????????????? MDR

Kaspersky Managed Detection and Response ???????????? ????? ??????? ??? ?????????????? ??????????? ? ??????? ?????????? ???????????? ? ????? ????????????? ? ??????? ?????????? ? ????????? ????????? ????????? ????????. ?????????? ?? ????????? ?????????? ???????????? "???????????? ????????????", ??????? ????? ????? ???? ?????????? ???????? ??????????????, ???? ???? ???????????? ?? ??? ??????????.

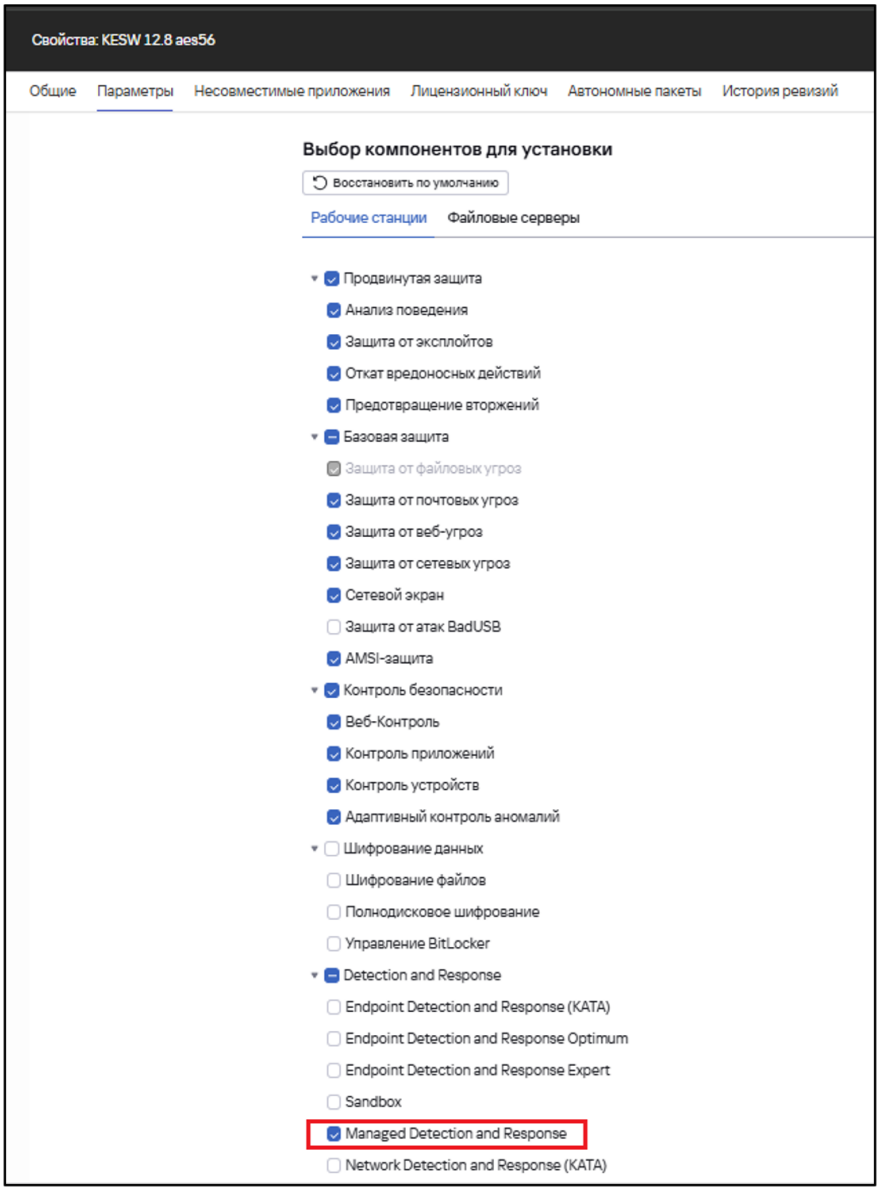
???????????? ???????????? MDR

???? ??????? ???? ???????????? ??? ???????????? ? ??????? MDR

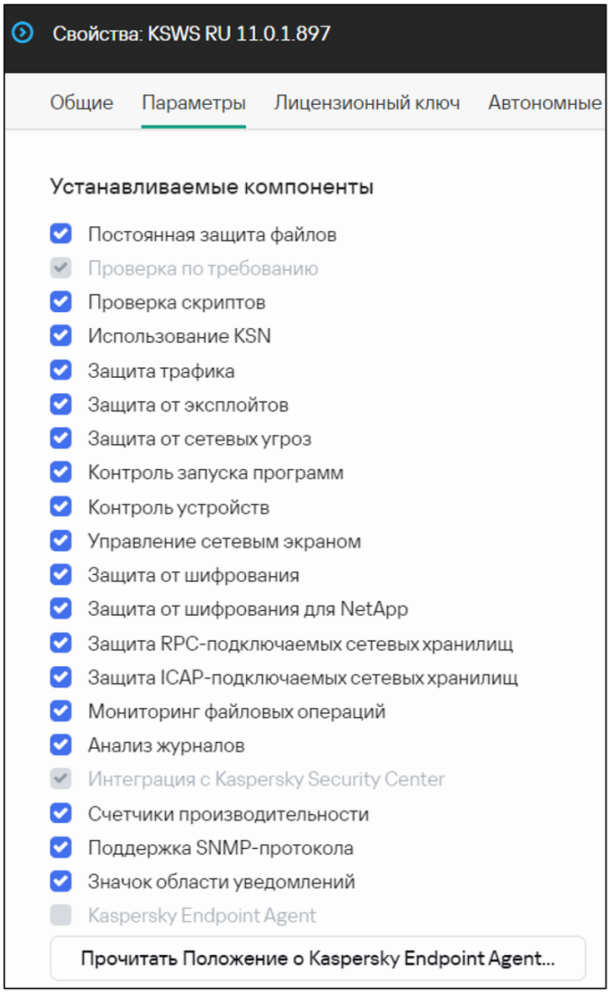
Подготовка инфраструктуры

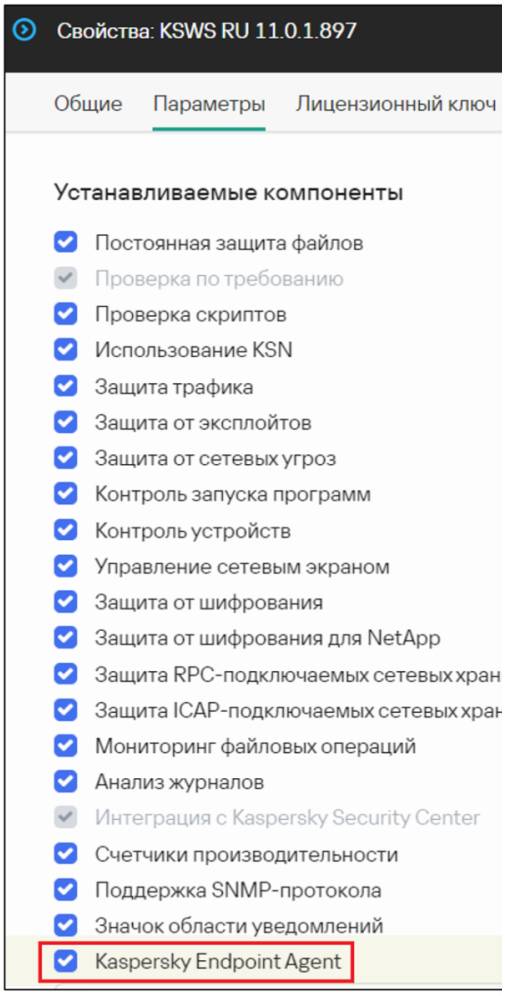
1. Проверка версий в инфраструктуре. Все KESW старше 12.6, KESL старше 12.1 и KESMac старше 12.0
2. На устройствах, где установлен KESW необходима проверка наличия установленного компонента MDR, иначе, запуск задачи Изменение состава компонентов и его доустановка (задача не требует перезагрузки). Если используется самозащита KES, то необходимо указать пароль от учётной записи KLAdmin.

В случае, если KES Windows ещё не установлен, необходимо указать использование компонента MDR в свойствах инсталляционного пакета:



