

# ????????? ????????????? MDR

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

## 1. ?????????? ?????????? KES

Раздел MDR

В KSC в политике KES проверьте, что компонент MDR включен, а файл blob подгружен.

Проверьте, что "замки" в политике закрыты. Они необходимы для принудительного применения политики.

Kaspersky Endpoint Security для Windows 14.0.0

Высокий уровень защиты

ОбщиеНастройка событийПараметры приложенияИстория ревизийПрофили политики

Защита устройств от угроз

Защита сетевых соединений и средств коммуникации

Контроль безопасности

Шифрование данных

Доверенная зона

Общие настройки

Встроенные агенты

Managed Detection and Response

Endpoint Detection and Response

Endpoint Detection and Response Expert (on-premise)

Network Detection and Response (KATA)

← Встроенные агенты

Managed Detection and Response

Managed Detection and Response ВКЛЮЧЕН

Обеспечивает взаимодействие с решением Kaspersky Managed Detection and Response. Решение Kaspersky Managed Detection and Response выполняет непрерывный поиск, обнаружение и устранение угроз, направленных на вашу организацию.

Для работы Managed Detection and Response включите компоненты защиты.

Узнать больше

Конфигурационный файл MDR

Для активации компонента Managed Detection and Response на управляемых устройствах требуется загрузить конфигурационный файл MDR.

Удалить конфигурационный файл MDR

Blob-файл загружен

Раздел KSN

В KSC в политике KES проверьте, что компонент KSN включён в **расширенном режиме**. Также убедитесь, что стоят корректные параметры использования **прокси-сервера KSN** согласно вашей архитектуре сети.

Kaspersky Endpoint Security для Windows 14.0.0

Высокий уровень защиты

ОбщиеНастройка событийПараметры приложенияИстория ревизийПрофили политики

Защита устройств от угроз

Защита сетевых соединений и средств коммуникации

Контроль безопасности

Шифрование данных

Доверенная зона

Общие настройки

Настройки обнаружения

Kaspersky Security Network

Взаимодействие с пользователем

Самозащита

Производительность

Настройки сети

Служба технической поддержки

Отчеты и хранилище

Интеграция с KSC

Настройки телеметрии

Настройки уведомлений

Встроенные агенты

Режим Легкого агента

← Общие настройки

Kaspersky Security Network

Использование Kaspersky Security Network (KSN) ВКЛЮЧЕНО

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.

Положение о Kaspersky Security Network

Инфраструктура

Kaspersky Security Network

Настройки KSN

Использовать расширенный режим KSN

В этом режиме приложение отправляет дополнительные данные в "Лабораторию Касперского" для пополнения антивирусных баз и быстрой реакции на новые угрозы.

Использовать облачный режим

В этом режиме приложение использует облегченную версию антивирусных баз для снижения нагрузки на операционную систему.

Неприменимо, если приложение используется в режиме Легкого агента.

Узнать больше

Статус компьютера при недоступности серверов KSN

Критический

Прокси-сервер KSN

Использовать Сервер администрирования как прокси-сервер KSN

Неприменимо, если приложение используется в режиме Легкого агента.

Узнать больше

Использовать серверы Kaspersky Security Network, если прокси-сервер KSN недоступен

2. ????????? ?????????????????? ????????????? MDR ?? ???????

Windows

Проверка в KSC

Для начала стоит проверить, что на устройствах под управлением ОС Windows стоит компонент MDR.

В веб-консоли KSC перейдите в одно из устройств --> Приложения --> Kaspersky Endpoint Security для Windows --> Компоненты. Для корректной работы должен быть статус "Выполняется" и отображаться номер версии.

