Интеграция KUMA с KSC

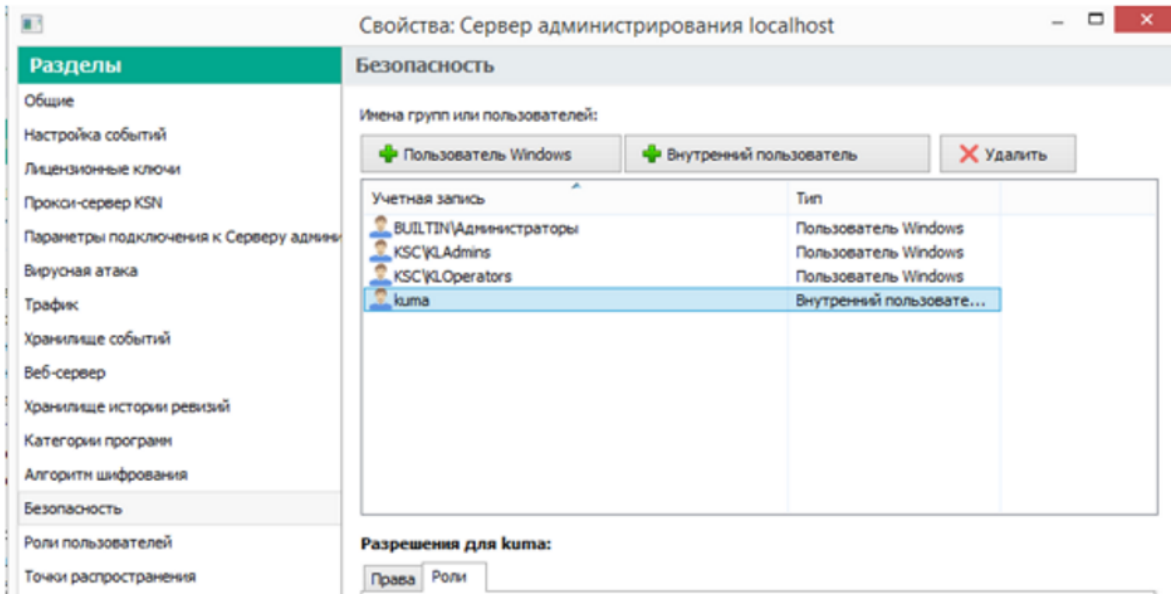
> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

> Официальная документация по данному разделу приведена в Онлайн-справке на продукт: https://support.kaspersky.com/KUMA/2.1/ru-RU/217923.htm

https://www.youtube.com/embed/u6v3qbDmu2Q?si=8K7B8BzkDDmL7KnX

Интеграция KUMA с KSC позволяет получить активы и данные по ним, которыми управляет KSC, возможность запуска задач реагирования, перемещение активов между группами KSC, закрытие уязвимостей (при наличии лицензии от Kaspersky Endpoint Security для бизнеса Расширенный и выше) из интерфейса KUMA.

Для интеграции необходимо заранее создать учетную запись (внутреннего пользователя) в KSC:



> Допускается также использовать доменную учетную запись пользователя для интеграции KUMA с KSC. Учетная запись пользователя в секрете KUMA указывается в формате: username@domain

Если на KSC включено MFA, то нужно сделать исключение для учетки KUMA. Согласно этой инструкции: https://support.kaspersky.com/help/KSC/14.2/ru-RU/211462.htm

В дополнение к исключению MFA для интеграционной УЗ KUMA можно настроить список адресов, с которых разрешено подключение к KSC: https://support.kaspersky.com/KSC/14.2/ru-RU/231374.htm

Созданной учетной записи необходимо назначить определенный набор прав доступа к функциям Kaspersky Security Center. Это можно сделать одним из следующих способов:

- настроить права для учетной записи индивидуально;
- создать роль пользователя с настроенным набором прав и присвоить данную роль учетной записи, которая будет использоваться для интеграции.

Перечень минимальных прав представлен на рисунке ниже. Данный набор прав позволяет:

