kaspersky

Kaspersky Managed Detection and Response

© 2024 АО "Лаборатория Касперского"

Содержание

Справка Kaspersky Managed Detection and Response
О решении Kaspersky Managed Detection and Response
Аппаратные и программные требования
Что нового
Архитектура Kaspersky Managed Detection and Response
Интерфейс Kaspersky Managed Detection and Response
Интерфейс решения MDR в Kaspersky Security Center
Настройка плагина MDR в Kaspersky Security Center
Настройка плагина MDR
Настройка прав доступа в Kaspersky Security Center
Просмотр и изменение параметров MDR в Kaspersky Security Center
Использование функций плагина MDR на виртуальном Сервере администрирования
Использование функций MDR в Kaspersky Security Center с помощью прокси-сервера
Изменение сертификатов для использования функций MDR в Kaspersky Security Center с прокси-сервером или антивирусным приложением
Скрытие и отображение функций MDR в Kaspersky Security Center
Интерфейс решения MDR в Консоли MDR
Переключение языка интерфейса в Kaspersky Security Center
Переключение языка для уведомлений и отчетов в Kaspersky Security Center
Переключение языка интерфейса в Консоли MDR
Активация Kaspersky Managed Detection and Response
Активация Kaspersky Managed Detection and Response в Kaspersky Security Center
Активация Kaspersky Managed Detection and Response в Консоли MDR
Деактивация Kaspersky Managed Detection and Response
Прекращение использования Kaspersky Managed Detection and Response
Временная приостановка использования Kaspersky Managed Detection and Response
Развертывание Kaspersky Managed Detection and Response
Локальное развертывание
Развертывание с помощью Kaspersky Security Center
Развертывание с помощью Kaspersky Security Center Web Console
Облачное развертывание
О конфигурационном файле MDR
Скачивание конфигурационного файла MDR из Kaspersky Security Center
Скачивание конфигурационного файла MDR из Консоли MDR
Лицензирование
Сравнение коммерческих типов лицензий:
О лицензии
О лицензионном сертификате
О коде активации
Предоставление нового кода активации
О Соглашении о MDR
О Соглашении об обработке данных
Отзыв согласия с условиями использования решения MDR
Предоставление данных
Задействованные субподрядчики по обработке данных
О Kaspersky Security Network
Периодическое обновление конфигурационных файлов KSN
Панели мониторинга в Консоли MDR
Получение сводной информации
Получение информации обо всех активах в файле CSV (Консоль MDR)
Получение информации об инциденте в формате PDF (Консоль MDR)
Получение сводной информации обо всех инцидентах в формате PDF
Настройка рассылки отчетов в Kaspersky Security Center
Изменение расписания рассылки информации об инцидентах
Настройка рассылки отчета в Консоли MDR
Получение уведомлений
Настройка уведомлений в Консоли MDR
Настройка уведомлений в Kaspersky Security Center
Получение расширенных уведомлений
Включение расширенных уведомлений в Консоли MDR
Включение расширенных уведомлений в Kaspersky Security Center
Управление пользователями
Приглашение новых пользователей в Консоль MDR
Изменение ролей пользователей в Консоли MDR

Изменение способов уведомления пользователей в Консоли MDR
Изменение доступа пользователей к тенантам в Консоли MDR
Управление активами
Просмотр и поиск активов в Консоли MDR
Фильтрация активов в Консоли MDR
Просмотр подробной информации об активах в Консоли MDR
Статусы активов
Проверка статуса активов в Kaspersky Security Center
Как избежать потери данных телеметрии от активов
Управление инцидентами
Об инцидентах
Просмотр и поиск инцидентов в Консоли MDR
Фильтрация инцидентов в Консоли MDR
Создание пользовательских инцидентов в Консоли MDR
Просмотр подробной информации об инцидентах в Консоли MDR
Типы реагирования на инциденты
Обработка реагирования на инциденты в Консоли MDR
Автоматическое подтверждение действий по реагированию в Консоли MDR
Закрытие инцидентов в Консоли MDR
Использование функций Kaspersky Endpoint Detection and Response Optimum
Мультитенантность
Просмотр тенантов в Kaspersky Security Center
Просмотр тенантов в Консоли MDR
Просмотр параметров тенанта в Kaspersky Security Center
Просмотр параметров тенанта в Консоли MDR
Изменение параметров тенанта в Kaspersky Security Center
Изменение параметров тенанта в Консоли MDR
Добавление тенантов в Kaspersky Security Center
Добавление тенантов в Консоли MDR
Удаление тенантов в Kaspersky Security Center
Удаление тенантов в Консоли MDR
Перемещение активов от корневого тенанта к новому тенанту
Разграничение прав доступа к тенантам
Управление решением с помощью REST API
Сценарий: авторизация на основе токенов
Создание API-подключения в Kaspersky Security Center
Создание API-подключения в Консоли MDR
Изменение API-подключения в Kaspersky Security Center
Изменение API-подключения в Консоли MDR
Создание токена доступа в Kaspersky Security Center
Создание токена доступа в Консоли MDR
Работа с REST API
Отзыв обновления токена в Kaspersky Security Center
Удаление API-подключения в Kaspersky Security Center
Удаление API-подключения в Консоли MDR
Известные проблемы
Обращение в Службу технической поддержки
Способы получения технической поддержки
Техническая поддержка через Kaspersky CompanyAccount
Источники информации о решении
Глоссарий
Endpoint Protection Platform (EPP)
EPP-программа
IOC
Актив
Действие по реагированию
Инцидент
Тактика MITRE
Телеметрия
Тенант
Техника MITRE
Информация о стороннем коде
Уведомления о товарных знаках

Справка Kaspersky Managed Detection and Response

Новые функции

- Что нового в последней версии решения

Аппаратные и программные требования

- Проверьте, какие операционные системы и EPP-программы поддерживаются.

Сравнение функций

- Сравнение коммерческих лицензий решений: MDR Optimum, MDR Expert, MDR Basic, MDR Advanced и MDR Prime

Начало работы

- Локальное развертывание
- Облачное развертывание
- Активация Kaspersky Managed Detection and Response

Мониторинг и отчеты

- Получение уведомлений
- Получение расширенных уведомлений
- Получение сводной информации
- Панели мониторинга

Предоставление данных / Защита персональных данных

- Предоставление данных
- Задействованные субподрядчики по обработке данных
- Kaspersky Security Network

О решении Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response представляет собой решение для автоматического обнаружения и анализа инцидентов безопасности в вашей инфраструктуре с помощью телеметрии и передовых технологий машинного обучения. Информация об инциденте передается специалистам "Лаборатории Касперского", которые затем могут либо обработать инцидент самостоятельно, либо дать рекомендации по его устранению.

Kaspersky Managed Detection and Response (MDR) обеспечивает круглосуточную защиту от растущего количества угроз, способных обойти автоматические средства защиты, для организаций, которым сложно найти квалифицированных специалистов или у которых ограничены внутренние ресурсы. В отличие от аналогичных предложений на рынке, решение использует успешный опыт эффективного исследования целевых атак для обеспечения непрерывной защиты даже от самых сложных угроз. Решение помогает повысить устойчивость компании к киберугрозам и освободить сотрудников, чтобы они могли сосредоточиться на других задачах.

Kaspersky Managed Detection and Response получает данные от EPP-программ, которые поддерживают MDR, обрабатывают данные и отправляют их по потокам Kaspersky Security Network в Kaspersky Managed Detection and Response. Список обрабатываемых данных см. в разделе Предоставление данных. EPP-программы устанавливаются на активы в ИТ-инфраструктуре вашей организации (например, на мобильные устройства, компьютеры или ноутбуки). Примером EPP-программы является Kaspersky Endpoint Security для Windows.

Вы можете интегрировать Kaspersky Managed Detection and Response с другими решениями "Лаборатории Касперского": Kaspersky Managed Detection and Response позволяет анализировать и отслеживать данные платформы Kaspersky Anti-Targeted Attack (KATA) Platform. Чтобы настроить интеграцию Kaspersky Managed Detection and Response с Kaspersky Anti-Targeted Attack Platform, сначала необходимо получить конфигурационный файл MDR. Информация о настройке интеграции приведена в справке Kaspersky Anti-Targeted Attack Platform .

> Kaspersky Anti-Targeted Attack Platform не является частью Kaspersky Managed Detection and Response. Для использования приложения Kaspersky Anti-Targeted Attack Platform ее необходимо приобрести отдельно.

Интеграция с Kaspersky Anti-Targeted Attack Platform недоступна при использовании лицензионного ключа для региона Саудовская Аравия.

Решение Kaspersky Managed Detection and Response (MDR) не предоставляется на территории и лицам Соединенных Штатов Америки согласно решению Министерства торговли США и сопутствующим нормативно правовым актам. Использование решения MDR на указанной территории является нарушением условий использования решения MDR. Во избежание нарушения условий использования решения MDR необходимо временно прекратить использование MDR на всех активах, расположенных на указанной территории. В случае временного перемещения актива на указанную территорию, например на время командировки, требуется временно приостановить использование MDR на этом активе.

Аппаратные и программные требования

Необходимые EPP-программы и поддерживаемые конфигурации

Для использования Kaspersky Managed Detection and Response в вашей инфраструктуре должна быть развернута как минимум одна из следующих EPP-программ:

- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Linux
- Kaspersky Endpoint Security для Mac
- Kaspersky Security для Windows Server с Kaspersky Endpoint Agent для Windows

  Для использования функции MDR на серверах под управлением ОС Windows рекомендуется использовать на этих серверах Kaspersky Endpoint Security для Windows вместо Kaspersky Security для Windows Server с Kaspersky Endpoint Agent.
- Kaspersky Security для виртуальных сред 5.2 Легкий агент

Операционные системы

Kaspersky Managed Detection and Response совместим с теми же операционными системами, что и EPP-программы перечисленные ниже. Дополнительные сведения приведены в разделе *Аппаратные и программные требования* в документации совместимых EPP-программ, перечисленных в таблице ниже.

Совместимые приложения и решения "Лаборатории Касперского"

Kaspersky Managed Detection and Response совместим с версиями приложений "Лаборатории Касперского" и решений, указанными в таблице ниже.

Приложения "Лаборатории Касперского"	Рекомендуемые версии и срок их поддержки	Совместимые версии и срок их поддержки	Примечания
Kaspersky Endpoint Security для Windows	12 и выше	11 и выше	
Kaspersky Endpoint Security для Windows в конфигурации Endpoint Detection and Response Agent (EDR Agent) Начиная с Kaspersky Endpoint Security для Windows версии 12.3, приложение включает конфигурацию Endpoint Detection and Response Agent (EDR Agent). Endpoint Detection and Response Agent – это приложение, которое устанавливается на отдельные рабочие станции и серверы в ИТ-инфраструктуре организации для поддержки решений Kaspersky Managed Detection and Response и Kaspersky Anti Targeted Attack Platform (EDR). EDR Agent постоянно отслеживает процессы, запущенные на этих устройствах, на открытых сетевых соединениях и на изменяемых файлах. Компоненты защиты и контроля недоступны для EDR Agent. EDR Agent совместим со сторонними EPP-программами. Это позволяет использовать сторонние инструменты безопасности инфраструктуры наряду с функцией обнаружения и реагирования со стороны "Лаборатории Касперского". Подробнее см. в справке Kaspersky Endpoint Security для Windows.	12.3 и выше	12.3 и выше	• Для активов с Kaspersky Endpoint Security для Windows в конфигурации EDR Agent статусы *Предупреждение* и *Критический* для компонентов защиты и управления не отображаются. • Вы не можете использовать возможности Kaspersky Endpoint Detection and Response Optimum для активов с Kaspersky Endpoint Security для Windows

			в конфигурации EDR Agent. • Список EPP-программ сторонних производителей, совместимых с EDR Agent, приведен в справке Kaspersky Endpoint Security для Windows.
Kaspersky Endpoint Security для Linux	11.4 и выше	11.2 и выше	Если вы используете Kaspersky Endpoint Security для Linux и у вас не установлены пакеты Linux Audit Daemon (auditd), события системного аудита записываются в журнал ядра `dmesg`. Рекомендуется установить пакет auditd для удобства управления ротацией журналов в Kaspersky Endpoint Security для Linux.
Kaspersky Endpoint Security для Mac	11.3 и выше	11.2 и выше	
Kaspersky Security для виртуальных сред Легкий агент	5.2 и выше	5.2 и выше	
Kaspersky Endpoint Agent	3.15 и выше	3.12 и выше	Kaspersky Endpoint Agent требуется только в том случае, если вы используете Kaspersky Security для Windows Server. Обратите внимание, что решение Kaspersky Managed Detection and Response совместимо с Kaspersky Endpoint Agent версий 3.9, 3.10 и 3.11, но срок технической поддержки этих версий истек. Если вы используете Kaspersky Endpoint Agent версий 3.9, 3.10 и 3.11 в качестве агента для решения Kaspersky Managed Detection and Response, "Лаборатория Касперского" рекомендует обновить Kaspersky Endpoint Agent до версии 3.15. Работа с Kaspersky Security Center Cloud Console доступна только для Kaspersky Endpoint Agent для Windows версии 3.12 и выше.
Kaspersky Security для Windows Server	Рекомендуется использовать Kaspersky Endpoint Security для Windows 12 и выше	11.x	Для использования функции MDR на серверах под управлением Windows рекомендуется установить на этих серверах Kaspersky Endpoint Security для Windows вместо Kaspersky Security для Windows Server с Kaspersky Endpoint Agent:

			• Обнаружение угроз MDR лучше работает с Kaspersky Endpoint Security для Windows. • Функциональность MDR для Kaspersky Security для Windows Server не разрабатывается, так как ограниченная поддержка Kaspersky Security для Windows Server заканчивается 30 июня 2025 г.
Kaspersky Security Center Windows	14.2	13 и выше.	С плагином MDR для Kaspersky Security Center.
Kaspersky Security Center Linux	15.1	15.1	С плагином MDR для Kaspersky Security Center.
Kaspersky Security Center Cloud Console.	нет данных	нет данных	Всегда используется последняя версия.
Плагин MDR для Kaspersky Security Center	Последняя версия	Последняя версия	В Kaspersky Security Center 13 Windows доступна последняя версия 2.1.13. Плагин MDR версии 2.1.14 и выше доступен только в Kaspersky Security Center 14 Windows и выше.
Агент администрирования Kaspersky Security Center	Версия, поставляемая с установленным Kaspersky Security Center Windows	13 и выше.	При обновлении Kaspersky Security Center вам также нужно обновить Агент администрирования Kaspersky Security Center до соответствующей версии.
Kaspersky Anti Targeted Attack Platform + Kaspersky Endpoint Detection and Response	5.1	4.0 и выше	Обратите внимание, что облачное решение Kaspersky Endpoint Detection and Response Expert не поддерживается.
Kaspersky Endpoint Detection and Response Optimum	2.3	2.0	Если вы используете Kaspersky Endpoint Security для Windows 11.7 или выше, EDR Optimum необходимо использовать без Kaspersky Endpoint Agent. Чтобы активировать функции Kaspersky Endpoint Detection and Response Optimum, вам необходимо добавить на свои активы один из следующих лицензионных ключей с помощью Kaspersky Security Center: • Kaspersky Endpoint Detection and Response Optimum • Надстройка Kaspersky Endpoint Detection and Response Optimum

Чтобы узнать больше о поддерживаемых версиях приложений и решений "Лаборатории Касперского", перейдите на страницу жизненного цикла приложений .

Консоль Kaspersky Managed Detection and Response

Аппаратные и программные требования для Консоли Kaspersky Managed Detection and Response:

- Монитор, поддерживающий разрешение 1024x768 и выше.
- Любой из следующих браузеров:
  - Apple Safari – 15 для macOS.
  - Google Chrome – 100.0.4896.88 и выше (официальная сборка).
  - Microsoft Edge – 100 и выше.
  - Mozilla Firefox – 91.8.0 и выше.

Сетевые каналы

По нашим статистическим данным, для стабильной работы Kaspersky Managed Detection and Response рекомендуется обеспечить следующую пропускную способность сетевого канала:

- В условиях средней нагрузки: полнодуплексный канал с пропускной способностью не менее 2 Мбит/с для 1000 активов.
- В условиях пиковой нагрузки: полнодуплексный канал с пропускной способностью не менее 4 Мбит/с для 1000 активов.

Эти значения пропускной способности являются приблизительными, так как необходимая пропускная способность сильно зависит от типа нагрузки актива, генерирующего события телеметрии.

Что нового

Kaspersky Managed Detection and Response предлагает следующие новые функции и улучшения.

24.06.2024

- Доступны новые действия по реагированию:
  - Поместить файл на карантин.
  - Восстановить файл из карантина.
  - Запустить скрипт на активе.
- Новый параметр фильтрации телеметрии по тенантам в веб-виджете **Статистика телеметрии**.
- Обновлена документация REST API, включая новые примеры скриптов.
- Улучшены шаблоны отчетов, которые вы отправляете по электронной почте.
- Теперь при настройке расписания сводного отчета вы можете указать тенантов, для которых вы хотите создать отчет. Отчет будет содержать данные только для указанных тенантов.

18.12.2023

- Консоль MDR теперь содержит панель мониторинга **Статистика телеметрии**, которая показывает количество событий телеметрии, событий безопасности и инцидентов.
- Kaspersky Managed Detection and Response теперь поддерживает Kaspersky Endpoint Security для Windows в конфигурации Endpoint Detection and Response Agent (EDR Agent) (с ограничениями).

29.11.2023

- Улучшено отображение статусов активов в Консоли MDR и плагине MDR для Kaspersky Security Center: в статусе актива теперь отображается работоспособность компонентов EPP-программы, статус обновления антивирусных баз актива и статус передачи телеметрии.

- Статус актива теперь показывает наличие потери телеметрии, что позволяет идентифицировать активы с проблемами доставки телеметрии. Эта функция включена по умолчанию для новых клиентов и будет постепенно включаться для существующих клиентов.

26.10.2023

Для клиентов, которые хранят свои данные телеметрии в Королевстве Саудовская Аравия, добавлен регион резиденции клиентов **Саудовская Аравия**.

9.11.2023

Выпущен плагин MDR версии 2.3.1 для Kaspersky Security Center. В этой версии функции управления инцидентами удалены из раздела MDR в Kaspersky Security Center. Вы можете управлять инцидентами в Консоли MDR.

20.7.2023

Выпущен плагин MDR версии 2.3.0 для Kaspersky Security Center. Плагин содержит следующие улучшения:

- Теперь вы можете настроить расширенные уведомления в плагине MDR.
- Теперь вы можете использовать функции MDR в Kaspersky Security Center с плагином MDR с помощью прокси-сервера.
- Теперь вы можете менять сертификаты для использования функций MDR в Kaspersky Security Center с прокси-сервером или антивирусным приложением.

23.06.2023

Для клиентов, которые хранят свои данные телеметрии в Бразилии, добавлен регион резиденции клиентов **Латинская Америка**.

27.07.2022

Выпущен плагин MDR версии 2.1.17. Эта версия плагина совместима с Kaspersky Security Center версии 14 и выше.

31.05.2022

Общие улучшения:

- Для клиентов, которые хранят свои данные телеметрии в Северной Европе, добавлен регион резиденции клиентов **США/Канада**.
- Изменено описание процесса развертывания MDR в справке.

Улучшения в плагине MDR:

- В разделе **Настройки** теперь можно изменить язык уведомлений в Telegram и по электронной почте, а также язык общения в чате об инцидентах.
- Улучшен интерфейс работы с изображениями и таблицами в карточках инцидентов.
- MDR Expert. В разделе **Использование решения** появилась возможность выяснить, сколько инцидентов может быть создано в соответствии с Соглашением об уровне обслуживания.

Исправленные ошибки и прочие улучшения:

- При поиске в списках инцидентов и активов теперь проверяется полное вхождение искомой подстроки в любом месте строки.
- После добавления лицензионного ключа MDR и конфигурационного файла KPSN в Kaspersky Endpoint Security для Mac 11.2 и более поздних версий для передачи телеметрии больше не нужно перезагружать Mac.
- При расчете количества лицензий для виртуальных машин с Kaspersky Security для виртуальных сред Легкий агент 5.2 и более поздних версий не учитываются активы, не передававшие телеметрию более 24 часов.

20.05.2022

Пользователи MDR Optimum теперь могут обсудить инцидент с аналитиками SOC "Лаборатории Касперского" в чате (со следующим ограничением: обрабатываются только запросы, касающиеся конкретного инцидента, Соглашение об уровне обслуживания не применяется).

18.10.2021

- В плагине Kaspersky Managed Detection and Response для Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console улучшена работа функции Работоспособность MDR:
  - Оптимизирован интерфейс функции Работоспособность MDR.
  - В списке активов отображаются все активы со всеми статусами, которые ранее были доступны только в Консоли MDR.
  - Добавлены параметры фильтрации и сортировки для работы со списком активов.

21.07.2021

- Реализована поддержка Kaspersky Managed Detection and Response в Kaspersky Security Center Cloud Console, что позволяет управлять решением из единой Консоли администрирования Kaspersky Security Center. Для решения Kaspersky Managed Detection and Response доступны следующие функции:
  - Работа с инцидентами:
    - Просмотр, создание и добавление комментариев к инцидентам.
    - Обращение в Kaspersky Security Operation Center (SOC) по поводу инцидента, применение или отклонение действий по реагированию, предлагаемых аналитиками SOC.
    - Реагирование на инцидент с помощью Kaspersky Endpoint Detection and Response.

    Доступны следующие действия по реагированию на инцидент:
    - Применение сетевой изоляции устройств.
    - Создание правил блокировки по хешу.
    - Создание задач на удаление, перемещение на карантин, завершение процесса и поиск по индикаторам компрометации (IoC), относящимся к инциденту.
  - Контроль событий Kaspersky Managed Detection and Response на панелях мониторинга в Kaspersky Security Center Web Console.
  - Настройка уведомлений о событиях Kaspersky Managed Detection and Response по электронной почте и Telegram.
  - Настройка периодической отправки сводной информации о работе MDR по электронной почте.
  - Просмотр устройств, на которых наблюдаются проблемы в работе MDR.
  - Новый мастер активации, позволяющий подключить MDR в единой консоли Kaspersky Security Center.
  - Автоматическая настройка KPSN. Теперь больше не требуется выполнять загрузку и выгрузку файла конфигурации вручную в параметрах Kaspersky Security Center.
  - Управление подключениями к публичному API MDR: просмотр, создание, изменение и удаление токенов.
  - Управление тенантами организации, включая создание.
  - Получение информации о количестве инцидентов, которые может зарегистрировать пользователь. Эти инциденты обрабатываются в соответствии с условиями соглашения об уровне обслуживания (SLA).

