????????? SMP

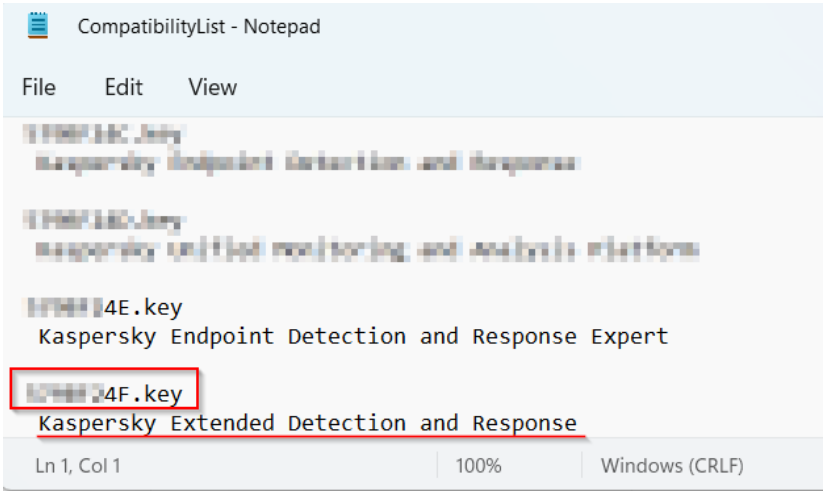
- Добавление лицензии с функционалом XDR
- Создание пользователя в SMP
- Интеграция SMP с KSC

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

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

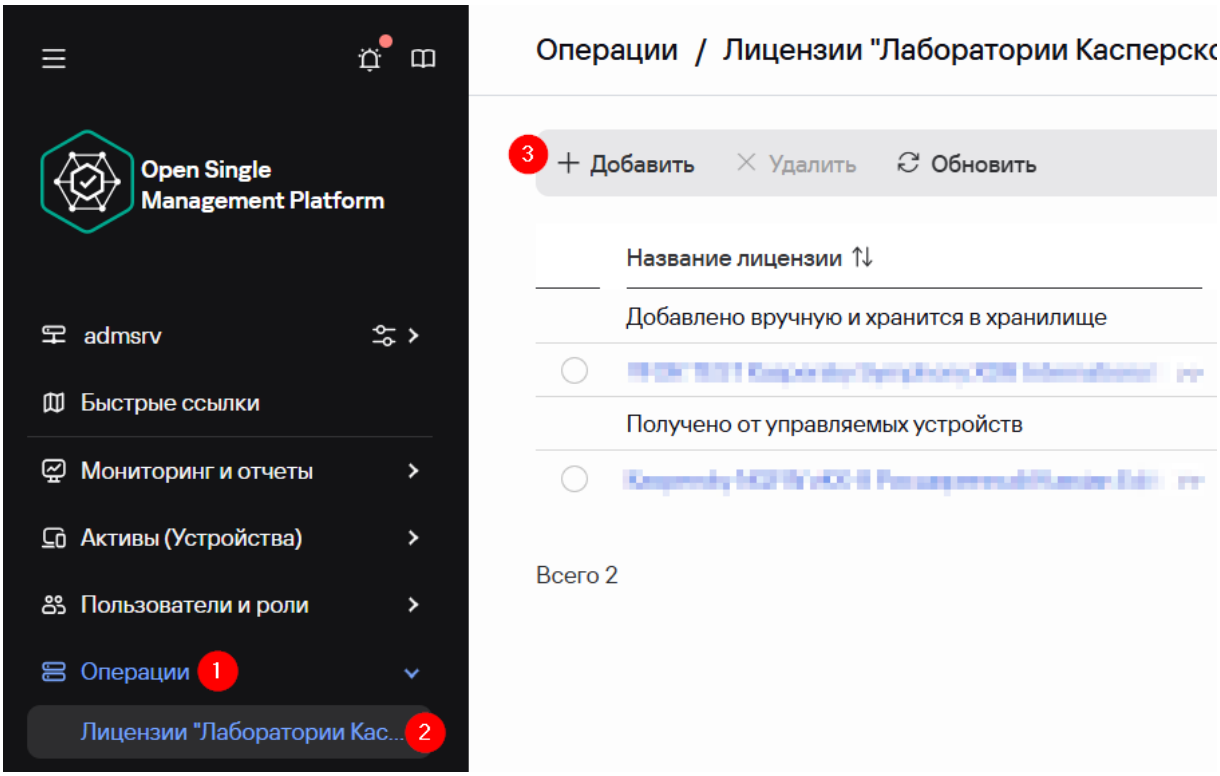
После установки SMP для доступа к функционалу XDR (алерты, инциденты с графом расследования, плейбуки и прочее) необходимо добавить лицензию на функционал. Для этого необходимо выполнить следующее:

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!)

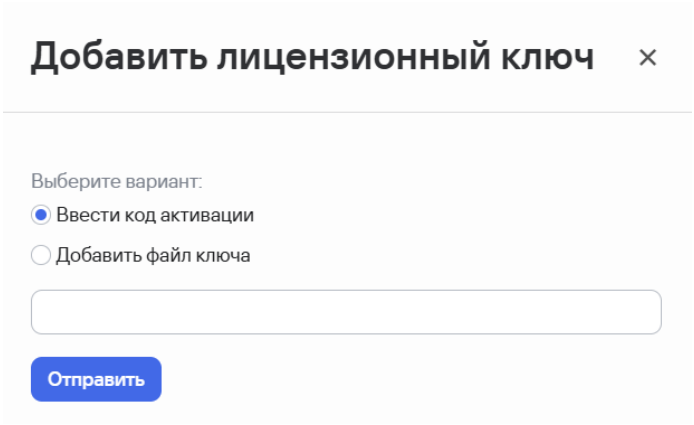


2. Зайти в веб-интерфейс консоли под встроенной учетной записью `admin`, либо под другой с аналогичными правами.

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

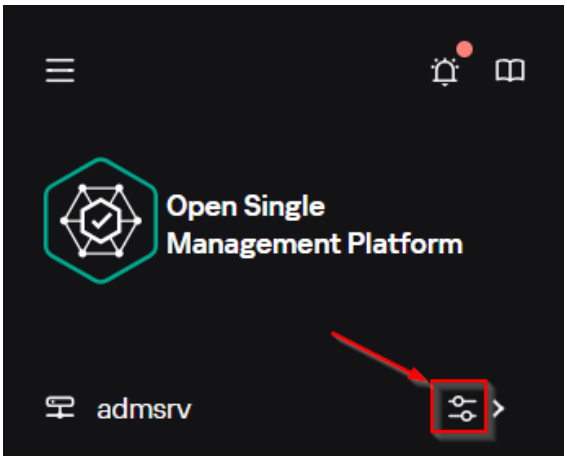


4. В появившемся окне можно либо ввести код активации, который доступен в архиве с лицензиями в файле `ActivationCodes*.txt`, либо загрузить файл ключа, полученный на шаге 1.

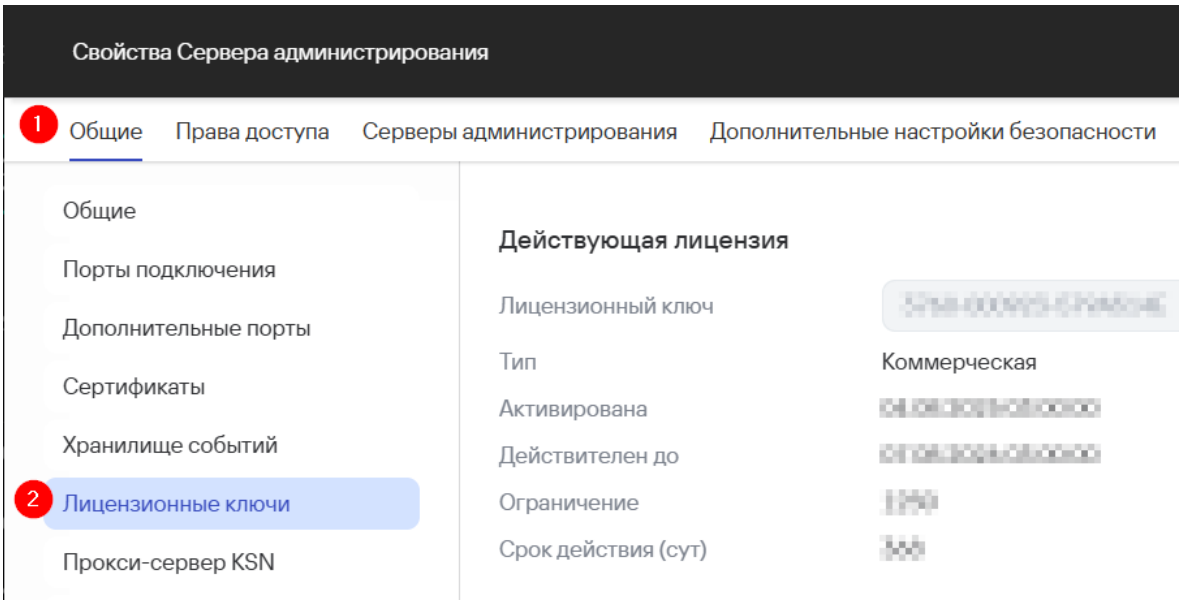


После добавления ключ отобразится в таблице с лицензиями.