## Информация

## Лицензии

## Компоненты

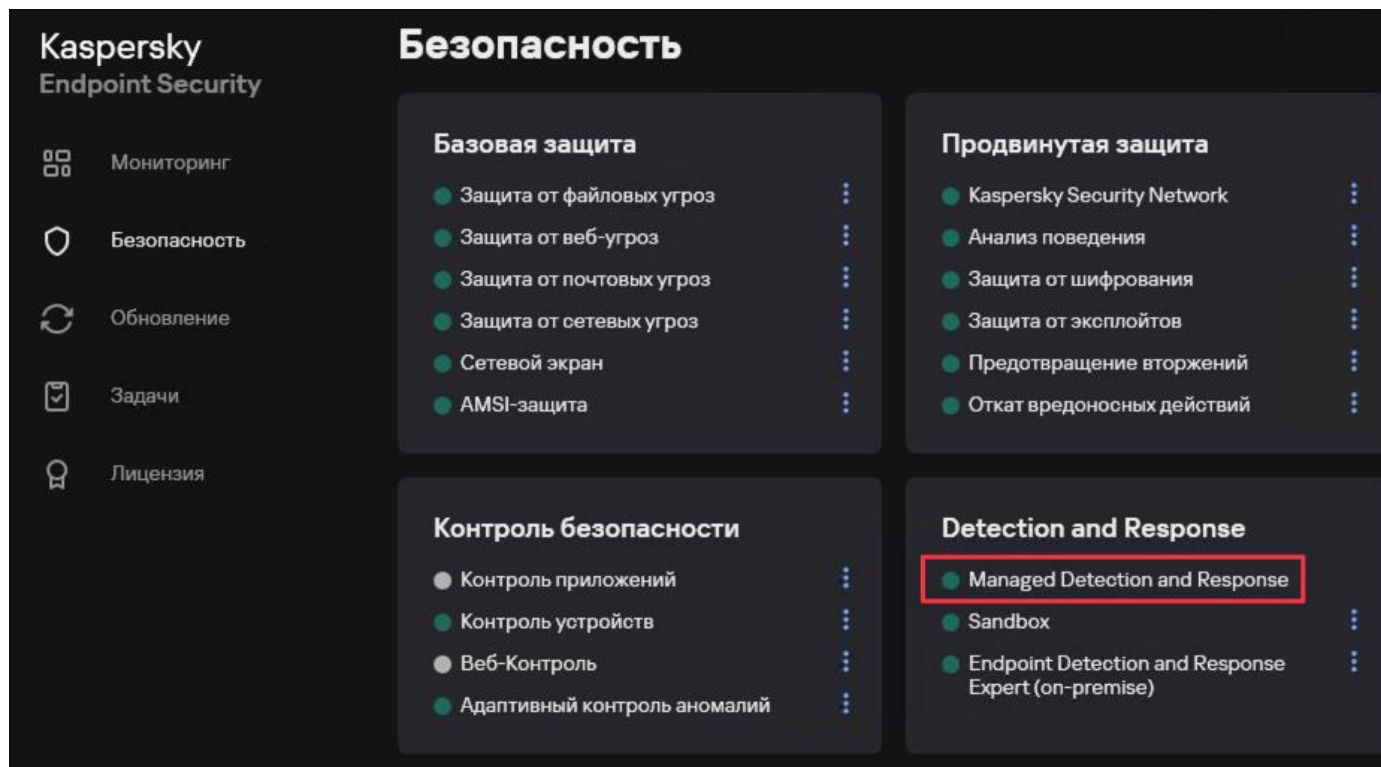
| Имя ↓                                               | Статус ↑↓                        | Версия ↑↓  |
|-----------------------------------------------------|----------------------------------|------------|
| AMSI-защита                                         | ✓ Выполняется                    | 14.0.0.504 |
| 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 |

Если номера версии нет (отображается как 0.0.0.0), значит компонент не установлен.

## Локальная проверка в KES

Также возможно проверить наличие компонента MDR локально в KES.

Откройте приложение Kaspersky Endpoint Security для Windows и перейдите в раздел "Безопасность".



### 3. ????????? ?????????????? ?????????? ?????????? ?????????? KES Windows

#### Выбор компонентов для установки

Обратите внимание, что по умолчанию компоненты для **desktopных** и **серверных** версий Windows необходимо указать **отдельно**

##### Изменение состава компонентов приложения

Общие Результаты Параметры Параметры приложения Расписание История ревизий

▼ Режим использования приложения на защищаемых устройствах

Компоненты приложения для установки

Настройки задачи

#### Компоненты приложения для установки Windows

Выбранный режим приложения:

Стандартный режим для защиты рабочих станций и серверов  
В этом режиме доступны все компоненты защиты и контроля Kaspersky Endpoint Security.

