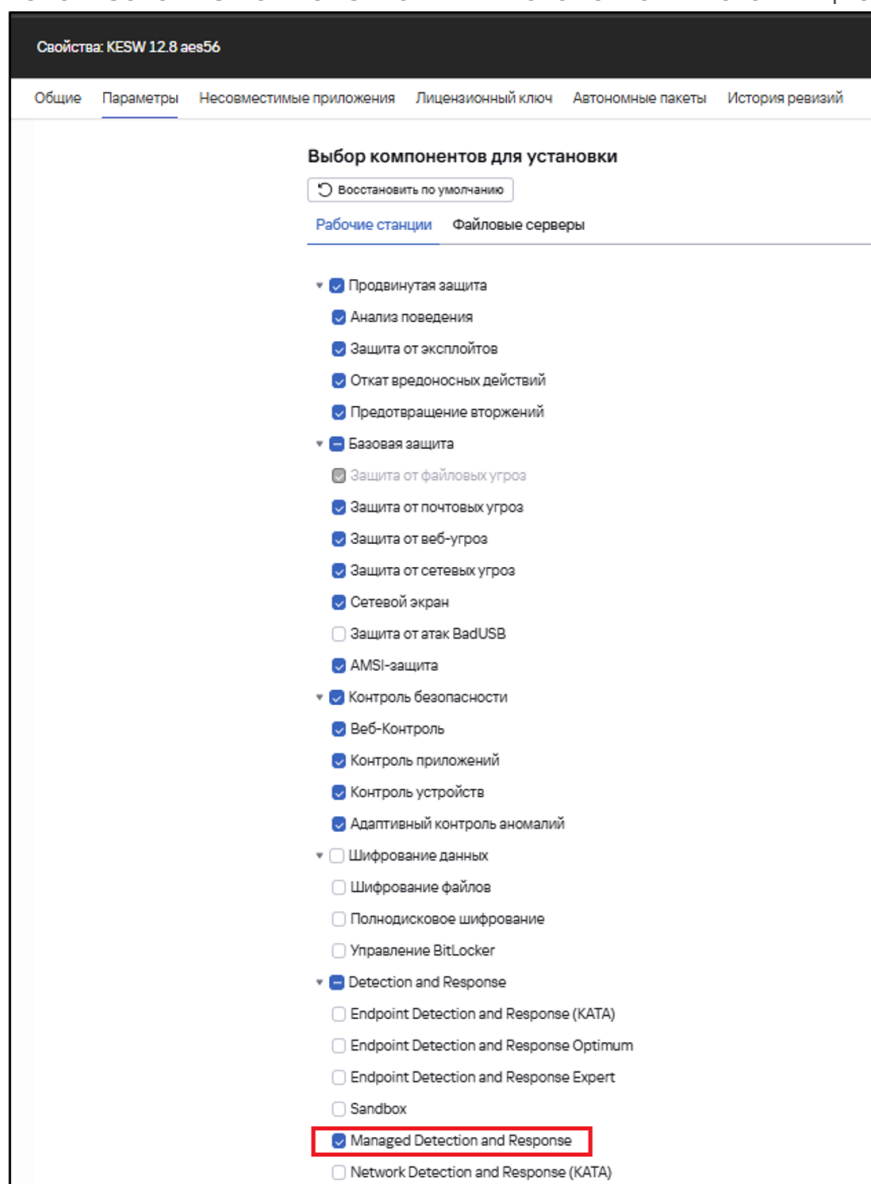
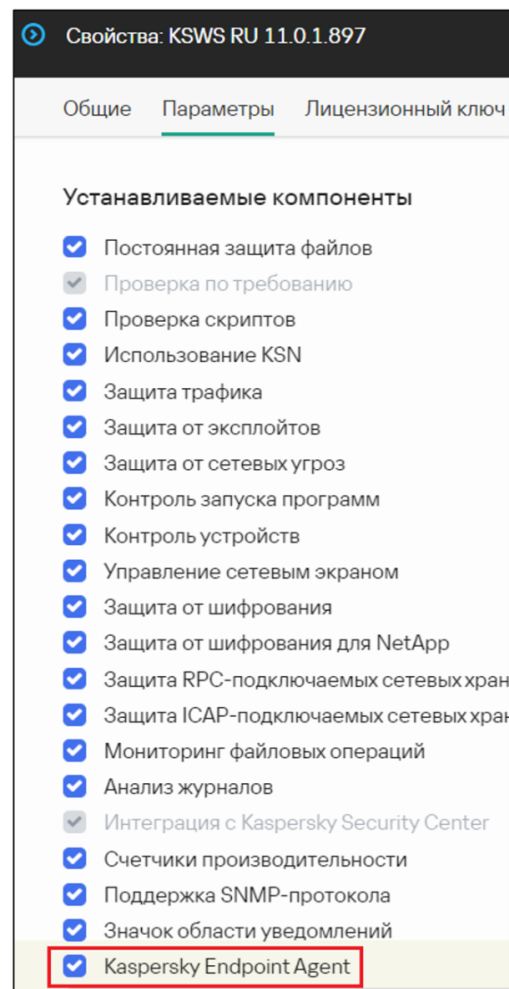