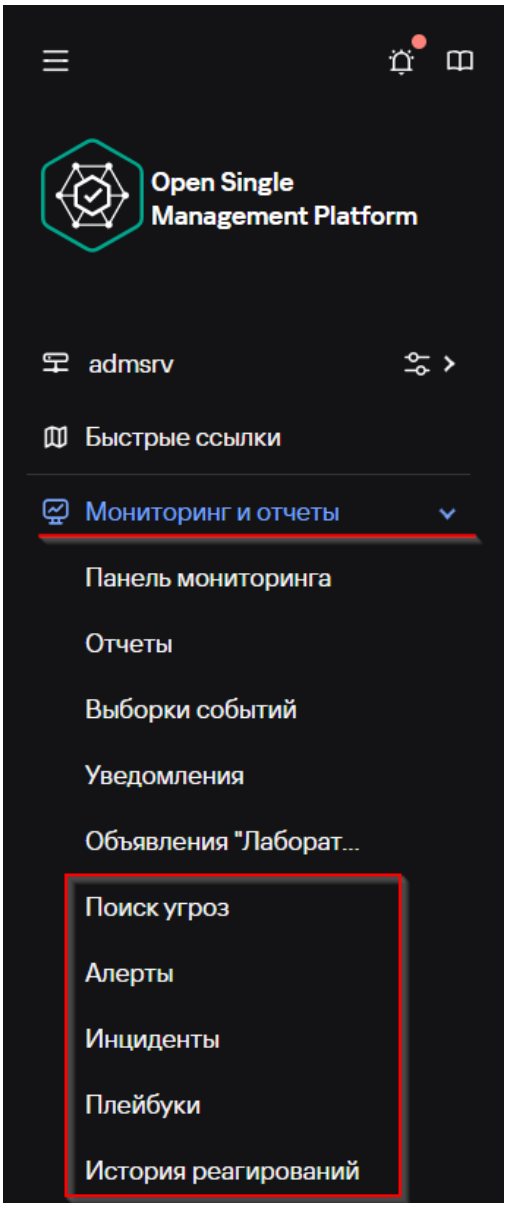
5. Далее необходимо перейти в настройки щелкнув по соответствующему значку в верхней части интерфейса



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

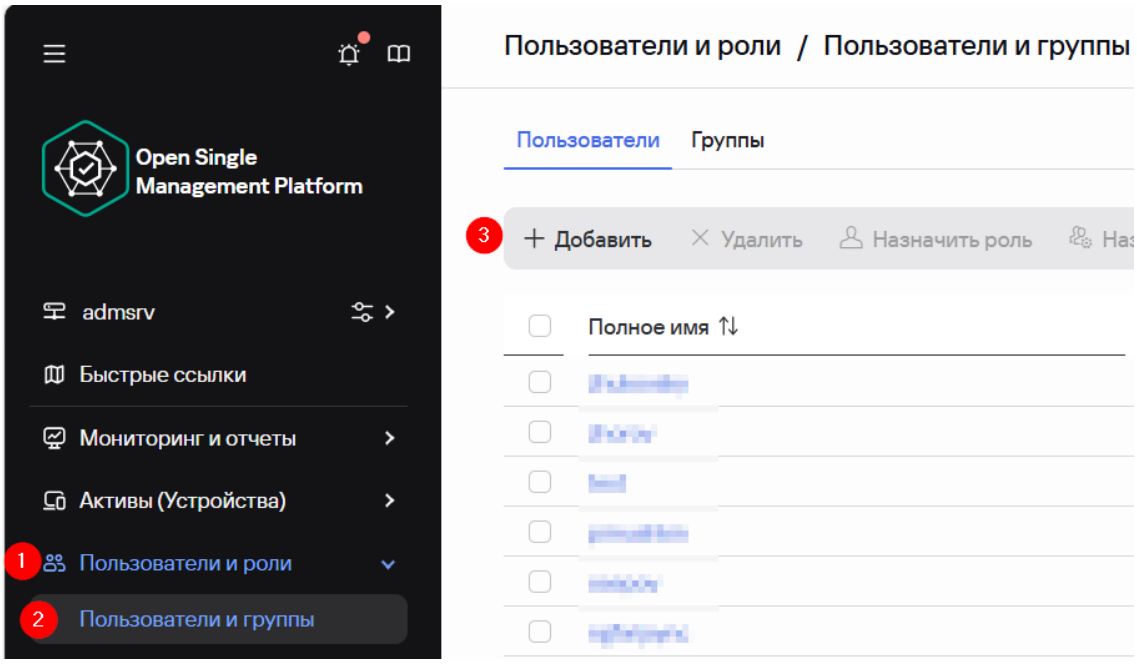
???????? ????????????? ? SMP

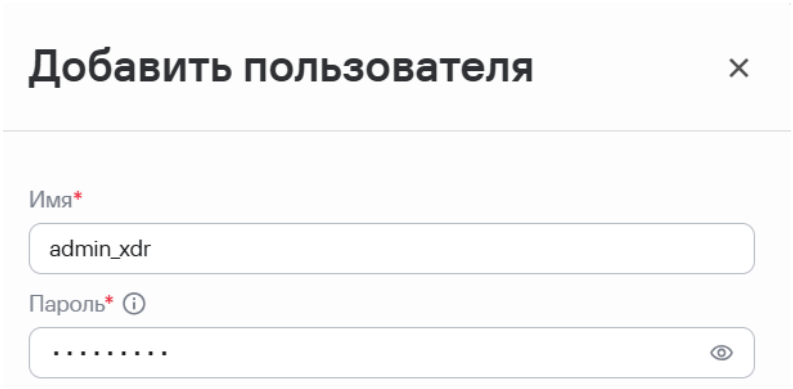
> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

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

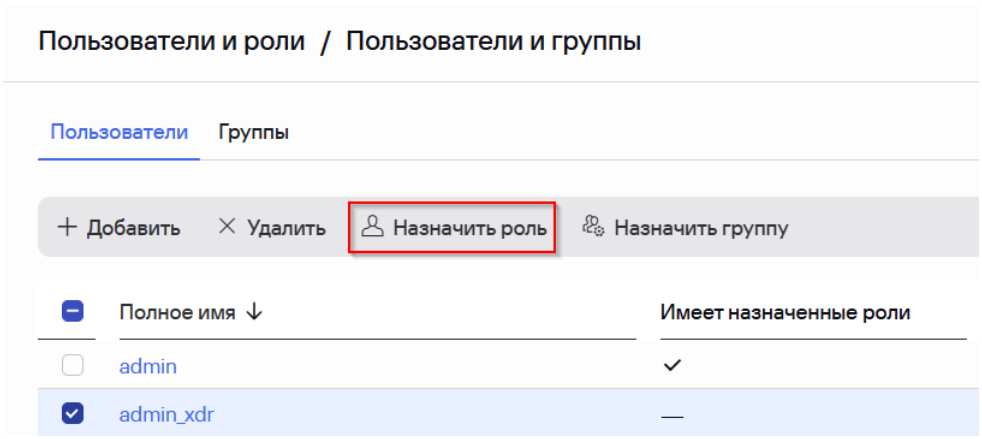
Для создания пользователя и назначения ему прав для доступа ко всему функционалу XDR необходимо выполнить следующие действия

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).

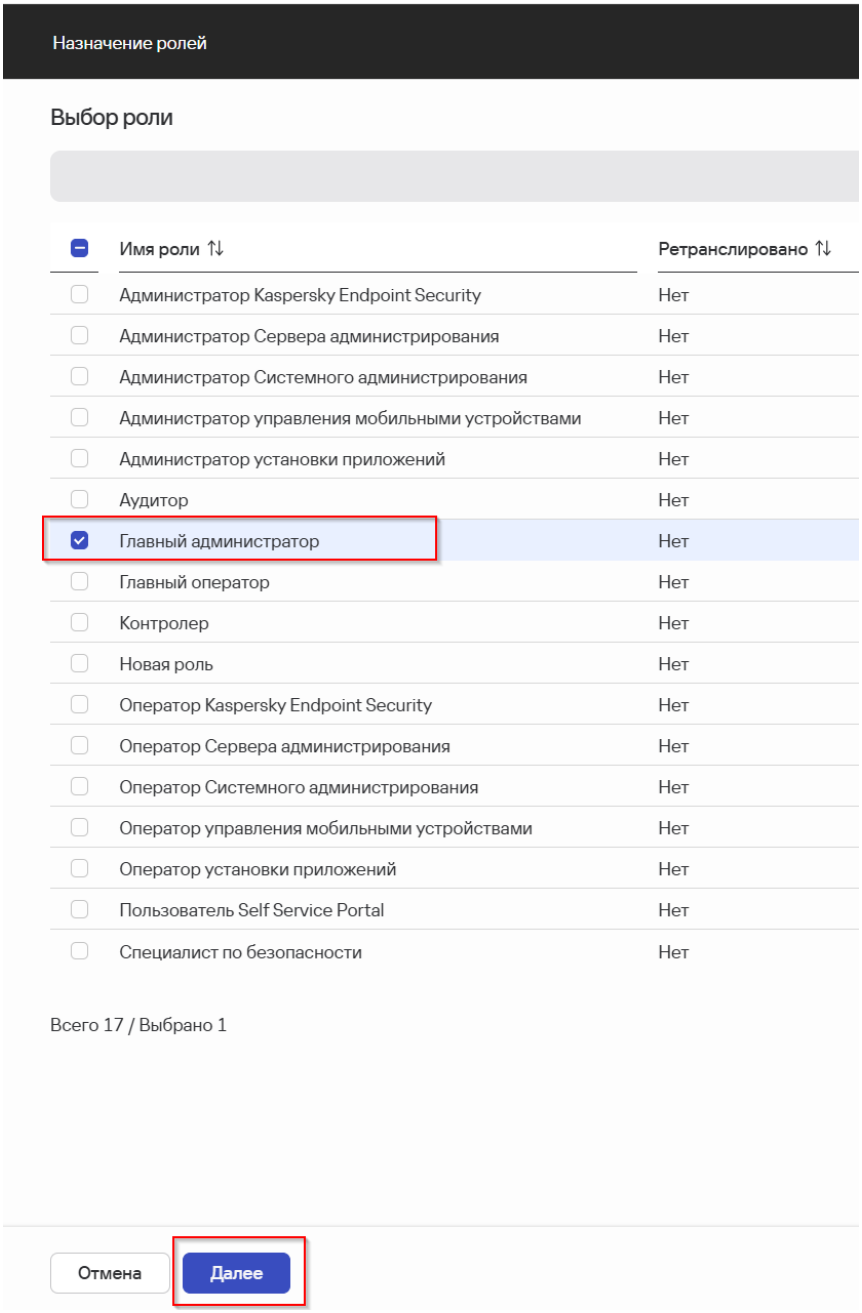




2. После добавления локального пользователя (либо при наличии доменного, полученного через интеграцию с AD) необходимо назначить роль. Для этого выберите галочкой нужного пользователя и нажмите **Назначить роль**.