    Эти функции также доступны в Kaspersky Security Center Web Console.
- В Консоль MDR добавлена возможность управлять несколькими учетными записями администратора MDR: создавать учетные записи и управлять их правами.
- Для работы с новыми версиями совместимых приложений больше не требуется дополнительная установка Kaspersky Endpoint Agent. Встроенные функции Kaspersky Managed Detection and Response совместимы со следующими EPP-программами:
  - Kaspersky Endpoint Security для Windows 11.6 и выше
  - Kaspersky Endpoint Security для Mac 11.2
  - Kaspersky Endpoint Security для Linux 11.2
  - Kaspersky Security для виртуальных сред 5.2 Легкий агент

Подробную информацию о различных сценариях развертывания см. в разделе Развертывание Kaspersky Managed Detection and Response.

- В Kaspersky Endpoint Security для Windows и для Linux добавлен фильтр по типу событий со встроенным функционалом Kaspersky Managed Detection and Response, что позволяет снизить нагрузку на каналы и потребление трафика при отправке данных телеметрии.

- Реализованы следующие типы реагирования на инциденты: получение файла с устройства, изоляция устройства, отключение изоляции устройства, удаление ключа реестра, завершение процесса.

  Выполнение этих действий возможно при наличии подтверждения от пользователя с ролью Администратор MDR.

- Веб-плагин для Kaspersky Security Center Web Console и Cloud Console поддерживает следующие языки: французский, немецкий, итальянский и испанский.

31.03.2021

Добавлен веб-плагин для Kaspersky Security Center Web Console, который позволяет использовать следующие функции решения Kaspersky Managed Detection and Response:

- Просмотр списка инцидентов.

- Создание инцидентов

- Добавление комментариев к инцидентам.

- Обращение в Kaspersky Security Operation Center по поводу инцидента.

- Принятие или отклонение действий по реагированию на инцидент, предложенных аналитиками SOC.

- Возможность самостоятельного реагирования на инцидент:

  - Сетевая изоляция активов.

  - Создание правил блокировки по хешу.

  - Создание задач на удаление, перемещение в карантин, завершение процесса и поиск по индикаторам компрометации (IoC), относящихся к инциденту.

- Контроль событий Kaspersky Managed Detection and Response на панелях мониторинга в Kaspersky Security Center Web Console.

- Настройка уведомлений по электронной почте и Telegram о событиях Kaspersky Managed Detection and Response

- Настройка периодической отправки сводной информации об инцидентах по электронной почте.

Архитектура Kaspersky Managed Detection and Response

На следующем рисунке показаны компоненты Kaspersky Managed Detection and Response и взаимодействие между ними.

Архитектура Kaspersky Managed Detection and Response

Описание компонентов Kaspersky Managed Detection and Response:

- Актив – это принадлежащее организации устройство, защищенное решениями "Лаборатории Касперского".

- Endpoint Protection Platform (EPP) – это программа "Лаборатории Касперского", защищающая активы и хранящиеся на них данные от вредоносных программ и других угроз.

- Kaspersky Endpoint Agent – программный компонент, который устанавливается на рабочие станции и серверы корпоративной ИТ-инфраструктуры. Kaspersky Endpoint Agent постоянно отслеживает процессы, запущенные на этих компьютерах, а также активные сетевые подключения и изменяемые файлы. В последних версиях EPP-программ он был заменен встроенным функционалом.

- Агент администрирования – это компонент Kaspersky Security Center, обеспечивающий взаимодействие между Сервером администрирования и приложениями "Лаборатории Касперского", установленными на конкретном сетевом узле (рабочей станции или сервере). Этот компонент является общим для всех приложений компании для Microsoft Windows. Для приложений "Лаборатории Касперского", разработанных для Unix-подобных операционных систем и macOS, существуют отдельные версии Агента администрирования.

- Kaspersky Security Center – это приложение, предназначенное для администраторов корпоративных сетей и сотрудников, отвечающих за защиту активов в различных организациях.

- Kaspersky Security Network – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

- Kaspersky Managed Detection and Response (далее также MDR) – это решение, обеспечивающее непрерывную управляемую защиту и позволяющее организациям автоматически выявлять труднообнаружимые угрозы и освобождать сотрудников группы ИТ-безопасности для решения задач, требующих их участия.

- Консоль MDR предоставляет веб-интерфейс для управления и обслуживания системы защиты сети организации клиента, управляемой Kaspersky Managed Detection and Response. Функции Консоли MDR дополняются веб-плагином Kaspersky Security Center, позволяющим управлять Kaspersky Managed Detection and Response из единой Консоли администрирования.

- MDR API – это программный интерфейс для управления и обслуживания системы защиты сети организации клиента, управляемой Kaspersky Managed Detection and Response.

Интерфейс Kaspersky Managed Detection and Response

В этом разделе приведена информация о пользовательском интерфейсе Kaspersky Managed Detection and Response.

С Kaspersky Managed Detection and Response можно работать, используя следующие интерфейсы:

- Раздел **MDR** в Kaspersky Security Center Web Console или в Kaspersky Security Center Cloud Console.

  Для того чтобы использовать Kaspersky Security Center Web Console с Kaspersky Managed Detection and Response, вам необходимо скачать и настроить плагин MDR в Kaspersky Security Center Web Console. В Kaspersky Security Center Cloud Console плагин MDR предустановлен.

  Чтобы получить доступ к функциям Kaspersky Managed Detection and Response, в Kaspersky Security Center Web Console или в Kaspersky Security Center Cloud Console выберите **Мониторинг и отчеты** → **MDR**.

- Портал Kaspersky Managed Detection and Response (далее также Консоль MDR).

  После входа Консоль MDR доступна по адресу https://mdr.kaspersky.com/. Для входа используйте адрес электронной почты и пароль учетной записи сайта "Лаборатории Касперского", созданные при активации Kaspersky Managed Detection and Response.

Возможности и доступные функции в этих интерфейсах в основном одинаковы, но некоторые задачи рекомендуется выполнять в одном из интерфейсов, поскольку имеется более широкий набор функций или доступных данных. Рекомендуемый интерфейс указан в описании задач и сценариев использования.

Интерфейс Kaspersky Security Center в основном предназначен для решения следующих задач:

- Активация Kaspersky Managed Detection and Response

- Проверка статуса активов

Интерфейс Консоли MDR в основном предназначен для решения следующих задач:

- Задачи сотрудников службы безопасности: управление инцидентами.

- Задачи администратора: управление пользователями MDR.

- Просмотр и управление активами.

Интерфейс решения MDR в Kaspersky Security Center

Вы можете работать с Kaspersky Managed Detection and Response с помощью раздела **MDR** в Kaspersky Security Center Web Console или в Kaspersky Security Center Cloud Console. Чтобы получить доступ к функциям Kaspersky Managed Detection and Response, в Kaspersky Security Center выберите **Мониторинг и отчеты** → **MDR**.

Раздел **MDR** в Kaspersky Security Center содержит следующие вкладки:

- **Инциденты**. Содержит ссылку на Консоль MDR, где вы можете управлять своими инцидентами.

- **Отчеты**. Содержит список задач по рассылке отчетов и функции для изменения, удаления и создания задач.

- **Параметры**. Позволяет включить расширенные уведомления и переключить язык для данных об инцидентах, уведомлений и отчетов.

- **Уведомления**. Позволяет включить уведомления по электронной почте и в Telegram.

- **API**. Содержит список API-подключений и функций для управления API-подключениями.

- **Тенанты**. Содержит список тенантов и функции для управления тенантами.

- **Работоспособность MDR**. Содержит списки неисправных активов и всех активов, которые были.

- **Начало работы**. Содержит инструкции по настройке решения MDR.

- **Использование MDR**. Содержит информацию о статусе активации решения, лицензии, регионе хранения телеметрии, конфигурационном файле KSN и статусе принятия Условий использования.

Также вы можете добавить веб-виджет **Активы MDR по статусу** на панель **Мониторинг и отчеты** → **Панель мониторинга** в Kaspersky Security Center.

Настройка плагина MDR в Kaspersky Security Center

В этом разделе описана первоначальная настройка плагина MDR в Kaspersky Security Center для работы с Kaspersky Managed Detection and Response.

Настройка плагина MDR

Для работы с решением Kaspersky Managed Detection and Response с помощью плагина MDR, необходимо настроить плагин MDR в приложениях:

- Kaspersky Security Center Web Console в приложении Kaspersky Security Center Windows.
- Kaspersky Security Center Web Console в приложении Kaspersky Security Center Linux.
- Kaspersky Security Center Cloud Console.

Предварительные требования

Убедитесь, что у вас есть доступ к Kaspersky Security Center Web Console или к Kaspersky Security Center Cloud Console со следующими минимальными правами доступа:

- Право **Чтение** для функциональной области Kaspersky Security Center **Общие функции: Интеграция приложений**.
- Право **Разрешить** для функциональной области **Доступ к инцидентам** в Kaspersky Managed Detection and Response.

Шаги

Настройка выполняется поэтапно:

1. **Скачивание плагина MDR**

   Пропустите этот шаг, если вы используете Kaspersky Security Center Cloud Console, поскольку плагин MDR предустановлен в Kaspersky Security Center Cloud Console.

   В Kaspersky Security Center Web Console скачайте плагин MDR, выбрав **Kaspersky Managed Detection and Response** в списке доступных плагинов. Подробную информацию о том, как получить веб-плагины, см. в справке Kaspersky Security Center Windows или в справке Kaspersky Security Center Linux.

2. **Установка прав доступа**

   Вручную назначьте права доступа всем пользователям плагина MDR или автоматически создайте роли MDR с заданными правами доступа, перейдя по ссылке на первом шаге на вкладке **Начало работы** в плагине MDR.

Результаты

По завершении этого сценария плагин MDR будет настроен для работы с Kaspersky Managed Detection and Response.

Настройка прав доступа в Kaspersky Security Center

Необходимо задать права доступа для каждого пользователя Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console, использующего функции MDR Kaspersky Security Center. Права доступа зависят от действий, которые вы хотите, чтобы пользователи могли выполнять.

Можно автоматически создавать роли MDR с заданными правами доступа, перейдя по ссылке на первом шаге на вкладке **Начало работы** в разделе **MDR** в Kaspersky Security Center.

Чтобы задать права доступа:

1. В Kaspersky Security Center перейдите в раздел **Пользователи и роли** → **Роли** и создайте роль. Подробнее о создании ролей см. в справке Kaspersky Security Center Windows, в справке Kaspersky Security Center Linux Help или в справке Kaspersky Security Center Cloud Console.
2. На вкладке **Права доступа** для новой роли установите значение **Разрешить** для следующих функциональных областей:
   - **Интеграция приложений**

Позволяет пользователям настроить интеграцию Kaspersky Security Center с другими приложениями и решениями "Лаборатории Касперского".

> Для пользователей, управляющих плагином MDR, необходимо установить право **Разрешить** для функциональной области **Интеграция приложений**. Это право позволяет пользователям активировать, настраивать, использовать и прекращать использование Kaspersky Managed Detection and Response.

- **Доступ к инцидентам**

  Необходимо установить право **Разрешить** для функциональной области **Доступ к инцидентам**, чтобы пользователи имели доступ к разделу **MDR** в Kaspersky Security Center. Если для функциональной области **Доступ к инцидентам** установлено право **Запретить**, пользователи увидят только вкладку **Начало работы** в разделе **MDR** в Kaspersky Security Center.

- **Управление тенантами**

  Позволяет пользователям создавать, просматривать и редактировать тенанты.

- **Доступ к REST API**

  Позволяет пользователям управлять решением Kaspersky Managed Detection and Response с помощью REST API.

В следующей таблице приведен минимальный набор прав доступа.

Минимальный набор прав доступа

Функциональная область	Разрешать	Запретить
Интеграция приложений	—	✓
Доступ к инцидентам	✓	—
Параметры автоподтверждения	—	✓
Управление действиями по реагированию	—	✓
Управление тенантами	—	✓
Сводная информация по инцидентам	—	✓
Доступ к REST API	—	✓

3. Назначьте созданную роль всем пользователям, которые будут использовать функции MDR в Kaspersky Security Center.

Права доступа установлены.

Просмотр и изменение параметров MDR в Kaspersky Security Center

Вы можете просматривать и изменять параметры плагина MDR, установленного в Kaspersky Security Center.

Чтобы просмотреть и настроить параметры плагина MDR:

1. В разделе **MDR** в Kaspersky Security Center откройте вкладку **Параметры**.
2. Если вы хотите включить расширенные уведомления, включите параметр **Включить расширенные уведомления по электронной почте** и установите флажок, чтобы подтвердить, что вы прочитали и поняли условия отправки расширенных уведомлений.
3. Вы можете использовать параметр **Язык**, чтобы выбрать английский или русский язык для отображения отчетов и уведомлений.
4. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить параметры.

   Кнопка **Сохранить** становится активной только в случае изменения параметров.

Использование функций плагина MDR на виртуальном Сервере администрирования

Чтобы использовать функции MDR в Kaspersky Security Center на виртуальном Сервере администрирования:

- Если вы используете Kaspersky Security Center для Windows:

  1. Загрузите конфигурационный файл MDR в Kaspersky Security Center Web Console или в Консоль MDR.
  2. В Kaspersky Security Center Web Console выберите главный (физический) Сервер администрирования, на котором расположен ваш виртуальный Сервер администрирования.
  3. Включите переключатель **Kaspersky Private Security Network** в свойствах главного (физического) Сервера администрирования.
  4. Нажмите на кнопку **Выбрать файл параметров прокси-сервера KSN** и выберите конфигурационный файл MDR, который вы скачали.

- Если вы используете Kaspersky Security Center Cloud Console:

  1. Активируйте Kaspersky Managed Detection and Response на главном (физическом) Сервере администрирования.

  2. На главном (физическом) Сервере администрирования перейдите в раздел **Мониторинг и отчеты** → **MDR**, откройте вкладку **Использование MDR** и убедитесь, что в разделе **KPSN** указаны правильные статус и версия конфигурационного файла KPSN. Пример правильного статуса и версии:

     ```
     Для отправки телеметрии в инфраструктуру MDR Лаборатории Касперского используется конфигурационный файл KPSN
      версии {{version}}
     ```

     Если статус или версия файла неверны, обратитесь в Службу технической поддержки.

Использование функций MDR в Kaspersky Security Center с помощью прокси-сервера

Если в сети, где работает Kaspersky Security Center, используется прокси-сервер, необходимо задать две переменные среды с параметрами прокси-сервера для протокола HTTP и протокола HTTPS, чтобы функции MDR в Kaspersky Security Center работали должным образом. Эти переменные среды должны быть заданы на устройстве, на котором установлено приложение Kaspersky Security Center Web Console.

Переменные окружения имеют следующий формат:

```
HTTP_PROXY=<protocol>://<proxy_user_name>:<proxy_user_password>@<host>:<port>
```

где:

- `<protocol>` – это http или https.
- `<proxy_user_name>` – имя пользователя для авторизации на прокси-сервере.
- `<proxy_user_password>` – пароль для авторизации на прокси-сервере.
- `<host>:<port>` – это имя или IP-адрес прокси-сервера и номер его порта.

  Пример переменных окружения:

  ```
  HTTP_PROXY=http://proxy_user_name:proxy_user_password@proxy.domain.com:8080
  HTTPS_PROXY=https://proxy_user_name:proxy_user_password@proxy.domain.com:443
  ```

Вы можете установить переменные окружения двумя способами:

- Если вы хотите применить параметры прокси-сервера ко всем приложениям на устройстве, на котором установлено приложение Kaspersky Security Center Web Console, добавьте эти переменные окружения с помощью компонента операционной системы Windows **Настройка системных переменных окружения**. Информацию об использовании этого компонента см. в документации к используемой вами версии операционной системы.
- Если вы хотите применить эти параметры прокси-сервера только к Kaspersky Security Center Web Console, добавьте эти переменные окружения в файл с расширением .ENV, расположенный в папке установки Kaspersky Security Center Web Console (по умолчанию C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\). Если файл с расширением .ENV отсутствует в папке установки, создайте его.

После настройки переменных окружения вам необходимо перезагрузить устройство, на котором установлено приложение Kaspersky Security Center Web Console, чтобы изменения вступили в силу.

Изменение сертификатов для использования функций MDR в Kaspersky Security Center с прокси-сервером или антивирусным приложением

Вам необходимо настроить цепочку сертификатов для настройки соединения Kaspersky Security Center Web Console с плагином MDR и инфраструктурой решения MDR в следующих случаях:

- В сети, где запущен Kaspersky Security Center, используется прокси-сервер с TLS-соединением.
- Антивирусное приложение с шифрованием TLS-трафика запущена на устройстве, на котором установлено приложение Kaspersky Security Center Web Console.

Чтобы настроить цепочку сертификатов:

1. Сохраните необходимые сертификаты в виде файлов на своем устройстве.

   - Чтобы сохранить файл сертификата приложения, шифрующей трафик, на устройстве с установленным приложением Kaspersky Security Center Web Console, в браузере Chrome откройте ссылку https://mdr-ksc.kaspersky.com/, нажмите на значок замка в адресной строке рядом с адресом сайта, выберите пункт **Безопасное подключение**, нажмите **Действительный сертификат**, перейдите на вкладку **Подробнее** и нажмите на кнопку **Экспорт**. Инструкции для других браузеров см. в документации для этих браузеров.

- Для того чтобы получить сертификат, используемый для подключения к прокси-серверу, обратитесь к администратору сети.

2. Добавьте сохраненные сертификаты в файл с расширением .PEM (например, KL_Root.pem).

3. Поместите созданный файл с расширением .PEM в папку установки Kaspersky Security Center Web Console (по умолчанию C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\).

4. Добавьте переменную окружения NODE_EXTRA_CA_CERTS в файл с расширением .ENV, расположенный в папке установки Kaspersky Security Center Web Console. Если файл с расширением .ENV отсутствует в папке установки, создайте его.

   Пример переменной:

   NODE_EXTRA_CA_CERTS="C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\KL_Root.pem"

Чтобы изменения вступили в силу после того, как вы задали переменную окружения, перезапустите устройство, на котором установлено приложение Kaspersky Security Center Web Console.

Скрытие и отображение функций MDR в Kaspersky Security Center

По умолчанию элементы интерфейса, связанные с Kaspersky Managed Detection and Response, отображаются в интерфейсе Kaspersky Security Center. Если вы не используете Kaspersky Managed Detection and Response, вы можете скрыть его функции из интерфейса. В дальнейшем можно изменить параметры интерфейса, чтобы отображались скрытые ранее элементы.

Чтобы скрыть функции MDR в Kaspersky Security Center Cloud Console:

1. В Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console наведите курсор мыши на имя пользователя в нижней части левой панели. Откроется меню параметров интерфейса.

2. Выберите **Параметры интерфейса**.

3. Выключите или включите параметр **Показать функции MDR**.

4. Нажмите на кнопку **Сохранить**.

   Kaspersky Security Center сохраняет значение этого параметра только для вашей учетной записи. Другие пользователи могут установить другое значение.

   Раздел **MDR** скрыт или отображен.

Интерфейс решения MDR в Консоли MDR

Вы можете работать с Kaspersky Managed Detection and Response в веб-интерфейсе, далее также Консоль MDR.

Окно Консоли MDR содержит следующие элементы:

- Главное меню в левой части окна.
- Рабочая область в правой части окна.

Главное меню

Главное меню состоит из следующих разделов:

- **Мониторинг**. Содержит веб-виджеты со сводной информацией об активных инцидентах, активах и действиях по реагированию.
- **Инциденты**. Содержит подробную информацию о ваших инцидентах и инструментах для работы с ними.
- **Активы**. Содержит подробную информацию об активах и инструментах для работы с ними.
- **Параметры**. Содержит вкладки для работы с учетными записями пользователей, уведомлениями, параметрами инцидентов, сводными отчетами, API, тенантами и общими параметрами.
- **О решении**. Содержит информацию о решении, ссылки на Соглашение MDR, Соглашение об обработке данных, эту справку и веб-сайт Службы технической поддержки.

В нижней части левой панели находится элемент управления **параметрами учетной записи**, который позволяет получить доступ к *руководству Начало работы*, изменить язык интерфейса, перейти на страницу профиля пользователя и выйти из Консоли MDR.

Рабочая область

В рабочей области отображается информация, которую вы выбираете для просмотра в Консоли MDR. Рабочая область также содержит элементы управления, которые можно использовать для настройки отображения информации.

Переключение языка интерфейса в Kaspersky Security Center

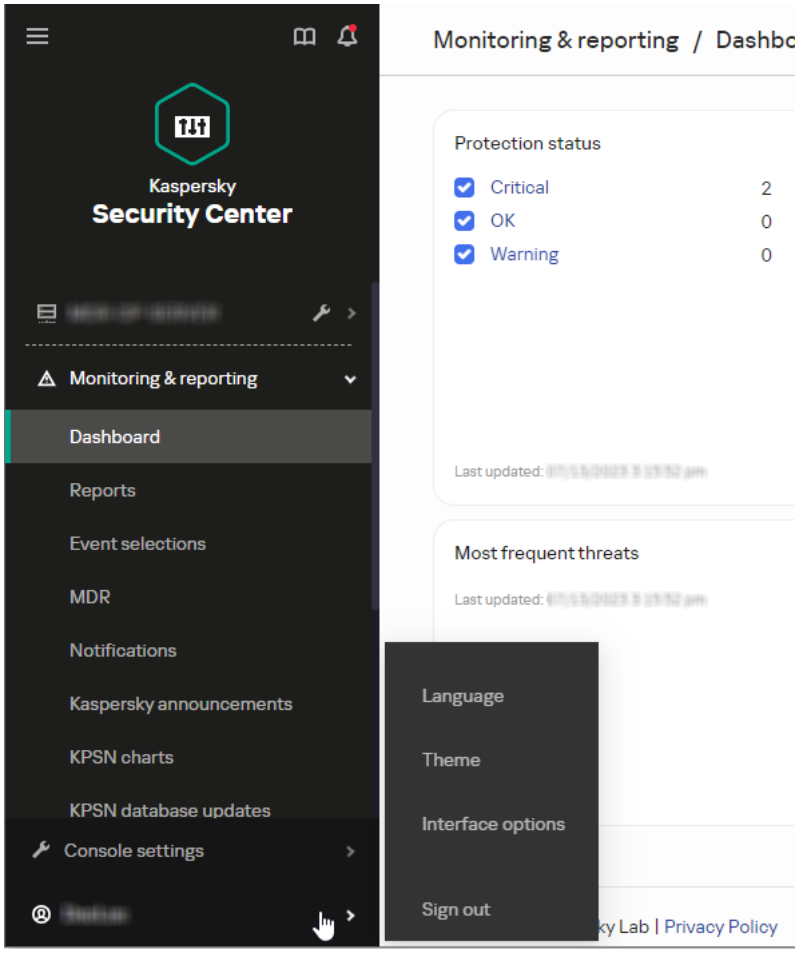
Интерфейс MDR в Kaspersky Security Center доступен на следующих языках:

- английском;
- русском;
- немецком;
- испанском;
- французском;
- итальянском.