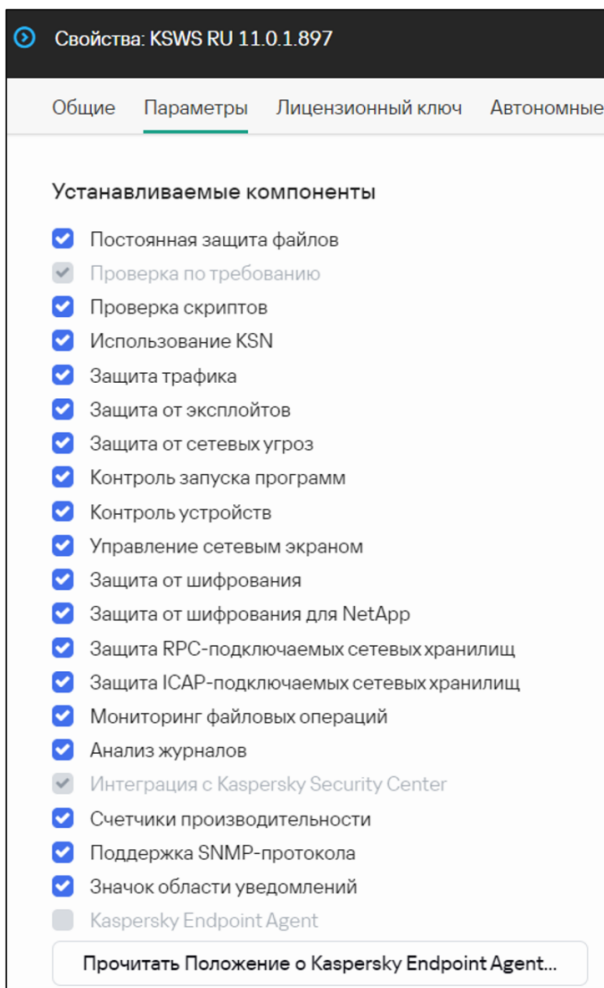