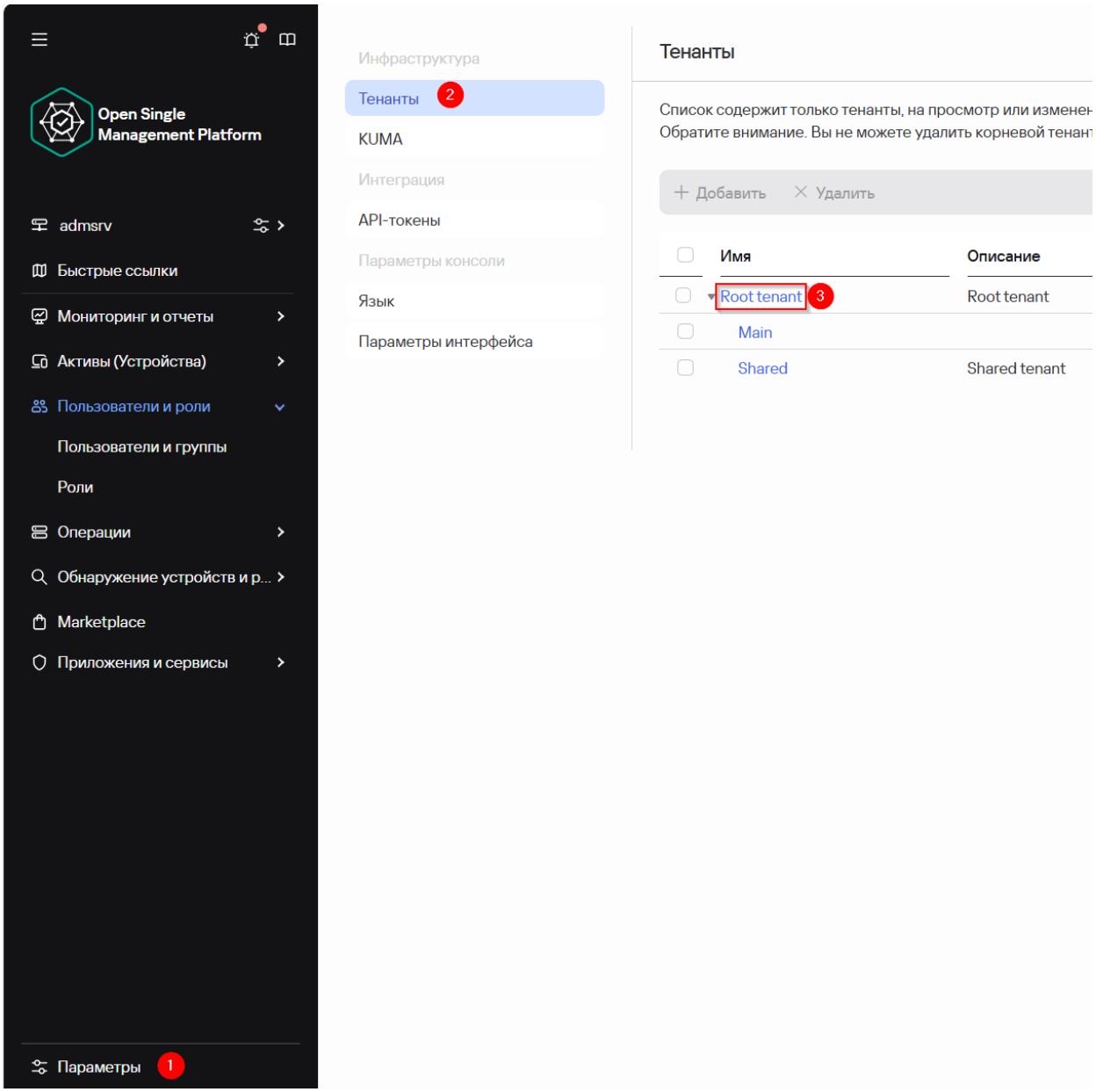
3. Выберите необходимую роль галочкой и нажмите далее



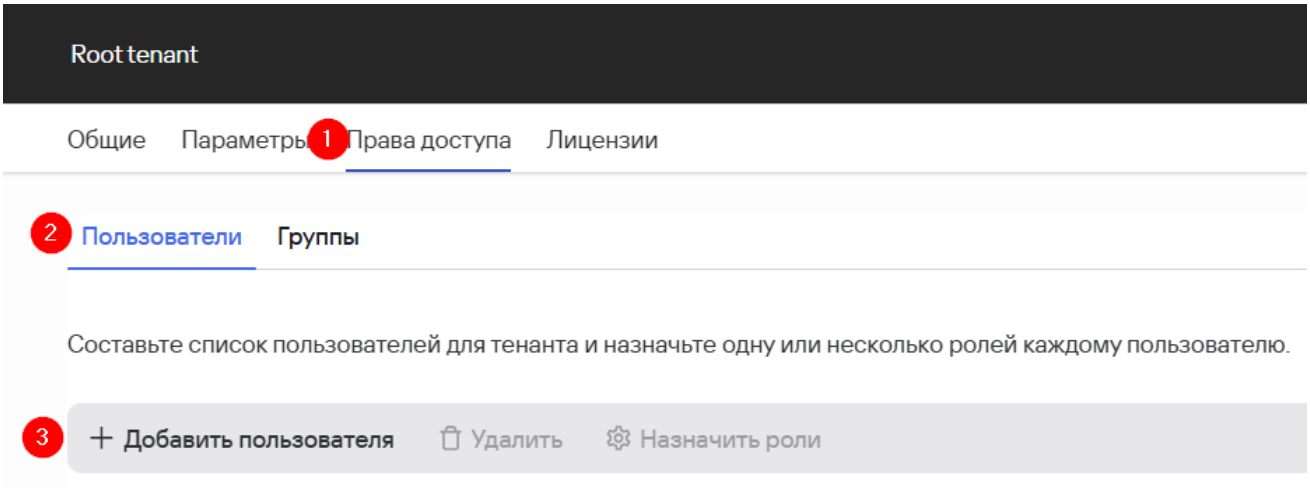
4. Выберите область действия и нажмите **Готово**

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

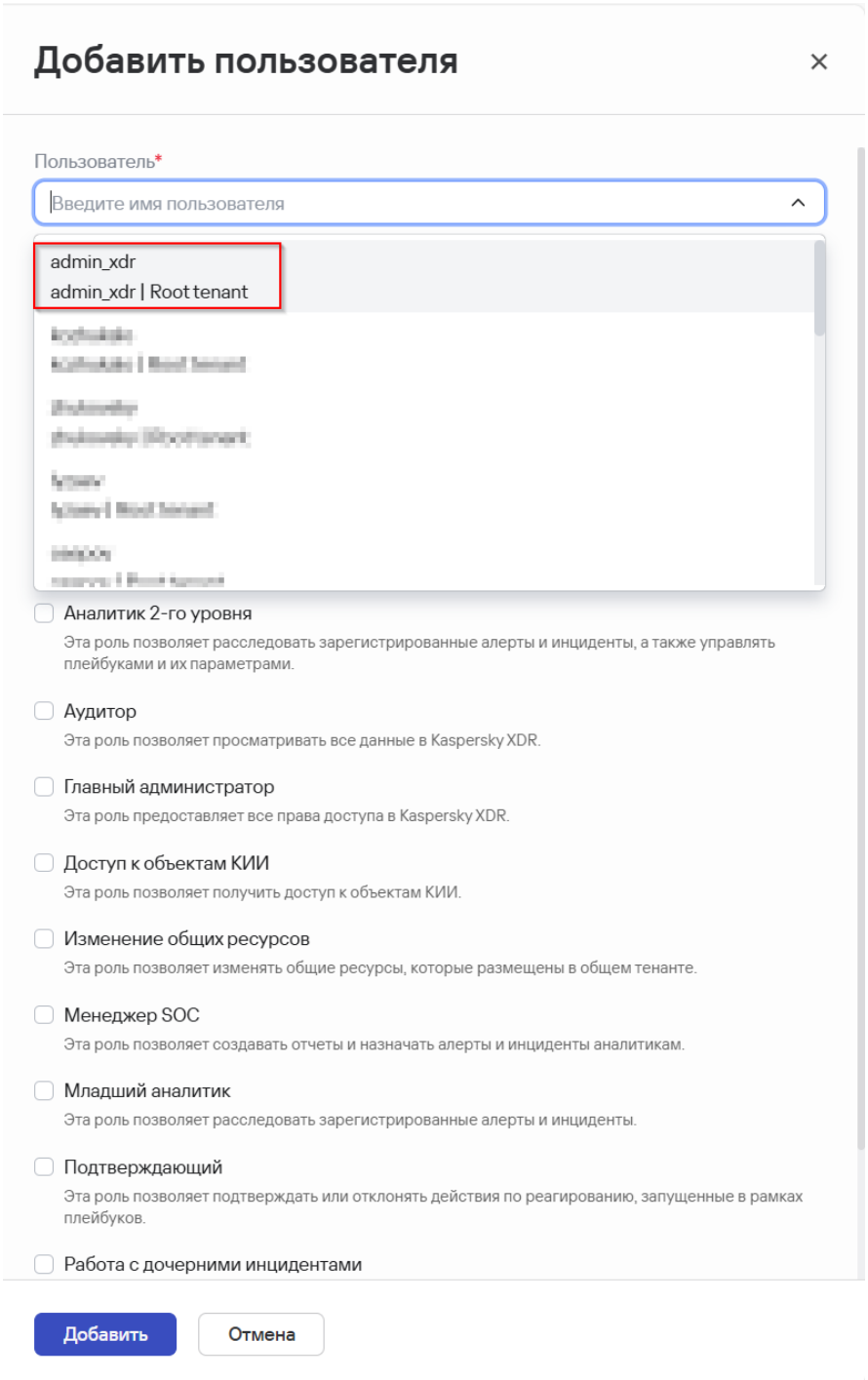


5. В открывшемся окне перейдите на вкладку **Права доступа**, в раздел **Пользователи** и нажмите на кнопку **Добавить пользователя**

