, Другое (marked with a red circle 2), Состояние источников, and Метрики. The main area is titled 'Обновление репозитория' (Repository Update). It includes a toggle for 'Отключить автоматическое обновление' (marked with a red circle 4), a dropdown for 'Интервал обновления в часах' set to 24 (marked with a red circle 5), and a status box showing the last update time (13.07.2026 20:05:11), the next scheduled update (14.07.2026 20:05:11), and the total number of packages (237) and resources (10208). Below this is a 'Запустить обновление' button. Further down are dropdowns for 'Источник обновления' (set to 'Серверы обновления "Лаборатории Касперс..."', marked with a red circle 6), 'Прокси-сервер' (set to 'Создать', marked with a red circle 7), and 'Адреса электронной почты для рассылки уведомлений' (marked with a red circle 8). At the bottom right is a 'Сохранить' button (marked with a red circle 9).

Далее запустите обновление репозитория вручную. Для этого:

- Нажмите **Запустить обновление**.
- Перейдите в раздел **Диспетчер задач** и убедитесь, что статус задачи **Обновление репозитория** в состоянии **Завершено**.



Kaspersky
Unified Monitoring and Analysis Platform

Выбрано тенантов: 1 >

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

CyberTrace

Диспетчер задач 1

Диспетчер задач

☒ Отображать только свои

Статус	Задача	Создал	Создана	Последнее обновление	Тенант
✓ Завершено	Обновление репозитория	Administrator	24.03.2025 18:31:17	24.03.2025 18:31:21	Main
✓ Завершено	Обновление репозитория	Administrator	24.03.2025 18:25:15	24.03.2025 18:25:18	Main

- Перейдите в раздел **Ресурсы** и нажмите **Импортировать ресурсы**.

Ресурсы и сервисы

Сервисы Подключить источник Создать коррелятор

Активные сервисы Коллекторы Корреляторы Хранилища Агенты

Маршрутизаторы событий

Ресурсы Импортировать ресурсы Экспортировать ресурсы

Правила корреляции Нормализаторы Коннекторы Правила агрегации Правила обогащения

Точки назначения Фильтры Правила реагирования Активные листы Словари

Прокси-серверы Секреты Контекстные таблицы Правила сегментации Шаблоны уведомлений

- В появившемся окне **Импорт ресурсов** укажите **Тенант** (по умолчанию, Main) и выберите **Источник импорта – Репозиторий**.
- В секции **Пакеты репозитория** появится список доступных пакетов ресурсов для загрузки.
- Найдите и выберите пакет **[OOTB] KUMA 4.0.1 resources** (для версии KUMA 4.0) или **[OOTB] KUMA 4.2 resources** (для версии KUMA 4.2).
- Нажмите **Импортировать**. Данные пакеты содержат ресурсы для KUMA 4.0 или 4.2 (нормализаторы, коннекторы, словари и т.д.). Дождитесь появления всплывающего уведомления **Ресурсы из пакета [OOTB] KUMA <версия> resources успешно импортированы**.

Подробнее об экспорте и импорте ресурсов смотрите [в онлайн-справке](#).

Тенант*

Main

Источник импорта*

Репозиторий

Пакеты репозитория

Вы можете запустить обновление в разделе [Обновление репозитория](#).
После обновления ресурсов требуется перезапустить использующие их сервисы, а также проверить привязки ресурсов, если вы их меняли.

🕒 Последнее обновление: 13.07.2026 15:21:11.

resource

☐	Название	Дата выпуска	Версия	Установленная версия	Количество ресурсов
☐	[OOTB] KUMA 4.2 resources	01.12.2025 22:02:17	1	1	430
☒	[OOTB] KUMA 4.0.1 resources	02.09.2025 15:57:05	1	1	438
☐	[OOTB] KUMA 4.0 resources	25.06.2025 11:18:11	1	1	432
☐	[OOTB] KUMA 3.4 resources	02.12.2024 10:59:21	1	1	381
☐	[OOTB] KUMA 3.2 resources	17.05.2024 12:58:21	1	1	331
☐	[OOTB] KUMA 3.0.1 resources	13.12.2023 15:58:44	1	1	311
☐	OOTB resources for KUMA 2.1	13.01.2023 11:32:48	1	1	143