3. При использовании KSWS, проверка последней версии продукта с установленным KEA внутри дистрибутива. При отсутствии компонента KEA внутри KSWS – переустановка KSWS с предварительным добавлением компонента KEA в инсталляционный пакет KSWS (см. скриншот ниже, может потребоваться принять Положение о KEA)





4. Рекомендуется рассмотрение перехода на KES for Windows вместо KSWS (функционал KSWS был перенесен в KES в версиях старше 12.0, а также подготовлено руководство по миграции), т.к. KSWS – EOL в 2025 и данный продукт не адаптирован для передачи телеметрии в MDR так хорошо, как KES Windows.
5. Проверка версий KSV LA: 5.2 для KSV LA Windows и 6.1 для KSV LA Linux (если используется)
6. Проверка того, что в инфраструктуре версия Network Agent совпадает с версией KSC и она соответствует KSC Windows 14.1 и выше / KSC Linux 15.1 и выше
7. Проверка наличия доступа в KSN со всех устройств (при отсутствии доступа в интернет с рабочей станции напрямую, включение «Режим KSN-proxy» в свойствах KSC и указание «Использовать KSN-proxy» в политике, тогда рабочие станции будут ходить через KSC)
8. Проверка того, что включены все необходимые параметры политики (см. раздел «Статус») и проведение нагрузочного тестирования. В случае значительного роста нагрузки необходимо обращение в тех. поддержку для получения рекомендаций по настройке исключений
9. По возможности рекомендуется настройка параметров аудита Windows в соответствии с рекомендациями, так картина будет видна «шире»