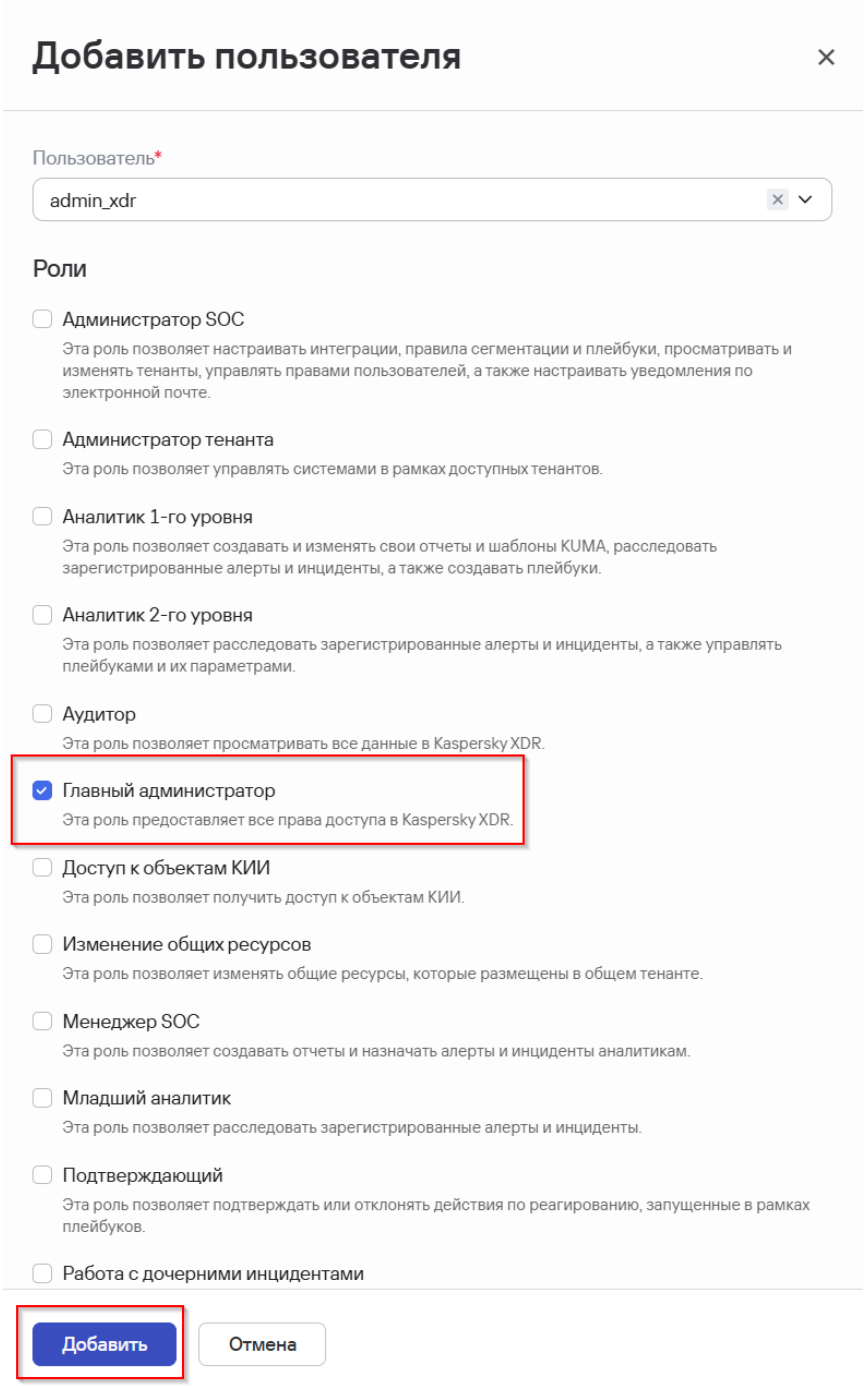


6. В выпадающем списке выберите нужного пользователя, которому собираетесь назначить роль

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



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



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 подченных KSC к SMP решает сразу несколько задач:

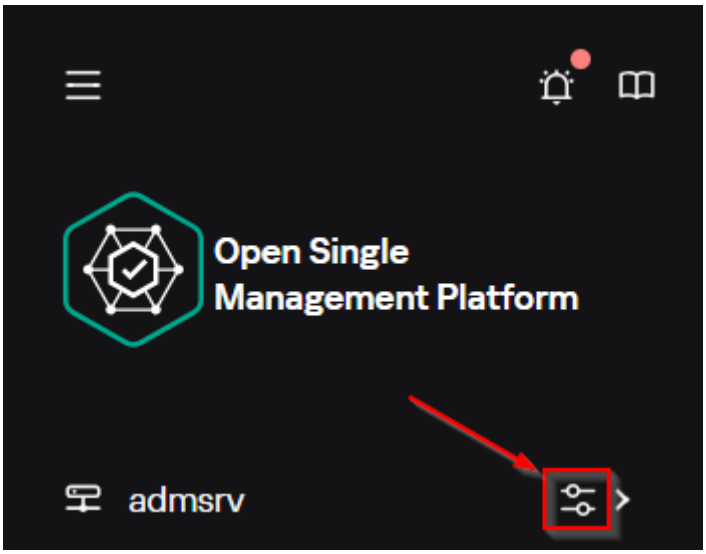
1. Управление подчиненными KSC и конечными точками
2. Возможность сбора актива, для отображения их в событиях, алертах и инцидентах
3. Возможность реагирования на активах как вручную, так и с помощью плейбуков.

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

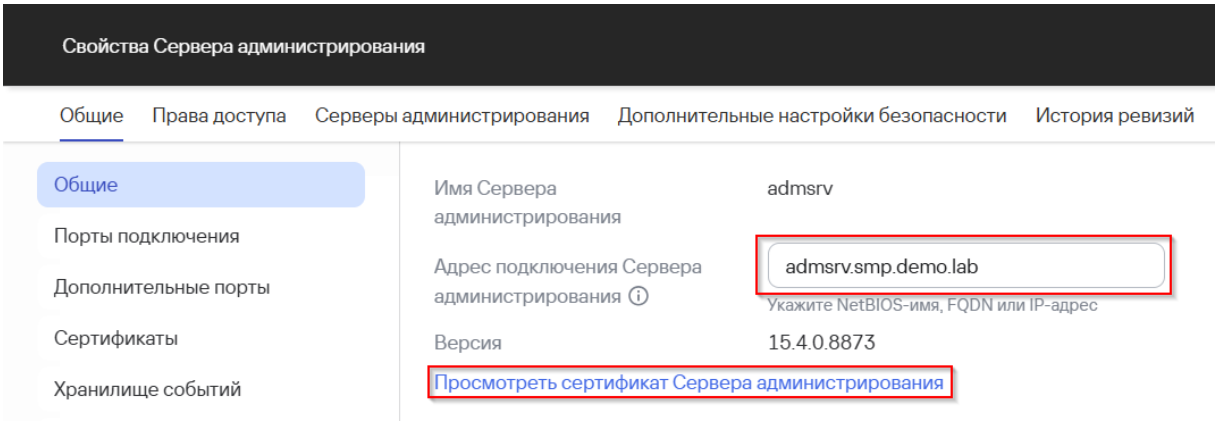
Для настройки всесторонней интеграции необходимо создать иерархию Серверов администрирования, а затем настроить получения активов с подчиненного Сервера администрирования. Рассмотрим необходимые шаги по порядку.

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

1. Перейти в настройки встроенного в SMP KSC

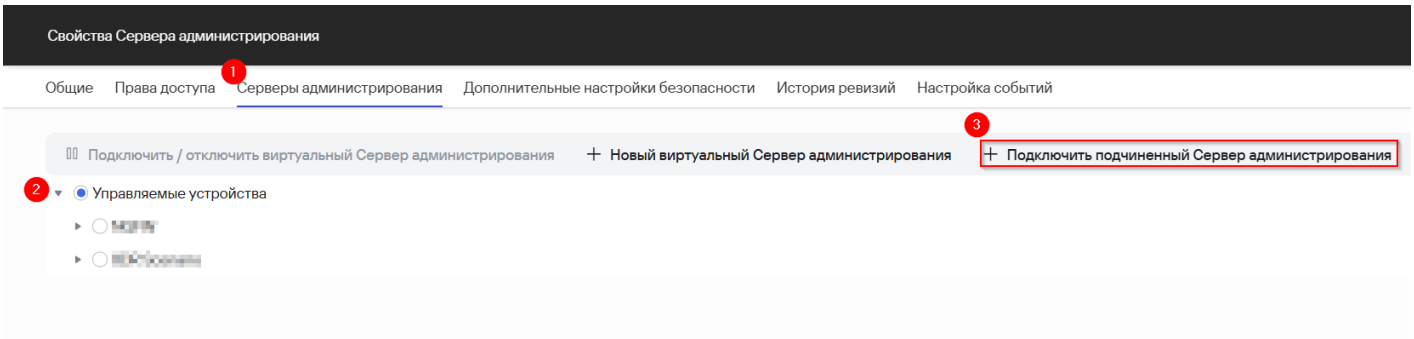


2. На вкладе **Общие** в разделе **Общие** необходимо записать **Адрес подключения Сервера администрирования**, а также скачать сертификат Сервера администрирования по ссылке "**Просмотреть сертификат Сервера администрирования**"

