

???????? SMP

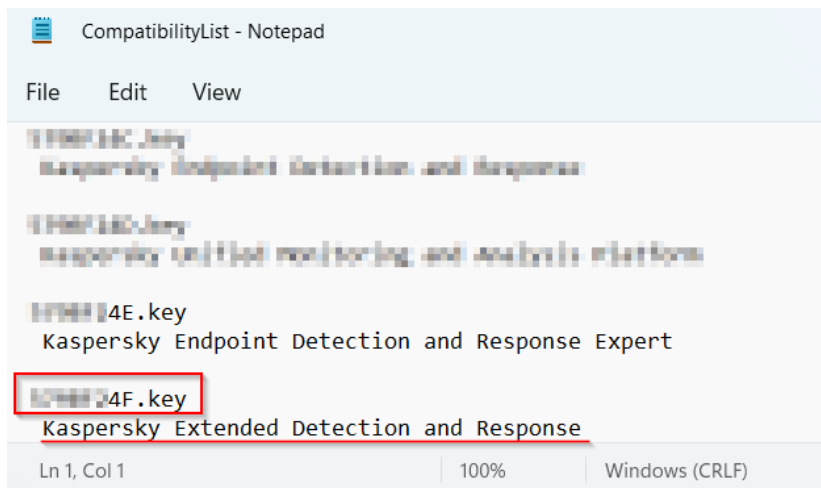
- [Добавление лицензии с функционалом XDR](#)
- [Создание пользователя в SMP](#)
- [Интеграция SMP с KSC](#)

???????????? ???? ? ???????????? XDR

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

После установки SMP для доступа к функционалу XDR (алерты, инциденты с графом расследования, плейбуки и прочее) необходимо добавить лицензию на функционал. Для этого необходимо выполнить следующее:

1. В полученном архиве с лицензионными ключами найти файл `CompatibilityList.txt` и в нем найти название ключа, которое соответствует функционалу **Kaspersky Extended Detection and Response** (не путать с Kaspersky Endpoint Detection and Response!)



```
CompatibilityList - Notepad
File Edit View
K099814C.key
Kaspersky Endpoint Detection and Response
K099814D.key
Kaspersky Unified monitoring and analysis platform
K099814E.key
Kaspersky Endpoint Detection and Response Expert
K099824F.key
Kaspersky Extended Detection and Response
Ln 1, Col 1 | 100% | Windows (CRLF)
```

2. Зайти в веб-интерфейс консоли под встроенной учетной записью `admin`, либо под другой с аналогичными правами.

3. Перейти в раздел **Операции - Лицензии "Лаборатории Касперского"** и нажать "**Добавить**"

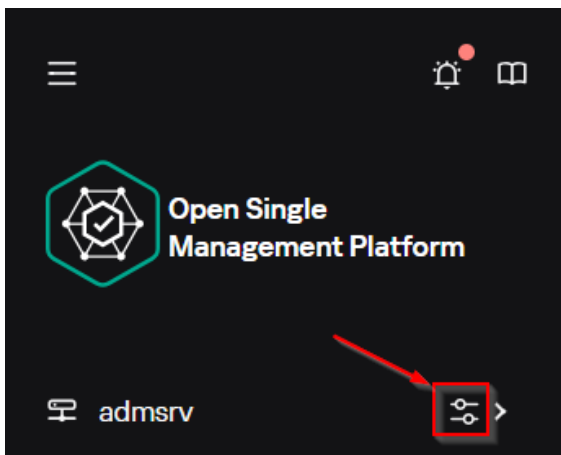
The screenshot shows the 'Open Single Management Platform' interface. On the left is a dark sidebar with a menu. The 'Операции' (Operations) item has a red badge with the number '1', and the 'Лицензии "Лаборатории Касперск"' (Licenses 'Kaspersky Labs') item has a red badge with the number '2'. The main content area is titled 'Операции / Лицензии "Лаборатории Касперск' and features a table of licenses. At the top of the table are buttons: '+ Добавить' (Add) with a red badge '3', '× Удалить' (Delete), and '↻ Обновить' (Refresh). The table has a header 'Название лицензии ↑↓' and two rows of data. The first row is 'Добавлено вручную и хранится в хранилище' (Added manually and stored in the repository) with a radio button. The second row is 'Получено от управляемых устройств' (Received from managed devices) with a radio button. Below the table, it says 'Всего 2' (Total 2).

4. В появившемся окне можно либо ввести код активации, который доступен в архиве с лицензиями в файле `ActivationCodes*.txt`, либо загрузить файл ключа, полученный на шаге 1.