В случае, если KES Windows ещё не установлен, необходимо указать использование компонента MDR в свойствах инсталляционного пакета:



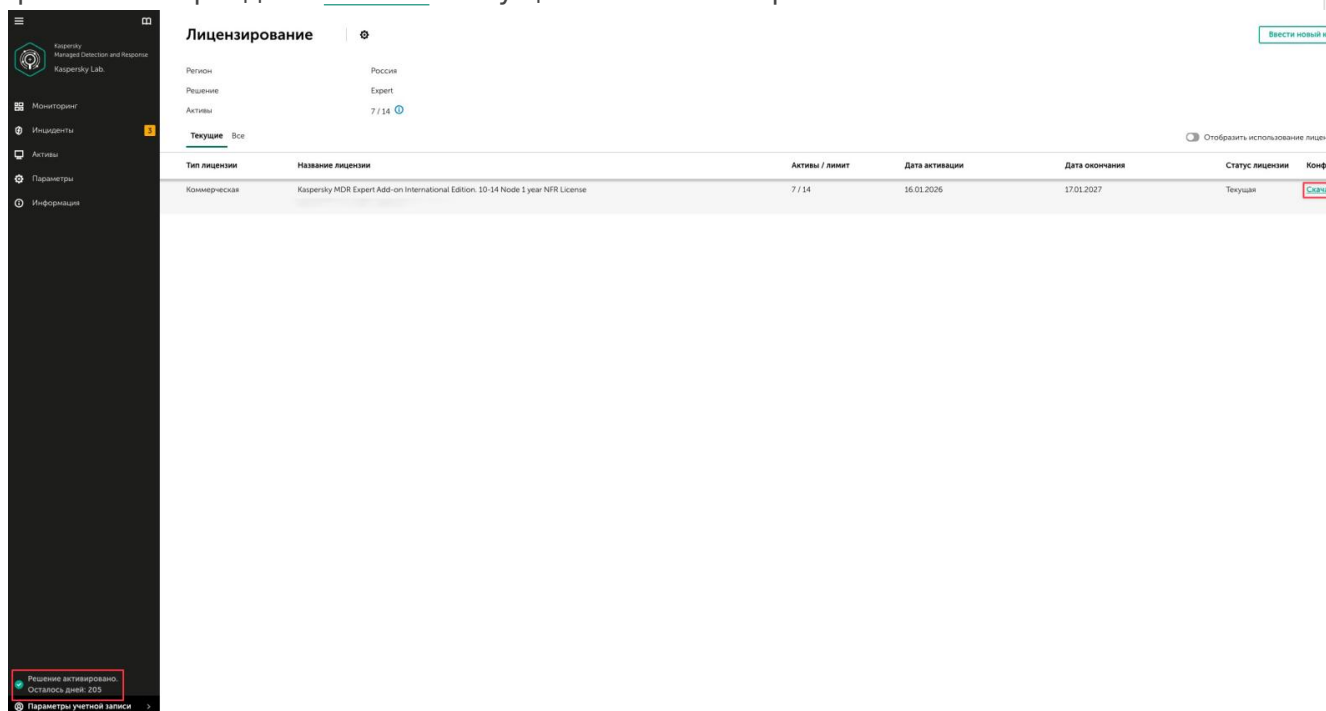
3. При использовании KSWs, проверка последней версии продукта с установленным KEA внутри дистрибутива. При отсутствии компонента KEA внутри KSWs – переустановка KSWs с предварительным добавлением компонента KEA в инсталляционный пакет KSWs (см. скриншот ниже, может потребоваться принять Положение о KEA)



4. Рекомендуется рассмотрение перехода на KES for Windows вместо KSW (функционал KSW был перенесен в KES в версиях старше 12.0, а также подготовлено [руководство по миграции](#)), т.к. KSW – [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-проху» в свойствах KSC и указание «Использовать KSN-проху» 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»

Свойства Сервера администрирования

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

Общие

Порты подключения

Дополнительные порты

Сертификаты

Хранилище событий

Лицензионные ключи

Вирусная атака

Параметры прокси-сервера KSN

Объявления "Лаборатории Касперского"

Веб-сервер

Хранилище истории ревизий

Категории приложений

Папка общего доступа Сервера администрирования

Параметры доступа к сети интернет

Иерархия Серверов

О Kaspersky Security Network

Kaspersky Security Network (KSN) предоставляет доступ к облачной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. В организациях, не имеющих возможности использовать KSN, может использоваться локальное решение Kaspersky Private Security Network.

[Узнать больше](#)

Параметры прокси-сервера KSN

Включить прокси-сервер KSN на Сервере администрирования [Включено]

По умолчанию, когда этот параметр включен, приложения безопасности отправляют запросы и статистику в KSN через Сервер администрирования. Вы можете изменить это поведение для каждого приложения безопасности в его политике.