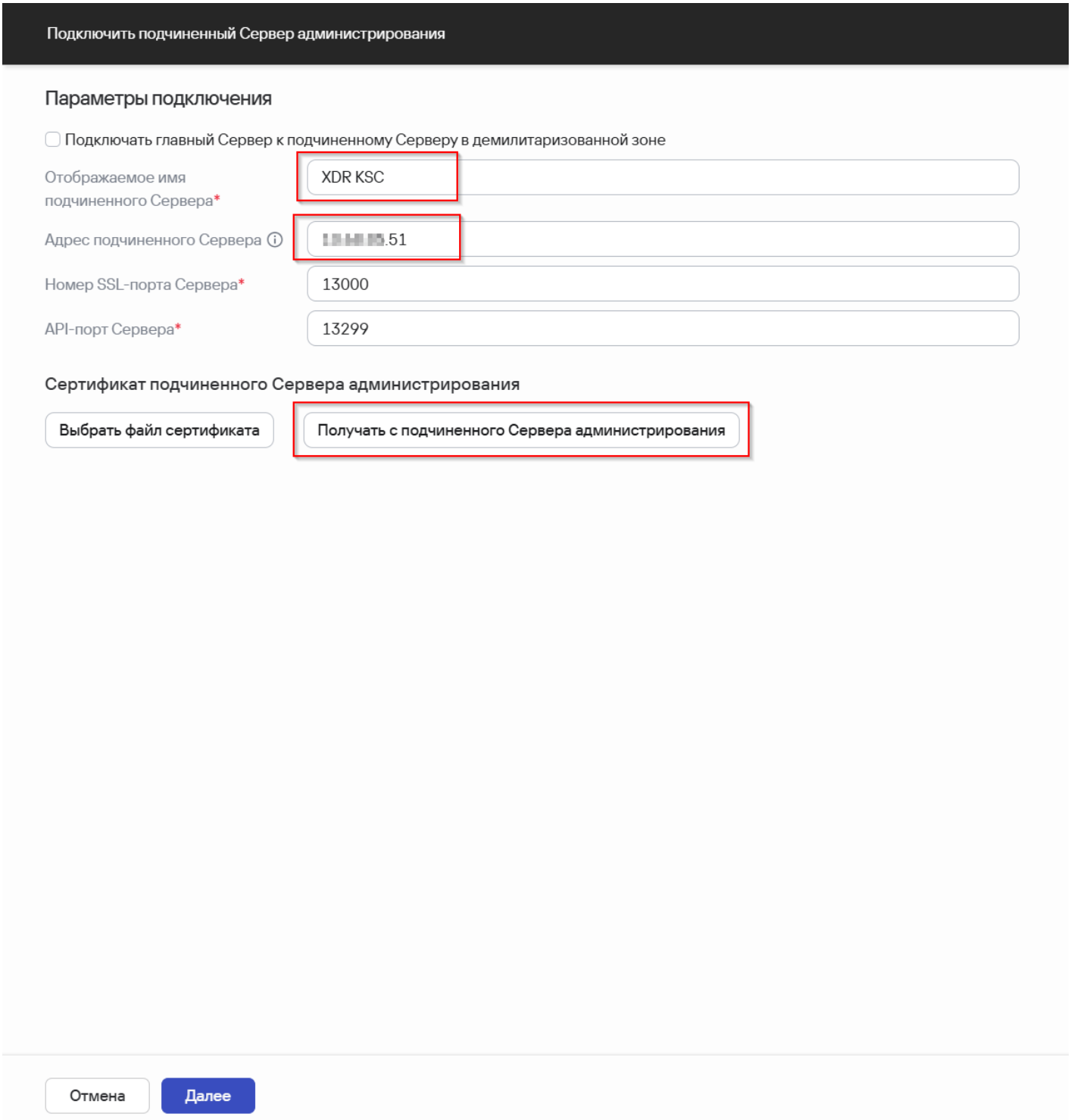


> Важно! Для организации иерархии необходимо использовать именно доменное имя (FQDN) сервера администрирования, встроенного в KSC. Использование IP недопускается.

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



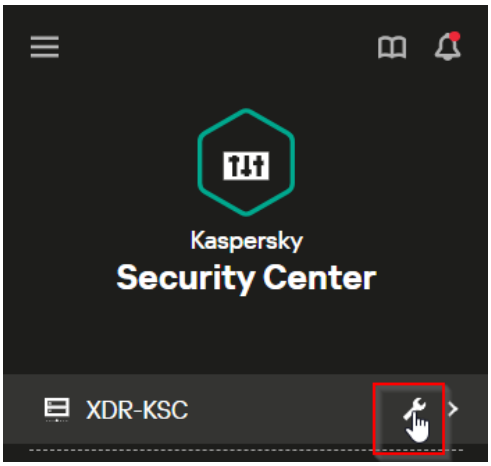
4. В появившемся окне необходимо заполнить параметры, подключаемого Сервера администрирования. В общем случае достаточно указать имя Сервера администрирования, которое будет отображаться в консоли, а также адрес подчиненного Сервера администрирования (здесь можно использовать как IP, так и доменное имя). 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).



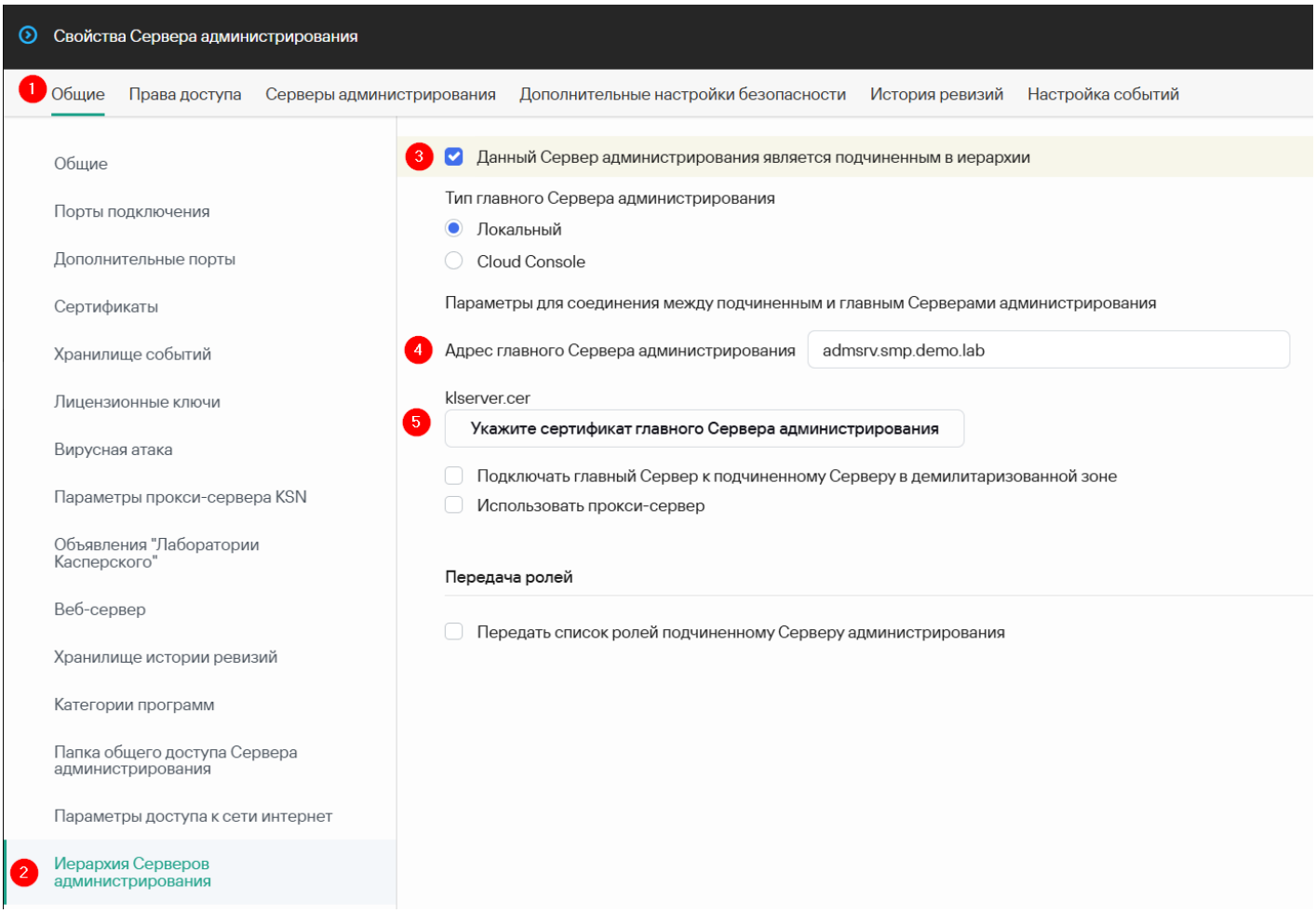
5. Если было сделано верно, то в окне отобразится сертификат подчиненного Сервера администрирования. После этого следует нажать кнопку **Далее** внизу окна. В результате

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

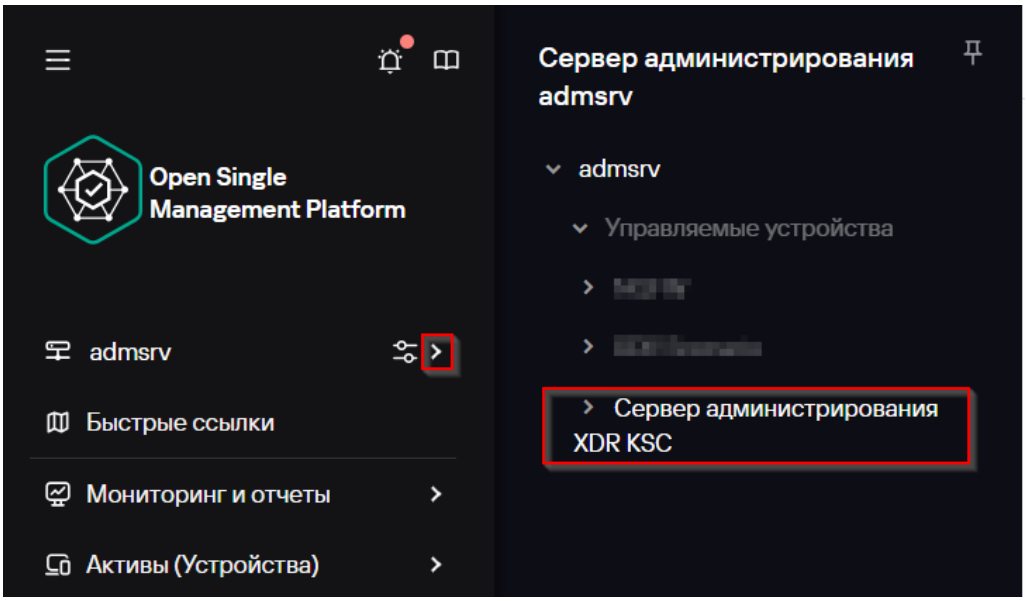
6. Для продолжения настройки необходимо перейти в интерфейс подчиненного Сервера администрирования и перейти в настройки



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.