Всего 7 / Выбрано 1

2

Импортировать

Отмена

- Повторите процедуру и выполните импорт пакета **[OOTB] SOC Content - RU for KUMA 3.2** (для версии KUMA 3.2+). Данный пакет содержит набор ресурсов, предназначенных для выявления подозрительного поведения в соответствии с различными техниками матрицы MITRE ATT&CK.

Подробнее об экспорте и импорте ресурсов смотрите [в онлайн-справке](#).

Тенант*

Main

Источник импорта*

Репозиторий

Пакеты репозитория

Вы можете запустить обновление в разделе [Обновление репозитория](#).
После импорта ресурсов требуется перезапустить использующие их сервисы, а также проверить наборы ресурсов, если вы их меняли.

⌚ Последнее обновление: 16.12.2024 14:33:12.

☐	Название	Дата выпуска	Версия	Установленная версия	Количество ресурсов
☐	[OOTB] SOC Content - ENG for KU...	28.10.2024 11:20:44	2	Не установлен	1429
☒	[OOTB] SOC Content - RU for KUM...	28.10.2024 10:57:12	2	Не установлен	1429
☐	[OOTB] Linux auditd syslog for KU...	14.10.2024 17:00:33	1	Не установлен	3
☐	[OOTB] Barracuda Cloud Email Se...	10.10.2024 19:47:14	1	Не установлен	1
☐	[OOTB] Yandex Cloud	08.10.2024 16:13:43	1	Не установлен	2
☐	[OOTB] InfoWatch Person Monitor ...	07.10.2024 22:05:58	1	Не установлен	4
☐	[OOTB] Kaspersky Industrial Cyber...	07.10.2024 14:49:56	1	Не установлен	1
☐	[OOTB] KSC PostgreSQL	02.10.2024 15:01:53	3	Не установлен	2
☐	[OOTB] CommuniGate Pro	01.10.2024 11:07:33	1	Не установлен	4
☐	[OOTB] NetApp SnapCenter file	27.09.2024 17:31:11	1	Не установлен	1
☐	[OOTB] Parsec ParsecNet	24.09.2024 16:21:47	1	Не установлен	3
☐	[OOTB] Barracuda Web Security G...	20.09.2024 14:48:59	1	Не установлен	1
☐	[OOTB] Postfix	16.09.2024 17:51:08	1	Не установлен	4

Импортировать

Отмена

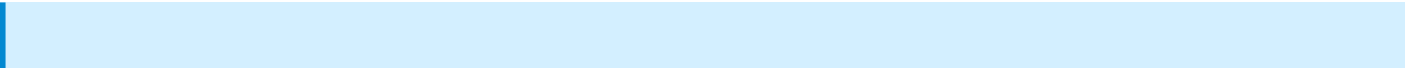
Импорт пакетов с OOTB-ресурсами успешно выполнен. Опционально можно импортировать другие пакеты из репозитория в случае необходимости.

Статья онлайн-справки «Обновление ресурсов»:
<https://support.kaspersky.ru/kuma/4.0/242817>

Импорт ресурсов из файла

Если у сервера KUMA отсутствует доступ в Интернет (решение используется в закрытом контуре) или необходимо выполнить перенос ресурсов из другой инсталляции KUMA ресурсы можно также импортировать из файлов.

Версия KUMA, в которую осуществляется импорт ресурсов, должна быть идентична или выше версии KUMA, из которой ресурсы были экспортированы



Для переноса ресурсов из более поздней версии KUMA в более раннюю можно использовать скрипт из [репозитория KUMA Community](#)

Ниже рассматривается пример импорта ресурсов Community Pack (пакет ресурсов от сообщества KUMA) из файла. Как правило, все необходимые ресурсы доступны в репозитории, но в качестве дополнительного источника можно использовать ресурсы сообщества KUMA.