Чтобы переключить язык интерфейса в Kaspersky Security Center:

1. В Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console наведите курсор мыши на имя пользователя в нижней части левой панели.

   Откроется меню параметров интерфейса.



Переключение языка интерфейса в Kaspersky Security Center

2. Выберите пункт **Язык**.

   Отобразится раздел **Параметры пользователя**.

3. На вкладке **Язык** выберите один из языков, который вы хотите применить к интерфейсу MDR в Kaspersky Security Center.

Язык будет изменен.

Вы можете изменить язык в любое время.

Переключение языка для уведомлений и отчетов в Kaspersky Security Center

- В Kaspersky Security Center вы можете выбрать английский или русский язык для отображения данных об инцидентах, уведомлений и отчетов.

Чтобы переключить язык для уведомлений и отчетов в Kaspersky Security Center:

1. В Kaspersky Security Center Web Console или в Kaspersky Security Center Cloud Console перейдите в раздел **MDR** → **Параметры**.

2. В области **Язык** выберите **Русский** или **Английский**.

3. Нажмите на кнопку **Сохранить**.

Язык будет изменен.

Вы можете изменить язык в любое время.

Переключение языка интерфейса в Консоли MDR

Интерфейс Консоли MDR доступен на следующих языках:

- английском;
- русском.

Чтобы изменить язык интерфейса Консоли MDR:

1. В окне Консоли MDR перейдите в раздел **Параметры учетной записи**, расположенный в нижней части на левой панели. Этот раздел содержит подраздел **Язык**.

2. В разделе **Язык** выберите язык, который вы хотите использовать в интерфейсе Консоли MDR.

Язык изменен. Вы можете изменить его на другой язык в любое время.

Активация Kaspersky Managed Detection and Response

Рекомендуется активировать Kaspersky Managed Detection and Response в Kaspersky Security Center с установленным плагином MDR, как описано в этом разделе.

Активация Kaspersky Managed Detection and Response в Kaspersky Security Center

Активация Kaspersky Managed Detection and Response недоступна в пробной рабочей области Kaspersky Security Center Cloud Console.

Чтобы активировать Kaspersky Managed Detection and Response:

1. Убедитесь, что плагин MDR установлен и настроен в Kaspersky Security Center.

2. В Kaspersky Security Center Web Console или в Kaspersky Security Center Cloud Console перейдите в раздел **Мониторинг и отчеты** → **MDR**.

3. Нажмите на кнопку **Активировать решение**.

4. Kaspersky Managed Detection and Response проверяет, включено ли фоновое соединение между Kaspersky Security Center Web Console и Сервером администрирования, и при необходимости предлагает включить его.

5. Если вы ранее не создавали учетную запись на Kaspersky Account, создайте ее и подтвердите, перейдя по ссылке подтверждения, отправленной на вашу электронную почту.

   Если ранее созданная учетная запись Kaspersky Account (то есть ваша электронная почта) использовалась для доступа к Kaspersky Managed Detection and Response, она может быть связана с данными MDR другой организации и может быть недоступна для применения нового кода активации. Чтобы использовать существующую учетную запись Kaspersky для новой активации, обратитесь в Службу технической поддержки.
   Обратите внимание: после того как сотрудники Службы технической поддержки удалят привязку вашей учетной записи Kaspersky Account к данным другой организации в MDR, ваша учетная запись Kaspersky Account больше не может использоваться для доступа к данным другой организации, для которых она использовалась ранее.

6. После активации вашей учетной записи Kaspersky Account в разделе **MDR** Kaspersky Security Center войдите в свою учетную запись Kaspersky Account.

7. Kaspersky Managed Detection and Response проверяет, есть ли у учетной записи активный лицензионный ключ для Kaspersky Managed Detection and Response:

   - Если активный лицензионный ключ отсутствует, введите код активации, полученный от "Лаборатории Касперского", выберите ваш регион и нажмите на кнопку **Активировать**.

Выбранный регион влияет на язык решения (русский или английский) и место хранения ваших данных телеметрии. При выборе региона **Европа** или **Канада** данные телеметрии хранятся в Северной Европе. При выборе региона **Латинская Америка** данные телеметрии хранятся в Бразилии. Если вы выберете **Саудовскую Аравию**, ваши данные телеметрии будут храниться в Королевстве Саудовская Аравия. Если вы выберете **Россия** или другие регионы, ваши данные телеметрии будут храниться в России.

- Если добавлен активный лицензионный ключ и есть тенанты, выберите тенанты, к которым пользователи этого Сервера администрирования будут иметь доступ.

Включенное фоновое соединение необходимо для работы Kaspersky Managed Detection and Response.

8. Прочтите и примите Соглашения, применимые к выбранному вами региону, нажав на кнопку **Принять**.

   Если вы не согласны с условиями использования Соглашений, вы не сможете использовать Kaspersky Managed Detection and Response.

9. Ознакомьтесь и примите Положение о KSN, включите использование KSN и примените файл конфигурации KSN для вашей организации.

   Если вы не согласны с условиями использования Положения о KSN, вы не сможете использовать Kaspersky Managed Detection and Response.

Активация будет завершена.

Чтобы прекратить использование Kaspersky Managed Detection and Response, см. раздел Прекращение использования Kaspersky Managed Detection and Response или обратитесь в Службу технической поддержки.

Активация Kaspersky Managed Detection and Response в Консоли MDR

Чтобы активировать Kaspersky Managed Detection and Response:

1. Если вы ранее не создавали учетную запись на Kaspersky Account, создайте ее и подтвердите, перейдя по ссылке подтверждения, отправленной на вашу электронную почту.

   Если ранее созданная учетная запись Kaspersky Account (то есть ваша электронная почта) использовалась для доступа к Kaspersky Managed Detection and Response, она может быть связана с данными MDR другой организации и может быть недоступна для применения нового кода активации. Чтобы использовать существующую учетную запись Kaspersky для новой активации, обратитесь в Службу технической поддержки.
   Обратите внимание: после того как сотрудники Службы технической поддержки удалят привязку вашей учетной записи Kaspersky Account к данным другой организации в MDR, ваша учетная запись Kaspersky Account больше не может использоваться для доступа к данным другой организации, для которых она использовалась ранее.

2. После активации вашей учетной записи Kaspersky Account в Консоли MDR войдите в свою учетную запись Kaspersky Account.

3. Для использования Консоли MDR введите полученный от "Лаборатории Касперского" код активации в соответствующее поле на странице.

4. Прочтите и примите Соглашения, применимые к вашему региону, нажав на кнопку **Подтвердить**.

   Если вы не согласны с условиями использования Соглашений, вы не сможете использовать Kaspersky Managed Detection and Response.

Активация будет завершена.

Чтобы прекратить использование Kaspersky Managed Detection and Response, ознакомьтесь с этой статьей или обратитесь в Службу технической поддержки.

Деактивация Kaspersky Managed Detection and Response

Если вы хотите остановить использование Kaspersky Managed Detection and Response, вы можете либо полностью прекратить его использование, либо временно приостановить его на определенных активах.

Прекращение использования Kaspersky Managed Detection and Response

При желании вы можете вручную прекратить использование Kaspersky Managed Detection and Response.

Когда вы прекращаете использование Kaspersky Managed Detection and Response, прекращается отправка телеметрии с ваших активов. Чтобы удалить данные о вашей организации из инфраструктуры Kaspersky Managed Detection and Response, обратитесь в Службу технической поддержки.

Чтобы прекратить использование Kaspersky Managed Detection and Response:

1. Если вы используете EPP-программы, поддерживающие политики, в Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console перейдите в раздел **Устройства** → **Политики и профили**.

   Если вы используете EPP-программу, которая не поддерживает политики, перейдите в раздел **Устройства** → **Задачи**.

   Откроется список политик (или список задач).

2. Выберите политику или задачу, созданную при развертывании Kaspersky Managed Detection and Response, чтобы настроить интеграцию между EPP-программой и Kaspersky Managed Detection and Response.

   Откроется окно параметров политики (или параметров задачи).

3. На вкладке **Параметры приложения** в левой панели выберите **Detection and Response** и в правой панели выберите **Managed Detection and Response**.

   Откроется панель параметров **Managed Detection and Response**.

4. Выключите параметр **Managed Detection and Response включено**.

   Название опции изменится на **Managed Detection and Response отключен**.

5. Сохраните изменения политики или задачи.

6. Отзовите согласие с условиями использования решения MDR.

7. Если вы используете приложение Kaspersky Security Center Web Console, работающее локально, для работы с Kaspersky MDR дополнительно рекомендуется удалить конфигурационный файл Kaspersky Security Network с Сервера администрирования Kaspersky Security Center.

Использование Kaspersky Managed Detection and Response будет прекращено.

Временная приостановка использования Kaspersky Managed Detection and Response

Для соблюдения условий использования решения MDR необходимо приостановить использование решения на активах, если они временно находятся на территории США (например на время командировки).

Чтобы временно приостановить использование решения MDR на определенных активах:

1. В Kaspersky Security Center создайте группу администрирования для управления активами, на которых вы хотите приостановить использование решения MDR. Вы можете изменить список активов в этой группе позже.

2. Для этой группы администрирования создайте политики EPP-программ, используемых для предоставления телеметрии MDR с активов, и выключите использование решения MDR и Kaspersky Security Network в параметрах политики.

   Подробную информацию о настройке политик см. в справках для конкретных EPP-программ. Например, справка Kaspersky Endpoint Security для Windows содержит инструкции по управлению политиками и настройке интеграции с решением MDR.

3. Переместите активы, на которых вы хотите приостановить использование решения MDR, в созданную группу администрирования.

   После синхронизации к активам будет применена новая политика, в которой выключено использование решения MDR и Kaspersky Security Network. Также можно вручную выполнить принудительную синхронизацию.

Чтобы возобновить использование Kaspersky Managed Detection and Response после приостановления:

1. Исключите актив из группы администрирования, которая используется для приостановки.

2. Примените обычную политику, в которой использование решения MDR включено и настроено для этого актива.

   Активы не будут контролироваться решением MDR до тех пор, пока к ним не будет применена политика, в которой разрешено и настроено использование решения MDR.

Развертывание Kaspersky Managed Detection and Response

В этом разделе приведена информация о развертывании Kaspersky Managed Detection and Response. Сценарии развертывания различаются в зависимости от используемых в вашей инфраструктуре приложений "Лаборатории Касперского".

Прежде всего, необходимо выполнить предварительные требования, зависящие от приложения, используемой для централизованного управления сетевой безопасностью:

- *Локальные приложения* – это Kaspersky Security Center (Консоль администрирования на базе Microsoft Management Console) и Kaspersky Security Center Web Console.

- *Облачное решение* – это Kaspersky Security Center Cloud Console.

Дальнейшие шаги по развертыванию Kaspersky Managed Detection and Response зависят от того, какие именно EPP-программы установлены на ваших активах.

KSN будет отключен до тех пор, пока не будет принято Положение о Kaspersky Security Network. Кроме того, активы в Kaspersky Security Center могут иметь статус *Критический*, и возникнет событие *Серверы KSN недоступны*. Использование KSN включается после применения политики, в которой администратор принимает условия использования KSN.

Локальное развертывание

В этом разделе описаны сценарии развертывания Kaspersky Managed Detection and Response с использованием локальных приложений: Kaspersky Security Center (Консоль администрирования на базе Microsoft Management Console) и Kaspersky Security Center Web Console.

Развертывание с помощью Kaspersky Security Center

Развернуть все | Свернуть все

Предварительные требования

- ИТ-инфраструктура должна соответствовать аппаратным и программным требованиям Kaspersky Managed Detection and Response.
- На каждом активе, который требуется защитить, должен быть разрешен исходящий незашифрованный сетевой трафик для портов 443 и 1443, а проверка трафика должна быть выключена. Эти порты используются для передачи данных телеметрии от активов на следующие серверы "Лаборатории Касперского":
  - *.ksn.kaspersky-labs.com
  - ksn-*.kaspersky-labs.com
  - ds.kaspersky.com

Развертывание Kaspersky Managed Detection and Response с помощью Kaspersky Security Center состоит из следующих шагов:

1. **Активация решения**

   Активируйте решение Kaspersky Managed Detection and Response с использованием вашей лицензии.

2. **Установка EPP-программ**

   Убедитесь, что на активах установлены EPP-программы, которые поддерживают функции Kaspersky Managed Detection and Response.

3. **Скачивание конфигурационного файла MDR**

   Скачайте конфигурационный файл MDR для вашей организации или отдельные архивы для каждого тенанта из раздела **Tenants** в Консоли MDR.

   Начиная с версии Kaspersky Endpoint Security для Windows 12.6, если у вас есть только корневой тенант и вы не используете решение MDR вместе с Kaspersky Endpoint Detection and Response Optimum, вам не нужно загружать конфигурационный файл MDR. См. инструкцию для Kaspersky Endpoint Security для Windows на шаге 5.

4. **Конфигурация Kaspersky Private Security Network (KPSN).**

   Настройте KPSN на активах, используя конфигурационный файл KSN из файла конфигурации MDR.

   Этот шаг гарантирует отправку телеметрии на выделенные серверы, соответствующие требованиям Общего регламента по защите данных (GDPR). Если вы не настроите KPSN, телеметрия не будет передаваться и услуга Kaspersky Managed Detection and Response не будет предоставлена.

5. **Интеграция с EPP-программами**

   Выполните сценарии развертывания для всех приложений "Лаборатории Касперского", установленных на ваших активах.

   - **Kaspersky Endpoint Security для Windows**

     Развертывание зависит от того, какая версия Kaspersky Endpoint Security для Windows установлена на ваших активах. Если в вашей инфраструктуре установлено несколько версий Kaspersky Endpoint Security для Windows, можно выполнять сценарии для этих версий в любом порядке.

     Kaspersky Endpoint Security для Windows 12.6 и выше с только корневым тенантом и без Kaspersky Endpoint Detection and Response Optimum

     Если у вас есть только корневой тенант, вы можете не загружать конфигурационный файл MDR, а добавить и распространить лицензионный ключ прямо в Kaspersky Security Center.

     Чтобы развернуть Kaspersky Managed Detection and Response в Kaspersky Endpoint Security для Windows 12.6 и выше:

1. Убедитесь, что все ваши активы принадлежат корневому тенанту.
2. Проверьте, обновлен ли Kaspersky Endpoint Security для Windows на всех активах до версии 12.6 или выше.
3. Убедитесь, что компонент Kaspersky Managed Detection and Response включен в Kaspersky Endpoint Security для Windows на всех активах.
4. Добавьте лицензионный ключ в хранилище лицензионных ключей Kaspersky Security Center.
5. Распространите лицензионный ключ на активы автоматически или с помощью задачи *Добавить лицензионный ключ*.

Подробнее об одновременном использовании решений MDR и EDR Optimum см. в справке Kaspersky Endpoint Security для Windows.

Kaspersky Endpoint Security для Windows версий 11.6–12.5 и выше с несколькими тенантами

Если вы переключаетесь на встроенные функции MDR в Kaspersky Endpoint Security для Windows после работы с решением с использованием функций Kaspersky Endpoint Agent, обязательно выключите Kaspersky Managed Detection and Response в политике Kaspersky Endpoint Agent после настройки интеграции с Kaspersky Managed Detection and Response в политике Kaspersky Endpoint Security для Windows для всех активов с Kaspersky Endpoint Security для Windows 11.6 и выше.

Обратите внимание, что если та же политика применяется к активам с Kaspersky Endpoint Security для Windows версии 11.5 и ниже, необходимо сначала создать и настроить отдельную политику для этих активов, чтобы поддерживать их интеграцию с Kaspersky Managed Detection and Response с помощью политики Kaspersky Endpoint Agent.

Kaspersky Endpoint Security для Windows 11.0–11.5

1. Создайте задачу **Удаленная установка приложения** в Kaspersky Security Center. В окне **Выбор дистрибутива для установки** выберите BAT-файл из файла конфигурации MDR.
2. Запустите задачу вручную или дождитесь ее запуска по расписанию, указанному в параметрах задачи.

   Убедитесь, что задача выполняется на всех активах.
3. Настройте Kaspersky Endpoint Security для Windows на ваших активах.

   Должны быть включены следующие компоненты:

   - Kaspersky Security Network

     В параметрах Kaspersky Security Network установите флажок **Включить расширенный режим KSN**.
   - Анализ поведения

     Включение этих компонентов обязательно. В противном случае Kaspersky Managed Detection and Response не будет работать, поскольку будет невозможна отправка телеметрии.

   Кроме того, Kaspersky Managed Detection and Response может использовать данные следующих компонентов:

   - Защита от веб-угроз
   - Защита от почтовых угроз
   - Сетевой экран

     Включение этих компонентов не является обязательным. Если эти компоненты останутся выключенными, Kaspersky Managed Detection and Response продолжит отправлять телеметрию, но с ограниченными данными.
4. Если вы включили Сетевой экран в Kaspersky Endpoint Security для Windows, создайте правило Сетевого экрана со следующими свойствами:

- В раскрывающемся списке **Действие** выберите пункт **Разрешить**.
- В раскрывающемся списке **Направление** выберите значение **Входящее / исходящее**.
- В раскрывающихся списках **Удаленные адреса** и **Локальные адреса** выберите пункт **Любой адрес**.

  После создания правила переместите его, чтобы оно стало первым в списке правил.

При использовании Kaspersky Endpoint Detection and Response Optimum (для Kaspersky Endpoint Security для Windows 11.6 и ниже)

1. Убедитесь, что Kaspersky Endpoint Agent установлен в составе Kaspersky Endpoint Security для Windows.

   Установка Kaspersky Endpoint Agent может быть выполнена:

   - В процессе установки Kaspersky Endpoint Security для Windows.
   - После установки Kaspersky Endpoint Security для Windows.

2. Проверьте актуальность версии Kaspersky Endpoint Agent для Windows и при необходимости обновите ее.

   Для работы Kaspersky Endpoint Security для Windows 11.5 требуется Kaspersky Endpoint Agent версии 3.10 или выше.

3. Настройте решение Kaspersky Endpoint Detection and Response Optimum.

4. Создайте политику Kaspersky Endpoint Agent.

5. Настройка интеграции между Kaspersky Endpoint Agent для Windows и Kaspersky Managed Detection and Response путем загрузки файла BLOB из файла конфигурации MDR в политику Kaspersky Endpoint Agent.

6. Настройте Kaspersky Endpoint Security для Windows на ваших активах.

   Должны быть включены следующие компоненты:

   - Kaspersky Security Network

     В параметрах Kaspersky Security Network установите флажок **Включить расширенный режим KSN**.

   - Анализ поведения

     > Включение этих компонентов обязательно. В противном случае Kaspersky Managed Detection and Response не будет работать, поскольку будет невозможна отправка телеметрии.

   Кроме того, Kaspersky Managed Detection and Response может использовать данные следующих компонентов:

   - Защита от веб-угроз
   - Защита от почтовых угроз
   - Сетевой экран

     > Включение этих компонентов не является обязательным. Если эти компоненты останутся выключенными, Kaspersky Managed Detection and Response продолжит отправлять телеметрию, но с ограниченными данными.

7. Если вы включили Сетевой экран в Kaspersky Endpoint Security для Windows, создайте правило Сетевого экрана со следующими свойствами:

   - В раскрывающемся списке **Действие** выберите пункт **Разрешить**.
   - В раскрывающемся списке **Направление** выберите значение **Входящее / исходящее**.
   - В раскрывающихся списках **Удаленные адреса** и **Локальные адреса** выберите пункт **Любой адрес**.

     После создания правила переместите его, чтобы оно стало первым в списке правил.

- Kaspersky Endpoint Security для Linux

- Kaspersky Endpoint Security для Mac
- **Kaspersky Security для Windows Server**

Развертывание зависит от того, какая версия Kaspersky Security для Windows Server установлена на ваших активах. Если в вашей инфраструктуре установлено несколько версий Kaspersky Security для Windows Server, можно выполнять сценарии для этих версий в любом порядке.

Kaspersky Security для Windows Server 11 и выше

1. Убедитесь, что Kaspersky Endpoint Agent для Windows установлен в составе Kaspersky Security для Windows Server.

   Установка Kaspersky Endpoint Agent для Windows может быть выполнена:

   - В процессе установки Kaspersky Security для Windows Server
   - После установки Kaspersky Security для Windows Server

2. Проверьте актуальность версии Kaspersky Endpoint Agent для Windows и при необходимости обновите ее.

3. Создайте политику Kaspersky Endpoint Agent для Windows с помощью Kaspersky Security Center.

4. Чтобы настроить интеграцию Kaspersky Endpoint Agent для Windows и Kaspersky Managed Detection and Response, загрузите файл BLOB из файла конфигурации MDR в политику.

5. Настройте Kaspersky Security для Windows Server на ваших активах. Каждый шаг можно выполнить локально в Kaspersky Security для Windows Server на каждом из активов или глобально в Kaspersky Security Center.

   1. Запустите задачу Использование KSN.

      Запуск задачи Использование KSN позволяет использовать Kaspersky Security Network в Kaspersky Security для Windows Server.

      В окне **Обработка данных** задачи Использование KSN установите все флажки на всех вкладках.

      В окне **Параметры** задачи Использование KSN на вкладке **Управление задачами** установите флажок **Запускать по расписанию**. В раскрывающемся списке **Периодичность** выберите пункт **При запуске приложения**.

      Убедитесь, что в подразделе **Использование KSN** отображается закрытый замок. Закрытый замок означает, что политика устанавливает указанные параметры для активов.

   2. Запустите задачу Защита трафика.

      Запуск задачи Защита трафика позволяет обрабатывать веб-трафик (включая трафик, получаемый по электронной почте), а также перехватывать и проверять объекты, передаваемые через веб-трафик, для обнаружения известных компьютерных и других угроз на защищаемом устройстве.

      В окне **Параметры** задачи Защита трафика на вкладке **Общие** в раскрывающемся списке **Режим задачи** выберите значение **Драйверный перехват**.