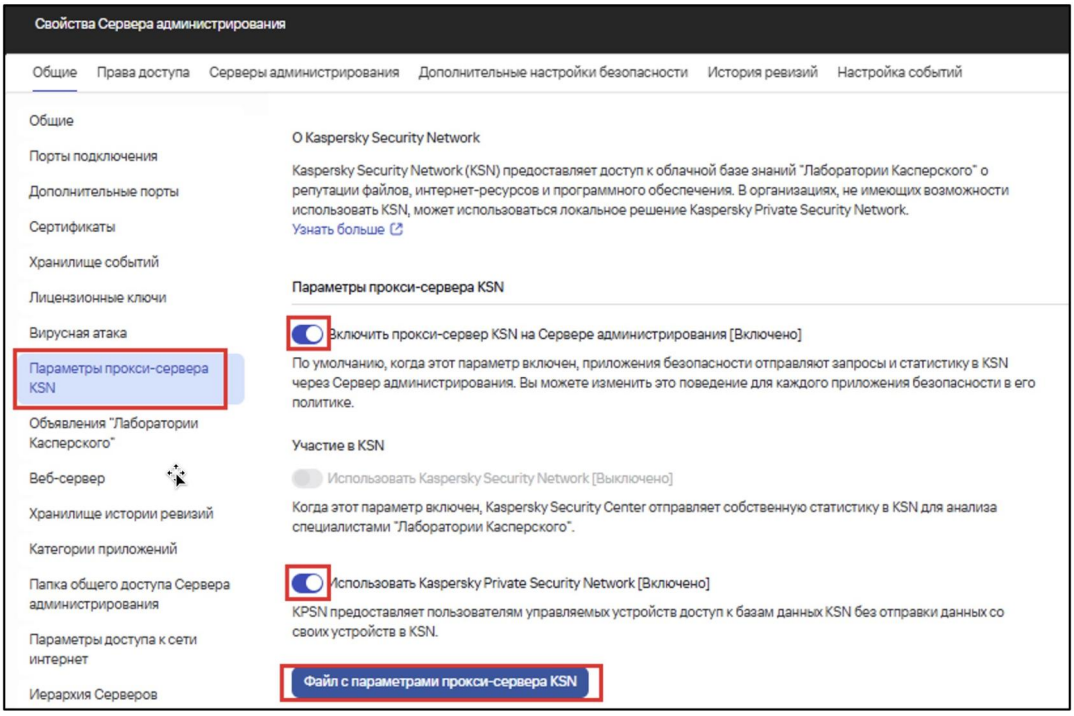
Подключение агентов

1. Регистрация на портале после подготовки инфраструктуры.
2. По результатам успешной регистрации, загрузка архива с BLOB и ksn_config-файлами из раздела License и осуществление настройки ниже.

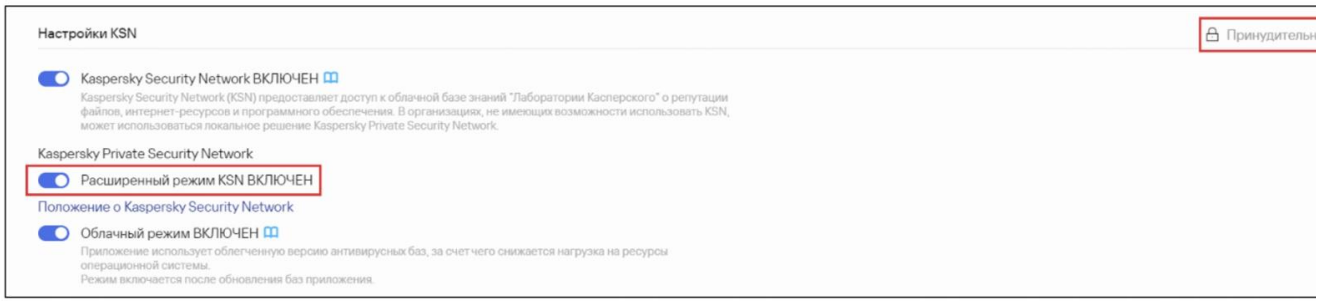
3.

> Для версий KES Windows от **12.6**, KES Linux от **12.3**, KES Mac от **12.2**, KESS от **4.0** данный пункт **НЕ** требуется к выполнению. Необходимо перейти далее к п. 4.