Ресурсы сообщества KUMA:

<https://box.kaspersky.com/d/f630e3ab02b64405881a/?p=%2F&mode=list>

https://github.com/KUMA-Community/kuma_content

Чтобы импортировать ресурсы из файла на примере Community Pack:

- Загрузите **пакет ресурсов нормализаторов** Community-Pack-RU+MITRE_<дата>_<время> по [ссылке](#) или **пакет ресурсов правил корреляции** Community-Pack-RU+MITRE_<дата>_<время> по [ссылке](#).
- В веб-интерфейсе KUMA перейдите в **Ресурсы** и выберите **Импортировать ресурсы**.
- В появившемся окне импорта ресурсов выберите **Тенант** (по умолчанию Main), в качестве **Источника импорта** укажите **Файл** и введите пароль (пароль от ресурсов сообщества `q123123Q!q123123Q!` или `q123123Q!KLaapt-M4`), после чего выберите ранее загруженный файл. Пароль от файла с ресурсами необходимо вводить до загрузки самого файла.
- После импорта файла раскройте дерево ресурсов и выберите необходимые ресурсы для импорта (рекомендуется импортировать только действительно необходимые для работы ресурсы), после чего нажмите кнопку **Импортировать**.

Импорт ресурсов



Подробнее об экспорте и импорте ресурсов смотрите [в онлайн-справке](#).

Тенант*

Источник импорта*

Пароль файла*

✓ Community-Pack-RU+MITRE_20241115_112432 (1)

Выберите импортируемые ресурсы:*

- ☒ Все ресурсы
 - ☐ Коннекторы
 - ☒ Нормализаторы
 - ☒ Community Pack
 - ☐ Cloud/VM
 - ☐ Network
 - ☐ [22-09-2022] Windows Server Essentials Experience (WSEE)
 - ☒ [2024-09-28] ALT Linux SambaDC (JSON)
 - ☐ [25-07-2023] 1C logs JSON
 - ☐ [07-07-2023] Unix AuditD (Syslog)
 - ☐ [20-10-2022] KSC Cloud Console
 - ☐ [07-07-2023] MS Windows Firewall Log
 - ☐ [22-09-2022] Dallas Lock
 - ☐ [22-09-2022] OpenVAS-CSV (File)
 - ☐ [2024-10-11] Avastpost FAM
 - ☐ [03-11-2022] KEDR telemetry
 - ☐ [2024-09-17] HoneyCorn Deception v4 (CEF)
 - ☐ [07-07-2023] PTsecurity AF 3.7 (CEF)
 - ☐ [2023-10-09] KCS Syslog-CEF
 - ☐ [20-10-2023] AuditD (Pacta Agent)

Импортировать

Отмена

- Дождитесь появления всплывающего уведомления **Ресурсы успешно импортированы**.

Ресурс успешно импортирован.

Чтобы импортировать набор ресурсов из файла ootb-content ("коробочный контент", поставляемый вместе с дистрибутивом KUMA):

- В веб-интерфейсе KUMA перейдите в **Ресурсы** и выберите **Импортировать ресурсы**.
- В появившемся окне импорта ресурсов выберите **Тенант** (по умолчанию Main), в качестве **Источника импорта** укажите **Файл** и введите пароль , после чего выберите файл ootb-content. Пароль от файла с ресурсами необходимо вводить до загрузки самого файла.
- После импорта файла выберите Все ресурсы и нажмите кнопку **Импортировать**.

Импорт ресурсов



Подробнее об экспорте и импорте ресурсов смотрите [в онлайн-справке](#).