      В окне **Параметры** задачи Защита трафика на вкладке **Управление задачами** установите флажок **Запускать по расписанию**. В раскрывающемся списке **Периодичность** выберите пункт **При запуске приложения**.

      Убедитесь, что в подразделе **Защита трафика** отображается закрытый замок. Закрытый замок означает, что политика устанавливает указанные параметры для активов.

   3. Запустите задачу Контроль запуска приложений.

      Запуск задачи Контроль запуска приложений позволяет отслеживать попытки пользователей запускать приложения, а также разрешает или запрещает запуск этих приложений.

      В окне **Параметры** задачи Контроль запуска приложений на вкладке **Общие** установите флажки **Контролировать загрузку DLL-модулей** и **Разрешать запуск приложений, доверенных в KSN**.

      В окне **Параметры** задачи Контроль запуска приложений на вкладке **Управление задачами** установите флажок **Запускать по расписанию**. В раскрывающемся списке **Периодичность** выберите пункт **При запуске приложений**.

      Убедитесь, что в подразделе **Контроль запуска приложений** отображается закрытый замок. Закрытый замок означает, что политика устанавливает указанные параметры для активов.

Kaspersky Security для Windows Server 10.1.*

1. Убедитесь, что вы установили Kaspersky Endpoint Agent для Windows как автономное приложение.

2. Проверьте актуальность версии Kaspersky Endpoint Agent для Windows и при необходимости обновите ее.

3. Создайте политику Kaspersky Endpoint Agent для Windows с помощью Kaspersky Security Center.

4. Чтобы настроить интеграцию Kaspersky Endpoint Agent для Windows и Kaspersky Managed Detection and Response, загрузите файл BLOB из файла конфигурации MDR в политику.

5. Настройте Kaspersky Security для Windows Server на ваших активах. Каждый шаг можно выполнить локально в Kaspersky Security для Windows Server на каждом из активов или глобально в Kaspersky Security Center.

   1. Запустите задачу Использование KSN.

      Запуск задачи Использование KSN позволяет использовать Kaspersky Security Network в Kaspersky Security для Windows Server.

      В окне **Обработка данных** задачи Использование KSN установите все флажки на всех вкладках.

      В окне **Параметры** задачи Использование KSN на вкладке **Управление задачами** установите флажок **Запускать по расписанию**. В раскрывающемся списке **Периодичность** выберите пункт **При запуске приложения**.

      Убедитесь, что в подразделе **Использование KSN** отображается закрытый замок. Закрытый замок означает, что политика устанавливает указанные параметры для активов.

   2. Запустите задачу Защита трафика.

      Запуск задачи Защита трафика позволяет обрабатывать веб-трафик (включая трафик, получаемый по электронной почте), а также перехватывать и проверять объекты, передаваемые через веб-трафик, для обнаружения известных компьютерных и других угроз на защищаемом устройстве.

      В окне **Параметры** задачи Защита трафика на вкладке **Общие** в раскрывающемся списке **Режим задачи** выберите значение **Драйверный перехват**.

      В окне **Параметры** задачи Защита трафика на вкладке **Управление задачами** установите флажок **Запускать по расписанию**. В раскрывающемся списке **Периодичность** выберите пункт **При запуске приложения**.

      Убедитесь, что в подразделе **Защита трафика** отображается закрытый замок. Закрытый замок означает, что политика устанавливает указанные параметры для активов.

   3. Запустите задачу Контроль запуска приложений.

      Запуск задачи Контроль запуска приложений позволяет отслеживать попытки пользователей запускать приложения, а также разрешает или запрещает запуск этих приложений.

      В окне **Параметры** задачи Контроль запуска приложений на вкладке **Общие** установите флажки **Контролировать загрузку DLL-модулей** и **Разрешать запуск приложений, доверенных в KSN**.

      В окне **Параметры** задачи Контроль запуска приложений на вкладке **Управление задачами** установите флажок **Запускать по расписанию**. В раскрывающемся списке **Периодичность** выберите пункт **При запуске приложений**.

      Убедитесь, что в подразделе **Контроль запуска приложений** отображается закрытый замок. Закрытый замок означает, что политика устанавливает указанные параметры для активов.

При использовании Kaspersky Endpoint Detection and Response Optimum (для Kaspersky Endpoint Security для Windows 11.6 и ниже)

1. Убедитесь, что Kaspersky Endpoint Agent установлен в составе Kaspersky Endpoint Security для Windows.

   Установка Kaspersky Endpoint Agent может быть выполнена:

   - В процессе установки Kaspersky Endpoint Security для Windows.
   - После установки Kaspersky Endpoint Security для Windows.

2. Проверьте актуальность версии Kaspersky Endpoint Agent для Windows и при необходимости обновите ее.

   Для работы Kaspersky Endpoint Security для Windows 11.5 требуется Kaspersky Endpoint Agent версии 3.10 или выше.

3. Настройте решение Kaspersky Endpoint Detection and Response Optimum.

4. Создайте политику Kaspersky Endpoint Agent.

5. Настройка интеграции между Kaspersky Endpoint Agent для Windows и Kaspersky Managed Detection and Response путем загрузки файла BLOB из файла конфигурации MDR в политику Kaspersky Endpoint Agent.

6. Настройте Kaspersky Endpoint Security для Windows на ваших активах.

   Должны быть включены следующие компоненты:

   - Kaspersky Security Network

     В параметрах Kaspersky Security Network установите флажок **Включить расширенный режим KSN**.

   - Анализ поведения

     > Включение этих компонентов обязательно. В противном случае Kaspersky Managed Detection and Response не будет работать, поскольку будет невозможна отправка телеметрии.

   Кроме того, Kaspersky Managed Detection and Response может использовать данные следующих компонентов:

   - Защита от веб-угроз
   - Защита от почтовых угроз
   - Сетевой экран

     > Включение этих компонентов не является обязательным. Если эти компоненты останутся выключенными, Kaspersky Managed Detection and Response продолжит отправлять телеметрию, но с ограниченными данными.

7. Если вы включили Сетевой экран в Kaspersky Endpoint Security для Windows, создайте правило Сетевого экрана со следующими свойствами:

   - В раскрывающемся списке **Действие** выберите пункт **Разрешить**.
   - В раскрывающемся списке **Направление** выберите значение **Входящее / исходящее**.
   - В раскрывающихся списках **Удаленные адреса** и **Локальные адреса** выберите пункт **Любой адрес**.

     После создания правила переместите его, чтобы оно стало первым в списке правил.

- **Kaspersky Security для виртуальных сред 5.2 Легкий агент**

1. Убедитесь, что Kaspersky Endpoint Agent установлен в составе Kaspersky Endpoint Security для Windows.

   Установка Kaspersky Endpoint Agent может быть выполнена:

   - В процессе установки Kaspersky Endpoint Security для Windows.
   - После установки Kaspersky Endpoint Security для Windows.

2. Проверьте актуальность версии Kaspersky Endpoint Agent для Windows и при необходимости обновите ее.

   Для работы Kaspersky Endpoint Security для Windows 11.5 требуется Kaspersky Endpoint Agent версии 3.10 или выше.

3. Настройте решение Kaspersky Endpoint Detection and Response Optimum.

4. Создайте политику Kaspersky Endpoint Agent.

5. Настройка интеграции между Kaspersky Endpoint Agent для Windows и Kaspersky Managed Detection and Response путем загрузки файла BLOB из файла конфигурации MDR в политику Kaspersky Endpoint Agent.

6. Настройте Kaspersky Endpoint Security для Windows на ваших активах.

   Должны быть включены следующие компоненты:

   - Kaspersky Security Network

     В параметрах Kaspersky Security Network установите флажок **Включить расширенный режим KSN**.

- Анализ поведения

  Включение этих компонентов обязательно. В противном случае Kaspersky Managed Detection and Response не будет работать, поскольку будет невозможна отправка телеметрии.

Кроме того, Kaspersky Managed Detection and Response может использовать данные следующих компонентов:

- Защита от веб-угроз
- Защита от почтовых угроз
- Сетевой экран

  Включение этих компонентов не является обязательным. Если эти компоненты останутся выключенными, Kaspersky Managed Detection and Response продолжит отправлять телеметрию, но с ограниченными данными.

7. Если вы включили Сетевой экран в Kaspersky Endpoint Security для Windows, создайте правило Сетевого экрана со следующими свойствами:

   - В раскрывающемся списке **Действие** выберите пункт **Разрешить**.
   - В раскрывающемся списке **Направление** выберите значение **Входящее / исходящее**.
   - В раскрывающихся списках **Удаленные адреса** и **Локальные адреса** выберите пункт **Любой адрес**.

     После создания правила переместите его, чтобы оно стало первым в списке правил.

- Kaspersky Security для виртуальных сред 5.2 Легкий агент
- **При использовании Kaspersky Endpoint Detection and Response Optimum (для Kaspersky Endpoint Security для Windows 11.6 и ниже)**

  1. Убедитесь, что Kaspersky Endpoint Agent установлен в составе Kaspersky Endpoint Security для Windows.

     Установка Kaspersky Endpoint Agent может быть выполнена:

     - В процессе установки Kaspersky Endpoint Security для Windows.
     - После установки Kaspersky Endpoint Security для Windows.

  2. Проверьте актуальность версии Kaspersky Endpoint Agent для Windows и при необходимости обновите ее.

     Для работы Kaspersky Endpoint Security для Windows 11.5 требуется Kaspersky Endpoint Agent версии 3.10 или выше.

  3. Настройте решение Kaspersky Endpoint Detection and Response Optimum.
  4. Создайте политику Kaspersky Endpoint Agent.
  5. Настройка интеграции между Kaspersky Endpoint Agent для Windows и Kaspersky Managed Detection and Response путем загрузки файла BLOB из файла конфигурации MDR в политику Kaspersky Endpoint Agent.
  6. Настройте Kaspersky Endpoint Security для Windows на ваших активах.

     Должны быть включены следующие компоненты:

     - Kaspersky Security Network

       В параметрах Kaspersky Security Network установите флажок **Включить расширенный режим KSN**.

     - Анализ поведения

       Включение этих компонентов обязательно. В противном случае Kaspersky Managed Detection and Response не будет работать, поскольку будет невозможна отправка телеметрии.

     Кроме того, Kaspersky Managed Detection and Response может использовать данные следующих компонентов:

- Защита от веб-угроз
- Защита от почтовых угроз
- Сетевой экран

Включение этих компонентов не является обязательным. Если эти компоненты останутся выключенными, Kaspersky Managed Detection and Response продолжит отправлять телеметрию, но с ограниченными данными.

7. Если вы включили Сетевой экран в Kaspersky Endpoint Security для Windows, создайте правило Сетевого экрана со следующими свойствами:
   - В раскрывающемся списке **Действие** выберите пункт **Разрешить**.
   - В раскрывающемся списке **Направление** выберите значение **Входящее / исходящее**.
   - В раскрывающихся списках **Удаленные адреса** и **Локальные адреса** выберите пункт **Любой адрес**.

     После создания правила переместите его, чтобы оно стало первым в списке правил.

- **Kaspersky Anti-Targeted Attack Platform**

Kaspersky Managed Detection and Response позволят выполнять анализ и мониторинг данных, получаемых от Kaspersky Anti-Targeted Attack (KATA) Platform.

Интеграция с Kaspersky Anti-Targeted Attack Platform недоступна при использовании лицензионного ключа для региона Саудовская Аравия.

Чтобы настроить интеграцию Kaspersky Managed Detection and Response с Kaspersky Anti-Targeted Attack Platform, сначала необходимо получить конфигурационный файл MDR. Информация о настройке интеграции приведена в справке Kaspersky Anti-Targeted Attack Platform.

Kaspersky Anti-Targeted Attack Platform не является частью Kaspersky Managed Detection and Response. Для использования приложения Kaspersky Anti-Targeted Attack Platform ее необходимо приобрести отдельно.

Если в инфраструктуре установлено несколько приложений "Лаборатории Касперского", можно выполнять сценарии для определенных приложений в любом порядке.

Вы можете проверить статус активов с помощью функции Работоспособность MDR.

Развертывание с помощью Kaspersky Security Center Web Console

Развернуть все | Свернуть все

Предварительные требования

- ИТ-инфраструктура должна соответствовать аппаратным и программным требованиям Kaspersky Managed Detection and Response.
- На каждом активе, который требуется защитить, должен быть разрешен исходящий незашифрованный сетевой трафик, для портов 443 и 1443, а проверка трафика должна быть отключена. Эти порты используются для передачи данных телеметрии от активов на следующие серверы "Лаборатории Касперского":
  - *.ksn.kaspersky-labs.com
  - ksn-*.kaspersky-labs.com
  - ds.kaspersky.com

Развертывание Kaspersky Managed Detection and Response с помощью Kaspersky Security Center Web Console состоит из следующих шагов:

1. **Установка плагина MDR**

Скачайте и настройте плагин MDR для управления решением с помощью Kaspersky Security Center Web Console.

2. **Активация решения**

   Активируйте решение Kaspersky Managed Detection and Response с использованием вашей лицензии.

3. **Скачивание конфигурационного файла MDR**

   Скачайте конфигурационный файл MDR для вашей организации или отдельные архивы для каждого тенанта из **раздела** Тенанты в Консоли MDR с помощью плагина MDR в Kaspersky Security Center Web Console.

   Начиная с версии Kaspersky Endpoint Security для Windows 12.6, если у вас есть только корневой тенант и вы не используете решение MDR вместе с Kaspersky Endpoint Detection and Response Optimum, вам не нужно загружать конфигурационный файл MDR. См. инструкцию для Kaspersky Endpoint Security для Windows на шаге 5.

4. **Установка EPP-программ**

   Убедитесь, что на активах установлены EPP-программы, которые поддерживают функции Kaspersky Managed Detection and Response.

5. **Интеграция с EPP-программами**

   Выполните сценарии развертывания для всех приложений "Лаборатории Касперского", установленных на ваших активах.

   - **Kaspersky Endpoint Security для Windows**

     Развертывание зависит от того, какая версия Kaspersky Endpoint Security для Windows установлена на ваших активах. Если в вашей инфраструктуре установлено несколько версий Kaspersky Endpoint Security для Windows, можно выполнять сценарии для этих версий в любом порядке.

     Kaspersky Endpoint Security для Windows 12.6 и выше с только корневым тенантом и без Kaspersky Endpoint Detection and Response Optimum

     Если у вас есть только корневой тенант, вы можете не загружать конфигурационный файл MDR, а добавить и распространить лицензионный ключ прямо в Kaspersky Security Center.

     Чтобы развернуть Kaspersky Managed Detection and Response в Kaspersky Endpoint Security для Windows 12.6 и выше:

     1. Убедитесь, что все ваши активы принадлежат корневому тенанту.
     2. Проверьте, обновлен ли Kaspersky Endpoint Security для Windows на всех активах до версии 12.6 или выше.
     3. Убедитесь, что компонент Kaspersky Managed Detection and Response включен в Kaspersky Endpoint Security для Windows на всех активах.
     4. Добавьте лицензионный ключ в хранилище лицензионных ключей Kaspersky Security Center.
     5. Распространите лицензионный ключ на активы автоматически или с помощью задачи *Добавить лицензионный ключ*.

     Если у вас только корневой тенант, вы можете не загружать конфигурационный файл MDR, а добавить и распространить лицензионный ключ прямо в Kaspersky Security Center Web Console.

     Чтобы развернуть Kaspersky Managed Detection and Response в Kaspersky Endpoint Security для Windows 12.6 и выше:

     1. Убедитесь, что все ваши активы принадлежат корневому тенанту.
     2. Проверьте, обновлен ли Kaspersky Endpoint Security для Windows на всех активах до версии 12.6 или выше.
     3. Убедитесь, что компонент Kaspersky Managed Detection and Response включен в Kaspersky Endpoint Security для Windows на всех активах.
     4. Добавьте лицензионный ключ в хранилище лицензионных ключей Kaspersky Security Center Web Console.
     5. Распространите лицензионный ключ на активы автоматически или с помощью задачи *Добавить лицензионный ключ*.

     Подробнее об одновременном использовании решений MDR и EDR Optimum см. в справке Kaspersky Endpoint Security для Windows.

     Kaspersky Endpoint Security для Windows версий 11.6–12.5 и выше с несколькими тенантами

Если вы переключаетесь на встроенные функции MDR в Kaspersky Endpoint Security для Windows после работы с решением с использованием функций Kaspersky Endpoint Agent, обязательно выключите Kaspersky Managed Detection and Response в политике Kaspersky Endpoint Agent после настройки интеграции с Kaspersky Managed Detection and Response в политике Kaspersky Endpoint Security для Windows для всех активов с Kaspersky Endpoint Security для Windows 11.6 и выше.

Обратите внимание, что если та же политика применяется к активам с Kaspersky Endpoint Security для Windows версии 11.5 и ниже, необходимо сначала создать и настроить отдельную политику для этих активов, чтобы поддерживать их интеграцию с Kaspersky Managed Detection and Response с помощью политики Kaspersky Endpoint Agent.

Kaspersky Endpoint Security для Windows 11.0–11.5

1. Создайте задачу **Удаленная установка приложения** в Kaspersky Security Center. В окне **Выбор дистрибутива для установки** выберите BAT-файл из файла конфигурации MDR.
2. Запустите задачу вручную или дождитесь ее запуска по расписанию, указанному в параметрах задачи.

   Убедитесь, что задача выполняется на всех активах.
3. Настройте Kaspersky Endpoint Security для Windows на ваших активах.

   Должны быть включены следующие компоненты:

   - Kaspersky Security Network

     В параметрах Kaspersky Security Network установите флажок **Включить расширенный режим KSN**.
   - Анализ поведения

     Включение этих компонентов обязательно. В противном случае Kaspersky Managed Detection and Response не будет работать, поскольку будет невозможна отправка телеметрии.

   Кроме того, Kaspersky Managed Detection and Response может использовать данные следующих компонентов:

   - Защита от веб-угроз
   - Защита от почтовых угроз
   - Сетевой экран

     Включение этих компонентов не является обязательным. Если эти компоненты останутся выключенными, Kaspersky Managed Detection and Response продолжит отправлять телеметрию, но с ограниченными данными.
4. Если вы включили Сетевой экран в Kaspersky Endpoint Security для Windows, создайте правило Сетевого экрана со следующими свойствами:

   - В раскрывающемся списке **Действие** выберите пункт **Разрешить**.
   - В раскрывающемся списке **Направление** выберите значение **Входящее / исходящее**.
   - В раскрывающихся списках **Удаленные адреса** и **Локальные адреса** выберите пункт **Любой адрес**.

     После создания правила переместите его, чтобы оно стало первым в списке правил.

При использовании Kaspersky Endpoint Detection and Response Optimum

1. Убедитесь, что Kaspersky Endpoint Agent установлен в составе Kaspersky Endpoint Security для Windows.

   Установка Kaspersky Endpoint Agent может быть выполнена:

   - В процессе установки Kaspersky Endpoint Security для Windows.

- После установки Kaspersky Endpoint Security для Windows.

2. Проверьте актуальность версии Kaspersky Endpoint Agent для Windows и при необходимости обновите ее.

   Для работы Kaspersky Endpoint Security для Windows 11.5 требуется Kaspersky Endpoint Agent версии 3.10 или выше.

3. Настройте решение Kaspersky Endpoint Detection and Response Optimum.

4. Создайте политику Kaspersky Endpoint Agent.

5. Настройка интеграции между Kaspersky Endpoint Agent для Windows и Kaspersky Managed Detection and Response путем загрузки файла BLOB из файла конфигурации MDR в политику Kaspersky Endpoint Agent.

6. Настройте Kaspersky Endpoint Security для Windows на ваших активах.

   Должны быть включены следующие компоненты:

   - Kaspersky Security Network

     В параметрах Kaspersky Security Network необходимо установить флажок **Включить расширенный режим KSN**.

   - Анализ поведения

     > Включение этих компонентов обязательно. В противном случае Kaspersky Managed Detection and Response не будет работать, поскольку будет невозможна отправка телеметрии.

   Кроме того, Kaspersky Managed Detection and Response может использовать данные следующих компонентов:

   - Защита от веб-угроз
   - Защита от почтовых угроз
   - Сетевой экран

     > Включение этих компонентов не является обязательным. Если эти компоненты останутся выключенными, Kaspersky Managed Detection and Response продолжит отправлять телеметрию, но с ограниченными данными.

7. Если вы включили Сетевой экран в Kaspersky Endpoint Security для Windows, создайте правило Сетевого экрана со следующими свойствами:

   - В раскрывающемся списке **Действие** выберите пункт **Разрешить**.
   - В раскрывающемся списке **Направление** выберите значение **Входящее / исходящее**.
   - В раскрывающихся списках **Удаленные адреса** и **Локальные адреса** выберите пункт **Любой адрес**.

     После создания правила переместите его, чтобы оно стало первым в списке правил.

- Kaspersky Endpoint Security для Linux
- Kaspersky Endpoint Security для Mac
- **Kaspersky Security для Windows Server**

  Развертывание зависит от того, какая версия Kaspersky Security для Windows Server установлена на ваших активах. Если в вашей инфраструктуре установлено несколько версий Kaspersky Security для Windows Server, можно выполнять сценарии для этих версий в любом порядке.

  Kaspersky Security для Windows Server 11 и выше

  1. Убедитесь, что Kaspersky Endpoint Agent для Windows установлен в составе Kaspersky Security для Windows Server.

     Установка Kaspersky Endpoint Agent для Windows может быть выполнена:

     - В процессе установки Kaspersky Security для Windows Server

- После установки Kaspersky Security для Windows Server

2. Проверьте актуальность версии Kaspersky Endpoint Agent для Windows и при необходимости обновите ее.

3. Создайте политику Kaspersky Endpoint Agent для Windows с помощью Kaspersky Security Center Web Console.

4. Чтобы настроить интеграцию Kaspersky Endpoint Agent для Windows и Kaspersky Managed Detection and Response, загрузите файл BLOB из файла конфигурации MDR в политику.

5. Настройте Kaspersky Security для Windows Server на ваших активах. Каждый шаг можно выполнить локально в Kaspersky Security для Windows Server на каждом из активов или глобально в Kaspersky Security Center.

   1. Запустите задачу Использование KSN.

      Запуск задачи Использование KSN позволяет использовать Kaspersky Security Network в Kaspersky Security для Windows Server.

      В окне **Обработка данных** задачи Использование KSN установите все флажки на всех вкладках.

      В окне **Параметры** задачи Использование KSN на вкладке **Управление задачами** установите флажок **Запускать по расписанию**. В раскрывающемся списке **Периодичность** выберите пункт **При запуске приложения**.