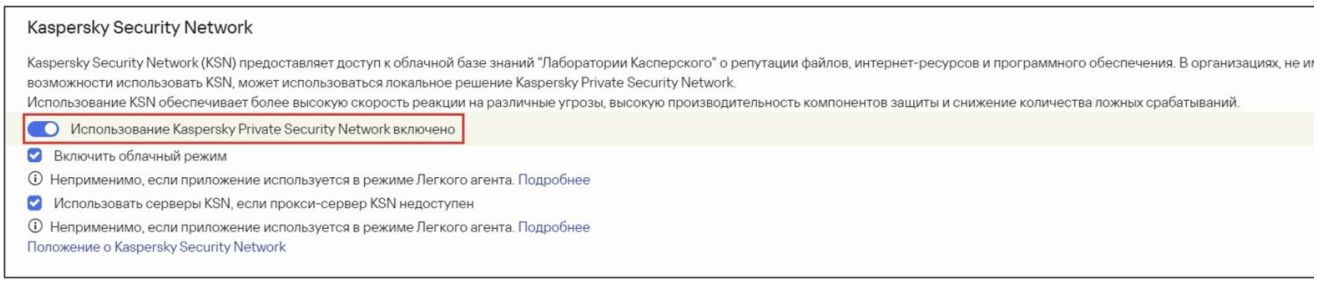
Переход в раздел **Свойства сервера администрирования** KSC. В окне свойств выбор раздела **Параметры прокси-сервера KSN**. Включение галочки **Использовать KPSN** и в поле «Файл с параметрами прокси-сервера KSN» загрузка файла конфигурации (ksn_config) из ранее скачанных. После загрузки файла принять лицензионное соглашение и нажать кнопку «Сохранить»



4. Проверка того, что в политиках включен KSN, у KSN закрыты замки и включен расширенный режим (Настройки KESL подтягиваются автоматически из настроек KSC, требуется только изменить параметр «Использование KPSN выключено» на «Использование KPSN включено»)



Настройка KSN в политике KES for Windows



Настройка KSN в политике KES for Linux

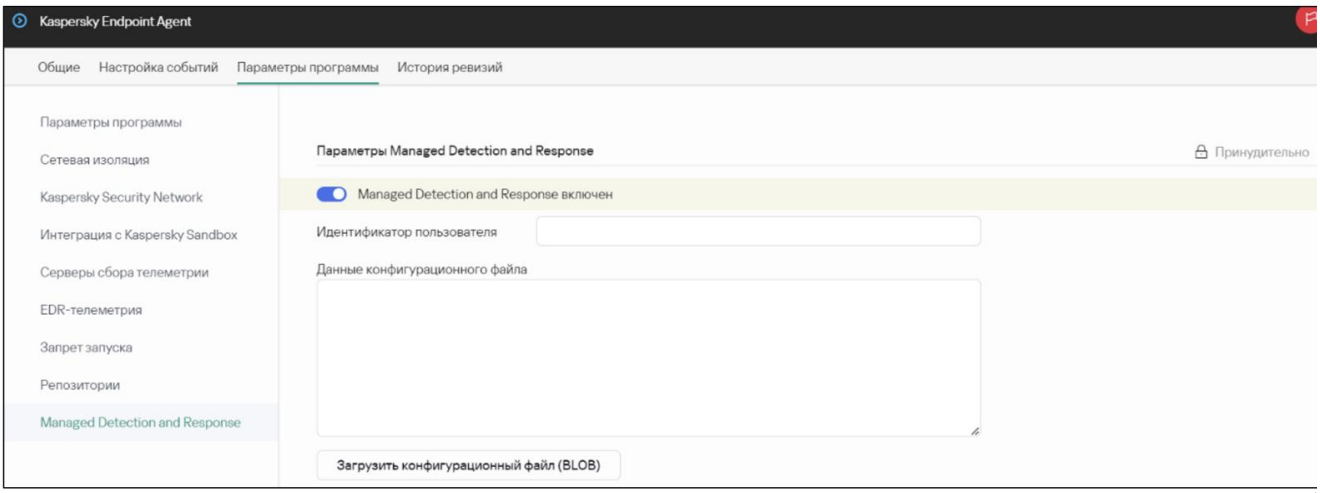
Настройка KSN в политике KES for Mac

5. В политике KES Windows и KES for Mac переход во вкладку **Параметры программы** и выбор раздела **Встроенные агенты / Managed Detection and Response.** Включение компонента и закрытие всех замков. Далее загрузка файла активации (mdr_blob), нажатием кнопки «Загрузить». После загрузки файла, выбор кнопки «Сохранить».
В политике KESL переход во вкладку **Параметры программы** и выбор раздела **Встроенные агенты / Managed Detection and Response** и аналогичное включение компонента с закрытием всех замков. Затем загрузка файла активации (mdr_blob) и выбор кнопки «Сохранить».