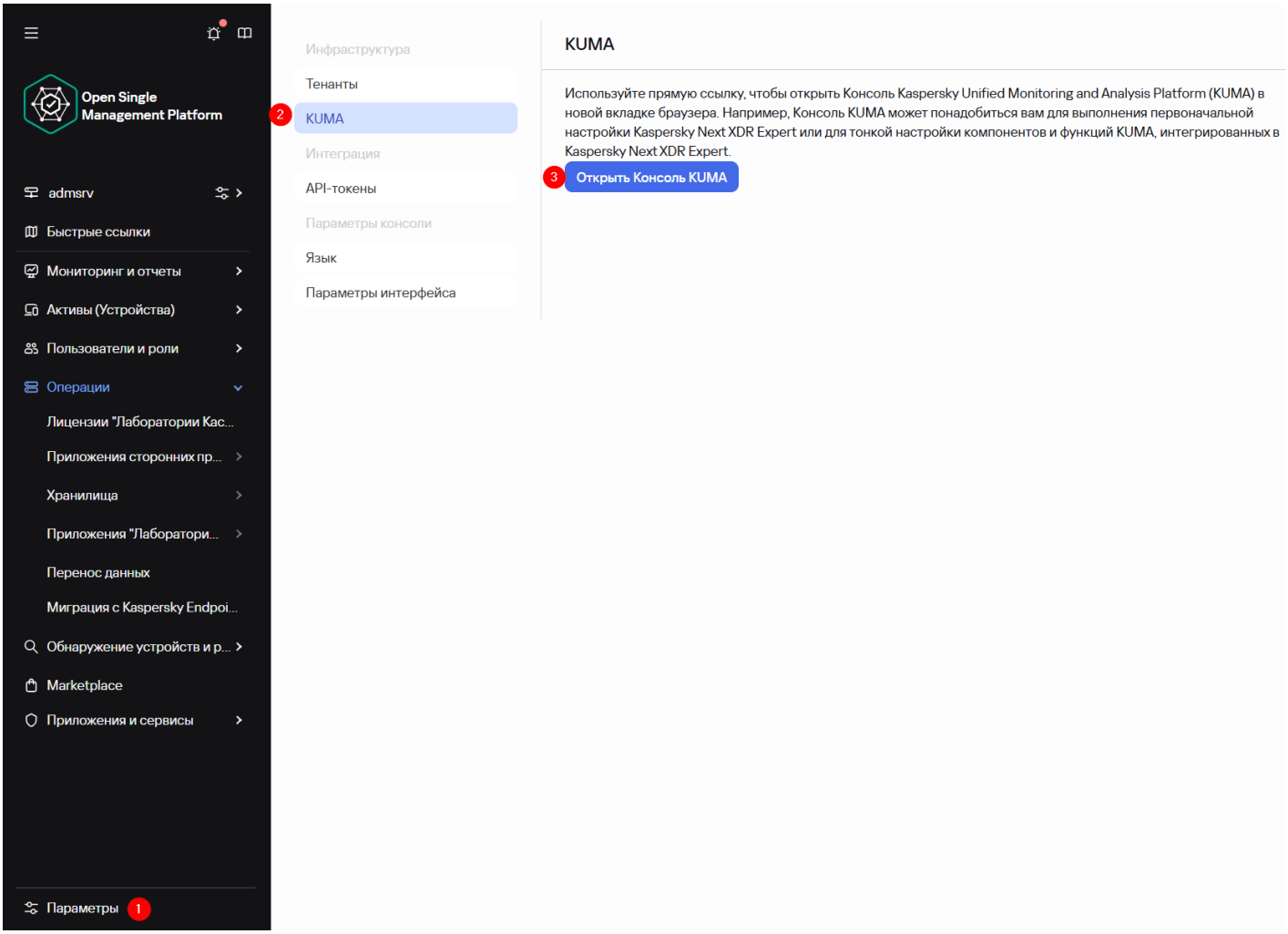


????????? ????????? ???????

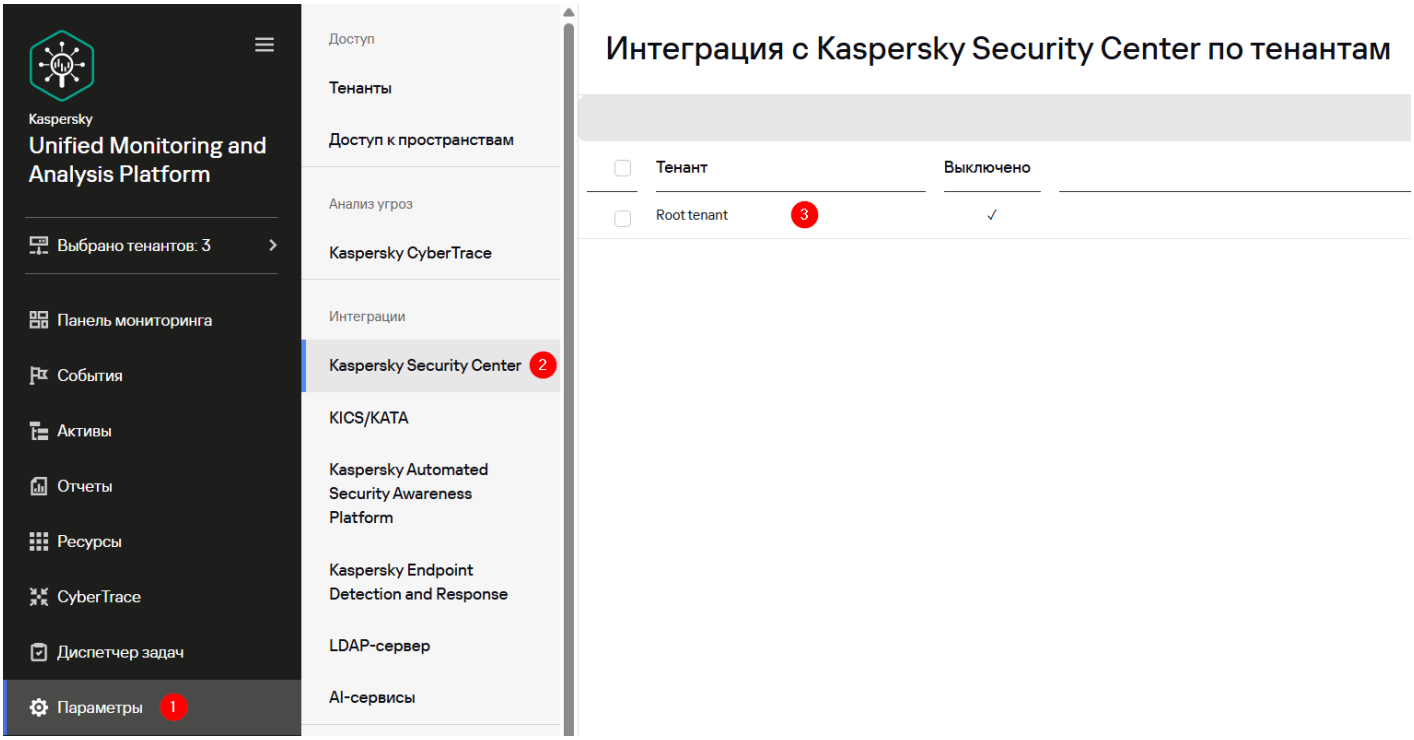
?????? Root

> 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 отлчиные от Root.

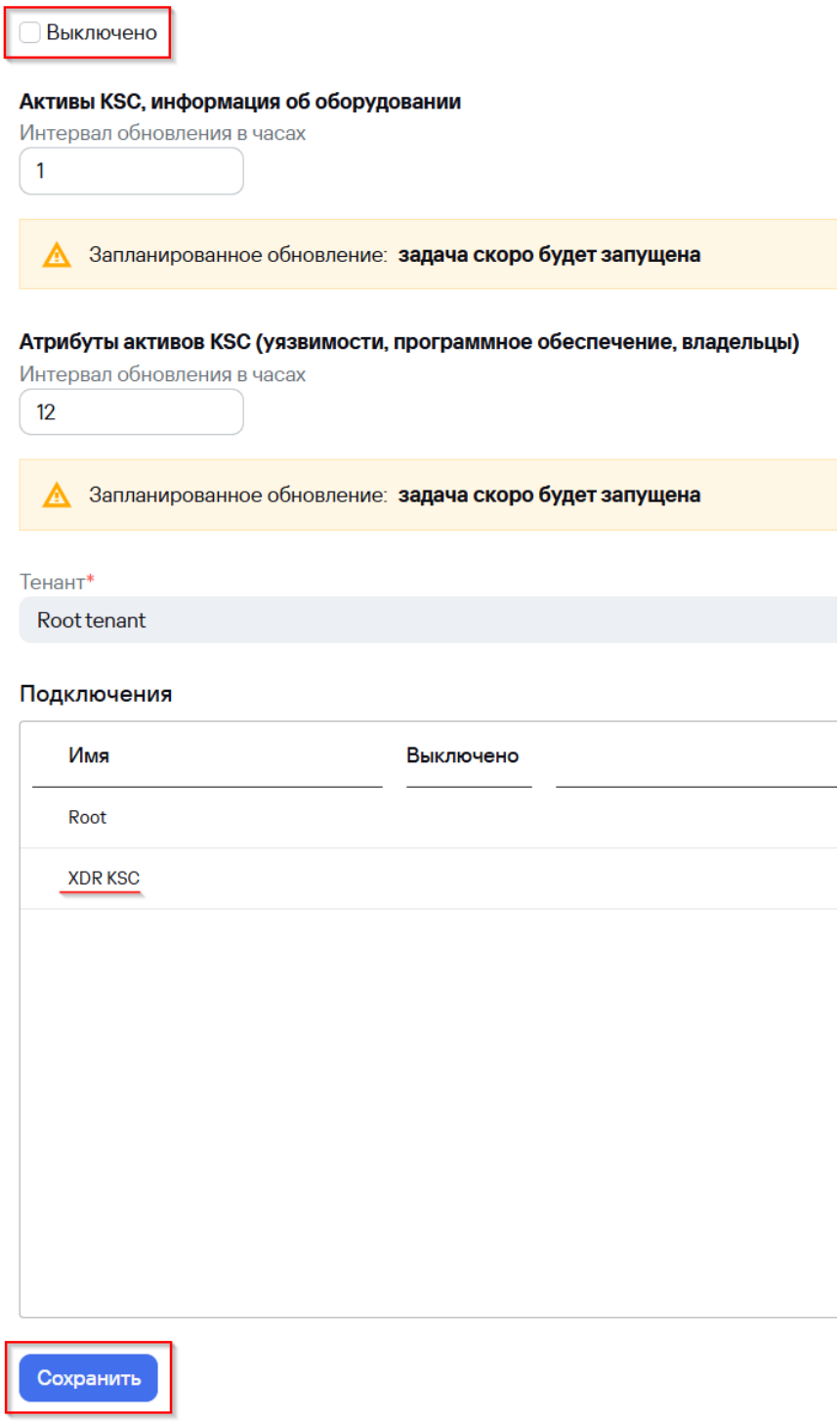
1. Если получение активов планируется в тенанте Root, то для начала необходимо открыть консоль KUMA. Для этого нужно перейти в **Параметры** - **KUMA** и нажать на кнопку **Открыть Консоль KUMA**