Тенант*

Источник импорта*

Пароль файла*

☒ ootb-content

Выберите импортируемые ресурсы:*

- ☒ Все ресурсы
 - ☒ Коннекторы
 - ☒ Нормализаторы
 - ☒ Фильтры
 - ☒ Правила обогащения
 - ☒ Правила агрегации
 - ☒ Точки назначения
 - ☒ Словари
 - ☒ Правила корреляции
 - ☒ Шаблоны уведомлений
 - ☒ Активные листы
 - ☒ Секреты
 - ☒ Коллекторы
 - ☒ Корреляторы
 - ☒ KUMA Packages
 - ☒ OOTB
 - ☒ [OOTB] Correlator
 - ☒ Хранилища
 - ☒ KUMA Packages
 - ☒ OOTB
 - ☒ [OOTB] Storage

Импортировать

Отмена

В результате будут загружены различные типы OOTB-ресурсов, в том числе ресурсы сервисов, установить которые можно согласно статье [Создание и установка сервисов](#).

Привязка правил корреляции

После импорта пакета ресурсов **[OOTB] SOC Content - RU for KUMA 3.2** (для версии KUMA 3.2+) с правилами корреляции необходимо привязать данные правила корреляции к коррелятору.

Чтобы привязать правила корреляции к коррелятору:

1. Перейдите в **Ресурсы** → **Активные сервисы**.
2. Нажмите на название сервиса **Коррелятора**.
3. В появившемся окне **Редактирование коррелятора** перейдите на шаг **Корреляция** и нажмите **Привязать**.

Общие

Глобальные переменные

Корреляция 1

Обогащение

Реагирование

Маршрутизация

Проверка параметров

Корреляция

С помощью правил корреляции задаются условия, по которым анализируются поступающие события и, если выполняются условия правил, создаются алерты. Подробнее см. [в онлайн-справке](#).

+ Добавить

Привязать 2

Удалить

↑ Поднять

↓ Опустить

⋮

--

Q

☐

Правила корреляции

Тип

Действия



Пусто

Найдено 0 / Выбрано 0

Сохранить

Отмена

4. В окне **Выбор правил корреляции** выберите категории правил корреляции или определенные правила корреляции SOC Package и нажмите **Привязать**.

Каждое правило корреляции предназначено для анализа событий определенного источника, поэтому рекомендуется учитывать какие источники событий подключены к KUMA и привязывать только те правила корреляции, которые предназначены для этих источников.

Посмотреть для событий какого источника предназначено правило корреляции можно в документе «Описание правил корреляции, содержащихся в SOC_package.xlsx»:

<https://support.kaspersky.ru/kuma/4.0/250594>

Выбор правил корреляции



☐ Main

☐ KUMA Packages

1

☐ OOTB

☒ SOC package

☒ Access token manipulation

☒ Account Lifecycle Events (ALCE)

☒ Active Defense Systems Status

☒ Authentication anomalies

☒ Boot or Logon Script Modification

☒ C2 behavior

☒ Clearing the event log

☒ Configuration discovery

☒ Container

☒ Credential Dumping

☒ Data collection

☒ Default Accounts

☒ Defense and Detection Systems Status

☒ File System Manipulation

☒ Group Lifecycle Events (GLCE)

☒ Inhibit System Recovery

☒ IoC correlation

☒ Malware infection

☒ Network Scanning

☒ Network profiling

☒ Operational rules

☒ Phishing

2

Привязать

Отмена

5. Выбранные правила корреляции привязаны к коррелятору.

Рекомендуется удалить предустановленные корреляционные правила с префиксом [OOTB]. Данные правила являются шаблонами для создания собственных правил корреляции. Для удаления правил с префиксом [OOTB] введите «ootb» в поле поиска, выберите все правила и нажмите **Удалить**.

6. Нажмите **Сохранить**.

Общие

Глобальные переменные

Корреляция

Обогащение

Реагирование

Маршрутизация

Проверка параметров

Корреляция

С помощью правил корреляции задаются условия, по которым анализируются поступающие события и, если выполняются условия правил, создаются алерты. Подробнее см. [в онлайн-справке](#).