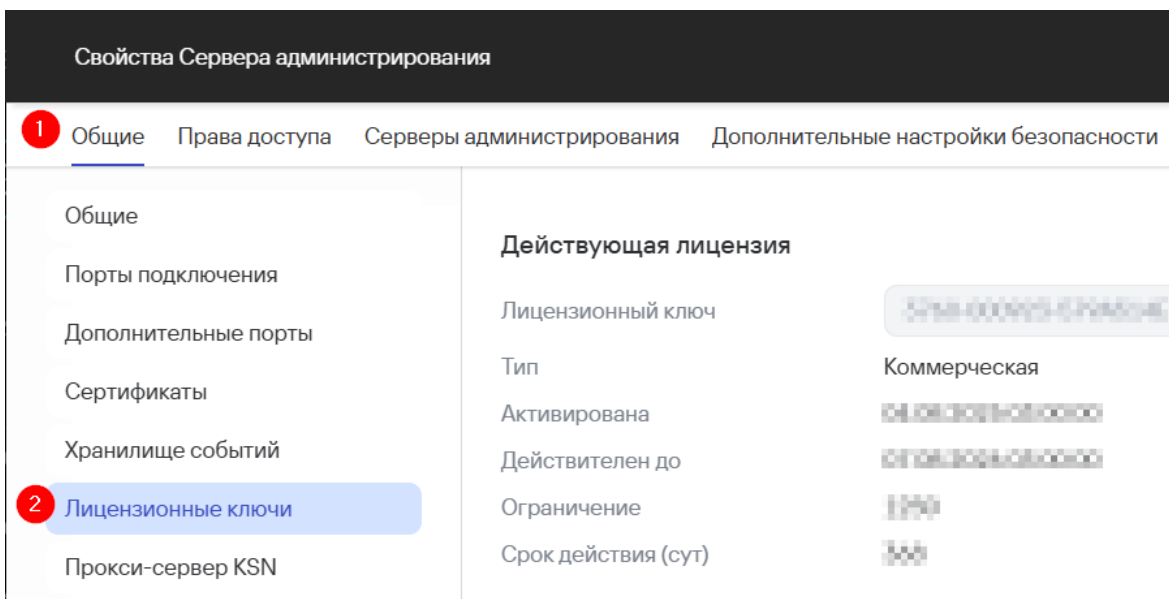
The dialog box is titled 'Добавить лицензионный ключ' (Add license key) and has a close button '×'. It contains the text 'Выберите вариант:' (Choose an option:). There are two radio buttons: 'Ввести код активации' (Enter activation code) which is selected, and 'Добавить файл ключа' (Add key file). Below the radio buttons is a text input field. At the bottom left is a blue button labeled 'Отправить' (Send).

После добавления ключ отобразится в таблице с лицензиями.

5. Далее необходимо перейти в настройки щелкнув по соответствующему значку в верхней части интерфейса



6. Затем перейти в раздел **Общие - Лицензионные ключи** и выбрать ранее добавленный ключ



7. После этого необходимо сохранить все изменения, подождать несколько минут и перезагрузить страницу. Новые разделы будут добавлены в консоль автоматически в раздел **"Мониторинг и отчеты"**.



Open Single
Management Platform

admsrv



Быстрые ссылки

Мониторинг и отчеты



Панель мониторинга

Отчеты

Выборки событий

Уведомления

Объявления "Лаборат...

Поиск угроз

Алерты

Инциденты

Плейбуки

История реагирований

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

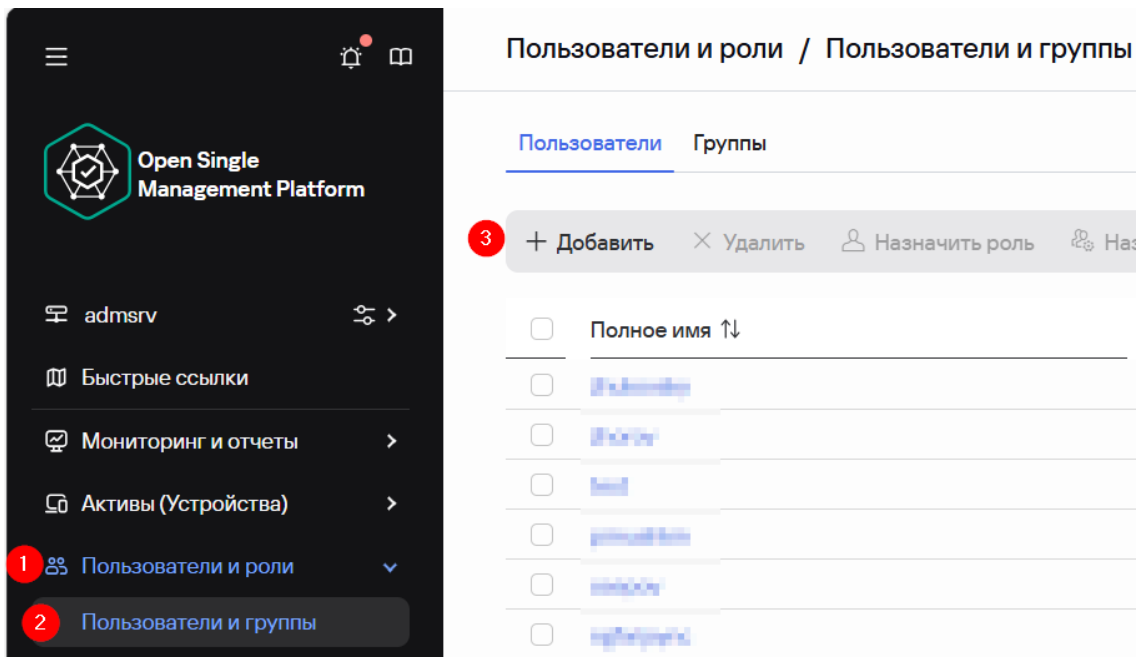
SMP

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

Процесс создания пользователя в SMP аналогичен процессу создания пользователя в KSC. Однако, для предоставления пользователю доступа к функционалу XDR и консоли KUMA потребуются дополнительные действия.

Для создания пользователя и назначения ему прав для доступа ко всему функционалу XDR необходимо выполнить следующие действия

1. Перейдите в интерфейс SMP на вкладку **Пользователи и роли - Пользователи и группы** и нажмите **Добавить** для добавления локального пользователя и укажите его логин и пароль (пропустите этот шаг для доменного пользователя).



Добавить пользователя



Имя*

admin_xdr

Пароль* ⓘ

.....



2. После добавления локального пользователя (либо при наличии доменного, полученного через интеграцию с AD) необходимо назначить роль. Для этого выберите галочкой нужного пользователя и нажмите **Назначить роль**.