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



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



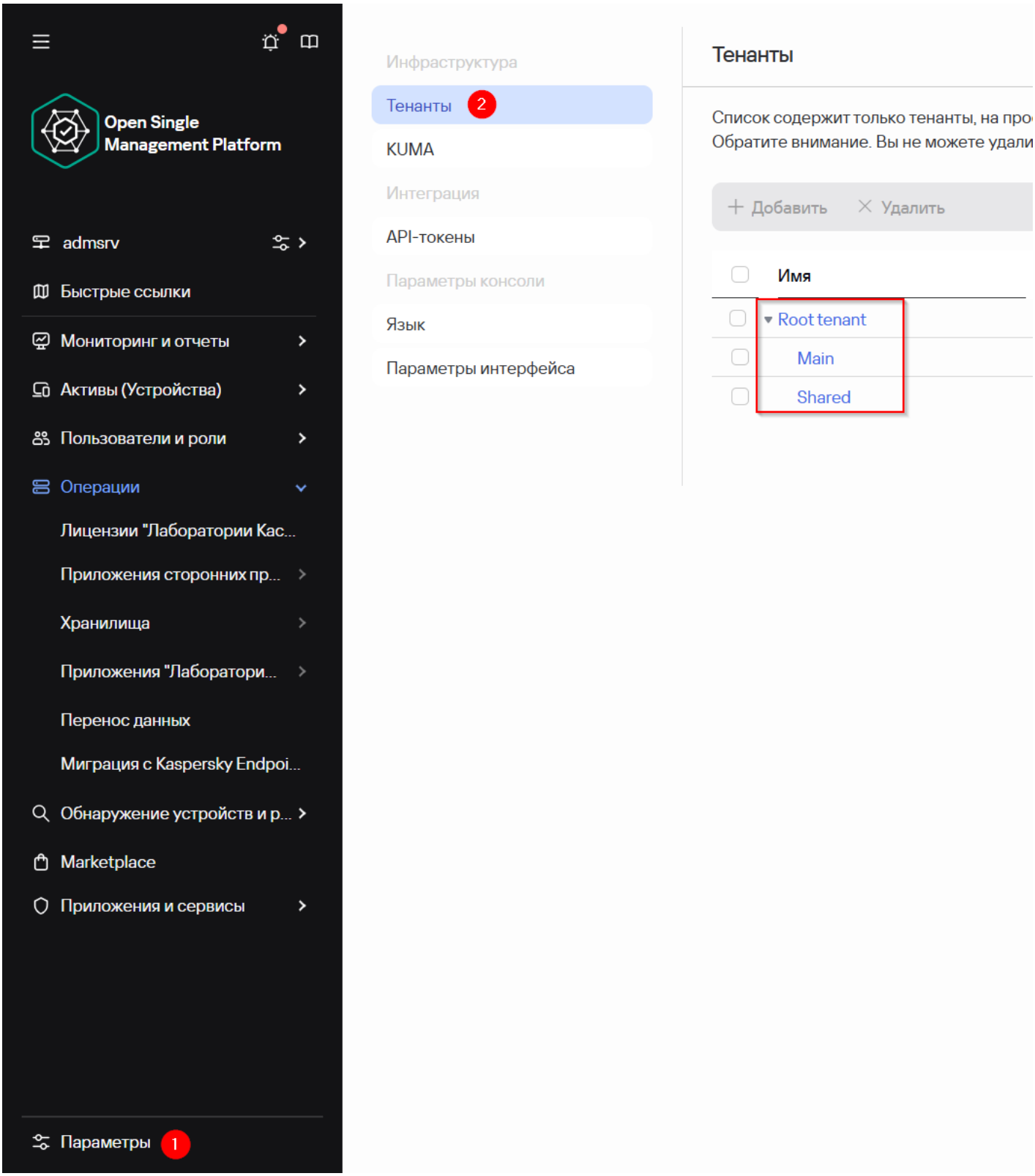
Интеграция настроена.

?????? ?? Root

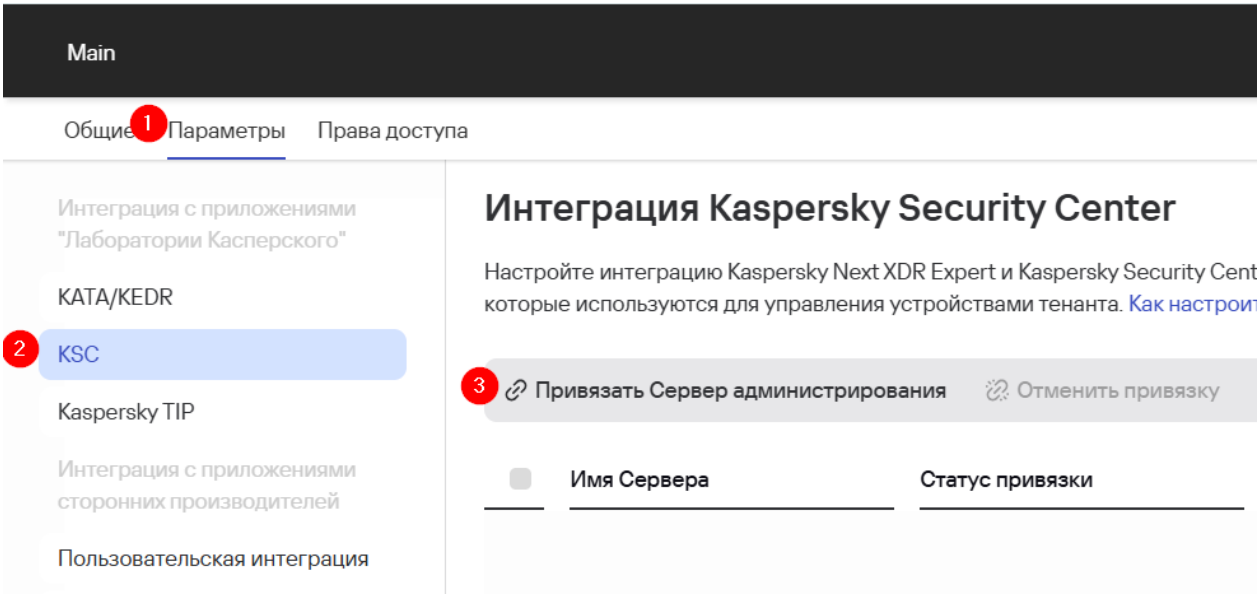
> Рекомендуемый способ

Для получения активов с подключенного KSC необходимо выполнить следующие шаги.

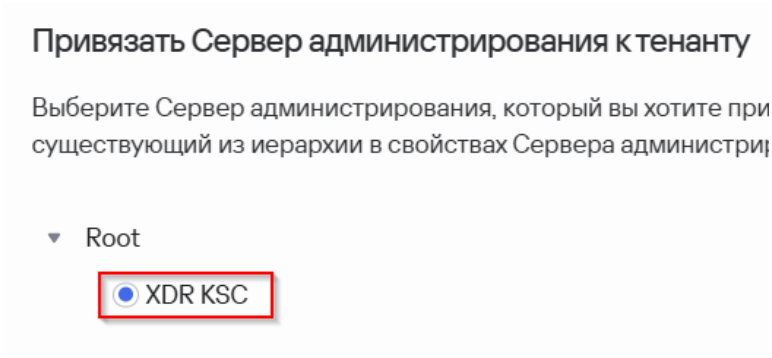
1. Перейти в **Параметры** - **Тенанты** и выбрать необходимый тенант для интеграции. В примере ниже для интеграции будет использован тенант **Main.**



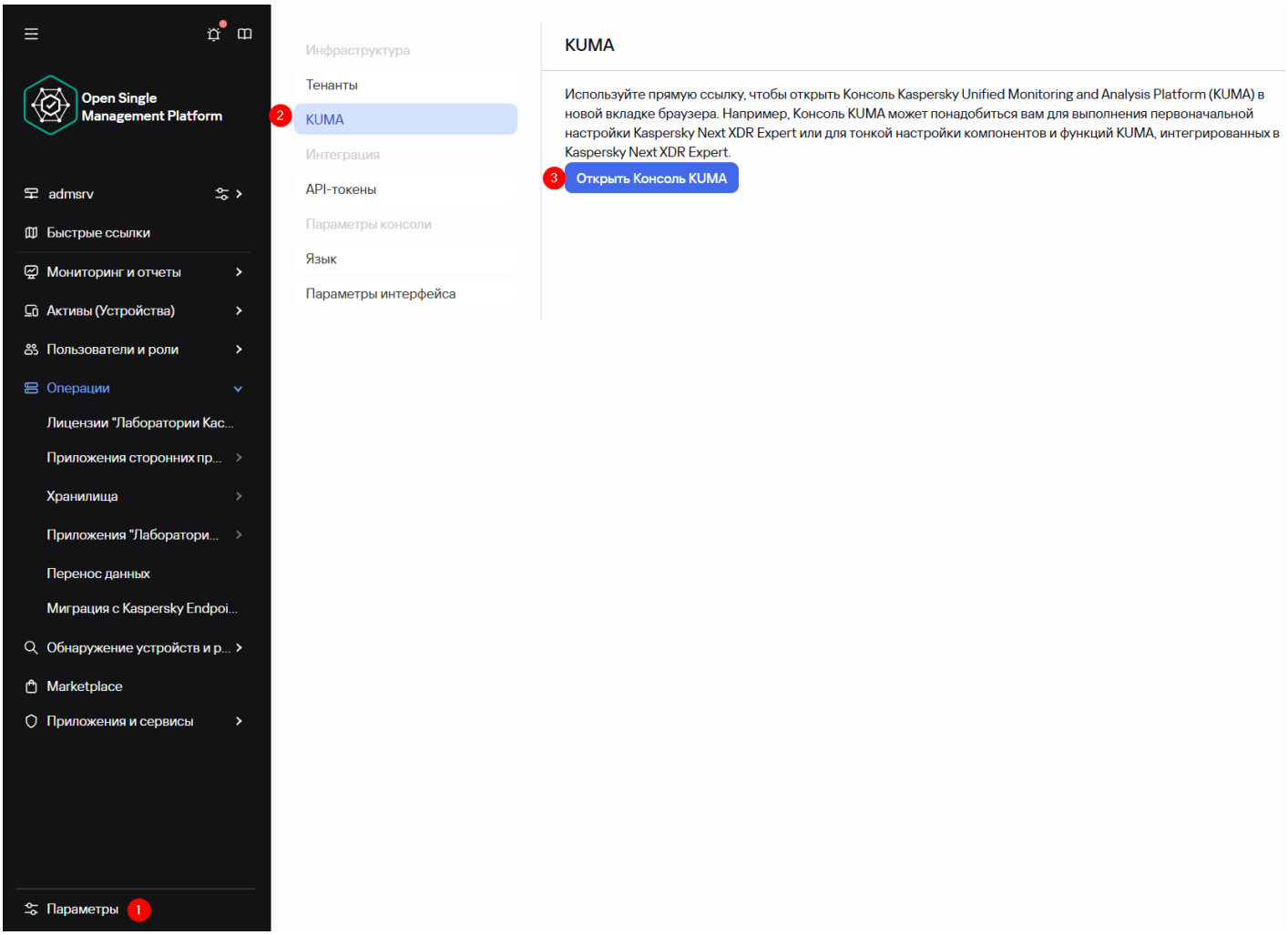
2. В настройках тенанта необходимо перейти на вкладку **Параметры** в раздел **KSC** и нажать **Привязать Сервер администрирования**