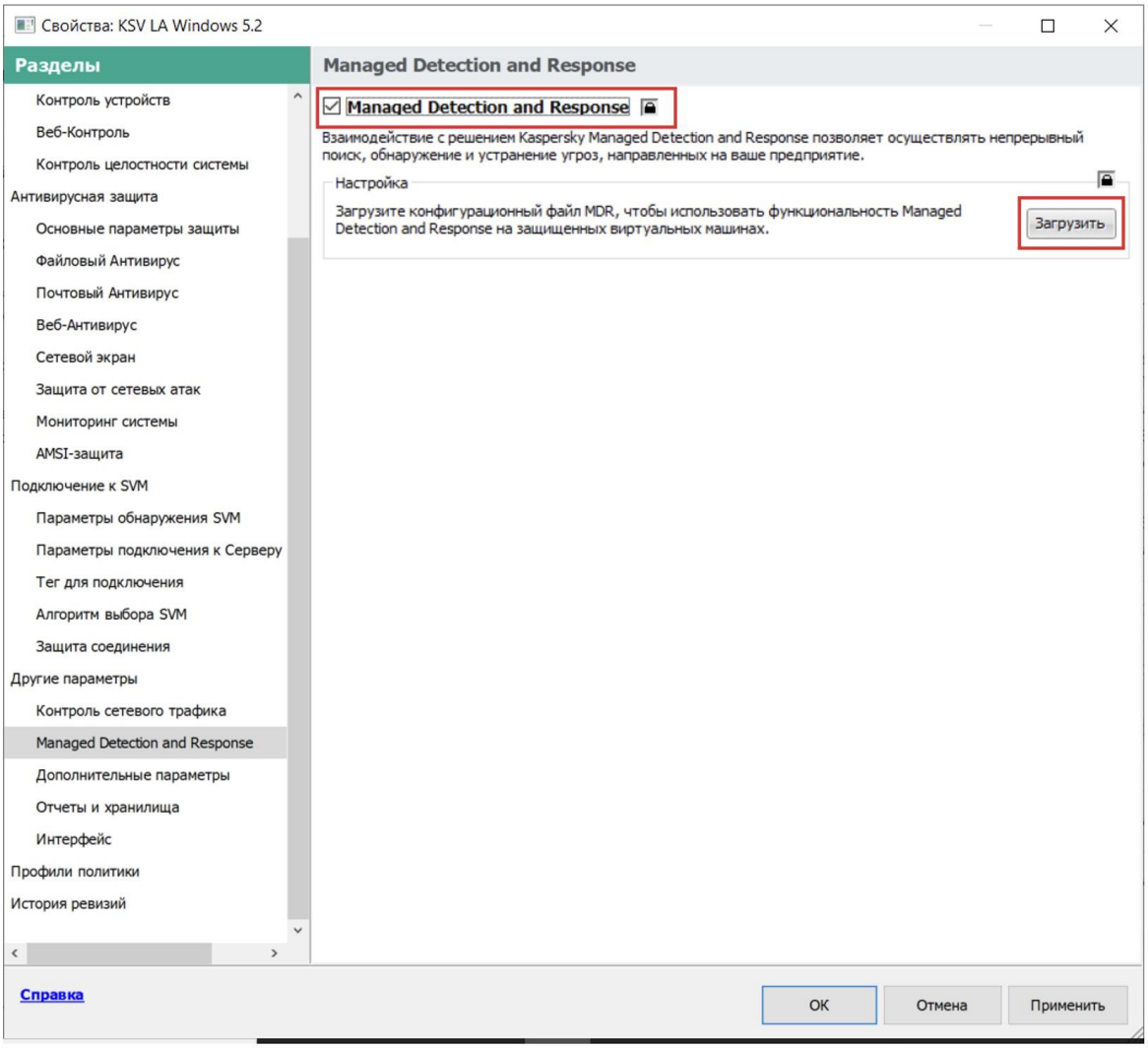
Включение компонента MDR в политике KES Windows / KES Linux