Пользователи и роли / Пользователи и группы

[Пользователи](#)

[Группы](#)

+ Добавить

× Удалить

Назначить роль

Назначить группу



Полное имя ↓

Имеет назначенные роли



admin



admin_xdr



3. Выберите необходимую роль галочкой и нажмите далее

Выбор роли

<input type="checkbox"/> Имя роли ↑↓	Ретранслировано ↑↓
<input type="checkbox"/> Администратор Kaspersky Endpoint Security	Нет
<input type="checkbox"/> Администратор Сервера администрирования	Нет
<input type="checkbox"/> Администратор Системного администрирования	Нет
<input type="checkbox"/> Администратор управления мобильными устройствами	Нет
<input type="checkbox"/> Администратор установки приложений	Нет
<input type="checkbox"/> Аудитор	Нет
<input checked="" type="checkbox"/> Главный администратор	Нет
<input type="checkbox"/> Главный оператор	Нет
<input type="checkbox"/> Контролер	Нет
<input type="checkbox"/> Новая роль	Нет
<input type="checkbox"/> Оператор Kaspersky Endpoint Security	Нет
<input type="checkbox"/> Оператор Сервера администрирования	Нет
<input type="checkbox"/> Оператор Системного администрирования	Нет
<input type="checkbox"/> Оператор управления мобильными устройствами	Нет
<input type="checkbox"/> Оператор установки приложений	Нет
<input type="checkbox"/> Пользователь Self Service Portal	Нет
<input type="checkbox"/> Специалист по безопасности	Нет