Участие в KSN

Использовать Kaspersky Security Network [Выключено]

Когда этот параметр включен, Kaspersky Security Center отправляет собственную статистику в KSN для анализа специалистами "Лаборатории Касперского".

Использовать Kaspersky Private Security Network [Включено]

KPSN предоставляет пользователям управляемых устройств доступ к базам данных KSN без отправки данных со своих устройств в KSN.

[Файл с параметрами прокси-сервера KSN](#)

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»)

Настройки KSN Принудительно

Kaspersky Security Network ВКЛЮЧЕН

Kaspersky Security Network (KSN) предоставляет доступ к облачной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. В организациях, не имеющих возможности использовать KSN, может использоваться локальное решение Kaspersky Private Security Network.

Kaspersky Private Security Network

Расширенный режим KSN ВКЛЮЧЕН

Положение о Kaspersky Security Network

Облачный режим ВКЛЮЧЕН

Приложение использует облегченную версию антивирусных баз, за счет чего снижается нагрузка на ресурсы операционной системы. Режим включается после обновления баз приложения.

Настройка KSN в политике KES for Windows

Kaspersky Security Network

Kaspersky Security Network (KSN) предоставляет доступ к облачной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. В организациях, не имеющих возможности использовать KSN, может использоваться локальное решение Kaspersky Private Security Network. Использование KSN обеспечивает более высокую скорость реакции на различные угрозы, высокую производительность компонентов защиты и снижение количества ложных срабатываний.

Использование Kaspersky Private Security Network включено

Включить облачный режим

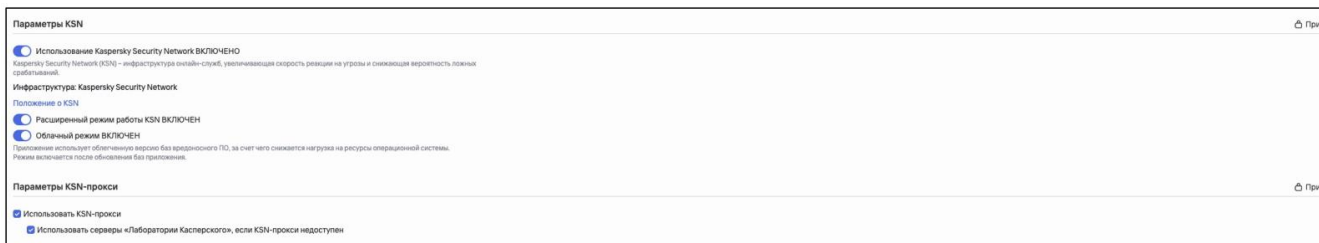
Неприменимо, если приложение используется в режиме Легкого агента. Подробнее

Использовать серверы KSN, если прокси-сервер KSN недоступен

Неприменимо, если приложение используется в режиме Легкого агента. Подробнее

Положение о Kaspersky Security Network

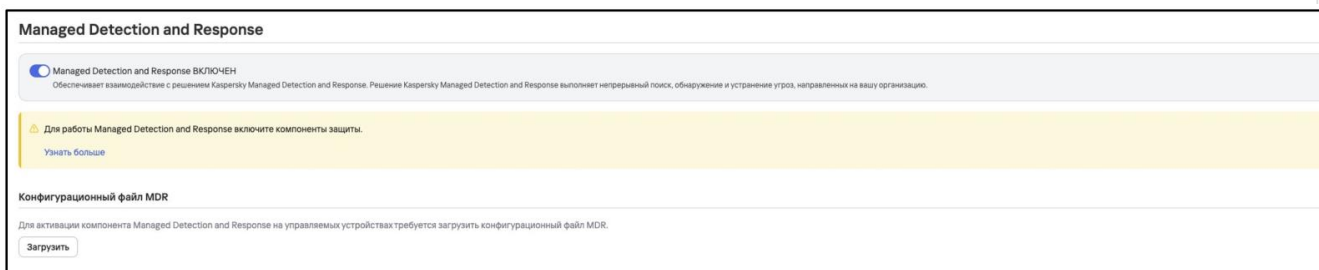
Настройка KSN в политике KES for Linux



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».