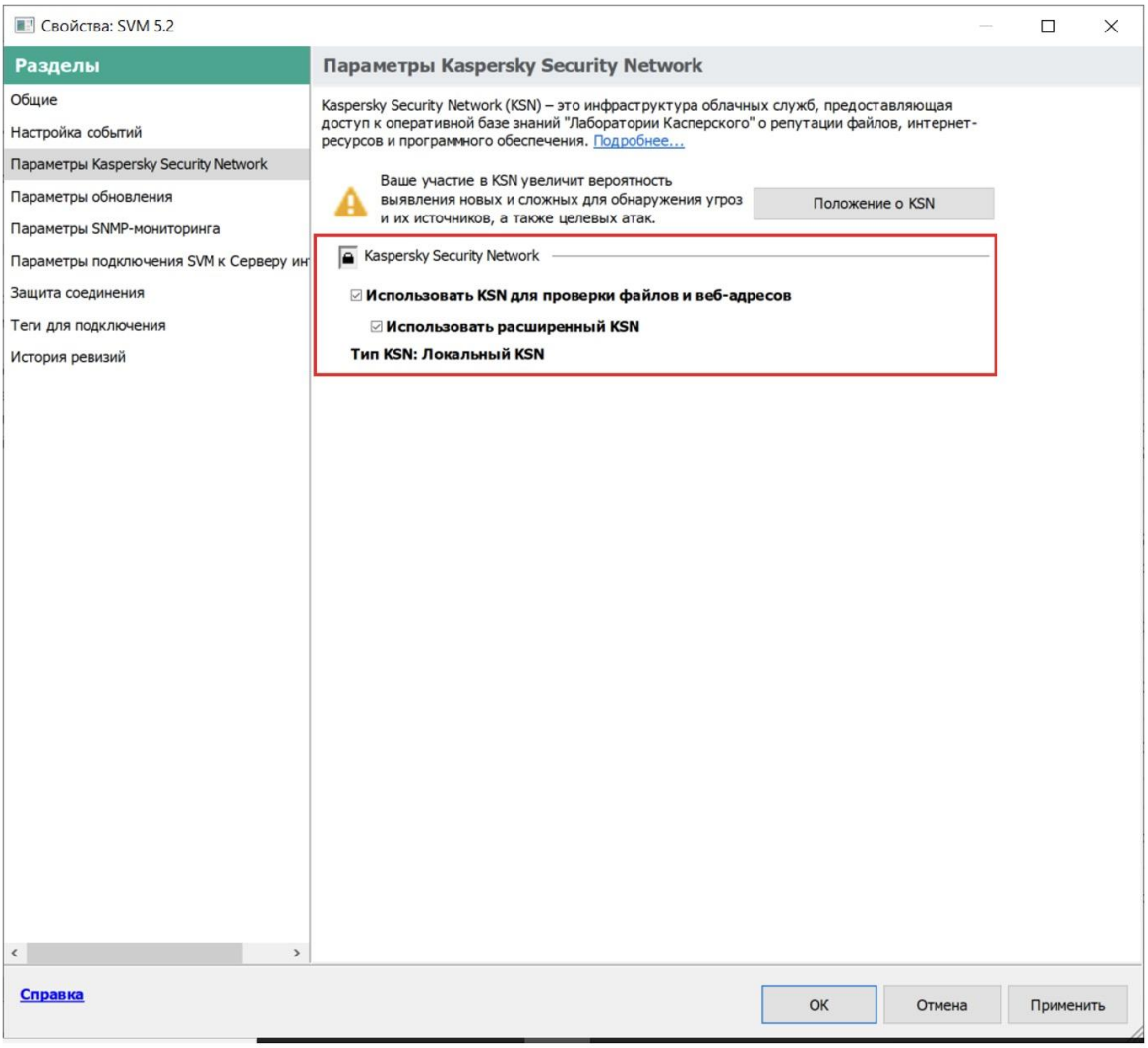
Включение компонента MDR в политике KES for Mac

6. Подключение устройств с KSWS осуществляется путем настройки политики KEA агента, установленного вместе с KSWS