Всего 17 / Выбрано 1

Отмена

Далее

4. Выберите область действия и нажмите **Готово**

Определение области

▼ admsrv

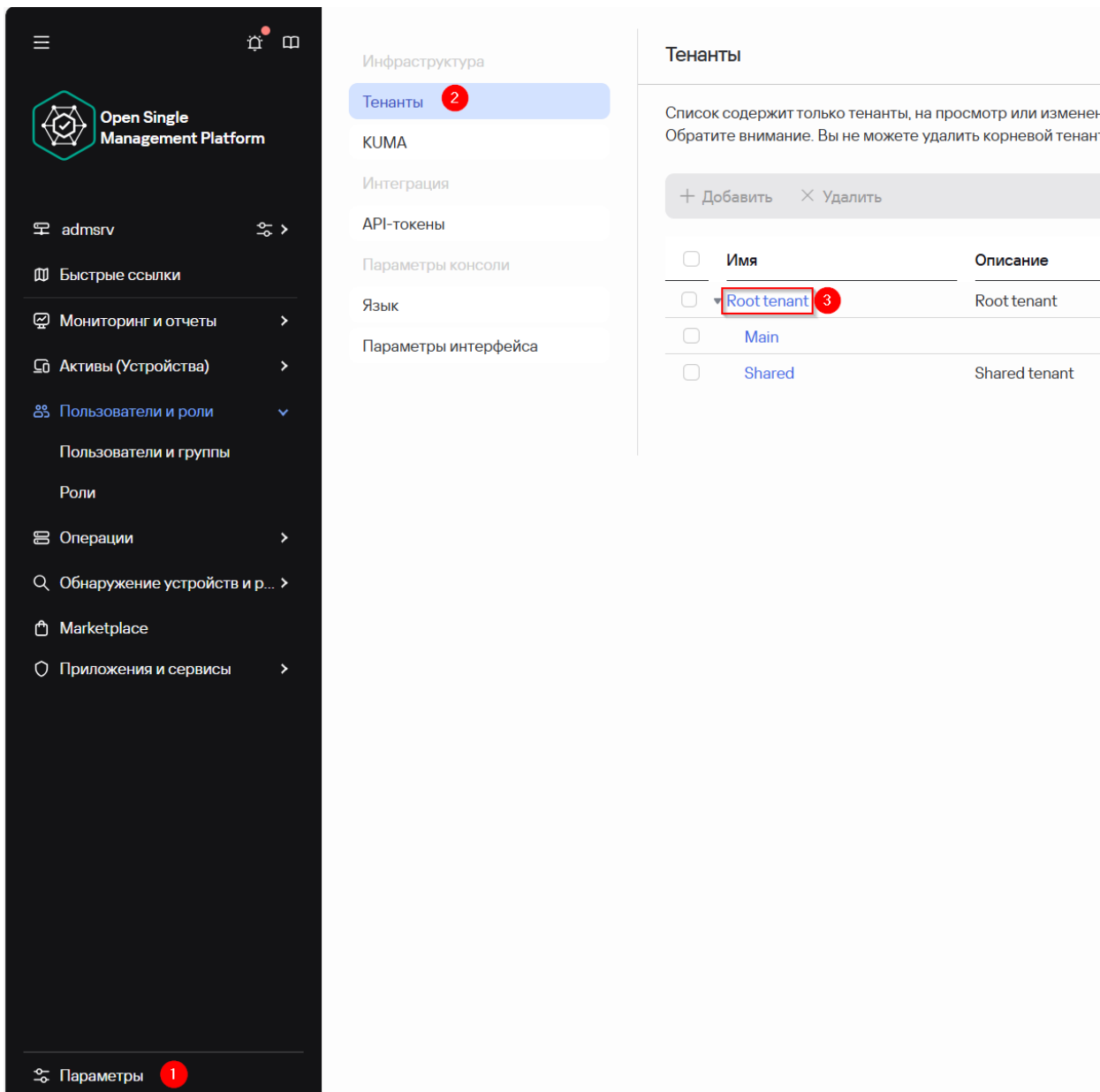
▶ Управляемые устройства

Назад

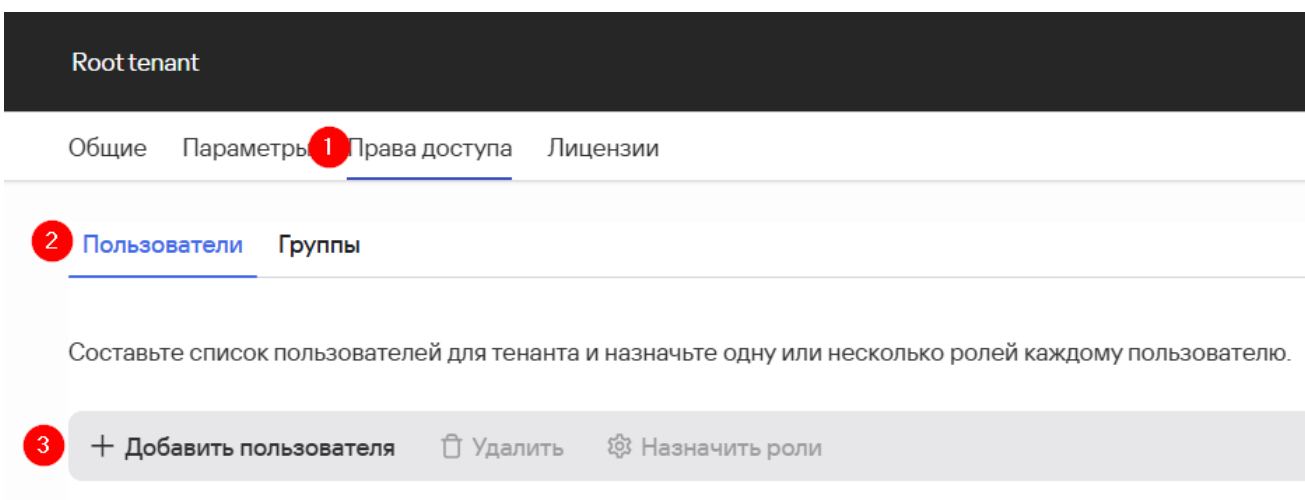
Готово

Пользователю назначена роль и теперь он может получить доступ к консоли SMP. Для получения доступа к функциям XDR необходимо дополнительно назначить роль пользователю в определенном тенанте.

4. Для этого перейдите в **Параметры - Тенанты** и нажмите на название необходимого тенанта для назначения пользователя



5. В открывшемся окне перейдите на вкладку **Права доступа**, в раздел **Пользователи** и нажмите на кнопку **Добавить пользователя**



6. В выпадающем списке выберите нужного пользователя, которому собираетесь назначить роль

Если нужного пользователя еще нет в списке, значит не прошел период синхронизации. Повторите попытку через несколько минут.

Добавить пользователя ×

Пользователь*

- admin_xdr**
admin_xdr | Root tenant
- admin_xdr
- admin_xdr | Root tenant
- admin_xdr
- admin_xdr | Root tenant
- admin_xdr
- admin_xdr | Root tenant
- admin_xdr
- admin_xdr | Root tenant

- Аналитик 2-го уровня**
Эта роль позволяет расследовать зарегистрированные алерты и инциденты, а также управлять плейбуками и их параметрами.
- Аудитор**
Эта роль позволяет просматривать все данные в Kaspersky XDR.
- Главный администратор**
Эта роль предоставляет все права доступа в Kaspersky XDR.
- Доступ к объектам КИИ**
Эта роль позволяет получить доступ к объектам КИИ.
- Изменение общих ресурсов**
Эта роль позволяет изменять общие ресурсы, которые размещены в общем тенанте.
- Менеджер SOC**
Эта роль позволяет создавать отчеты и назначать алерты и инциденты аналитикам.
- Младший аналитик**
Эта роль позволяет расследовать зарегистрированные алерты и инциденты.
- Подтверждающий**
Эта роль позволяет подтверждать или отклонять действия по реагированию, запущенные в рамках плейбуков.
- Работа с дочерними инцидентами**

Добавить

7. После выбора пользователя укажите выберите галочкой необходимые для него роли и нажмите кнопку **Добавить**

Добавить пользователя



Пользователь*

admin_xdr



Роли

- Администратор SOC**
Эта роль позволяет настраивать интеграции, правила сегментации и плейбуки, просматривать и изменять тенанты, управлять правами пользователей, а также настраивать уведомления по электронной почте.
- Администратор тенанта**
Эта роль позволяет управлять системами в рамках доступных тенантов.
- Аналитик 1-го уровня**
Эта роль позволяет создавать и изменять свои отчеты и шаблоны KUMA, расследовать зарегистрированные алерты и инциденты, а также создавать плейбуки.
- Аналитик 2-го уровня**
Эта роль позволяет расследовать зарегистрированные алерты и инциденты, а также управлять плейбуками и их параметрами.
- Аудитор**
Эта роль позволяет просматривать все данные в Kaspersky XDR.
- Главный администратор**
Эта роль предоставляет все права доступа в Kaspersky XDR.
- Доступ к объектам КИИ**
Эта роль позволяет получить доступ к объектам КИИ.
- Изменение общих ресурсов**
Эта роль позволяет изменять общие ресурсы, которые размещены в общем тенанте.
- Менеджер SOC**
Эта роль позволяет создавать отчеты и назначать алерты и инциденты аналитикам.
- Младший аналитик**
Эта роль позволяет расследовать зарегистрированные алерты и инциденты.
- Подтверждающий**
Эта роль позволяет подтверждать или отклонять действия по реагированию, запущенные в рамках плейбуков.
- Работа с дочерними инцидентами**

Добавить

Отмена

8. Не забудьте нажать кнопку **Сохранить** в таблице пользователей для применения изменений к Тенанту.

Готово. Пользователь создан, ему назначена роль для доступа SMP и роль доступа к функционалу XDR.

???????????? SMP ? KSC

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

SMP может выступать в роли KSC, к которому напрямую подключаются конечные устройства, а также в роли главного KSC в иерархии. Второй вариант является более приоритетным при построении архитектуры.