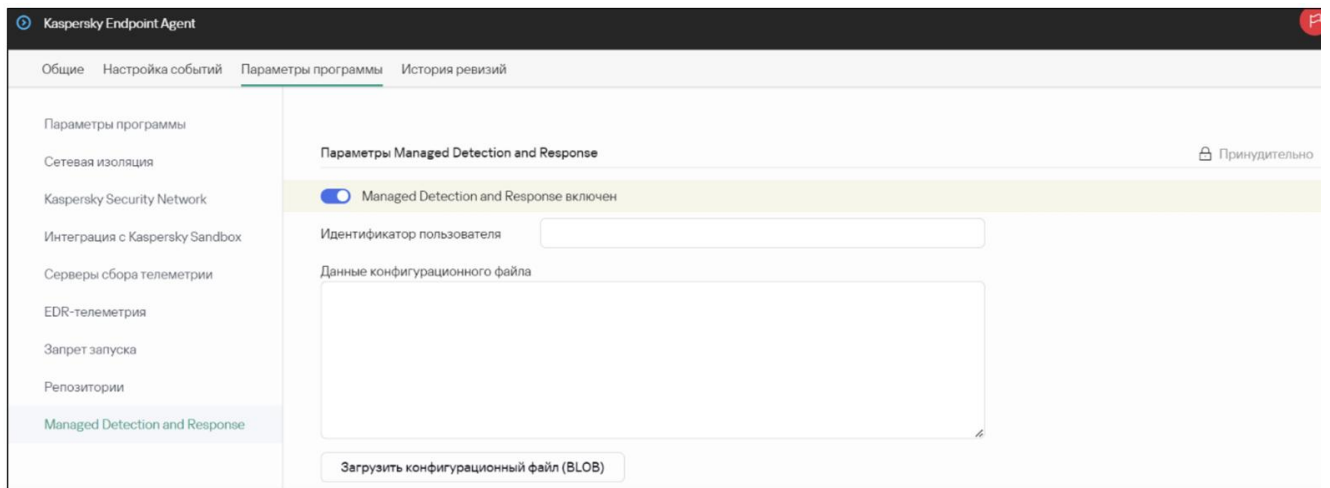


Включение компонента MDR в политике KES Windows / KES Linux

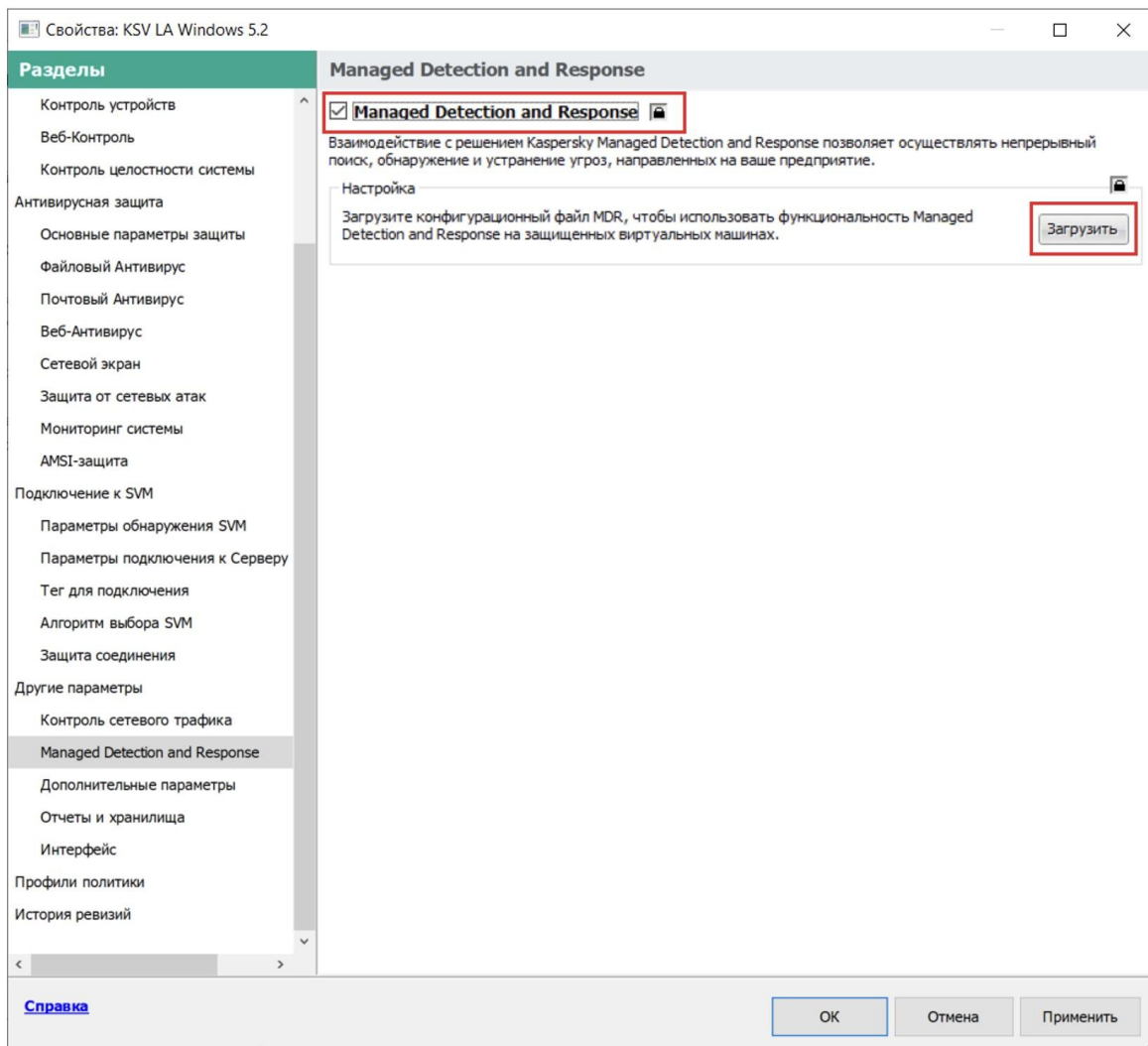


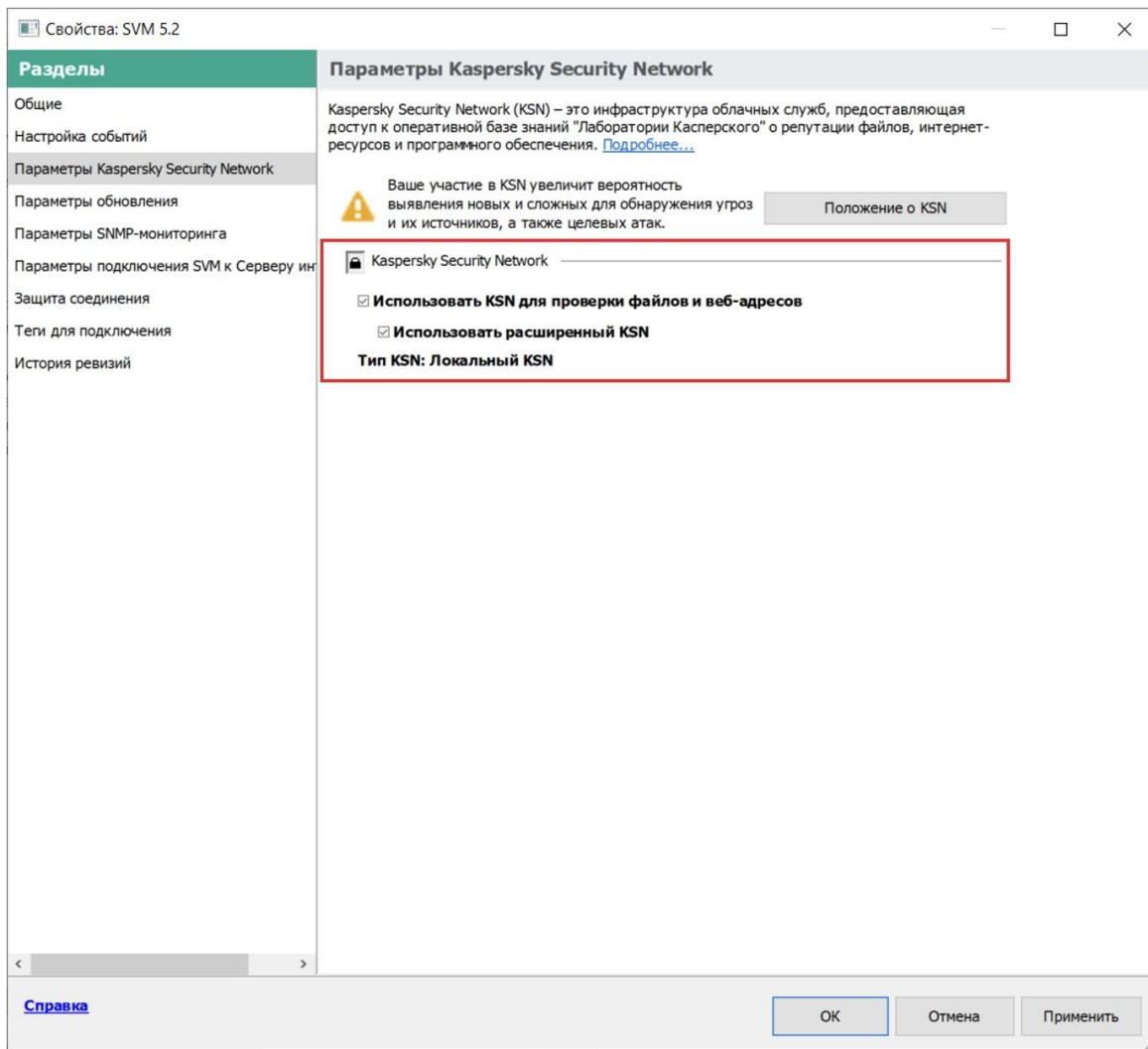
Включение компонента MDR в политике KES for Mac

6. Подключение устройств с KSW5 осуществляется путем настройки политики KEA агента, установленного вместе с KSW5



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»

KESW					
Общие	Приложения	Действующие политики и профили политик	Задачи	События	Проблемы безопасности
▶ Запустить □ Остановить ↻ Обновить					
<input type="checkbox"/>	Имя ↑↓	Статус ↑↓	Версия ↑↓		
<input type="checkbox"/>	Агент администрирования Kaspersky Security Center	▶ Выполняется	16.2.0.1023		
<input type="checkbox"/>	Kaspersky Endpoint Security для Windows 14.0.0	▶ Выполняется	14.0.0.504		