3

+ Добавить

🔗 Привязать

🗑 Удалить

⬆ Поднять

⬇ Опустить

⋮

ootb

1

🔍

2

✓	Правила корреляции	Тип	Действия
✓	[OOTB][AD][Technical] 4768. TGT Requested	operational	Изменение активного листа
✓	[OOTB][AD] Membership of sensitive group was modified	simple	В дальнейшую обработку
✓	[OOTB][AD] Multiple accounts failed to log on from the same host	standard	В дальнейшую обработку
✓	[OOTB][AD] Successful authentication with the same account on multiple hosts	standard	В дальнейшую обработку
✓	[OOTB][AD] Granted TGS without TGT (Golden Ticket)	standard	В дальнейшую обработку
✓	[OOTB][AD] An account failed to log on from different hosts	standard	В дальнейшую обработку
✓	[OOTB][AD] The account added and deleted from the group in a	standard	В дальнейшую обработку

Найдено 12 / Выбрано 12

Сохранить

Отмена

Чтобы коррелятор применил изменения конфигурации необходимо обновить параметры сервиса:

- Перейдите в **Ресурсы → Активные сервисы**.
- Нажмите ПКМ на сервис **Коррелятора** и выберите **Обновить параметры**.

Ресурсы и сервисы / Сервисы

Сервисы

+ Добавить

🔄 Обновить параметры

🔄 Перезапустить

🔗 Перейти к событиям

📄 Смотреть активные листы

📊 Смотреть контекстные таблицы

⋮

сорт

✕

🔄

⚙

Статус	Тип	Сервис	Версия	Тенант	Полное доменное имя	IP-адрес	Порт API
Вкл	Коррелятор	1	[OOTB] Correlator	Main	kuma-aiio.truecompany.local	10.68.85.89	7231

📄 Копировать идентификатор

📖 Журнал

🔗 Перейти к событиям

📄 Смотреть активные листы

📊 Смотреть контекстные таблицы

🔄 Обновить параметры

🔄 Перезапустить

🗑 Сбросить сертификат

🗑 Удалить

2

Настройка параметров наполнения алертов

Начиная с версии 4.0 события алертов KUMA хранятся в ClickHouse вместо MongoDB, поэтому после установки KUMA или обновления с предыдущей версии, необходимо выполнить настройку параметров наполнения алертов и указать хранилище для событий алертов.

Без указания хранилища новые алерты будут создаваться без событий.

Чтобы настроить параметры наполнения алертов:

- В веб-интерфейсе KUMA перейдите в раздел **Параметры** → **Другое** → **Алерты**.
- В открывшемся окне **Алерты** перейдите на вкладку **Наполнение алертов** и задайте значение следующих параметров:
 - В раскрывающемся списке **Статус** выберите значение, при котором алерт будет наполняться событиями. Рекомендуется значение по умолчанию: **Новый**.
- В поле **Алерт создан не позднее (часы)** укажите время, в течение которого алерт будет наполняться событиями. Значение параметра должно быть целым числом. Отсчет времени осуществляется от момента создания алерта. Значение по умолчанию: 336 часов (2 недели). Минимальное значение: 1 час.
- В раскрывающемся списке **Хранилище событий** выберите хранилище, в котором будут храниться события алерта. Можно указать только одно хранилище. В списке отображаются ресурсы хранилища, а не запущенные сервисы. Для того чтобы алерты наполнялись событиями, сервис хранилища должен быть запущен.

Параметры наполнения алертов настроены.



Unified Monitoring and Analysis Platform

Выбрано тенантов: 3

Панели мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

CyberTrace

Диспетчер задач

Параметры

Доступ

Интеграции

Другое

Состояние источников

Метрики

Administrator

Общее

Алерты

Лицензия

Инциденты

Обновление репозитория

Активы

Мониторинг сервисов

Теги

Поля расширенной схемы событий

Алерты

СегментацияПравила уведомленийНаполнение алертов

Новые корреляционные события добавляются в существующий алерт, если он удовлетворяет условиям.

Статус

Новый

Алерт создан не позднее (часы)

336

Хранилище событий*

Storage

Storage

Main

Сохранить

Revision #6

Updated 2026-08-18 15:07:59 UTC by Dmitry Borisov