SMP может выступать главным сервером в иерархии как для KSC на базе Linux, так и для KSC на базе Windows.

Добавление подчиненных KSC к SMP решает сразу несколько задач:

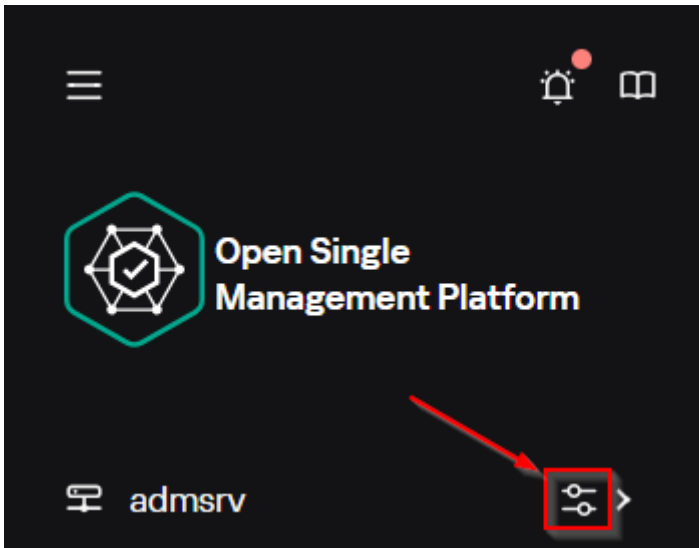
1. Управление подчиненными KSC и конечными точками
2. Возможность сбора актива, для отображения их в событиях, алертах и инцидентах
3. Возможность реагирования на активах как вручную, так и с помощью плейбуков.

Важно! Для отображения активов в алертах/инцидентах и возможности реагирования на них, необходимо настроить интеграцию SMP и KSC!

Для настройки всесторонней интеграции необходимо создать иерархию Серверов администрирования, а затем настроить получения активов с подчиненного Сервера администрирования. Рассмотрим необходимые шаги по порядку.

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

1. Перейти в настройки встроенного в SMP KSC



2. На вкладке **Общие** в разделе **Общие** необходимо записать **Адрес подключения Сервера администрирования**, а также скачать сертификат Сервера администрирования по ссылке "**Просмотреть сертификат Сервера администрирования**"

Свойства Сервера администрирования

Общие | Права доступа | Серверы администрирования | Дополнительные настройки безопасности | История ревизий

Общие

Имя Сервера администрирования	admsrv
Адрес подключения Сервера администрирования ⓘ	admsrv.smp.demo.lab <small>Укажите NetBIOS-имя, FQDN или IP-адрес</small>
Версия	15.4.0.8873

[Просмотреть сертификат Сервера администрирования](#)

Важно! Для организации иерархии необходимо использовать именно доменное имя (FQDN) сервера администрирования, встроенного в KSC. Использование IP недопускается.

3. Далее необходимо перейти на вкладку Серверы администрирования, выбрать соответствующую группу, например, Управляемые устройства и нажать на кнопку Подключить подчиненный Сервер администрирования

Свойства Сервера администрирования

Общие | Права доступа | Серверы администрирования | Дополнительные настройки безопасности | История ревизий | Настройка событий

Подключить / отключить виртуальный Сервер администрирования + Новый виртуальный Сервер администрирования + Подключить подчиненный Сервер администрирования

Управляемые устройства

- МОНУ
- МОНУ/Иконки

4. В появившемся окне необходимо заполнить параметры, подключаемого Сервера администрирования. В общем случае достаточно указать имя Сервера администрирования, которое будет отображаться в консоли, а также адрес подчиненного Сервера администрирования (здесь можно использовать как IP, так и доменное имя). Сертификат Сервера администрирования можно получить аналогичным образом описанным на шаге 1 настоящей инструкции, либо выбрать пункт **Получать с подчиненного Сервера администрирования** (как сделано в настоящей статье).