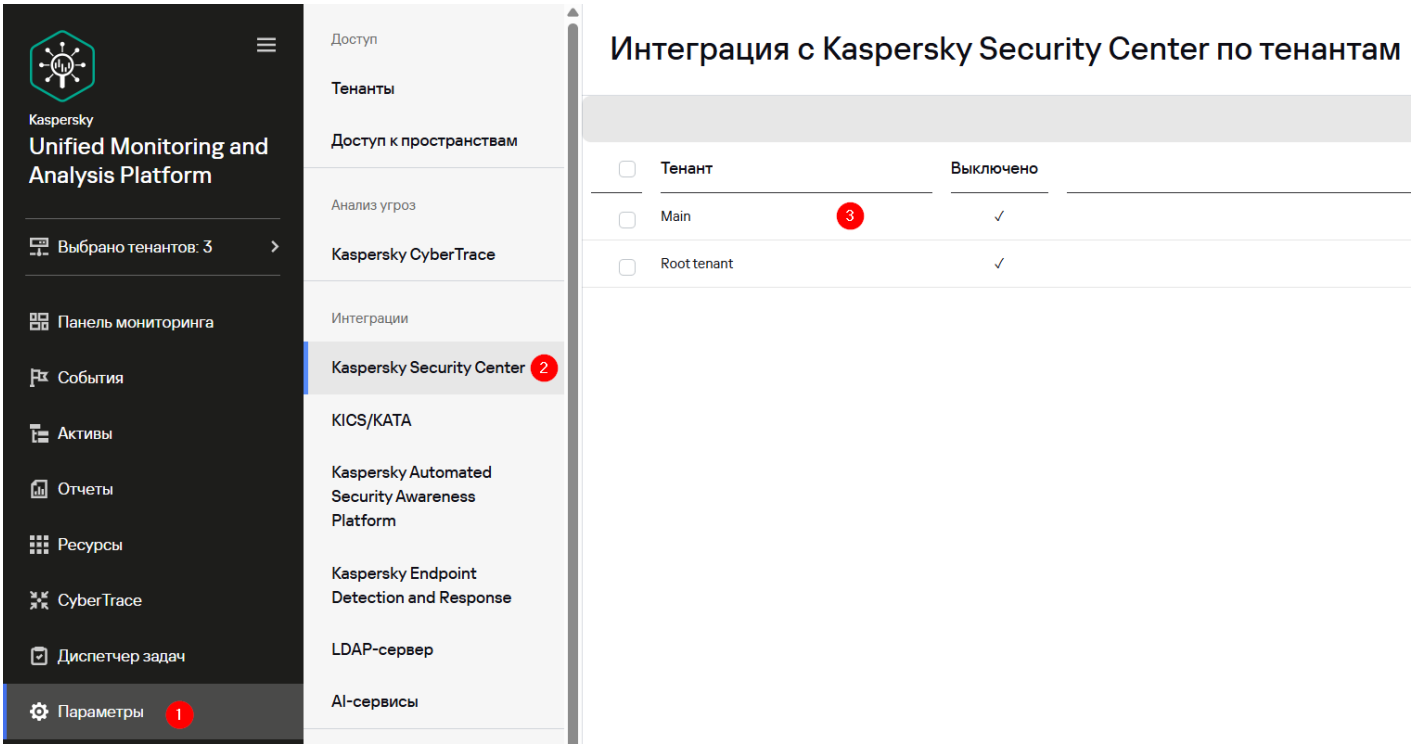
В открывшемся окне необходимо выбрать Сервер администрирования, с которым настроена ирерархия и нажать кнопку **Привязать**, а затем нажать кнопку **Сохранить** для сохранения всех настроек.



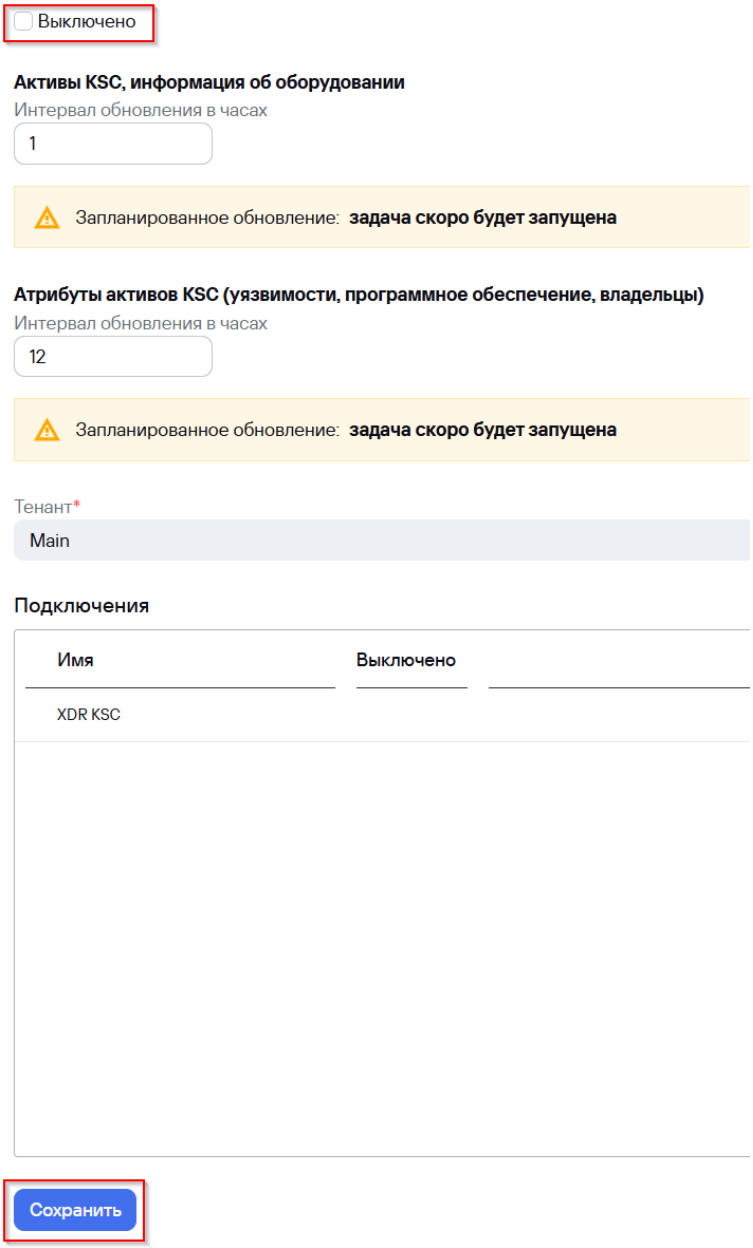
После этого необходимо открыть консоль KUMA. Для этого нужно перейти в **Параметры** - **KUMA** и нажать на кнопку **Открыть Консоль KUMA**



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



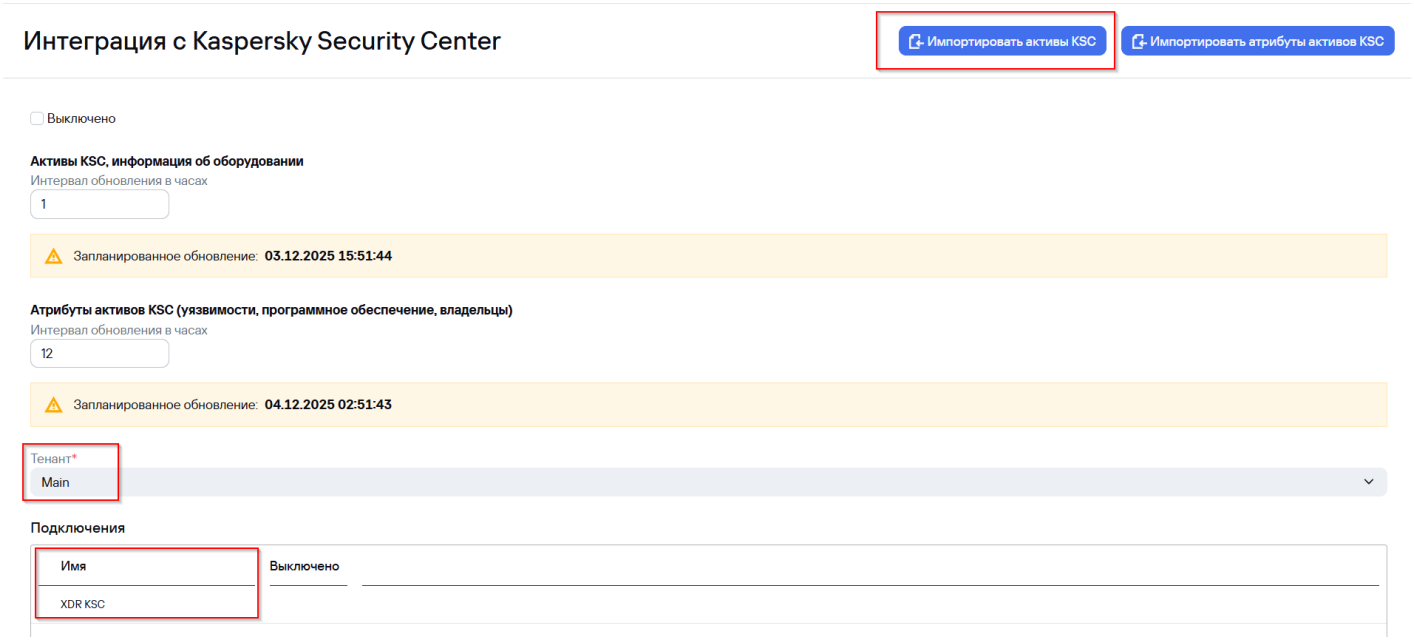
Интеграция настраивается автоматически после привязки, но выключена по умолчанию. Для ее включения необходимо снять галочку с параметра Выключено и нажать кнопку Сохранить.



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**.



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