Kaspersky Endpoint Security для Windows 14.0.0

Общие События Настройка событий Параметры приложения

Информация

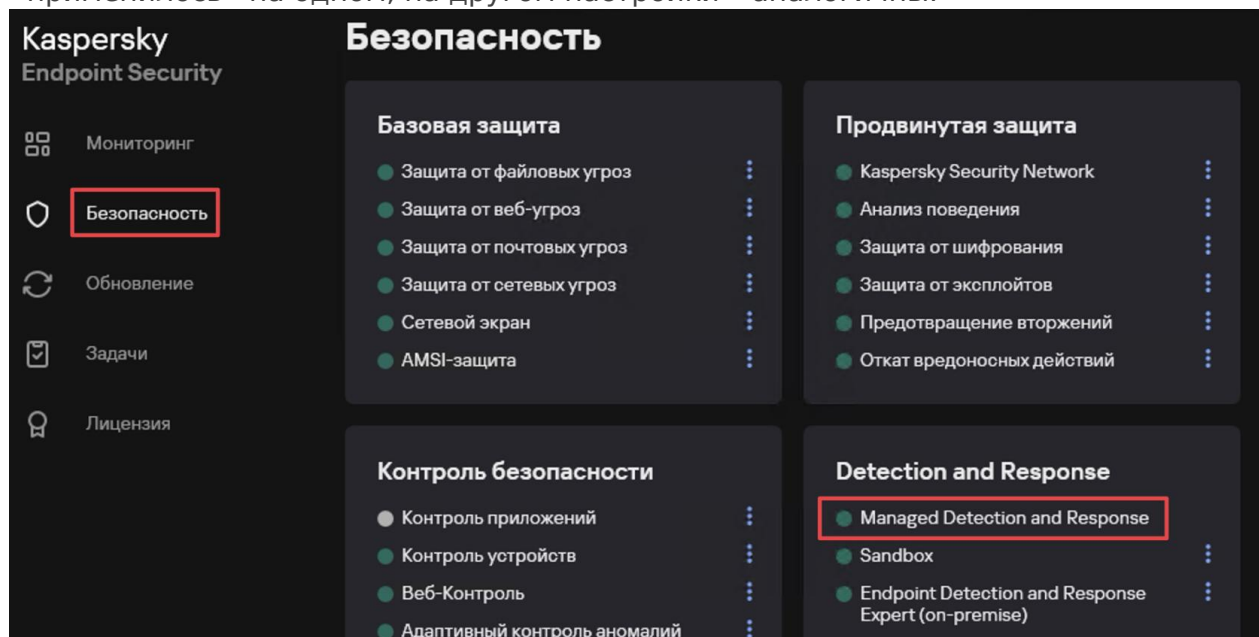
Лицензии

Компоненты

Имя ↓	Статус ↑↓	Версия ↑↓
AMSI-защита	✓ Выполняется	14.0.0.504
Cloud Discovery	✗ Не поддерживается лицензией >>	0.0.0.0
Endpoint Detection and Response Expert	✗ Не поддерживается лицензией >>	0.0.0.0
Endpoint Detection and Response Expert (on-premise)	✓ Выполняется	14.0.0.504
Endpoint Detection and Response Optimum	✗ Не поддерживается лицензией >>	0.0.0.0
Kaspersky Security Network	✓ Выполняется	14.0.0.504
Managed Detection and Response	✓ Выполняется	14.0.0.504
Network Detection and Response (KATA)	✓ Выполняется	14.0.0.504

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 троя) / 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 `$ kesi-control --app-info`
Убедиться, что компонент «Managed Detection and Response» имеет статус Active / Включено.

```
root@linux-client:/home/administrator# kسل-control --app-info
Название: Kaspersky Endpoint Security 12.4 для Linux
Версия: 12.4.0.1391

Политика: Kaspersky Security Center
Дата применения политики: 2026-06-24 14:35:18
Группа администрирования: Управляемые устройства/Linux
Название политики: Kaspersky Endpoint Security для Linux (12.4.0)

Информация о лицензии приложения: Ключ действителен
Дата окончания срока действия лицензии Kaspersky Endpoint Security: 2027-04-24 00:00:00
Статус файла MDR BLOB: Действительный
Дата окончания срока действия лицензии из файла MDR BLOB: 2027-01-17 00:00:00

Состояние резервного хранилища: Нет объектов в резервном хранилище
Использование резервного хранилища: Нет объектов в резервном хранилище

Дата последнего запуска задачи Scan_My_Computer: Никогда не запускалась

Дата последнего выпуска баз приложения: 2026-06-22 17:48:00
Базы приложения загружены: Да

Состояние обновляемого модуля ядра: Запущен

Использование Kaspersky Security Network: Расширенный режим KSN

Инфраструктура Kaspersky Security Network: Kaspersky Security Network

Интеграция с Kaspersky Managed Detection and Response: Включена
```

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