Подключить подчиненный Сервер администрирования

Параметры подключения

Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне

Отображаемое имя подчиненного Сервера*

Адрес подчиненного Сервера ⓘ

Номер SSL-порта Сервера*

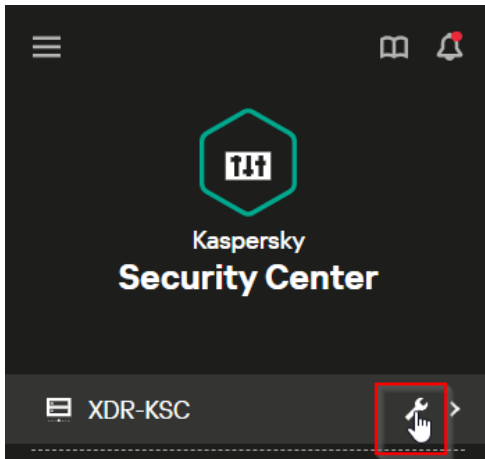
API-порт Сервера*

Сертификат подчиненного Сервера администрирования

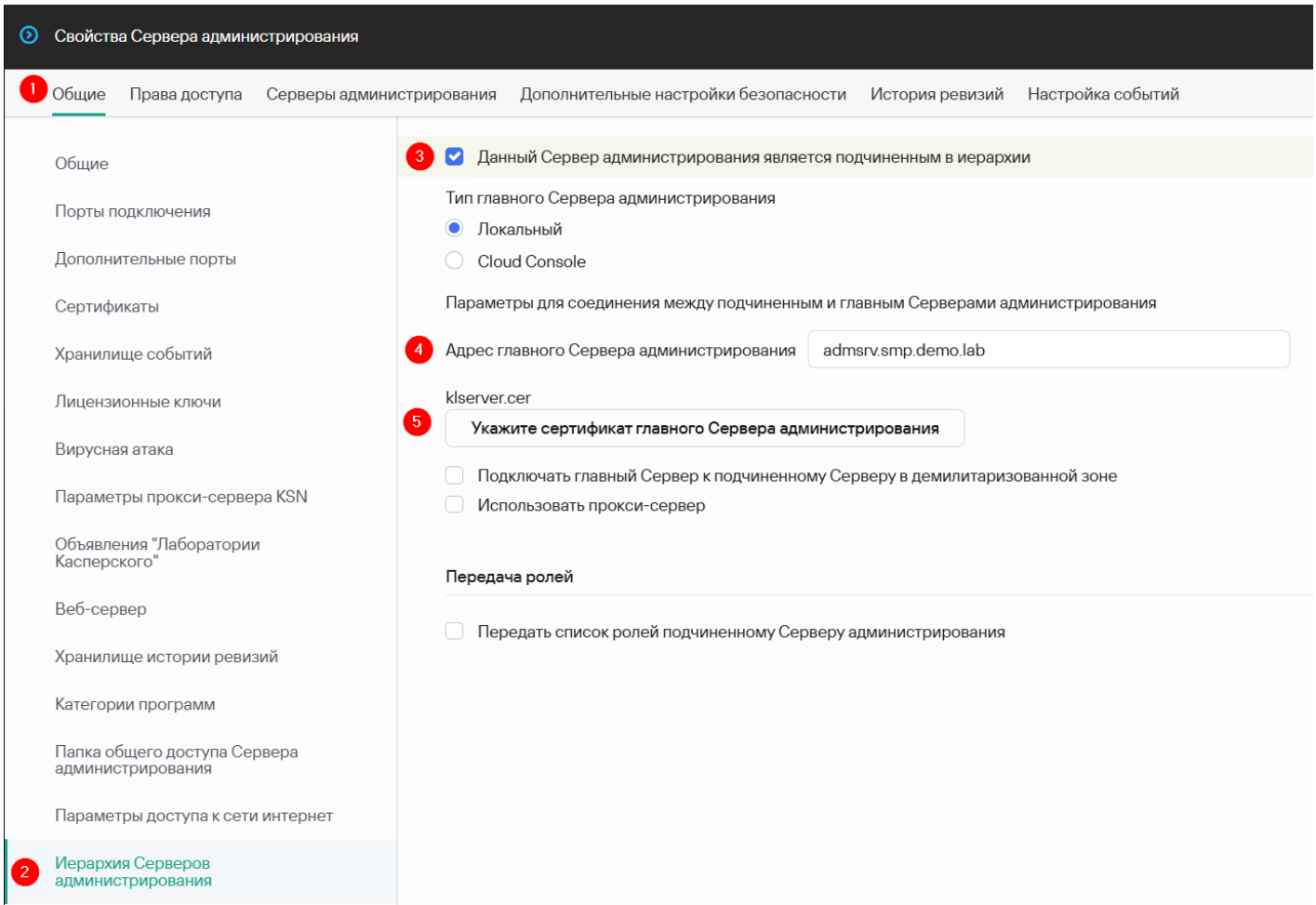
5. Если было сделано верно, то в окне отобразится сертификат подчиненного Сервера администрирования. После этого следует нажать кнопку **Далее** внизу окна. В результате

будет отображена инструкция по действиям, которые необходимо выполнить на подчиненном Сервере администрирования. После ознакомления следует нажать кнопку **Готово**.

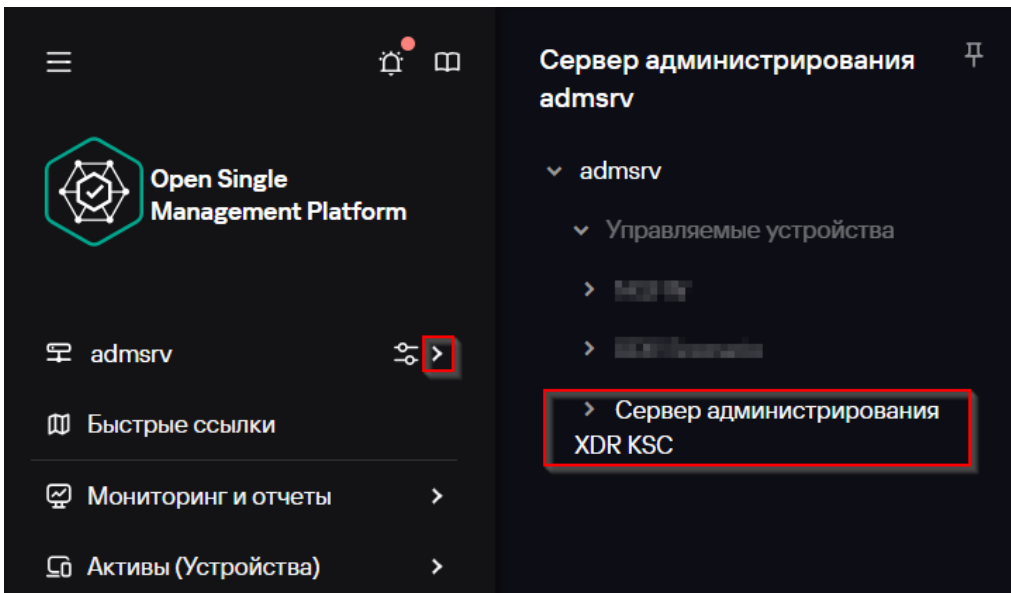
6. Для продолжения настройки необходимо перейти в интерфейс подчиненного Сервера администрирования и перейти в настройки



7. На вкладке **Общие** в разделе **Иерархия Серверов администрирования** необходимо поставить галочку в пункте **Данный Сервер администрирования является подчиненным в иерархии**. Далее появятся дополнительные настройки, где необходимо указать адрес и сертификат главного Сервера администрирования (были получены на шаге 1 данной инструкции) и нажать кнопку **Сохранить**.