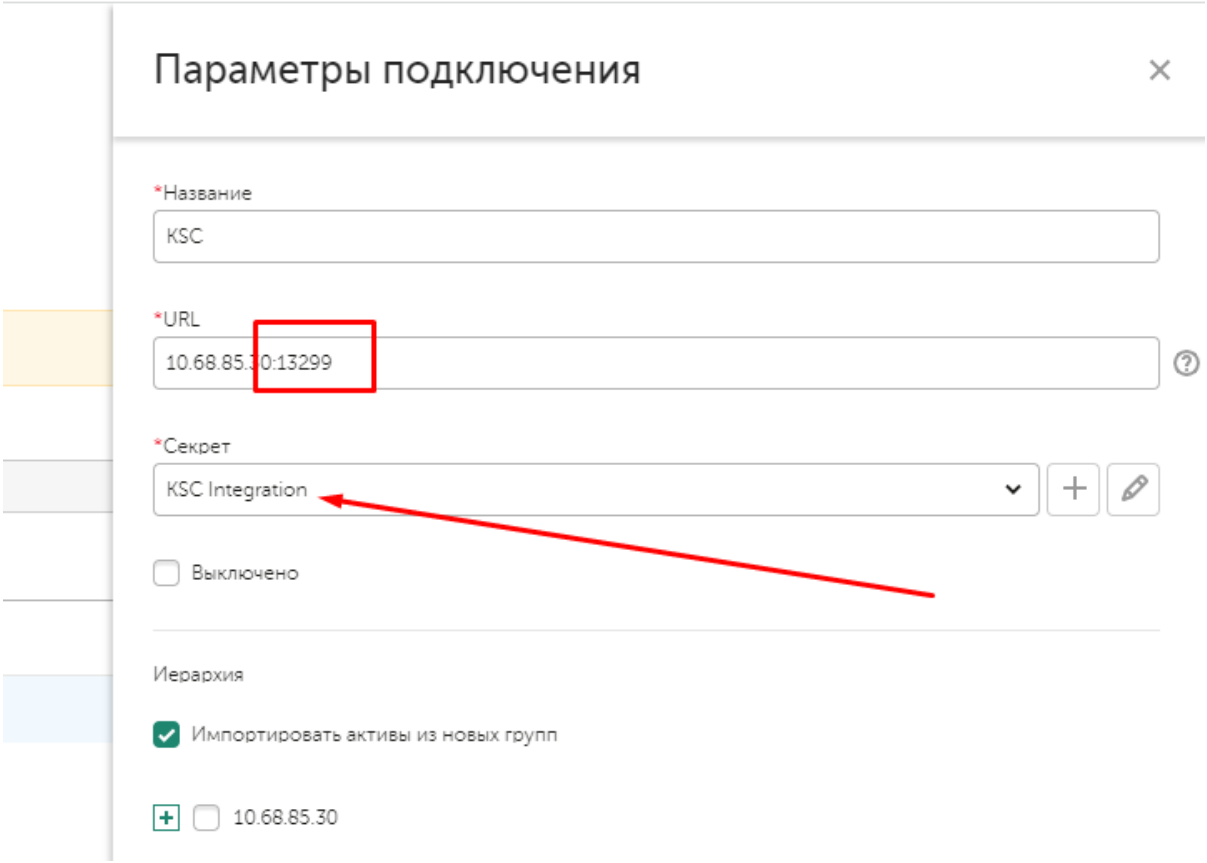
- выполнять импорт информации об активах;
- перемещать устройства между группами KSC;
- вручную запускать задачи поиска вредоносного ПО или обновления антивирусных баз из интерфейса KUMA;
- автоматически запускать задачи поиска вредоносного ПО или обновления антивирусных баз с помощью правил реагирования KUMA.

Права

Имя	Разрешить	Запретить
Сервер администрирования Kaspersky Security Center	■	☐
Общий функционал	■	☐
Управление группами администрирования	☑	☐
Запись	☑	☐
Доступ к объектам независимо от их списков ACL	☑	☐
Чтение	☑	☐
Базовая функциональность	■	☐
Чтение	☐	☐
Запись	☐	☐
Выполнение	☑	☐
Выполнение операций с выборками устройств	☐	☐
Удаленные объекты	☐	☐
Управление ключами шифрования	☐	☐
Обработка событий	☐	☐
Операции с Сервером администрирования	☐	☐
FUNC_AREA_HOST_TAGS	☐	☐
Развертывание программ "Лаборатории Касперского"	☐	☐
Управление лицензионными ключами	☐	☐
Интеграция программы	☐	☐
Управление отчетами	☐	☐
Иерархия Серверов администрирования	☐	☐
FUNC_AREA_SERVICE_ACCOUNTS	☐	☐
Права пользователей	☐	☐
Виртуальные Серверы администрирования	☐	☐
Mobile Device Management	☐	☐
Управление системой	☐	☐
Kaspersky Endpoint Security для Windows (12.1.0)	■	☐
Адаптивный контроль аномалий	☐	☐
Компоненты защиты	■	☐
Чтение	☐	☐
Запись	☑	☐
Выполнение	☑	☐
Выполнение операций с выборками устройств	☐	☐
Контроль программ	☐	☐
Базовая функциональность	■	☐
Чтение	☐	☐
Запись	☑	☐
Выполнение	☑	☐
Выполнение операций с выборками устройств	☐	☐
Detection and Response	☐	☐
Контроль устройств	☐	☐
Шифрование	☐	☐
Предотвращение вторжений	☐	☐
Исключения	☐	☐
Веб-Контроль	☐	☐

> Права пользователю нужно выдавать не только в свойствах KSC, но и в свойствах групп управляемых устройств, убедитесь, что не отключено наследование, чтобы права корректно распространялись на подгруппы

На стороне KUMA необходимо указать адрес и порт 13299 (этот порт используется по умолчанию), а также УЗ, о которой говорилось выше.



При нажатии в KUMA на кнопку "Сохранить", не должно всплавать сообщений об ошибке.

> Если при выгрузке, отсутствует какая-либо группа или возникает ошибка - убедитесь, что включено наследование параметров сервера в каталогах и отсутсвуют "мертвые души" в иерархии

Revision #15
Created 10 August 2023 10:15:14 by Boris Rzr
Updated 19 February 2025 10:43:17 by Boris Rzr