      Убедитесь, что в подразделе **Использование KSN** отображается закрытый замок. Закрытый замок означает, что политика устанавливает указанные параметры для активов.

   2. Запустите задачу Защита трафика.

      Запуск задачи Защита трафика позволяет обрабатывать веб-трафик (включая трафик, получаемый по электронной почте), а также перехватывать и проверять объекты, передаваемые через веб-трафик, для обнаружения известных компьютерных и других угроз на защищаемом устройстве.

      В окне **Параметры** задачи Защита трафика на вкладке **Общие** в раскрывающемся списке **Режим задачи** выберите значение **Драйверный перехват**.

      В окне **Параметры** задачи Защита трафика на вкладке **Управление задачами** установите флажок **Запускать по расписанию**. В раскрывающемся списке **Периодичность** выберите пункт **При запуске приложения**.

      Убедитесь, что в подразделе **Защита трафика** отображается закрытый замок. Закрытый замок означает, что политика устанавливает указанные параметры для активов.

   3. Запустите задачу Контроль запуска приложений.

      Запуск задачи Контроль запуска приложений позволяет отслеживать попытки пользователей запускать приложения, а также разрешает или запрещает запуск этих приложений.

      В окне **Параметры** задачи Контроль запуска приложений на вкладке **Общие** установите флажки **Контролировать загрузку DLL-модулей** и **Разрешать запуск приложений, доверенных в KSN**.

      В окне **Параметры** задачи Контроль запуска приложений на вкладке **Управление задачами** установите флажок **Запускать по расписанию**. В раскрывающемся списке **Периодичность** выберите пункт **При запуске приложений**.

      Убедитесь, что в подразделе **Контроль запуска приложений** отображается закрытый замок. Закрытый замок означает, что политика устанавливает указанные параметры для активов.

Kaspersky Security для Windows Server 10.1.*

1. Убедитесь, что вы установили Kaspersky Endpoint Agent для Windows как автономное приложение.

2. Проверьте актуальность версии Kaspersky Endpoint Agent для Windows и при необходимости обновите ее.

3. Создайте политику Kaspersky Endpoint Agent для Windows с помощью Kaspersky Security Center Web Console.

4. Чтобы настроить интеграцию Kaspersky Endpoint Agent для Windows и Kaspersky Managed Detection and Response, загрузите файл BLOB из файла конфигурации MDR в политику.

5. Настройте Kaspersky Security для Windows Server на ваших активах. Каждый шаг можно выполнить локально в Kaspersky Security для Windows Server на каждом из активов или глобально в Kaspersky Security Center.

   1. Запустите задачу Использование KSN.

      Запуск задачи Использование KSN позволяет использовать Kaspersky Security Network в Kaspersky Security для Windows Server.

      В окне **Обработка данных** задачи Использование KSN установите все флажки на всех вкладках.

В окне **Параметры** задачи Использование KSN на вкладке **Управление задачами** установите флажок **Запускать по расписанию**. В раскрывающемся списке **Периодичность** выберите пункт **При запуске приложения**.

Убедитесь, что в подразделе **Использование KSN** отображается закрытый замок. Закрытый замок означает, что политика устанавливает указанные параметры для активов.

2. Запустите задачу Защита трафика.

   Запуск задачи Защита трафика позволяет обрабатывать веб-трафик (включая трафик, получаемый по электронной почте), а также перехватывать и проверять объекты, передаваемые через веб-трафик, для обнаружения известных компьютерных и других угроз на защищаемом устройстве.

   В окне **Параметры** задачи Защита трафика на вкладке **Общие** в раскрывающемся списке **Режим задачи** выберите значение **Драйверный перехват**.

   В окне **Параметры** задачи Защита трафика на вкладке **Управление задачами** установите флажок **Запускать по расписанию**. В раскрывающемся списке **Периодичность** выберите пункт **При запуске приложения**.

   Убедитесь, что в подразделе **Защита трафика** отображается закрытый замок. Закрытый замок означает, что политика устанавливает указанные параметры для активов.

3. Запустите задачу Контроль запуска приложений.

   Запуск задачи Контроль запуска приложений позволяет отслеживать попытки пользователей запускать приложения, а также разрешает или запрещает запуск этих приложений.

   В окне **Параметры** задачи Контроль запуска приложений на вкладке **Общие** установите флажки **Контролировать загрузку DLL-модулей** и **Разрешать запуск приложений, доверенных в KSN**.

   В окне **Параметры** задачи Контроль запуска приложений на вкладке **Управление задачами** установите флажок **Запускать по расписанию**. В раскрывающемся списке **Периодичность** выберите пункт **При запуске приложений**.

   Убедитесь, что в подразделе **Контроль запуска приложений** отображается закрытый замок. Закрытый замок означает, что политика устанавливает указанные параметры для активов.

- **Kaspersky Security для виртуальных сред 5.2 Легкий агент**

1. Убедитесь, что Kaspersky Endpoint Agent установлен в составе Kaspersky Endpoint Security для Windows.

   Установка Kaspersky Endpoint Agent может быть выполнена:

   - В процессе установки Kaspersky Endpoint Security для Windows.
   - После установки Kaspersky Endpoint Security для Windows.

2. Проверьте актуальность версии Kaspersky Endpoint Agent для Windows и при необходимости обновите ее.

   Для работы Kaspersky Endpoint Security для Windows 11.5 требуется Kaspersky Endpoint Agent версии 3.10 или выше.

3. Настройте решение Kaspersky Endpoint Detection and Response Optimum.

4. Создайте политику Kaspersky Endpoint Agent.

5. Настройка интеграции между Kaspersky Endpoint Agent для Windows и Kaspersky Managed Detection and Response путем загрузки файла BLOB из файла конфигурации MDR в политику Kaspersky Endpoint Agent.

6. Настройте Kaspersky Endpoint Security для Windows на ваших активах.

   Должны быть включены следующие компоненты:

   - Kaspersky Security Network

     В параметрах Kaspersky Security Network установите флажок **Включить расширенный режим KSN**.

   - Анализ поведения

     Включение этих компонентов обязательно. В противном случае Kaspersky Managed Detection and Response не будет работать, поскольку будет невозможна отправка телеметрии.

   Кроме того, Kaspersky Managed Detection and Response может использовать данные следующих компонентов:

- Защита от веб-угроз
- Защита от почтовых угроз
- Сетевой экран

  Включение этих компонентов не является обязательным. Если эти компоненты останутся выключенными, Kaspersky Managed Detection and Response продолжит отправлять телеметрию, но с ограниченными данными.

7. Если вы включили Сетевой экран в Kaspersky Endpoint Security для Windows, создайте правило Сетевого экрана со следующими свойствами:
   - В раскрывающемся списке **Действие** выберите пункт **Разрешить**.
   - В раскрывающемся списке **Направление** выберите значение **Входящее / исходящее**.
   - В раскрывающихся списках **Удаленные адреса** и **Локальные адреса** выберите пункт **Любой адрес**.

     После создания правила переместите его, чтобы оно стало первым в списке правил.

- Kaspersky Security для виртуальных сред 5.2 Легкий агент
- **При использовании Kaspersky Endpoint Detection and Response Optimum (для Kaspersky Endpoint Security для Windows 11.6 и ниже)**

  1. Убедитесь, что Kaspersky Endpoint Agent установлен в составе Kaspersky Endpoint Security для Windows.

     Установка Kaspersky Endpoint Agent может быть выполнена:

     - В процессе установки Kaspersky Endpoint Security для Windows.
     - После установки Kaspersky Endpoint Security для Windows.

  2. Проверьте актуальность версии Kaspersky Endpoint Agent для Windows и при необходимости обновите ее.

     Для работы Kaspersky Endpoint Security для Windows 11.5 требуется Kaspersky Endpoint Agent версии 3.10 или выше.

  3. Настройте решение Kaspersky Endpoint Detection and Response Optimum.
  4. Создайте политику Kaspersky Endpoint Agent.
  5. Настройка интеграции между Kaspersky Endpoint Agent для Windows и Kaspersky Managed Detection and Response путем загрузки файла BLOB из файла конфигурации MDR в политику Kaspersky Endpoint Agent.
  6. Настройте Kaspersky Endpoint Security для Windows на ваших активах.

     Должны быть включены следующие компоненты:

     - Kaspersky Security Network

       В параметрах Kaspersky Security Network установите флажок **Включить расширенный режим KSN**.

     - Анализ поведения

       Включение этих компонентов обязательно. В противном случае Kaspersky Managed Detection and Response не будет работать, поскольку будет невозможна отправка телеметрии.

     Кроме того, Kaspersky Managed Detection and Response может использовать данные следующих компонентов:

     - Защита от веб-угроз
     - Защита от почтовых угроз
     - Сетевой экран

Включение этих компонентов не является обязательным. Если эти компоненты останутся выключенными, Kaspersky Managed Detection and Response продолжит отправлять телеметрию, но с ограниченными данными.

7. Если вы включили Сетевой экран в Kaspersky Endpoint Security для Windows, создайте правило Сетевого экрана со следующими свойствами:
   - В раскрывающемся списке **Действие** выберите пункт **Разрешить**.
   - В раскрывающемся списке **Направление** выберите значение **Входящее / исходящее**.
   - В раскрывающихся списках **Удаленные адреса** и **Локальные адреса** выберите пункт **Любой адрес**.

     После создания правила переместите его, чтобы оно стало первым в списке правил.

- Kaspersky Anti-Targeted Attack Platform

  Kaspersky Managed Detection and Response позволят выполнять анализ и мониторинг данных, получаемых от Kaspersky Anti-Targeted Attack (KATA) Platform.

  Интеграция с Kaspersky Anti-Targeted Attack Platform недоступна при использовании лицензионного ключа для региона Саудовская Аравия.

  Чтобы настроить интеграцию Kaspersky Managed Detection and Response с Kaspersky Anti-Targeted Attack Platform, сначала необходимо получить конфигурационный файл MDR. Информация о настройке интеграции приведена в справке Kaspersky Anti-Targeted Attack Platform.

  Kaspersky Anti-Targeted Attack Platform не является частью Kaspersky Managed Detection and Response. Для использования приложения Kaspersky Anti-Targeted Attack Platform ее необходимо приобрести отдельно.

Если в инфраструктуре установлено несколько приложений "Лаборатории Касперского", можно выполнять сценарии для определенных приложений в любом порядке.

Если вы не используете плагин MDR, вручную настройте KPSN на активах с помощью файла конфигурации KSN из файла конфигурации MDR. Этот шаг гарантирует отправку телеметрии на выделенные серверы, соответствующие требованиям Общего регламента по защите данных (GDPR). Если вы не настроили KPSN и не использовали плагин MDR для первоначального развертывания Kaspersky Managed Detection and Response, ваша телеметрия не передается и служба Kaspersky Managed Detection and Response не предоставляется.

Вы можете проверить статус активов с помощью функции Работоспособность MDR.

Облачное развертывание

Развернуть все | Свернуть все

Развертывание Kaspersky Managed Detection and Response с помощью Kaspersky Security Center Console состоит из следующих шагов:

1. **Активация решения**

   Активируйте решение Kaspersky Managed Detection and Response с использованием вашей лицензии.

2. **Установка EPP-программ**

   Убедитесь, что на активах установлены EPP-программы, которые поддерживают функции Kaspersky Managed Detection and Response.

3. **Скачивание конфигурационного файла MDR**

   Скачайте конфигурационный файл MDR для вашей организации или отдельные архивы для каждого тенанта из **раздела** Тенанты в Консоли MDR с помощью плагина MDR в Kaspersky Security Center Cloud Console.

   Начиная с версии Kaspersky Endpoint Security для Windows 12.6, если у вас есть только корневой тенант и вы не используете решение MDR вместе с Kaspersky Endpoint Detection and Response Optimum, вам не нужно загружать конфигурационный файл MDR. См. инструкцию для Kaspersky Endpoint Security для Windows на шаге 4.

4. **Интеграция с EPP-программами**

   Выполните сценарии развертывания для всех приложений "Лаборатории Касперского", установленных на ваших активах.

- Kaspersky Endpoint Security для Windows

Развертывание зависит от того, какая версия Kaspersky Endpoint Security для Windows установлена на ваших активах. Если в вашей инфраструктуре установлено несколько версий Kaspersky Endpoint Security для Windows, можно выполнять сценарии для этих версий в любом порядке.

Kaspersky Endpoint Security для Windows 12.6 и выше с только корневым тенантом и без Kaspersky Endpoint Detection and Response Optimum

Если у вас есть только корневой тенант, вы можете не загружать конфигурационный файл MDR, а добавить и распространить лицензионный ключ прямо в Kaspersky Security Center.

Чтобы развернуть Kaspersky Managed Detection and Response в Kaspersky Endpoint Security для Windows 12.6 и выше:

1. Убедитесь, что все ваши активы принадлежат корневому тенанту.
2. Проверьте, обновлен ли Kaspersky Endpoint Security для Windows на всех активах до версии 12.6 или выше.
3. Убедитесь, что компонент Kaspersky Managed Detection and Response включен в Kaspersky Endpoint Security для Windows на всех активах.
4. Добавьте лицензионный ключ в хранилище лицензионных ключей Kaspersky Security Center.
5. Распространите лицензионный ключ на активы автоматически или с помощью задачи *Добавить лицензионный ключ*.

Если у вас только корневой тенант, вы можете не загружать конфигурационный файл MDR, а добавить и распространить лицензионный ключ прямо в Kaspersky Security Center Cloud Console.

Чтобы развернуть Kaspersky Managed Detection and Response в Kaspersky Endpoint Security для Windows 12.6 и выше:

1. Убедитесь, что все ваши активы принадлежат корневому тенанту.
2. Проверьте, обновлен ли Kaspersky Endpoint Security для Windows на всех активах до версии 12.6 или выше.
3. Убедитесь, что компонент Kaspersky Managed Detection and Response включен в Kaspersky Endpoint Security для Windows на всех активах.
4. Добавьте лицензионный ключ в хранилище лицензионных ключей Kaspersky Security Center Cloud Console.
5. Распространите лицензионный ключ на активы автоматически или с помощью задачи *Добавить лицензионный ключ*.

Подробнее об одновременном использовании решений MDR и EDR Optimum см. в справке Kaspersky Endpoint Security для Windows.

Kaspersky Endpoint Security для Windows версий 11.6–12.5 и выше с несколькими тенантами

Если вы переключаетесь на встроенные функции MDR в Kaspersky Endpoint Security для Windows после работы с решением с использованием функций Kaspersky Endpoint Agent, обязательно выключите Kaspersky Managed Detection and Response в политике Kaspersky Endpoint Agent после настройки интеграции с Kaspersky Managed Detection and Response в политике Kaspersky Endpoint Security для Windows для всех активов с Kaspersky Endpoint Security для Windows 11.6 и выше.

Обратите внимание, что если та же политика применяется к активам с Kaspersky Endpoint Security для Windows версии 11.5 и ниже, необходимо сначала создать и настроить отдельную политику для этих активов, чтобы поддерживать их интеграцию с Kaspersky Managed Detection and Response с помощью политики Kaspersky Endpoint Agent.

Kaspersky Endpoint Security для Windows 11.3–11.5

1. Создайте задачу **Удаленная установка программы** в Kaspersky Security Center Cloud Console. В окне **Выбор дистрибутива для установки** выберите BAT-файл из файла конфигурации MDR.
2. Запустите задачу вручную или дождитесь ее запуска по расписанию, указанному в параметрах задачи.

Убедитесь, что задача выполняется на всех активах.

3. Настройте Kaspersky Endpoint Security для Windows на ваших активах.

   Должны быть включены следующие компоненты:

   - Kaspersky Security Network

     В параметрах Kaspersky Security Network установите флажок **Включить расширенный режим KSN**.

   - Анализ поведения

     > Включение этих компонентов обязательно. В противном случае Kaspersky Managed Detection and Response не будет работать, поскольку будет невозможна отправка телеметрии.

   Кроме того, Kaspersky Managed Detection and Response может использовать данные следующих компонентов:

   - Защита от веб-угроз
   - Защита от почтовых угроз
   - Сетевой экран

     > Включение этих компонентов не является обязательным. Если эти компоненты останутся выключенными, Kaspersky Managed Detection and Response продолжит отправлять телеметрию, но с ограниченными данными.

4. Если вы включили Сетевой экран в Kaspersky Endpoint Security для Windows, создайте правило Сетевого экрана со следующими свойствами:

   - В раскрывающемся списке **Действие** выберите пункт **Разрешить**.
   - В раскрывающемся списке **Направление** выберите значение **Входящее / исходящее**.
   - В раскрывающихся списках **Удаленные адреса** и **Локальные адреса** выберите пункт **Любой адрес**.

     После создания правила переместите его, чтобы оно стало первым в списке правил.

При использовании Kaspersky Endpoint Detection and Response Optimum

1. Убедитесь, что Kaspersky Endpoint Agent установлен в составе Kaspersky Endpoint Security для Windows.

   Установка Kaspersky Endpoint Agent может быть выполнена:

   - В процессе установки Kaspersky Endpoint Security для Windows.
   - После установки Kaspersky Endpoint Security для Windows.

2. Проверьте актуальность версии Kaspersky Endpoint Agent для Windows и при необходимости обновите ее.

   Для работы с Kaspersky Security Center Cloud Console требуется Kaspersky Endpoint Agent 3.11.

3. Настройте решение Kaspersky Endpoint Detection and Response Optimum.

4. Создайте политику Kaspersky Endpoint Agent.

5. Настройка интеграции между Kaspersky Endpoint Agent для Windows и Kaspersky Managed Detection and Response путем загрузки файла BLOB из файла конфигурации MDR в политику Kaspersky Endpoint Agent.

6. Настройте Kaspersky Endpoint Security для Windows на ваших активах.

   Должны быть включены следующие компоненты:

   - Kaspersky Security Network

     В параметрах Kaspersky Security Network необходимо установить флажок **Включить расширенный режим KSN**.

   - Анализ поведения

Включение этих компонентов обязательно. В противном случае Kaspersky Managed Detection and Response не будет работать, поскольку будет невозможна отправка телеметрии.

Кроме того, Kaspersky Managed Detection and Response может использовать данные следующих компонентов:

- Защита от веб-угроз
- Защита от почтовых угроз
- Сетевой экран

7. Если вы включили Сетевой экран в Kaspersky Endpoint Security для Windows, создайте правило Сетевого экрана со следующими свойствами:
   - В раскрывающемся списке **Действие** выберите пункт **Разрешить**.
   - В раскрывающемся списке **Направление** выберите значение **Входящее / исходящее**.
   - В раскрывающихся списках **Удаленные адреса** и **Локальные адреса** выберите пункт **Любой адрес**.

     После создания правила переместите его, чтобы оно стало первым в списке правил.

     Включение этих компонентов не является обязательным. Если эти компоненты останутся выключенными, Kaspersky Managed Detection and Response продолжит отправлять телеметрию, но с ограниченными данными.

- Kaspersky Endpoint Security для Linux
- Kaspersky Endpoint Security для Mac
- **Kaspersky Security для Windows Server**

1. Убедитесь, что Kaspersky Endpoint Agent для Windows установлен в составе Kaspersky Security для Windows Server.

   Установка Kaspersky Endpoint Agent для Windows может быть выполнена:

   - В процессе установки Kaspersky Security для Windows Server
   - После установки Kaspersky Security для Windows Server

2. Проверьте актуальность версии Kaspersky Endpoint Agent для Windows и при необходимости обновите ее.

   Для работы с Kaspersky Security Center Cloud Console требуется Kaspersky Endpoint Agent 3.11.

3. Создайте политику Kaspersky Endpoint Agent для Windows с помощью Kaspersky Security Center Cloud Console.

4. Чтобы настроить интеграцию Kaspersky Endpoint Agent для Windows и Kaspersky Managed Detection and Response, загрузите файл BLOB из файла конфигурации MDR в политику.

5. Настройте Kaspersky Security для Windows Server на ваших активах. Каждый шаг можно выполнить локально в Kaspersky Security для Windows Server на каждом из активов или глобально в Kaspersky Security Center.

   1. Запустите задачу Использование KSN.

      Запуск задачи Использование KSN позволяет использовать Kaspersky Security Network в Kaspersky Security для Windows Server.

      В окне **Обработка данных** задачи Использование KSN установите все флажки на всех вкладках.

      В окне **Параметры** задачи Использование KSN на вкладке **Управление задачами** установите флажок **Запускать по расписанию**. В раскрывающемся списке **Периодичность** выберите пункт **При запуске приложения**.

      Убедитесь, что в подразделе **Использование KSN** отображается закрытый замок. Закрытый замок означает, что политика устанавливает указанные параметры для активов.

   2. Запустите задачу Защита трафика.

      Запуск задачи Защита трафика позволяет обрабатывать веб-трафик (включая трафик, получаемый по электронной почте), а также перехватывать и проверять объекты, передаваемые через веб-трафик, для обнаружения известных компьютерных и других угроз на защищаемом устройстве.

В окне **Параметры** задачи Защита трафика на вкладке **Общие** в раскрывающемся списке **Режим задачи** выберите значение **Драйверный перехват**.

В окне **Параметры** задачи Защита трафика на вкладке **Управление задачами** установите флажок **Запускать по расписанию**. В раскрывающемся списке **Периодичность** выберите пункт **При запуске приложения**.

Убедитесь, что в подразделе **Защита трафика** отображается закрытый замок. Закрытый замок означает, что политика устанавливает указанные параметры для активов.

3. Запустите задачу Контроль запуска приложений.

   Запуск задачи Контроль запуска приложений позволяет отслеживать попытки пользователей запускать приложения, а также разрешает или запрещает запуск этих приложений.

   В окне **Параметры** задачи Контроль запуска приложений на вкладке **Общие** установите флажки **Контролировать загрузку DLL-модулей** и **Разрешать запуск приложений, доверенных в KSN**.

   В окне **Параметры** задачи Контроль запуска приложений на вкладке **Управление задачами** установите флажок **Запускать по расписанию**. В раскрывающемся списке **Периодичность** выберите пункт **При запуске приложений**.

   Убедитесь, что в подразделе **Контроль запуска приложений** отображается закрытый замок. Закрытый замок означает, что политика устанавливает указанные параметры для активов.

- **Kaspersky Anti-Targeted Attack Platform**

  Kaspersky Managed Detection and Response позволят выполнять анализ и мониторинг данных, получаемых от Kaspersky Anti-Targeted Attack (KATA) Platform.

  Интеграция с Kaspersky Anti-Targeted Attack Platform недоступна при использовании лицензионного ключа для региона Саудовская Аравия.