Если все было сделано верно, то в консоли SMP появится подчиненный Сервер администрирования, а также возможность перейти в него.



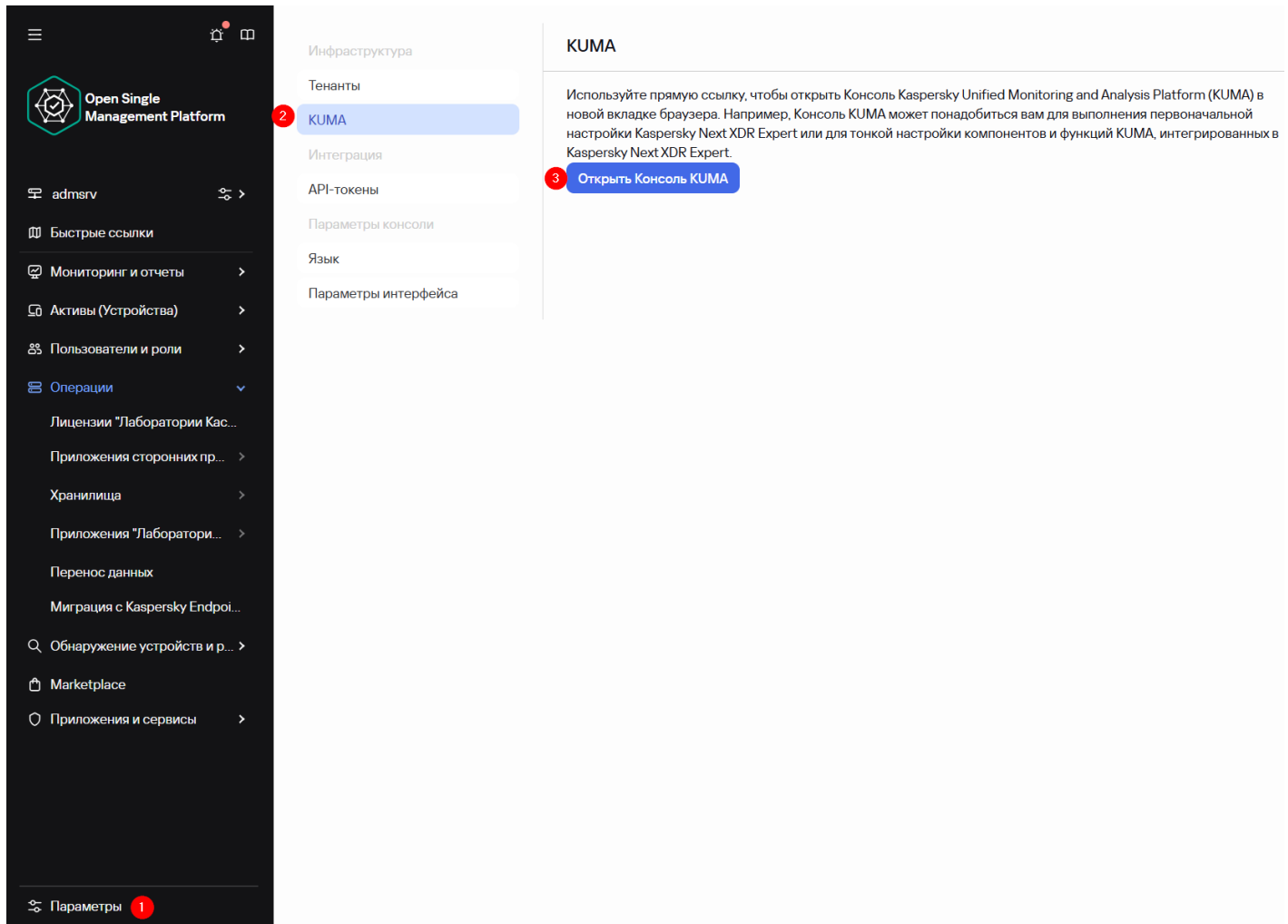
????????? ?????????????? ??????????

??????? Root



Настраивать интеграцию для тенанта Root разрешается, но не рекомендуется по причине того, что все сервисы KUMA по умолчанию находятся в тенанте Main, либо других тенантах. Поэтому для корректного отображения активов в событиях рекомендуется настраивать получение активов в тенанты отличные от Root.

1. Если получение активов планируется в тенанте Root, то для начала необходимо открыть консоль KUMA. Для этого нужно перейти в **Параметры - KUMA** и нажать на кнопку **Открыть Консоль KUMA**



2. В консоли KUMA необходимо открыть **Параметры - Kaspersky Security Center** и нажать на **Root tenant**

Кaspersky
Unified Monitoring and Analysis Platform

Выбрано тенантов: 3

Панель мониторинга

События

Активы

Отчеты

Ресурсы

CyberTrace

Диспетчер задач

Параметры 1

Доступ

Тенанты

Доступ к пространствам

Анализ угроз

Kaspersky CyberTrace

Интеграции

Kaspersky Security Center 2

KICS/KATA

Kaspersky Automated Security Awareness Platform

Kaspersky Endpoint Detection and Response

LDAP-сервер

AI-сервисы

Интеграция с Kaspersky Security Center по тенантам

<input type="checkbox"/> Тенант	Выключено
<input type="checkbox"/> Root tenant 3	✓


3. Интеграция для тенанта Root настроена автоматически, но по умолчанию отключена. Для включения интеграции необходимо снять галочку с параметра **Выключено** и нажать кнопку **Сохранить**.