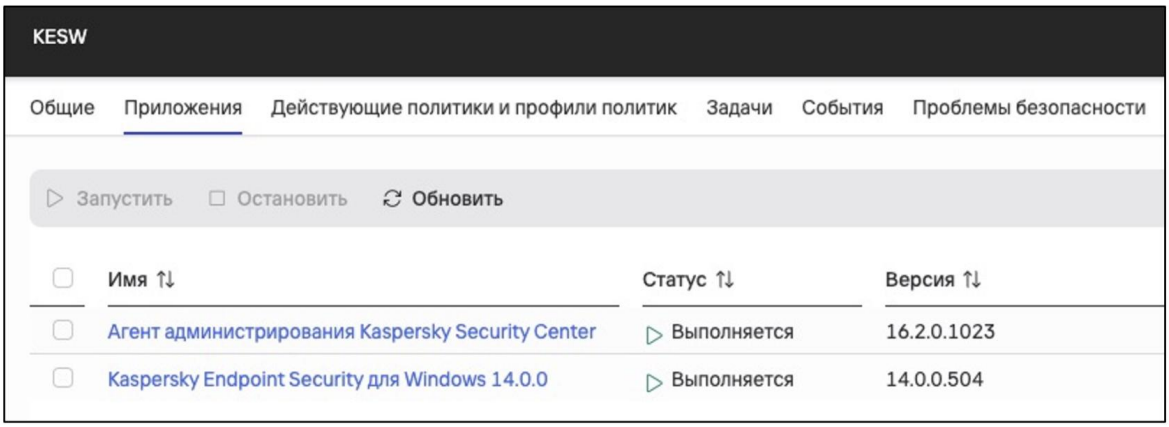


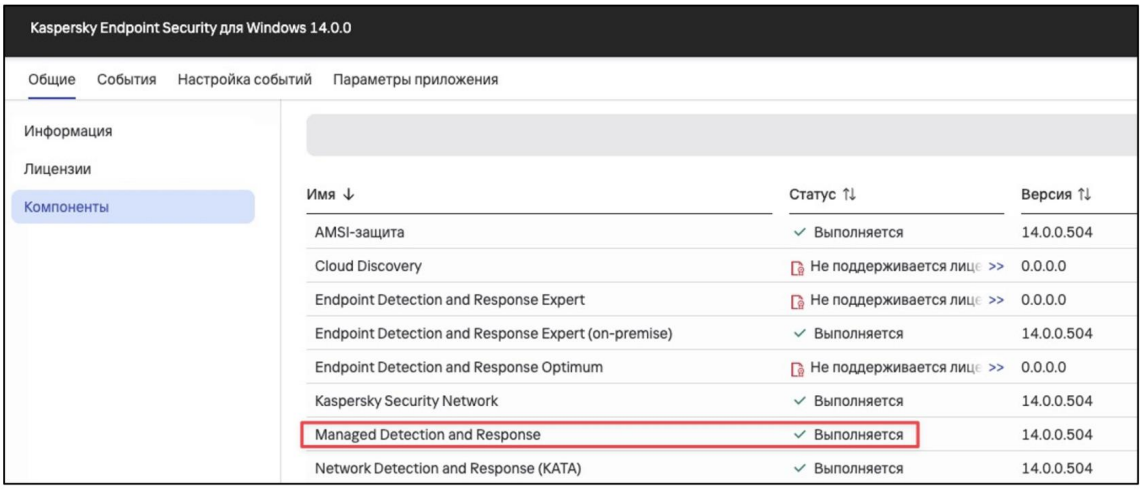
7. Подключение к MDR решения KSV LA 6.2 и выше для Windows (KSV LA 6.0 и выше для Linux) осуществляется в полите KES и описано выше в п. 3 – 5 Настройка передачи телеметрии с устройства с установленным KSV LA 5.2 для Windows осуществляется в политике KSV LA (интеграция с LA Linux возможна только с версии 6.0), настройка передачи KSN запросов осуществляется в политике SVM (Доступно только в MMC-консоли)





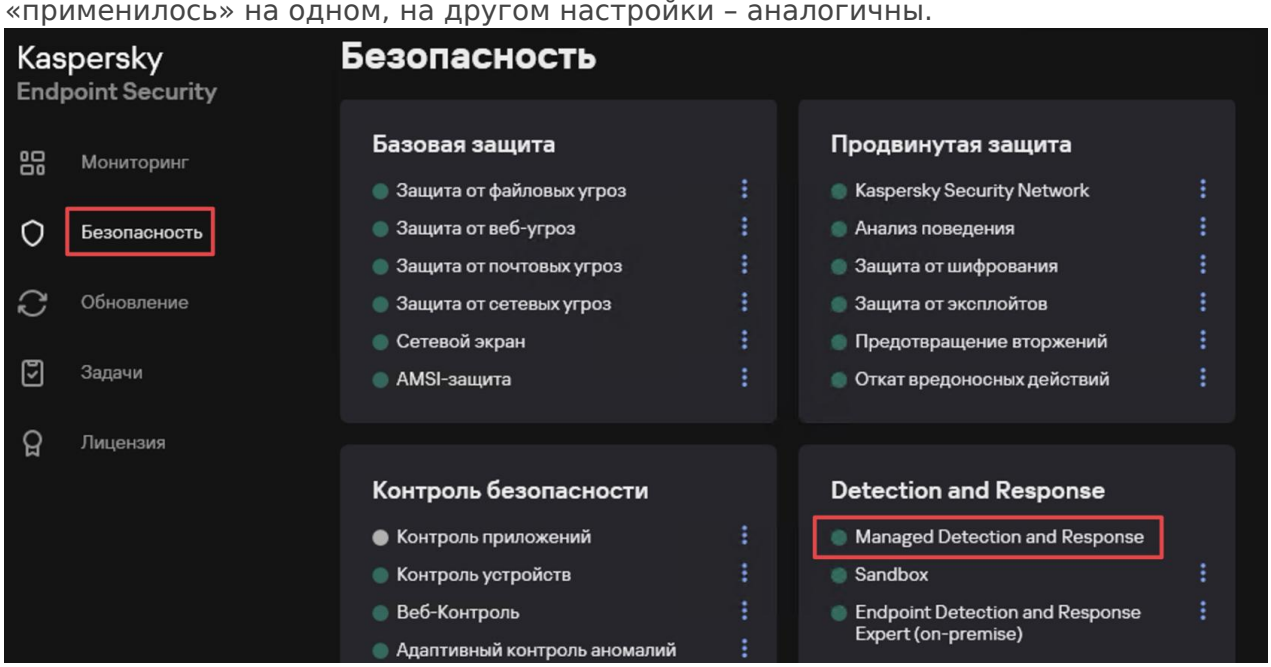
8. После проделанных операций на устройствах, которые должны быть подключены к MDR, переход в раздел **Устройства / Управляемые устройства**, выбор подключенного к MDR устройства, во вкладке **Программы** выбор программы через, которую настраивался MDR и в разделе **Компоненты** проверка того, что задача «Managed Detection and Response» имеет статус «Выполняется»