  Чтобы настроить интеграцию Kaspersky Managed Detection and Response с Kaspersky Anti-Targeted Attack Platform, сначала необходимо получить конфигурационный файл MDR. Информация о настройке интеграции приведена в справке Kaspersky Anti-Targeted Attack Platform.

  Kaspersky Anti-Targeted Attack Platform не является частью Kaspersky Managed Detection and Response. Для использования приложения Kaspersky Anti-Targeted Attack Platform ее необходимо приобрести отдельно.

Если в инфраструктуре установлено несколько приложений "Лаборатории Касперского", можно выполнять сценарии для определенных приложений в любом порядке.

5 **Создание точки распространения**

Выполните следующие действия:

1. Проверьте, есть ли у вас хотя бы одна точка распространения в вашей сети или настройте устройство в сети вашей организации в качестве точки распространения. Точка распространения будет выступать в роли прокси-сервера для устройств, участвующих в Kaspersky Security Network.

2. **Включите прокси-сервер KSN на стороне точки распространения** в свойствах точки распространения в разделе **Прокси-сервер KSN (точки распространения)**.

3. Настройте **Область действия** точки распространения, выбрав группу администрирования и/или сетевое местоположение.

Вы можете проверить статус активов с помощью функции Работоспособность MDR.

О конфигурационном файле MDR

Kaspersky Managed Detection and Response использует конфигурационный файл MDR, чтобы включить решение в EPP-программах "Лаборатории Касперского" для рабочих станций (таких как Kaspersky Endpoint Security для Windows), установленных на активах, и чтобы **настроить интеграцию с Kaspersky Anti-Targeted Attack Platform**.

Kaspersky Managed Detection and Response позволят выполнять анализ и мониторинг данных, получаемых от Kaspersky Anti-Targeted Attack (KATA) Platform.

Интеграция с Kaspersky Anti-Targeted Attack Platform недоступна при использовании лицензионного ключа для региона Саудовская Аравия.

Чтобы настроить интеграцию Kaspersky Managed Detection and Response с Kaspersky Anti-Targeted Attack Platform, сначала необходимо получить конфигурационный файл MDR. Информация о настройке интеграции приведена в справке Kaspersky Anti-Targeted Attack Platform.

Kaspersky Anti-Targeted Attack Platform не является частью Kaspersky Managed Detection and Response. Для использования приложения Kaspersky Anti-Targeted Attack Platform ее необходимо приобрести отдельно.

Конфигурационный файл MDR может не понадобиться в следующих случаях:

Обратите внимание, что даже если вы не используете конфигурационный файл MDR, необходимо активировать решение с помощью Консоли MDR или плагина MDR в Kaspersky Security Center.

- Вы используете Kaspersky Endpoint Security для Windows 12.6 или выше в качестве EPP-программы.
- У вас есть только корневой тенант.
- Вы не используете решение Kaspersky Endpoint Detection and Response Optimum одновременно с решением Kaspersky MDR.

В этом случае Kaspersky Endpoint Security для Windows применяет лицензию Kaspersky Security Center. Если вы используете тенанты, отличные от корневого, вам необходимо загрузить конфигурационный файл MDR для каждого тенанта.

Файл конфигурации MDR формируется автоматически средствами Kaspersky Managed Detection and Response, при активации решения с помощью кода активации. Конфигурационный файл MDR представляет собой ZIP-архив, содержащий следующие файлы:

- Файл конфигурации Kaspersky Security Network.
- Файл BLOB (P7) для развертывания программ EPP, поддерживающих интеграцию с MDR с помощью политик Kaspersky Security Center.
- Файл BAT для развертывания устаревших конфигураций с предыдущими версиями EPP-программ, не поддерживающих интеграцию с MDR с помощью политик Kaspersky Security Center.

  Вы можете скачать конфигурационный файл MDR с файлом BLOB (P7) или с файлом BAT. Подробную информацию о различных сценариях развертывания см. в разделе Развертывание Kaspersky Managed Detection and Response.

Скачайте конфигурационный файл MDR и используйте его в соответствии с инструкциями для EPP-программ, установленных на ваших активах:

- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Linux
- Kaspersky Endpoint Security для Mac

Скачивание конфигурационного файла MDR из Kaspersky Security Center

Чтобы скачать конфигурационный файл MDR из Kaspersky Security Center:

1. В Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console в левой панели нажмите **MDR** и перейдите на вкладку **Начало работы**.
2. В пункте 3 перейдите по ссылке **Скачать**, чтобы скачать конфигурационный файл MDR. Этот ZIP-архив содержит конфигурационный файл KPSN, файл BLOB (P7) и файл BAT.

Скачивание конфигурационного файла MDR из Консоли MDR

Чтобы скачать конфигурационный файл MDR из Консоли MDR:

1. Откройте страницу **Начало работы** в Консоли MDR (https://mdr.kaspersky.com/guide). Страница **Начало работы** доступна только для пользователей, выполнивших вход.
2. В пункте 3 перейдите по ссылке **Конфигурационный файл MDR (включая файл BLOB)** или **Конфигурационный файл MDR (включая файл BAT)**.

Уведомление о том, включено ли решение, постоянно отображается в нижней части Консоли MDR.

Лицензирование

В этом разделе описаны основные аспекты лицензирования решения Kaspersky Managed Detection and Response.

Сравнение коммерческих типов лицензий:

Набор функций, доступных в Kaspersky Managed Detection and Response, зависит от вашей коммерческой лицензии (см. таблицу ниже).

Сравнение коммерческих лицензий Kaspersky Managed Detection and Response

Функция	MDR / MDR Expert	MDR Optimum*	MDR Basic*	MDR Advanced*	MDR Prime*
Круглосуточный мониторинг, выявление и обработка инцидентов	✓	✓	✓	✓	✓
Автоматический поиск угроз	✓	✓	✓	✓	✓
Набор сценариев реагирования и автоматическое реагирование на инциденты	✓	✓	✓	✓	✓
Проверка работоспособности системы безопасности и доступности активов	✓	✓	✓	✓	✓
Kaspersky MDR Web Console с панелями мониторинга и отчетами	✓	✓	✓	✓	✓
Возможность получать расширенные сведения об инцидентах	✓	✓	✓	✓	✓
Срок хранения истории инцидентов	1 год	1 год	1 год	1 год	1 год
Срок хранения необработанных данных	3 месяца	1 месяц	1 месяц	3 месяца	3 месяца
Управляемый поиск угроз и расследование инцидентов	✓	—	—	✓	✓
Расширенная экспертная поддержка для управления инцидентами	✓	—	—	✓	✓
Доступ к Kaspersky Threat Intelligence Portal	✓	—	—	✓	✓
API для экспорта данных Kaspersky MDR	✓	—	—	✓	✓
Клиенты могут создавать пользовательский инцидент для обработки с помощью решения Kaspersky MDR**	✓	—	—	✓	✓
Локализованное хранение данных и рабочие группы	—	—	✓	✓	✓
Мультитенантность	✓	✓	✓	✓	✓
Добавление и изменение комментариев к инцидентам	✓	✓	✓	✓	✓
Добавление и изменение приложений к инцидентам	✓	✓	✓	✓	✓
Расширенное расследование инцидентов: анализ для установления предыстории, обстоятельств и детального механизма атаки	—	—	—	✓ Клиенты не могут выбрать инциденты для расширенного расследования, нет гарантированного времени реагирования на инциденты.	✓ Клиенты могут выбрать инциденты для расширенного расследования (в пределах приобретенного срока), гарантированное время реагирования на инциденты.

*Этот уровень доступен только для некоторых регионов и может быть недоступен для покупки новыми тенантами. Обратитесь к поставщику решения Kaspersky Managed Detection and Response для получения подробной информации о доступных вам типах коммерческих лицензий.

**Решение Kaspersky Managed Detection and Response обеспечивает обработку трех обращений в неделю в соответствии с целевыми показателями предоставления решения. Количество обращений, обрабатываемых согласно целевым показателям предоставления решения, увеличивается пропорционально: на каждые 10 000 подключенных конечных устройств количество обращений увеличивается на 1.

О лицензии

Лицензия – это ограниченное по времени право на использование приложения, предоставляемое на основании Условий использования.

Лицензия предоставляет право на получение следующих видов услуг:

- использование приложения в соответствии с Условиями использования;
- получение технической поддержки.

Объем предоставляемых услуг и срок использования приложения зависят от типа лицензии, по которой было активировано приложение.

Предусмотрены следующие типы лицензий:

- *Пробная* – бесплатная лицензия, предназначенная для ознакомления с приложением.

  Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Managed Detection and Response прекращает выполнять все свои функции. Чтобы продолжить использование приложения, вам нужно приобрести коммерческую лицензию.

  Вы можете активировать приложение по пробной лицензии только один раз.

- *Коммерческая* – платная лицензия, предоставляемая при приобретении приложения.

  По истечении срока действия коммерческой лицензии приложение продолжает работать, но с ограниченной функциональностью (не предоставляется телеметрия). Чтобы продолжить использование Kaspersky Managed Detection and Response в режиме полной функциональности, необходимо продлить срок действия коммерческой лицензии.

  Рекомендуется продлить лицензию до истечения срока ее действия, чтобы обеспечить максимальную защиту от всех угроз безопасности.

- *Подписка* – платная лицензия, позволяющая использовать приложение с ежемесячной или ежегодной оплатой, с автоматическим продлением до отмены или истечения срока действия.

  Лицензия по подписке бывает двух типов:

  - *Срочная* – автоматически продлевается в конце каждого расчетного периода до заданной даты истечения срока.
  - *С неограниченным сроком* – автоматически продлевается в конце каждого расчетного периода до отмены клиентом.

  Вы можете управлять лицензией по подписке на Портале управления лицензиями "Лаборатории Касперского".

  Если вы измените объем лицензии, например измените количество активов, информация о лицензии будет обновлена в Консоли MDR в течение 24 часов.

  При отмене или по истечении срока действия лицензии по подписке приложение продолжает работать, но с ограниченной функциональностью (не предоставляется телеметрия). Чтобы продолжить использование Kaspersky Managed Detection and Response в режиме полной функциональности, необходимо продлить срок действия лицензии по подписке.

  Рекомендуется продлить лицензию до истечения срока ее действия, чтобы обеспечить максимальную защиту от всех угроз безопасности.

Лицензия Kaspersky Managed Detection and Response также позволяет использовать решение Kaspersky Endpoint Detection and Response Optimum. Решение становится доступно на активе после настройки интеграции Kaspersky Managed Detection and Response с Kaspersky Endpoint Agent.

О лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа или кодом активации.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- лицензионный ключ или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о приложении, которую можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать приложение по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Код активации требуется указать для добавления лицензионного ключа для активации Kaspersky Managed Detection and Response. Код активации отправляется на адрес электронной почты, указанный при приобретении решения Kaspersky Managed Detection and Response.

Для активации решения с помощью кода активации необходим доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

Если вы потеряли код активации, обратитесь к партнеру "Лаборатории Касперского", у которого вы приобрели лицензию.

Предоставление нового кода активации

Если требуется обновить решение или продлить срок действия лицензии, необходимо указать новый код активации Kaspersky Managed Detection and Response.

> Эта функция доступна, только если установлено разрешение **Интеграция приложений** в Kaspersky Security Center Web Console или в Kaspersky Security Center Cloud Console.

Чтобы ввести новый код активации для Kaspersky Managed Detection and Response:

1. В разделе **MDR** окна Kaspersky Security Center перейдите на вкладку **Использование MDR**.
2. В разделе **Использование лицензии** перейдите по ссылке **Ввести новый код активации**.
3. В окне с уведомлением нажмите на кнопку **OK**.

   Отобразится начальный экран Kaspersky Managed Detection and Response.
4. Нажмите на кнопку **Активировать решение**.
5. Kaspersky Managed Detection and Response проверяет, выполнен ли вход в систему:
   - Если вход в систему выполнен, введите новый код активации, выберите регион и нажмите на кнопку **Активировать**.
   - Если вход в систему не выполнен, выполните вход, введите новый код активации, выберите регион и нажмите на кнопку **Активировать**.
6. Выберите тенанты, к которым будет доступ у пользователей этого Сервера администрирования.

Новый код активации будет применен. Kaspersky Managed Detection and Response будет работать в соответствии с предоставленной лицензией.

О Соглашении о MDR

Соглашение MDR – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать решение.

> Прежде чем начать использовать решение, ознакомьтесь с Соглашением MDR.

Соглашение о MDR доступно:

- Во время активации Kaspersky Managed Detection and Response.
- По ссылке **Условия использования решения MDR** в разделе **Условия использования решения MDR** (**MDR** → **Использование MDR** → **Условия использования решения MDR**).

Вы принимаете условия Соглашения MDR, подтверждая свое согласие с Соглашением MDR при активации решения. Если вы не принимаете Соглашение MDR, отмените активацию Kaspersky Managed Detection and Response и не используйте решение.

О Соглашении об обработке данных

Соглашение об обработке данных (DPA) является неотъемлемой частью Соглашения об Kaspersky Managed Detection and Response. Соглашение об обработке данных применяется к обработке пользовательских данных "Лаборатории Касперского" от имени пользователя.

Содержание *Соглашения об обработке данных* (DPA), его доступность в интерфейсах решения и список данных пользователя зависят от региона, в котором используется решение.

Соглашение об обработке данных доступно для просмотра:

- Во время активации Kaspersky Managed Detection and Response (для некоторых регионов).
- В разделе **Информация** в Консоли Kaspersky Managed Detection and Response: https://mdr.kaspersky.com/about (для некоторых регионов).

  Раздел **Информация** доступен только для пользователей, выполнивших вход.

- В наборе документов, который вы получаете при покупке решения Kaspersky Managed Detection and Response (только для некоторых регионов).

Прежде чем начать использовать решение, ознакомьтесь с Соглашением об обработке данных.

Вы подтверждаете, что полностью прочитали и поняли Соглашение об обработке данных при активации решения или при покупке решения Kaspersky Managed Detection and Response. Если вы не согласны с тем, что ваши данные будут обрабатываться в соответствии с Соглашением об обработке данных, отмените активацию Kaspersky Managed Detection and Response и не используйте решение.

Отзыв согласия с условиями использования решения MDR

Если вы решили прекратить использование Kaspersky Managed Detection and Response, отзовите свое согласие с условиями использования решения MDR, а затем отключите использование Kaspersky Managed Detection and Response на активах.

Эта функция доступна, только если установлено разрешение **Интеграция приложений** в Kaspersky Security Center Web Console или в Kaspersky Security Center Cloud Console.

Чтобы отозвать согласие с условиями использования решения MDR:

1. В разделе MDR окна Kaspersky Security Center перейдите на вкладку **Использование MDR**.
2. Разверните раздел **Условия использования решения MDR**, щелкнув по его названию.
3. Перейдите по ссылке **Отозвать подтверждение принятия условий использования решения MDR**.
4. Подтвердите, что вы хотите отозвать свое согласие с условиями использования решения MDR.

   Ваше согласие с условиями использования решения MDR будет отозвано.

Чтобы удалить информацию о вашей организации из инфраструктуры MDR, обратитесь в Службу технической поддержки.

Предоставление данных

Для корректной работы компонентов Kaspersky Managed Detection and Response требуется обработка данных на стороне "Лаборатории Касперского". Компоненты не отправляют данные без разрешения администратора Kaspersky Managed Detection and Response.

Список пользовательских данных зависит от региона, в котором используется решение. Для вашего региона список пользовательских данных может отличаться от приведенного в этом разделе.

"Лаборатория Касперского" обеспечивает защиту всех полученных данных в соответствии с законодательством и применимыми правилами "Лаборатории Касперского". Данные передаются по безопасным каналам связи.

Список данных о событиях, происходящих на устройствах Пользователя

В целях выявления новых комплексных угроз безопасности данных и их источников, а также угроз вторжения, и принятия оперативных мер по усилению защиты данных, хранящихся и обрабатываемых Клиентом с помощью компьютера, для получения Услуги Клиент обязуется автоматически предоставлять следующие данные:

- Дата установки и активации программного обеспечения, полные имя и версия программного обеспечения, включая информацию об установленных обновлениях и языковой локализации программного обеспечения.
- Данные об установленном на компьютере программном обеспечении, включая версию операционной системы дату ее загрузки и установленных обновлений, объектах ядра, драйверах, службах, точках автозапуска, программах, которые запускаются автоматически при различных системных событиях (например, запуск операционной системы, вход пользователя в систему и т. д.), и их конфигурациях, расширениях браузеров, расширениях Microsoft Internet Explorer, расширениях системы печати, расширениях Проводника Windows, расширениях оболочки операционной системы, контрольных суммах загруженных объектов (MD5), элементах Active Setup, приложениях панели управления, версиях браузеров и почтовых клиентов.
- Данные о разрешенных возможностях на основе файловой системы, эффективный бит возможностей файловой системы, версия возможностей файловой системы, переменные среды, имена системных вызовов.
- Данные об унаследованных возможностях на основе файловой системы.

- Данные об имени компьютера, IP-адресах, шлюзах по умолчанию, MAC-адресах и оборудовании, включая контрольную сумму серийного номера жесткого диска, последние 12 байтов идентификатора компьютерной безопасности (SID), идентификатор зоны безопасности, извлеченный из потока NTFS.

- Данные о программных средствах, используемых для устранения проблем в программном обеспечении, установленном на компьютере Пользователя или для изменения его функциональных возможностей, а также коды возврата, полученные после установки каждого элемента программного обеспечения.

- Данные о состоянии антивирусной защиты компьютера, включая версию, дату и время выпуска используемых антивирусных баз, статистику обновлений и подключений к службам Лаборатории Касперского, идентификаторы задания, идентификаторы и версии программных компонентов, выполняющих проверку, флаги, обозначающие внутреннюю тестовую среду Kaspersky, коды первичной ошибки для конкретного события, коды вторичной ошибки для конкретного события, порядковые номера событий.

- Лицензионный ключ и серийный номер продуктов "Лаборатории Касперского", названия и версии этих продуктов. Идентификаторы установок продуктов Лаборатории Касперского, описание клиента из файла информации о лицензии.

- Данные об учетных записях пользователей: имя учетной записи, имя пользователя, идентификатор операционной системы, информация для входа, права, членство в группах, типы сеансов входа в систему, имя пакета аутентификации, имена доменов, DNS имена, используемые при аутентификации сеансов входа в систему, имя сервера, используемого для аутентификации, основное имя пользователя (UPN) учетной записи, SID.

- Полное содержимое журналов операционной системы.

- Данные системных вызовов.

- Данные об обнаружениях от приложений "Лаборатории Касперского", поддерживающих работу Kaspersky Managed Detection and Response.

- Данные о полученных электронных письмах, включая: адреса электронной почты отправителя и получателя, тему, информацию о вложениях: имя прикрепленного файла, размер, хеш (MD5) и результаты анализа формата файла.

- Данные о координатах области экрана, с которой снят снимок экрана.

- Данные о сетевых подключениях, включая IP-адреса и порты отправителя и получателя, индексы зон IPv6, информация о направлении сетевого подключения (входящее/исходящее), типы и маски выполненных DNS-запросов, коды ошибок для операции запроса DNS, действия по реагированию на запрос DNS, информация о запрошенном DNS-сервере.

- Данные и методы HTTP-соединений, включая посещенные веб-адреса, источники ссылок, агента пользователя, данные сетевого протокола аутентификации: MD5-хеш данных для аутентификации Kerberos, имя учетной записи или компьютера, имя области Kerberos, которой принадлежит имя сервера, домен, к которому принадлежит имя клиента, основное имя пользователя (UPN) учетной записи, криптографический пакет, который использовался для выданного билета Kerberos, маска флагов билета Kerberos в шестнадцатеричном формате, время выдачи билета Kerberos, время истечения срока действия билета Kerberos, окончательный срок действия билета (после которого билет не может быть продлен), имя контроллера домена, используемого для выдачи тикета Kerberos.

- Данные о протоколах прикладного уровня: объем поискового запроса LDAP, фильтр для поискового запроса LDAP, отличительное имя для поискового запроса LDAP, список атрибутов для поискового запроса LDAP.

- Данные о .NET: полное имя загруженной сборки .NET, флаги сборки для загруженной сборки .NET, флаги модуля для загруженного .NET-модуля, имя домена, в который загружена сборка .NET, флаги для сгенерированной заглушки MSIL, данные управляемого метода: пространство имен управляемого метода взаимодействия, имя управляемого метода взаимодействия, сигнатура управляемого метода взаимодействия, сигнатура собственного метода, сигнатура метода-заглушки.

- Данные о файлах, обрабатываемых в операционной системе: имя и путь, размер, атрибуты, типы файлов и объектов, результаты анализа формата файла, контрольная сумма (MD5), веб-адрес, с которого был загружен файл, адрес электронной почты отправителя, от которого был получен файл, и тема сообщения электронной почты, содержимое файловой системы, структуры VERSIONINFO из метаданных файла, информация об издателе, если файл подписан, ID пользователя-владельца файла, идентификатор группы владельцев файла, время последнего доступа к файлу, время последнего изменения метаданных файла, время создания файла, маски флагов проверки цифровой подписи, временные метки и коды операций над файлами и объектами, количество запусков исполняемого файла, идентификатор формата файла, полный путь к объекту и пути к контейнеру объекта, содержимое файла автозапуска, имя файла и путь к файлу на удаленном сетевом ресурсе, к которому выполняется обращение.

- Содержимое каталога "\etc\".

- Данные выводов команд.

- Данные аудита: результат операции, описание операции, тип события и пользователь операции.

- Данные о процессе: идентификатор процесса (PID), трассировка вызова процесса, информация об исполняемом файле процесса и его командной строки, информация о родительском процессе, MD5-хеш кода ошибки вычисления исполняемого файла, коды первичных ошибок, информация о целостности процесса, информация о сеансе входа, командная строка, аргументы командной строки для процесса, переменные среды для целевого процесса, уникальный идентификатор журнала активности процесса, название и/или адрес места инъекции кода, информация о правах доступа для процесса, коды ошибок вычисления хеша MD5 для объекта из командной строки процесса, список файловых упаковщиков, которыми упакован объект, начальный рабочий каталог для целевого процесса, массив идентификаторов процессов (PID), которые были завершены.

- Данные о реестре: имена, разделы и значения.

- Данные об удаленных операциях: имя удаленного компьютера и полное (FQDN) имя удаленного компьютера, на котором была выполнена удаленная операция, имя учетной записи пользователя, которая инициировала удаленную операцию, предоставляемый системой идентификатор удаленного процесса, инициировавшего удаленную операцию, время начала удаленного процесса, инициировавшего удаленную операцию, имя пространства имен для потребителя событий WMI, имя фильтра, используемого потребителем событий WMI, имя созданного потребителя событий WMI, исходный код потребителя событий WMI.