Выключено

Активы KSC, информация об оборудовании

Интервал обновления в часах


1

 Запланированное обновление: **задача скоро будет запущена**

Атрибуты активов KSC (уязвимости, программное обеспечение, владельцы)

Интервал обновления в часах

12

 Запланированное обновление: **задача скоро будет запущена**

Тенант*

Root tenant

Подключения

Имя	Выключено
Root	
<u>XDR KSC</u>	

Сохранить

Интеграция настроена.

?????? ?? Root

Рекомендуемый способ

Для получения активов с подключенного KSC необходимо выполнить следующие шаги.

1. Перейти в **Параметры - Тенанты** и выбрать необходимый тенант для интеграции. В примере ниже для интеграции будет использован тенант **Main**.

Open Single Management Platform

admsrv

Быстрые ссылки

Мониторинг и отчеты

Активы (Устройства)

Пользователи и роли

Операции

Лицензии "Лаборатории Кас..."

Приложения сторонних пр...

Хранилища

Приложения "Лаборатори..."

Перенос данных

Миграция с Kaspersky Endpoi...

Обнаружение устройств и р...

Marketplace

Приложения и сервисы

Параметры

Инфраструктура

Тенанты 2

KUMA

Интеграция

API-токены

Параметры консоли

Язык

Параметры интерфейса

Тенанты

Список содержит только tenants, на про...
Обратите внимание. Вы не можете удал...

+ Добавить × Удалить

Имя

Root tenant

Main

Shared

2. В настройках тенанта необходимо перейти на вкладку **Параметры** в раздел **KSC** и нажать **Привязать Сервер администрирования**

Интеграция с приложениями
"Лаборатории Касперского"

KATA/KEDR

2 KSC

Kaspersky TIP

Интеграция с приложениями
сторонних производителей

Пользовательская интеграция

Интеграция Kaspersky Security Center

Настройте интеграцию Kaspersky Next XDR Expert и Kaspersky Security Center, которые используются для управления устройствами тенанта. [Как настроить](#)

3 [Привязать Сервер администрирования](#) [Отменить привязку](#)

Имя Сервера

Статус привязки

В открывшемся окне необходимо выбрать Сервер администрирования, с которым настроена иерархия и нажать кнопку **Привязать**, а затем нажать кнопку **Сохранить** для сохранения всех настроек.

Привязать Сервер администрирования к тенанту

Выберите Сервер администрирования, который вы хотите привязать к существующей иерархии в свойствах Сервера администрирования.

▼ Root

 XDR KSC

После этого необходимо открыть консоль KUMA. Для этого нужно перейти в **Параметры - KUMA** и нажать на кнопку **Открыть Консоль KUMA**

Инфраструктура

Тенанты

2 KUMA

Интеграция

API-токены

Параметры консоли

Язык

Параметры интерфейса

KUMA

Используйте прямую ссылку, чтобы открыть Консоль Kaspersky Unified Monitoring and Analysis Platform (KUMA) в новой вкладке браузера. Например, Консоль KUMA может понадобиться вам для выполнения первоначальной настройки Kaspersky Next XDR Expert или для тонкой настройки компонентов и функций KUMA, интегрированных в Kaspersky Next XDR Expert.

3 Открыть Консоль KUMA

Параметры **1**

В консоли KUMA необходимо открыть Параметры Kaspersky Security Center и выбрать тенант, для которого была настроена привязка

Интеграция с Kaspersky Security Center по тенантам

Тенант	Выключено
<input type="checkbox"/> Main 3	✓
<input type="checkbox"/> Root tenant	✓

Доступ

Тенанты

Доступ к пространствам

Анализ угроз

Kaspersky CyberTrace

Интеграции

2 Kaspersky Security Center

KICS/KATA

Kaspersky Automated Security Awareness Platform

Kaspersky Endpoint Detection and Response

LDAP-сервер

AI-сервисы

Панель мониторинга

События

Активы

Отчеты

Ресурсы

CyberTrace

Диспетчер задач

Параметры **1**

Выбрано тенантов: 3


Интеграция настраивается автоматически после привязки, но выключена по умолчанию. Для ее включения необходимо снять галочку с параметра Выключено и нажать кнопку Сохранить.

Выключено

Активы KSC, информация об оборудовании

Интервал обновления в часах


1

 Запланированное обновление: **задача скоро будет запущена**

Атрибуты активов KSC (уязвимости, программное обеспечение, владельцы)

Интервал обновления в часах

12

 Запланированное обновление: **задача скоро будет запущена**

Тенант*

Main

Подключения

Имя	Выключено
XDR KSC	

Интеграция настроена.

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

1. Для проверки успешности интеграции необходимо в консоли KUMA на вкладке **Параметры - Kaspersky Security Center** перейти в требуемый тенант для проверки и нажать кнопку **Импортировать активы KSC**.

Импортировать активы KSC

Импортировать атрибуты активов KSC

Выключено

Активы KSC, информация об оборудовании

Интервал обновления в часах

1

⚠ Запланированное обновление: 03.12.2025 15:51:44

Атрибуты активов KSC (уязвимости, программное обеспечение, владельцы)

Интервал обновления в часах

12

⚠ Запланированное обновление: 04.12.2025 02:51:43

Тенант*

Main

Подключения

Имя

Выключено

XDR KSC

2. После этого следует перейти в **Диспетчер задач** и убедиться, что задача завершена успешно и в свойствах отображено количество полученных активов.

Диспетчер задач

Отображать только свои

Состояние	Задача	Создал	Создана	Время обновления	Тенант
<input checked="" type="checkbox"/> Завершено	Импорт атрибутов активов KSC	admin	03.12.2025 14:51:18	03.12.2025 14:51:25	Main
<input checked="" type="checkbox"/> Завершено	Импорт активое KSC	admin	03.12.2025 14:51:17	03.12.2025 14:51:19	Main

Информация о задаче

Скачано

8