9. После этого локально на устройстве, которое должно было попасть в мониторинг необходима проверка того, что настройки проведены корректно:

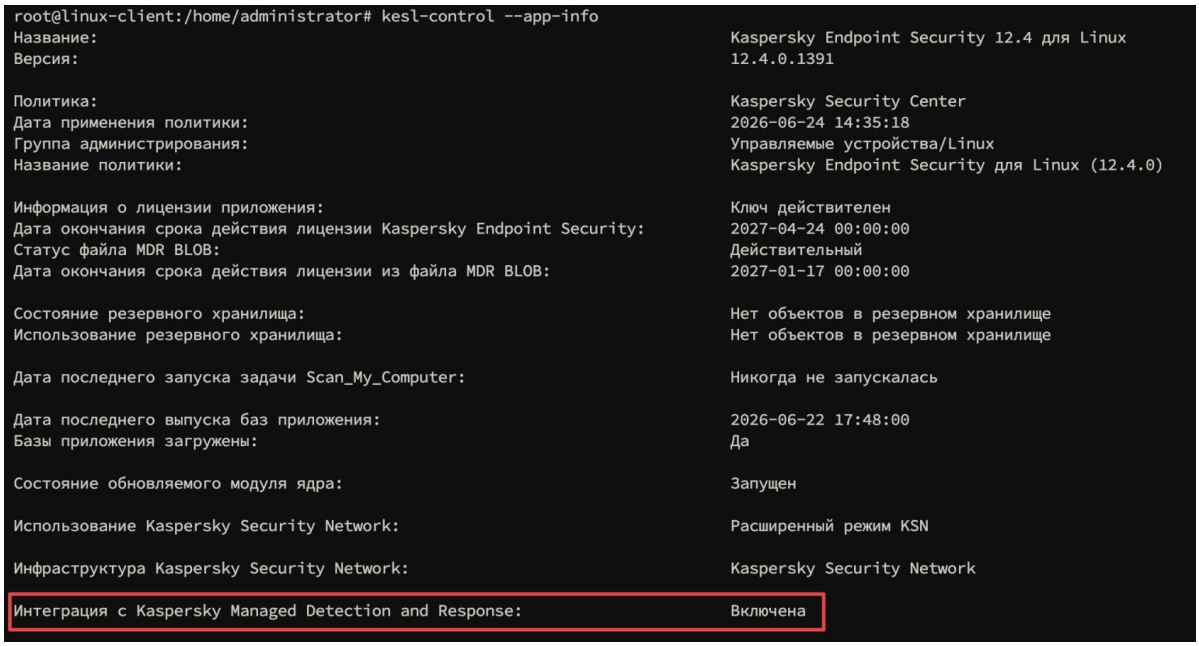
- В Windows нажать правой кнопкой мыши по файлу и выбрать «Проверить репутацию в KSN» - вердикт должен возвращаться (не должно быть вердикта «Нет связи с KSN»)
- Открыть интерфейс KES Windows (из трея) / KES for Mac и перейти в раздел «Безопасность», в нем должен появиться раздел «Detection and Response», в котором компонент «Managed Detection and Response» должен иметь «Зеленый» статус – достаточно проверить на одном устройстве, если «применилось» на одном, на другом настройки – аналогичны.



- Для проверки на устройстве Linux в терминале ввести команду

$ kesl-control --app-info

Убедиться, что компонент «Managed Detection and Response» имеет статус Active / Включено.



Если все шаги проделаны, через какое-то время в интерфейсе начнут появляться устройства в портале MDR в разделе «Активы

Особенности обновления лицензионного ключа

Если сервис использовался ранее, то для замены blob файла необходимо:

1. Открыть редактирование политики
2. Перейти в раздел Detection and Response > Managed Detection and Response
3. Нажать кнопку «Удалить»
4. Применить политику
5. Закрыть редактирование политики
6. Убедиться что начался процесс распространения новой политики
7. Заново открыть редактирование политики
8. Перейти в раздел Detection and Response > Managed Detection and Response
9. Нажать кнопку «Добавить» и прикрепить новый blob

Revision #10
Created 26 June 2026 13:47:11 by Сергей
Updated 26 June 2026 16:03:42 by Сергей