- Данные об ошибках: код ошибки расчета сумм MD5, код ошибки доступа к файлу, коды первичных ошибок, коды вторичных ошибок.

- Данные о событиях выполнения задач по реагированию, созданных специалистами "Лаборатории Касперского" и специалистами Пользователя: название и тип события, дата и время возникновения события, настройки и результаты выполнения задачи по реагированию (информация об объекте (путь к объекту, название и размер объекта, контрольные суммы объекта MD5 и SHA256), информация о помещении объекта в карантин, информация об удалении объекта, информация о завершении процесса, информация об удалении ключа/ветки реестра, информация о запуске процесса, информация об объектах, запрошенных специалистами "Лаборатории Касперского" для детального анализа с согласия Пользователя (имя, путь, размер и тип объекта, контрольные суммы объекта MD5 и SHA256, описание объекта, дата и время обработки запроса файла, содержимое файла), информация об установке и снятии сетевой изоляции устройства, информация об ошибках в результате выполнения задачи на реагирование).

- Данные о скриптах, запускаемых на компьютере: аргументы командной строки, содержимое скрипта или части скрипта, запущенного на компьютере и содержимое объекта или части объекта, полученного по AMSI.

- Данные о командах, полученных консольным приложением, включая интерпретаторы, с использованием перенаправления ввода через канал или файл, а также командах, выполненных пользователем в консольных приложениях, включая интерпретаторы.

Список данных о событиях, выявленных в результате анализа сетевого трафика:

В целях выявления новых комплексных событий безопасности данных и их источников, а также угроз вторжения, и принятия оперативных мер по усилению защиты данных, хранящихся и обрабатываемых Клиентом с помощью компьютера, для получения Услуги Клиент обязуется автоматически предоставлять следующие данные:

- Данные об идентификаторе, версии, типе и временной отметке записи в антивирусной базе данных, используемой для обнаружения события информационной безопасности, название угрозы на основе классификации "Лаборатории Касперского", временная отметка используемых антивирусных баз, код типа файла, идентификатор формата файла, идентификатор задачи программного обеспечения, обнаружившего событие, индикатор проверки репутации или проверки подписи файла.

- Данные для определения репутации файлов и веб-ресурсов, включая IP-адрес и доменное имя веб-адреса, для которого запрашивается репутация, имя файла, который исполнялся в момент обнаружения события, путь к файлу и контрольные суммы (MD5) файла и пути к нему.

- Данные об эмуляции исполняемого файла, включая размер файла и его контрольные суммы (MD5, SHA256, SHA1), версию компонента эмуляции, глубину эмуляции, массив свойств логических блоков и функций внутри логических блоков, полученные во время эмуляции и данные из PE-заголовков исполняемого файла.

- Данные обо всех обнаруженных объектах, включая имя и размер объекта, полный путь к объекту на компьютере, контрольные суммы (MD5, SHA256) обрабатываемых файлов, имя события, связанного с объектом, дата и время обнаружения, признак наличия цифровой подписи файла, название организации, подписавшей файл, статус доверенности и уровень угрозы файла, идентификатор и приоритет правила, используемого для обнаружения и тип технологии обнаружения.

- Тип источника, из которого был загружен объект, IP-адрес источника (или контрольная сумма (MD5) IP-адреса, если он локальный), веб-адрес источника, веб-адрес источника ссылки, имя, доменное имя и контрольная сумма (MD5) имени устройства, отправившего запрос на загрузку, и служебная информации о веб-браузере, отправившем запрос на загрузку.

- Контрольные суммы (MD5) локальной и доменной частей адресов электронной почты отправителя и получателя, а также контрольная сумма (MD5) темы сообщения электронной почты.

- Локальный и удаленный IP-адреса сетевого подключения, номера локальных и удаленных портов и идентификатор протокола подключения.

- Веб-адрес и имя целевого устройства, а также IP-адреса устройства.

- Идентификатор операционной системы, установленной на виртуальной машине, используемой программным обеспечением для анализа объектов.

- Дополнительная информация о событиях, включая индекс частоты встречаемости файла в локальной сети Пользователя, дата проникновения файла в локальную сеть и на компьютер Пользователя, идентификаторы учетных записей, с которых был запущен процесс, контрольные суммы их имен пользователей, а также имена их доменов или рабочих групп, информация о правах учетных записей пользователей.

- Информация о сетевой активности процесса, включая доменные имена сетевых ресурсов, используемых для установления соединения, и IP-адреса доменов, частота подключения к выбранному сетевому ресурсу, размер и тип передаваемых данных.

- Информация об использовании домена сетевого ресурса, включая индекс частоты запросов к домену из локальной сети, временную отметку первого запроса к домену из локальной сети, длительность запросов от различных пользователей и контрольные суммы их имен, имен их компьютеров, инициировавших запросы к домену, дополнительная информация о причинах обнаружения.

- Служебная информация о компоненте обработки статистики, включая дату и время начала и окончания периода, используемого для анализа статистических данных, объем свободной и использованной дисковой памяти, время последней обработки события, время работы

различных алгоритмов обнаружения, сообщения об ошибках компонента, сообщения об успешном запуске различных алгоритмов обнаружения.

- Данные, передаваемые в службу технической поддержки.

Предоставление данных при использовании Kaspersky Endpoint Agent

Подробную информацию о предоставлении данных при использовании Kaspersky Endpoint Agent см. в справке Kaspersky Endpoint Agent для Windows.

Задействованные субподрядчики по обработке данных

Следующие субподрядчики участвуют в обработке пользовательских данных в соответствии с Соглашением об обработке данных Kaspersky Managed Detection and Response:

Субподрядчики, задействованные АО "Лаборатория Касперского"

Имя и адрес другого процессора	Регион использования лицензионного ключа	Предмет договора субподряда	Информация о договоре субподряда
Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855, Luxembourg Hd.: AWS EMEA Legal Sparkoo Technologies Ireland Co., Limited, Address 2nd Floor, Mespil Court, Mespil Road, Ballsbridge, Dublin 4, Dublin D04 E516	Европа, Канада, США	Служба облачной инфраструктуры	Дополнение по обработке данных AWS Дополнение по обработке данных Sparkoo Technologies Ireland Co., Limited
General Cloud computing company (Alibaba Cloud), King Abdullah Financial District Floor 6 - P.O BOX 34555, Post Code 11312, Riyadh, Saudi Arabia	Королевство Саудовская Аравия	Служба облачной инфраструктуры	Дополнение по обработке данных и стандартные договорные условия (alibabacloud.com)
ООО "Яндекс.Облако", 119021, г. Москва, ул. Льва Толстого, д.16, пом.528.	Россия и другие регионы, за исключением перечисленных выше	Служба облачной инфраструктуры	Предложение о заключении договора на использование сервисов Платформы "Яндекс.Облако"

Используемый процессор зависит от региона, выбранного при активации Kaspersky Managed Detection and Response для обеспечения соответствия требованиям законодательства в отношении обработки пользовательских данных.

О Kaspersky Security Network

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения.

Более подробную информацию об отправке в "Лабораторию Касперского", хранении и уничтожении статистической информации, полученной во время использования KSN, вы можете прочитать в Положении о Kaspersky Security Network и на веб-сайте "Лаборатории Касперского".

Инфраструктура KSN

Kaspersky Security Network поддерживает следующие инфраструктурные решения:

- Глобальный KSN – это решение, которое используют большинство приложений "Лаборатории Касперского". Участники KSN получают информацию от Kaspersky Security Network, а также отправляют в "Лабораторию Касперского" данные об объектах, обнаруженных на компьютере пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз Kaspersky Security Network.

- KPSN (Kaspersky Private Security Network) – это решение, позволяющее пользователям компьютеров, на которые установлены приложения "Лаборатории Касперского", получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в KSN со своих компьютеров. KPSN разработан для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky Security Network по следующим причинам:

  - Отсутствие подключения локальных рабочих мест к сети интернет.

  - Законодательный запрет или ограничение корпоративной безопасности на отправку любых данных за пределы страны или за пределы локальной сети организации.

KPSN необходим для работы Kaspersky Managed Detection and Response. KPSN настраивается автоматически в Kaspersky Security Center при активации решения Kaspersky Managed Detection and Response. При отзыве согласия с условиями использования решения MDR, KPSN автоматически отключается.

Подробную информацию о настройке KPSN см. в справке Kaspersky Security Center.

Периодическое обновление конфигурационных файлов KSN

Чтобы обеспечить безопасную передачу данных телеметрии клиентов в Kaspersky Managed Detection and Response, "Лаборатория Касперского" периодически обновляет ключи шифрования данных телеметрии MDR. Открытый ключ передается как часть конфигурационного файла KSN.

При использовании плагина MDR для Kaspersky Security Center Cloud Console или локальной версии Kaspersky Security Center в некоторых случаях конфигурационный файл KSN обновляется автоматически (подробности приведены в таблице ниже). Зачастую вам необходимо заменить установленный конфигурационный файл KSN вручную.

Если конфигурационный файл KSN не обновлен на ваших активах, данные телеметрии не будут отправляться в Kaspersky Managed Detection and Response.

Не позднее чем за месяц до истечения срока действия текущего конфигурационного файла KSN, "Лаборатория Касперского" уведомит вас о скором истечении срока действия конфигурационного файла KSN. Существует два варианта уведомления:

- Создается инцидент, уведомляющий о скором истечении срока действия текущего конфигурационного файла KSN.
- Уведомление о приближающемся истечении срока действия текущего файла конфигурации KSN будет опубликовано в Консоли MDR. Это уведомление видят все пользователи, выполняющие вход в Консоль MDR.

Действия, необходимые для обновления конфигурационного файла KSN

Решение, используемое для управления активами	Интерфейс, который используют ваши SOC-аналитики	Требуемые действия
Kaspersky Security Center Cloud Console.	Плагин MDR установлен в Kaspersky Security Center Cloud Console	Подключитесь к Kaspersky Security Center Cloud Console. При входе в приложение плагин MDR пытается установить новый конфигурационный файл KSN в Kaspersky Security Center Cloud Console. При успешном обновлении файла с помощью плагина MDR вы получите уведомление об изменении конфигурационного файла KSN. Если конфигурационный файл KSN не удалось обновить с помощью плагина MDR, вы получите уведомление о причине проблемы: • Ваша учетная запись имеет недостаточно прав для обновления файла. • Непредвиденная ошибка при обновлении конфигурационного файла KSN. Если уведомления не отображаются, вероятно, конфигурационный файл KSN был успешно обновлен при подключении другого специалиста к Kaspersky Security Center Cloud Console. При появлении уведомления о недостаточных правах для обновления конфигурационного файла KSN, обратитесь к администратору сервера Kaspersky Security Center Cloud Console (роль **Главный администратор**): Попросите администратора подключиться к Kaspersky Security Center Cloud Console. Когда администратор подключится, конфигурационный файл KSN будет обновлен. Вы можете проверить актуальность конфигурационного файла KSN в любое время. Для этого в Kaspersky Security Center в разделе **MDR** перейдите на вкладку **Использование MDR**. Отобразится информация о текущей версии конфигурационного файла KSN. Если доступна новая версия конфигурационного файла KSN, вы можете использовать кнопку для обновления конфигурационного файла KSN. Если при обновлении возникла непредвиденная ошибка, обратитесь в Службу технической поддержки "Лаборатории Касперского".
Kaspersky Security Center Cloud Console.	Консоль MDR ИЛИ Вы используете API для скачивания инцидентов и последующей обработки в собственной системе	Подключитесь к Kaspersky Security Center Cloud Console. Запустите мастер первоначальной настройки, чтобы активировать плагин MDR. Если у вашей учетной записи недостаточно прав для активации плагина MDR, обратитесь к администратору сервера Kaspersky Security Center Cloud Console. Следуйте приведенным выше инструкциям для сервера Kaspersky Security Center Cloud Console и плагина MDR. Если при обновлении возникла непредвиденная ошибка, обратитесь в Службу технической поддержки "Лаборатории Касперского".
Локальная версия Kaspersky Security Center 14 и выше	Плагин MDR установлен в локальной версии Kaspersky Security Center	Войдите в Kaspersky Security Center. При входе в приложение плагин MDR пытается установить новый конфигурационный файл KSN на Сервер Kaspersky Security Center Cloud. При успешном обновлении файла с помощью плагина MDR вы получите уведомление об изменении конфигурационного файла KSN.

		Если конфигурационный файл KSN не удалось обновить с помощью плагина MDR, вы получите уведомление о причине проблемы: • Ваша учетная запись имеет недостаточно прав для обновления файла. • Непредвиденная ошибка при обновлении конфигурационного файла KSN. Если уведомления не отображаются, вероятно, конфигурационный файл KSN был успешно обновлен при подключении другого специалиста к Kaspersky Security Center Cloud Console. При появлении уведомления о недостаточных правах для обновления конфигурационного файла KSN, обратитесь к администратору сервера Kaspersky Security Center: Попросите администратора подключиться к Серверу администрирования Kaspersky Security Center. Когда администратор подключится, конфигурационный файл KSN будет обновлен. Если администратор не получает уведомления об изменении конфигурационного файла KSN, необходимо проверить версию установленного плагина MDR и при необходимости обновить его до текущей версии (2.1.17 или выше). Вы можете проверить актуальность конфигурационного файла KSN в любое время. Для этого в Kaspersky Security Center в разделе **MDR** перейдите на вкладку **Использование MDR**. Отобразится информация о текущей версии конфигурационного файла KSN. Если доступна новая версия конфигурационного файла KSN, вы сможете загрузить его, нажав на кнопку. Если при обновлении возникла непредвиденная ошибка, обратитесь в Службу технической поддержки "Лаборатории Касперского".
Локальная версия Kaspersky Security Center 14 и выше	Консоль MDR (плагин MDR не установлен в локальной версии Kaspersky Security Center) ИЛИ Для скачивания инцидентов и последующей обработки в собственной системе используется API	Попросите администратора Консоли MDR выполнить следующие действия: 1. Скачать ZIP-архив MDR со страницы **Начало работы**. 2. Извлечь конфигурационный файл KSN из загруженного ZIP-архива. 3. Отправить этот файл администратору Сервера администрирования Kaspersky Security Center. Попросите администратора сервера Kaspersky Security Center загрузить полученный конфигурационный файл KSN, выбрав **Свойства Сервера администрирования** → **Параметры прокси-сервера KSN** → **Файл параметров прокси-сервера KSN**. Если при обновлении возникла непредвиденная ошибка, обратитесь в Службу технической поддержки "Лаборатории Касперского".
Локальная версия Kaspersky Security Center 13.* и выше	Плагин MDR установлен в локальной версии Kaspersky Security Center ИЛИ Для скачивания инцидентов и последующей обработки в собственной системе используется API	

Если в вашей сети установлено несколько серверов Kaspersky Security Center, конфигурационный файл KSN необходимо обновить на каждом сервере.

Обновление конфигурационного файла KSN на серверах KATA

Если в вашей сети есть серверы KATA, подключенные к Kaspersky Managed Detection and Response, вам необходимо обновить конфигурационный файл MDR на этих серверах KATA.

Попросите администратора Консоли MDR скачать ZIP-архив для конфигурационного файла MDR со страницы **Начало работы** – https://mdr.kaspersky.com/guide .

Страница **Начало работы** консоли MDR доступна только для пользователей, выполнивших вход.

После того как вы получите конфигурационный ZIP-архив для MDR, попросите администратора сервера KATA загрузить конфигурационный файл MDR на серверы KATA. Если при обновлении конфигурационного файла MDR возникают проблемы, администратору сервера KATA следует обратиться в Службу технической поддержки "Лаборатории Касперского" для получения инструкций по обновлению конфигурационного файла MDR на сервере KATA.

Панели мониторинга в Консоли MDR

В Консоли MDR можно просматривать сводную информацию в панели мониторинга.

Чтобы просмотреть панели мониторинга:

1. В Консоли MDR перейдите к разделу **Мониторинг**.

   Откроется страница **Общая информация**.

2. На странице **Общая информация** представлены следующие панели мониторинга:

   - **Максимальное количество активов для лицензии**

     Круговая диаграмма, показывающая количество подключенных активов в сравнении с максимальным количеством активов, доступных в рамках лицензии.

   - **Активы по статусам**

     Круговая диаграмма, показывающая распределение активов по их статусам.

   - **Активные инциденты**

     Круговая диаграмма, показывающая распределение активных инцидентов в соответствии с их статусами.

   - **Действие по реагированию.**

     Круговая диаграмма, показывающая распределение действий по реагированию в соответствии с их статусами.

     > Количество подключенных активов соответствует активам, доступным в Консоли MDR за последние 7 дней. Чтобы получить количество подключенных активов за определенный период времени, в Консоли MDR перейдите в пункт меню **Активы**.

   - **Статистика телеметрии**

     Панель мониторинга, которая отображает статистику телеметрии решения MDR для клиента, включая статистику по конкретным тенантам. Вы можете просмотреть данные за 1 день, за 7, 30, 90, 180 дней, за 1 год или за все время непрерывного использования решения MDR.

     В этой панели отображается количество каждого из следующих объектов:

     - *События телеметрии* – это все события, отправляемые с клиентских активов в Kaspersky Managed Detection and Response.
     - *Подозрительные события* – это события телеметрии, которые Kaspersky Managed Detection and Response определяет как события, требующие дополнительной проверки.
     - *События безопасности* – это события телеметрии, которые правила обнаружения определяют как потенциальные инциденты.
     - *Инциденты* – это действия, которые технология обнаружения определяет как критические. Инциденты требуют немедленной реакции (действий по реагированию) со стороны Kaspersky Managed Detection and Response.
     - *Сработавшие правила обнаружения* – это ряд уникальных правил обнаружения, срабатывающих при определенных событиях телеметрии в течение определенного периода времени.

   - **Количество инцидентов**

     График, показывающий количество инцидентов и их статусы по дням недели.

Панели мониторинга обновляются при каждом обновлении страницы **Общая информация**.

Получение сводной информации

Kaspersky Managed Detection and Response предоставляет несколько типов отчетов со сводной информацией, которые можно получать по электронной почте. В этом разделе приведены инструкции по настройке получения сводной информации.

Получение информации обо всех активах в файле CSV (Консоль MDR)

Вы можете получить информацию обо всех активах, относящихся к вашей учетной записи, в CSV-файле. К сводной информации не применяются фильтры, то есть количество активов в этой сводной информации равно количеству всех активов, которые видны в Консоли MDR.

Вы можете скрыть активы со статусом **Отсутствует** в сводной информации, установив соответствующий флажок в разделе **Параметры**.

Чтобы получить сводную информацию в формате CSV:

1. В Консоли MDR перейдите к разделу **Активы**.
   Откроется список активов.
2. Нажмите на кнопку **Получить по почте сводную информацию в формате CSV**, расположенную в верхней части окна.

Сводная информация будет отправлена на адрес электронной почты, указанный при активации Kaspersky Managed Detection and Response.

Получение информации об инциденте в формате PDF (Консоль MDR)

Вы можете получить сводную информацию о конкретном инциденте в формате PDF.

Чтобы получить сводную информацию в формате PDF:

1. В окне Консоли MDR выберите пункт меню **Инциденты**.
   Откроется список инцидентов.
2. Нажмите на инцидент, информацию о котором вы хотите получить.
   Откроется карточка инцидента.
3. Перейдите по ссылке **Получить по почте сводную информацию в формате PDF** в верхней части окна.

Сводная информация будет отправлена на адрес электронной почты, указанный при активации Kaspersky Managed Detection and Response.

Получение сводной информации обо всех инцидентах в формате PDF

Вы можете настроить отправку сводного отчета, который содержит данные об открытых инцидентах.

Отчет отправляется по электронной почте в открытом, незашифрованном формате PDF, на указанные вами адреса и в соответствии с заданным расписанием.

Отчет всегда содержит данные за последние семь дней. День формирования отчета не включен в отчет. Если вы настроили получение сводного отчета каждый день, ваш ежедневный отчет будет содержать данные за предыдущие семь дней, кроме сегодняшнего дня. Если вы настроили получение сводного отчета каждую среду, отчет будет содержать данные с прошлой среды по последний вторник.

Вы можете настроить отправку сводного отчета как в Консоли MDR, так и в Kaspersky Security Center.

Настройка рассылки отчетов в Kaspersky Security Center

Чтобы настроить получение сводного отчета в PDF-файле:

1. В разделе **MDR** в Kaspersky Security Center перейдите на вкладку **Отчеты**.
2. Нажмите на значок плюса в строке **Задачи рассылки отчета**.
   Появится панель **Новая задача рассылки отчета**.
3. Включите переключатель **Отправка по расписанию**.
4. Укажите следующие параметры:
   - В поле **Имя** укажите название задачи рассылки отчета. Название может содержать латинские буквы, цифры и специальные символы. Оно не должно быть длиннее 100 символов.
   - В поле **Адреса получателей** укажите адрес электронной почты пользователя, который получит отчет. Можно указать несколько адресов электронной почты.
   - Установите флажок, подтверждающий ваше согласие на отправку сводного отчета на указанные адреса электронной почты.

     Обратите внимание, что сводные отчеты содержат данные для всех тенантов, могут содержать конфиденциальные данные и будут отправляться в открытом, незашифрованном формате PDF.

   - Флажок, требующий подтверждения адресов электронной почты с помощью кода безопасности, установлен по умолчанию. Вы можете снять флажок, если не хотите проверять адреса электронной почты. Если вы не подтвердите адрес электронной почты, вы все равно можете сохранить внесенные изменения. Если вы снимете флажок, внимательно проверьте введенные адреса электронной почты, так как они будут добавлены без дополнительных подтверждений. В этом случае пользователи будут получать сводные отчеты, которые содержат данные для всех тенантов, могут содержать конфиденциальные данные и будут отправлены в открытом виде, незашифрованном формате PDF.

- В раскрывающемся списке **Расписание** выберите, как часто следует отправлять сводную информацию:
  - **Ежедневно**
  - **Еженедельно**
  - **Ежемесячно**
  - **Ежегодно**
  - **По рабочим дням**
  - **Другая**

  При выборе значения **Другая** появляются кнопки для указания дней недели. Укажите хотя бы один день недели.
- В поле **Время (UTC)** укажите время UTC в 24-часовом формате, когда необходимо отправить отчет. Например, 15:00.

  Расписание влияет только на время получения отчета, но не влияет на период данных в отчете.