1 Рабочие станции 2 Файловые серверы

- ▶ ☒ Защита сетевых соединений и средств коммуникации
- ▶ ☒ Защита устройств от угроз
- ▶ ☒ Контроль безопасности
- ▶ ☐ Шифрование данных
- ▼ ☒ Detection and Response
  - ☐ Endpoint Detection and Response Expert (on-premises)
  - ☐ Endpoint Detection and Response Optimum
  - ☐ Endpoint Detection and Response Expert (cloud)
  - ☐ Sandbox
  - ☒ Managed Detection and Response
  - ☐ Network Detection and Response (KATA)
  - ☐ Интеграция с KUMA

Также необходимо указать пароль самозащиты (из раздела "**Защита паролем**" в политике KES) для выполнения данной задачи

Иначе, выполнение задачи будет завершаться соответствующей ошибкой об отсутствии пароля для изменения состава компонентов.

Изменение состава компонентов приложения

Общие

Результаты

Параметры

Параметры приложения

Расписание

История ревизий

▼

Режим использования приложения на защищаемых устройствах

Компоненты приложения для установки

1

Настройки задачи

Настройки задачи

Windows

✓

Проверять на наличие несовместимого ПО

✓

Удалять несовместимые приложения сторонних производителей

⚠

Наличие несовместимых приложений может привести к некорректной работе приложения.Рекомендуется отключать провер

☐

Использовать пароль для удаления Kaspersky Endpoint Agent и Kaspersky Security для Windows Server

Advanced settings

2

✓

Использовать пароль для изменения состава компонентов приложения

☐

Использовать режим совместимости с Azure WVD

Неприменимо, если приложение используется в режиме Легкого агента. ⓘ

Имя пользователя

3

KLAdmin

Пароль

.....

Имя пользователя и пароль должны соответствовать значениям, заданным в политике.

## 4. ?????????? ?????????????? KSN

Если компонент KSN работает исправно, а компонент MDR выдаёт ошибку стоит попробовать выключить и заново включить компонент KSN в политике, чтобы **заново принять "Положение о KSN"**.

### С сервера KSC

????? ?? ?????????????? "?????????-???????? KSN", ?????????????? ?????????????? ?  
 ?????????????????? ?????????? ?????????????????????????????? KSC ? ?????????????? KSN

KSC Linux (???-?????????)

Откройте раздел свойств сервера администрирования --> Прокси-сервер KSN --> Статистика. Если статус отличен от "Подключено" значит KSC не может подключиться к серверам KSN.

В таком случае необходимо проверить, что адреса серверов KSN, указанные в [справке](#), добавлены в разрешённые на сетевом оборудовании и/или на хосте с KSC.

Свойства Сервера администрирования

Общие

Права доступа

Серверы администрирования

Двухфакторная аутентификация

Общие

Параметры

Статистика

SNMP

Алгоритм шифрования

Веб-сервер

Вирусная атака

Глобальные подсети

Дополнительные порты

Заблокированные частые события

Иерархия Серверов администрирования

Информация об используемой базе данных

Лицензионные ключи

Лицензионные соглашения

Объявления "Лаборатории Касперского"

Папка общего доступа Сервера администрирования

Параметры доступа к сети интернет

Порты подключения

Прокси-сервер KSN

Сертификаты

Данные обновляются каждые 15 секунд.

Подключено

Подключено

Число записей в кеше

31017

Число пакетов, обработанных в кеше

41062

Полученных пакетов

40725

Копировать в буфер обмена

Также вы можете проверить сетевую доступность серверов KSN/MDR командой в терминале:

Для KSC Linux:

```
openssl s_client -showcerts -connect ds.kaspersky.com:443
```

Для KSC Windows:

```
powershell Test-NetConnection ds.kaspersky.com -port 443
```

## Локально на хосте с KES

??? ???????????? ?????? ??????? ??????? KSN

Проверьте, что с эндпоинта доступен **13111 порт** сервера KSC  
На Windows-хосте:

```
powershell Test-NetConnection <адрес KSC> -port 13111
```

На Linux-хосте:

```
nc -vz <адрес KSC> 13111
```

??? ?????????????? ? KSN ??????????

Для проверки прямого подключения хостов к KSN используйте те же команды, что для проверки доступности с сервера KSC:

Для Linux-хостов:

```
openssl s_client -showcerts -connect ds.kaspersky.com:443
```

Для Windows-хостов:

```
powershell Test-NetConnection ds.kaspersky.com -port 443
```

Revision #1

Created 27 July 2026 11:05:33 by Сергей

Updated 27 September 2026 17:08:38 by Сергей