  Отчет всегда содержит данные за последние семь дней. День формирования отчета не включен в отчет. Если вы настроили получение сводного отчета каждый день, ваш ежедневный отчет будет содержать данные за предыдущие семь дней, кроме сегодняшнего дня. Если вы настроили получение сводного отчета каждую среду, отчет будет содержать данные с прошлой среды по последний вторник.

5. Нажмите на кнопку **Сохранить** в нижней части панели.
6. Если выбран параметр **Подтвердить указанный адрес электронной почты кодом безопасности**, на каждый указанный адрес электронной почты будет отправлен уникальный код подтверждения. Срок действия кода подтверждения – 10 минут. В открывшемся разделе подтверждения вставьте код подтверждения для указанных адресов электронной почты.

   Если три раза подряд был указан неправильный код или код с истекшим сроком действия, появится кнопка **Отправить повторно**. Нажмите на эту кнопку, чтобы получить новые коды подтверждения.

   После проверки всех адресов электронной почты отобразится раздел с соответствующим сообщением. Нажмите на кнопку **Закрыть** в нижней части раздела.

Сводный отчет будет отправлен на указанные адреса электронной почты в соответствии с указанным расписанием. Вы можете изменить это расписание позже.

Изменение расписания рассылки информации об инцидентах

Чтобы изменить расписание задачи рассылки отчетов:

1. В разделе **MDR** в Kaspersky Security Center перейдите на вкладку **Отчеты**.

   Откроется список задач рассылки отчетов.

   Каждая строка соответствует одному отчету со сводной информацией. В списке отображается следующая информация об отчете:
   - **Дата**

     Дата создания отчета.
   - **Название**

     Произвольное, удобочитаемое название отчета.
   - **Расписание**

     Дата и время отправки сводной информации.
   - **Электронная почта**

     Адреса электронной почты для отправки сводной информации.
2. Выберите строку с задачей, расписание которой вы хотите изменить.

   Отобразится раздел **Редактировать расписание**.
3. При необходимости измените положение переключателя **Отправка по расписанию**.
4. При необходимости измените значения полей.
5. Нажмите на кнопку **Сохранить** в нижней части раздела.
6. Если вы добавили новые адреса электронной почты, подтвердите их в появившемся разделе.

Расписание задачи настроено.

Настройка рассылки отчета в Консоли MDR

Вы можете настроить расписание рассылки сводного отчета, который содержит данные об открытых инцидентах. Каждый набор параметров рассылки сохраняется в виде расписания. Вы можете создать не более 50 расписаний для организации и не более 10 расписаний для каждого тенанта.

Для создания или изменения расписаний рассылки отчетов у вас должна быть роль Администратор MDR.

Чтобы настроить получение сводного отчета в PDF-файле:

1. В Консоли MDR в разделе **Параметры** перейдите на вкладку **Расписание**.
2. Нажмите на кнопку **Добавить**.

   Откроется окно **Добавить новое расписание**.
3. Переведите переключатель в положение **Включено**.
4. Внимательно прочтите приведенное ниже уведомление об условиях отправки сводных отчетов. Затем установите флажок, чтобы подтвердить, что вы прочитали и поняли условия. Если флажок не установлен, вы не можете сохранить внесенные изменения.
5. Укажите следующие параметры:
   - В поле **Имя расписания** укажите любое имя сводного отчета. Название отчета может содержать латинские буквы, цифры и специальные символы; оно не должно быть длиннее 100 символов.
   - В поле **Тенант** выберите тенант, для которого вы хотите получить сводный отчет. Отчет будет содержать данные только от выбранного тенанта. Если вы хотите получить сводный отчет обо всех тенантах, выберите **Все тенанты**.
   - В поле **Адреса электронной почты** укажите адрес электронной почты или разделенный запятыми список адресов электронной почты пользователей, которые будут получать сводный отчет.

     Проверьте введенные адреса электронной почты, так как они будут добавлены без дополнительных подтверждений. Сводные отчеты могут содержать конфиденциальные данные и будут отправлены в открытом, незашифрованном формате PDF.
   - В поле **День отправки** выберите день недели, в который будет выполняться отправка сводной информации на указанные адреса электронной почты. Вы можете выбрать один день или **каждый день**.
   - В поле **Время, UTC** укажите время UTC в 24-часовом формате. Например, 15:00.

     Расписание влияет только на время получения отчета, но не влияет на период данных в отчете.

     Отчет всегда содержит данные за последние семь дней. День формирования отчета не включен в отчет. Если вы настроили получение сводного отчета каждый день, ваш ежедневный отчет будет содержать данные за предыдущие семь дней, кроме сегодняшнего дня. Если вы настроили получение сводного отчета каждую среду, отчет будет содержать данные с прошлой среды по последний вторник.
6. Нажмите на кнопку **Сохранить**.

Сводный отчет будет еженедельно или ежедневно отправляться на указанные адреса электронной почты.

Получение уведомлений

В Kaspersky Managed Detection and Response можно настроить отправку уведомлений о событиях, произошедших с инцидентами, и о действиях по реагированию на инциденты по мере их обработки.

Kaspersky Managed Detection and Response отправляет уведомления клиентам через Telegram или по электронной почте, в зависимости от установленных вами параметров. Текст уведомления содержит описание события и ссылку на объект, где произошло событие.

Уведомления можно настроить в Консоли MDR и в разделе **MDR** в Kaspersky Security Center.

Настройка уведомлений в Консоли MDR

Развернуть все | Свернуть все

Чтобы настроить отправку уведомлений в Консоли MDR:

1. В консоли в разделе **Параметры** перейдите на вкладку **Параметры уведомлений**.
2. Установите флажки, соответствующие событиям, о которых вы хотите получать уведомления по электронной почте.

   Доступные флажки:
   - **Все** – все события, о которых Kaspersky Managed Detection and Response отправляет уведомления.
   - **Инциденты** – уведомления о создании, обновлении, разрешении и закрытии инцидентов.

- **Расширенные уведомления** – уведомления, которые содержат описание атаки, обнаруженной в рамках инцидента, и рекомендации по реагированию. Флажок доступен, если на вкладке **Общие параметры** включена функция расширенных уведомлений.

- **Комментарии** – уведомления о создании, обновлении и удалении комментариев в инцидентах.

- **Реагирование** – уведомления о создании, подтверждении и отклонении действий по реагированию.

- **Информация об истечении срока действия лицензии** – уведомления о следующих событиях: до истечения срока действия лицензии осталось менее 30 дней, срок действия лицензии истек. Kaspersky Managed Detection and Response отправляет эти уведомления ежедневно, но прекращает их отправку после истечения срока действия лицензии или после продления лицензии.

3. Нажмите на кнопку **Подписаться**, расположенную над флажками, чтобы подписаться на уведомления от чат-бота Telegram. При нажатии на кнопку **Подписаться** появится сгенерированная приложением уникальная ссылка для активации чат-бота Telegram. Вы можете использовать эту ссылку для одной учетной записи Telegram.

   Используйте эту ссылку только на устройстве (настольном или мобильном), на котором установлено приложение Telegram. По ссылке невозможно активировать чат-бот в веб-версии Telegram.

   Если вы хотите получать уведомления на другую учетную запись Telegram, нажмите на кнопку **Отписаться**, а затем повторите процедуру подписки, чтобы сгенерировать новую ссылку и использовать ее для активации чат-бота для другой учетной записи.

4. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить параметры. Кнопка **Сохранить** становится активной только в случае изменения параметров.

Доставка уведомлений настроена.

Настройка уведомлений в Kaspersky Security Center

Развернуть все | Свернуть все

*Чтобы настроить отправку уведомлений в разделе **MDR** в Kaspersky Security Center:*

1. В разделе **MDR** в Kaspersky Security Center перейдите на вкладку **Уведомления**.

   Откроется вкладка **Параметры**.

2. Если вы хотите получать уведомления по электронной почте, включите параметр **Уведомлять по электронной почте**, укажите адрес электронной почты и следующие параметры уведомления:

   - Укажите адрес электронной почты в поле **Электронная почта** и установите хотя бы один из флажков. В противном случае не удастся сохранить параметры.

   - **Инциденты** – уведомления о создании, разрешении и закрытии инцидентов.

     - **Расширенные уведомления** – уведомления, которые содержат описание атаки, обнаруженной в рамках инцидента, и рекомендации по реагированию. Флажок доступен, если на вкладке **Параметры** включена функция расширенных уведомлений.

   - **Комментарии** – уведомления о создании, обновлении и удалении комментариев в инцидентах.

   - **Реагирование** – уведомления о создании, подтверждении и отклонении действий по реагированию.

3. Если вы хотите получать уведомления с помощью Telegram, включите параметр **Уведомлять по Telegram** и установите хотя бы один из следующих флажков:

   - **Инциденты** – уведомления о создании, разрешении и закрытии инцидентов.

   - **Комментарии** – уведомления о создании, обновлении и удалении комментариев в инцидентах.

   - **Реагирование** – уведомления о создании, подтверждении и отклонении действий по реагированию.

   Нажмите на кнопку **Получить ссылку**, расположенную над флажками, чтобы подписаться на уведомления от чат-бота Telegram. При нажатии на кнопку **Получить ссылку** появится сгенерированная приложением уникальная ссылка для активации чат-бота Telegram. Вы можете использовать эту ссылку для одной учетной записи Telegram.

4. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить параметры. Кнопка **Сохранить** становится активной только в случае изменения параметров.

   Если вы выберете уведомление по электронной почте, уникальный код подтверждения будет отправлен на указанный вами адрес электронной почты. Срок действия кода подтверждения – 10 минут.

   Отобразится раздел подтверждения.

   В открывшемся разделе подтверждения вставьте код подтверждения для указанного адреса электронной почты.

   Если три раза подряд был указан неправильный код или код с истекшим сроком действия, появится кнопка **Отправить повторно**. Нажмите на эту кнопку, чтобы получить новый код подтверждения.

5. После проверки адреса электронной почты отобразится раздел с соответствующим сообщением.

6. Нажмите на кнопку **Закрыть** в нижней части раздела.

Доставка уведомлений настроена.

Получение расширенных уведомлений

Вы можете настроить отправку расширенных уведомлений об инцидентах пользователям MDR по электронной почте. Расширенные уведомления содержат описание атаки, обнаруженной в рамках инцидента, и рекомендации по реагированию. Описание атаки включает в себя выборку данных, получаемых решением MDR в событиях телеметрии с устройств, подключенных к решению MDR, в связи с чем описание может содержать следующую конфиденциальную информацию:

- Имя хоста
- IP-адреса устройства
- Имя учетной записи
- Пароль от учетной записи (если на устройстве был запущен скрипт, содержащий пароль)
- URL-адреса службы
- Имя файла
- Адрес электронной почты
- Названия отделов и тенантов

Полный список данных, получаемых MDR-решением, содержится в разделе Предоставление данных.

Включение расширенных уведомлений в Консоли MDR

Чтобы включить отправку расширенных уведомлений:

1. В Консоли MDR в разделе **Параметры** перейдите на вкладку **Общие параметры**.
2. Включите параметр **Включить расширенные уведомления** и установите флажок ниже, чтобы подтвердить, что вы прочитали и поняли условия отправки расширенных уведомлений.
3. Нажмите на кнопку **Сохранить**.

Теперь вы можете подписаться на расширенные уведомления в разделе **Настройки уведомлений** в Консоли MDR.

Включение расширенных уведомлений в Kaspersky Security Center

Чтобы включить отправку расширенных уведомлений:

1. В разделе **MDR** Kaspersky Security Center выберите вкладку **Настройка**.
2. Включите параметр **Включить расширенные уведомления по электронной почте** и установите флажок ниже, чтобы подтвердить, что вы прочитали и поняли условия отправки расширенных уведомлений.
3. Нажмите на кнопку **Сохранить**.

Теперь вы можете подписаться на расширенные уведомления на вкладке **Уведомления**.

Управление пользователями

Развернуть все | Свернуть все

Пользователи Kaspersky Managed Detection and Response могут иметь разные роли с разными функциями, доступными для каждой роли. *Ролевая модель* – это набор правил, определяющих роли пользователей.

В Kaspersky Managed Detection and Response имеются следующие роли:

- **Администратор MDR**

Суперпользователь, имеющий доступ ко всем функциям Kaspersky Managed Detection and Response, предоставляемым в рамках лицензии. Администратор MDR может предоставить доступ к источникам данных клиентов другим пользователям. При активации Kaspersky Managed Detection and Response вы автоматически становитесь администратором MDR, поэтому для активации рекомендуется использовать корпоративный адрес электронной почты вместо личного. Создание учетной записи администратора MDR с использованием личного адреса электронной почты может создать угрозу безопасности, например, кражу учетной записи администратора MDR.

В Kaspersky Security Center этой роли соответствуют следующие права доступа:

Функциональная область	Разрешать	Запретить
Доступ к инцидентам	✓	—
Параметры автоподтверждения	✓	—
Управление действиями по реагированию	✓	—
Управление тенантами	✓	—
Сводная информация по инцидентам	✓	—
Доступ к REST API	✓	—

- Старший специалист по безопасности.

Сотрудник, имеющий доступ к функциям Kaspersky Managed Detection and Response, предоставляемым в рамках лицензии, но не имеющий доступа к REST API. Старший специалист по безопасности имеет право принимать и отклонять действия по реагированию.

В Kaspersky Security Center этой роли соответствуют следующие права доступа:

Функциональная область	Разрешать	Запретить
Доступ к инцидентам	✓	—
Параметры автоподтверждения	✓	—
Управление действиями по реагированию	✓	—
Управление тенантами	—	✓
Сводная информация по инцидентам	—	✓
Доступ к REST API	—	✓

- Специалист по безопасности.

Сотрудник, имеющий доступ к функциям Kaspersky Managed Detection and Response, предоставляемым в рамках лицензии, но не имеющий доступа к REST API. Специалист по безопасности не имеет права принимать и отклонять действия по реагированию.

В Kaspersky Security Center этой роли соответствуют следующие права доступа:

Функциональная область	Разрешать	Запретить
Доступ к инцидентам	✓	—
Параметры автоподтверждения	—	✓
Управление действиями по реагированию	—	✓
Управление тенантами	—	✓
Сводная информация по инцидентам	—	✓
Доступ к REST API	—	✓

Приглашение новых пользователей в Консоль MDR

Развернуть все | Свернуть все

Чтобы пригласить нового пользователя Kaspersky Managed Detection and Response:

1. В окне Консоли MDR выберите пункт меню **Параметры**.

   Откроется список пользователей.

2. Нажмите на кнопку **Добавить**, расположенную над списком пользователей.

   Отобразится карточка приглашения.

3. В поле **Электронная почта** укажите адрес электронной почты.

4. В поле **Роль пользователя** укажите роль нового пользователя.

   Доступны следующие роли пользователей:

- Администратор MDR

  Суперпользователь, имеющий доступ ко всем функциям Kaspersky Managed Detection and Response, предоставляемым в рамках лицензии. Администратор MDR может предоставить доступ к источникам данных клиентов другим пользователям. При активации Kaspersky Managed Detection and Response вы автоматически становитесь администратором MDR, поэтому для активации рекомендуется использовать корпоративный адрес электронной почты вместо личного. Создание учетной записи администратора MDR с использованием личного адреса электронной почты может создать угрозу безопасности, например, кражу учетной записи администратора MDR.

  В Kaspersky Security Center этой роли соответствуют следующие права доступа:

Функциональная область	Разрешать	Запретить
Доступ к инцидентам	✓	—
Параметры автоподтверждения	✓	—
Управление действиями по реагированию	✓	—
Управление тенантами	✓	—
Сводная информация по инцидентам	✓	—
Доступ к REST API	✓	—

  Только пользователь с ролью Администратор MDR может назначить роль **Администратор MDR** новому пользователю.

- Старший специалист по безопасности.

  Сотрудник, имеющий доступ к функциям Kaspersky Managed Detection and Response, предоставляемым в рамках лицензии, но не имеющий доступа к REST API. Старший специалист по безопасности имеет право принимать и отклонять действия по реагированию.

  В Kaspersky Security Center этой роли соответствуют следующие права доступа:

Функциональная область	Разрешать	Запретить
Доступ к инцидентам	✓	—
Параметры автоподтверждения	✓	—
Управление действиями по реагированию	✓	—
Управление тенантами	—	✓
Сводная информация по инцидентам	—	✓
Доступ к REST API	—	✓

- Специалист по безопасности.

  Сотрудник, имеющий доступ к функциям Kaspersky Managed Detection and Response, предоставляемым в рамках лицензии, но не имеющий доступа к REST API. Специалист по безопасности не имеет права принимать и отклонять действия по реагированию.

  В Kaspersky Security Center этой роли соответствуют следующие права доступа:

Функциональная область	Разрешать	Запретить
Доступ к инцидентам	✓	—
Параметры автоподтверждения	—	✓
Управление действиями по реагированию	—	✓
Управление тенантами	—	✓

Сводная информация по инцидентам	—	✓
Доступ к REST API	—	✓

5. При необходимости выберите одно или несколько значений в раскрывающемся списке **Тенант**.

   В Консоли можно выбрать существующие тенанты или значение **Не имеет тенантов**.

   Пользователь может просматривать только активы и инциденты, связанные с указанными тенантами. Пользователь может просмотреть активы и инциденты, не назначенные ни одному тенанту, если выбрано значение **Не имеет тенантов**.

   Наряду с выбором значения **Не имеет тенантов** можно указать названия тенантов.

6. Нажмите на кнопку **Пригласить**.

   Карточка приглашения закроется.

Сообщение со ссылкой-приглашением будет отправлено с адреса noreply@mail.account.uis.kaspersky.com на указанный адрес электронной почты.

Приглашенному пользователю необходимо подтвердить свой адрес электронной почты, перейдя по ссылке в сообщении. Пользователь не сможет выполнить вход и использовать Kaspersky Managed Detection and Response, пока его адрес электронной почты не будет подтвержден. Разрешения, соответствующие роли пользователя, будут предоставлены после первого входа пользователя в систему.

Изменение ролей пользователей в Консоли MDR

Можно изменить роль существующего пользователя. Например, сотрудник с ролью Специалист по безопасности получает дополнительные обязанности, для которых требуется роль Старший специалист по безопасности.

Чтобы изменить роль существующего пользователя:

1. В окне Консоли MDR выберите пункт меню **Параметры**.

   Откроется список пользователей.

2. Выберите строку, содержащую пользователя, роль которого вы хотите изменить.

   Отобразится карточка пользователя.

3. Измените роль пользователя, выбрав другую роль в раскрывающемся списке ролей в карточке пользователя.

Роль существующего пользователя изменена.

Изменение способов уведомления пользователей в Консоли MDR

Изменение способов уведомления пользователей доступно только для пользователей с ролью Администратор MDR. Пользователь с этой ролью может редактировать параметры уведомлений всех активных пользователей, включая самого себя.

Пользователи со статусом "активный" могут получать уведомления от Kaspersky Managed Detection and Response по электронной почте и Telegram.

Чтобы изменить способы уведомления пользователей:

1. В окне Консоли MDR выберите пункт меню **Параметры**.

   Откроется список пользователей.

2. Выберите строку, содержащую пользователя, роль которого вы хотите изменить.

   Отобразится карточка пользователя.

3. В карточке пользователя укажите следующие параметры:

   - **Уведомления по электронной почте включены**

     Уведомления отправляются на адрес электронной почты пользователя, указанный при приглашении.

   - **Уведомления через Telegram включены**

     Пользователь получает уведомления от чат-бота Telegram.

Если пользователь потерял доступ к учетной записи Telegram, установите флажок **Отключить уведомления для аккаунта Telegram**. Затем попросите пользователя войти в Консоль MDR, перейти в раздел **Параметры** → **Параметры уведомлений** и повторить процедуру подписки, чтобы сгенерировать новую ссылку для активации подписки Telegram для другой учетной записи Telegram.

4. В нижней части карточки пользователя нажмите на кнопку **Сохранить**, чтобы закрыть карточку.

Способы уведомления пользователей отредактированы и сохранены.

Изменение доступа пользователей к тенантам в Консоли MDR

Вы можете изменить доступ пользователей к тенантам в своей учетной записи, например, если при добавлении нового тенанта требуется, чтобы существующий пользователь имел к нему доступ.

Чтобы изменить права доступа к тенантам:

1. В окне Консоли MDR выберите пункт меню **Параметры**.

   Откроется список пользователей.

2. Выберите строку, содержащую пользователя, права доступа которого вы хотите изменить.

   Отобразится карточка пользователя.

3. В карточке пользователя измените значения в раскрывающемся списке **Тенант**.

4. В нижней части карточки пользователя нажмите на кнопку **Сохранить**, чтобы закрыть карточку.

Права доступа пользователей к тенантам будут изменены.

Управление активами

Актив – это устройство с установленной EPP-программой от "Лаборатории Касперского" (например, Kaspersky Endpoint Security для Windows). В этом разделе представлена информация о просмотре, сортировке и фильтрации активов.

Просмотр и поиск активов в Консоли MDR

Развернуть все | Свернуть все

С помощью списка активов можно просматривать и выполнять поиск доступных активов.

Чтобы просмотреть список активов:

1. В окне Консоли MDR перейдите к пункту **Активы**.

   Откроется список активов. Каждая строка соответствует одному активу. Можно щелкнуть в любом месте строки, чтобы посмотреть информацию об активе.

   Над списком могут отображаться следующие атрибуты актива:

   - **Имя актива**

     Сетевое имя компьютера.

     По нажатию на **Имя актива** можно просмотреть информацию об активе в Kaspersky Security Center Web Console.

   - **Идентификатор актива**

     Уникальный идентификатор актива. Идентификатор актива автоматически формируется в Kaspersky Managed Detection and Response до первой отправки телеметрии активом.

   - **Приложения**

     Программы Endpoint Protection Platform (EPP), установленные на активе и настроенные для использования с Kaspersky Managed Detection and Response.

   - **Интерфейсы**

     Количество доступных сетевых интерфейсов устройства.

   - **Операционная система**

     Операционная система актива.

- **Домен**

  Сетевой домен, которому принадлежит актив.

- **Тенант**

  Имя тенанта, если актив принадлежит одному из тенантов. Если актив не принадлежит ни одному из тенантов, поле остается пустым.

- **Последнее появление**

  Количество дней с момента последнего появления актива в Консоли.

  Активы отсортированы в соответствии с этим значением в порядке убывания.

  По умолчанию отображаются активы, видимые в сети за последние 30 дней. Можно увеличить этот временной интервал, отфильтровав активы.

- **Статус.**

  Статус отражает текущее состояние актива. Для активов со статусами *OK*, *Предупреждение* или *Критический* в приложении дополнительно перечислены проблемы (если были) за последние 72 часа.

  Для активов с Kaspersky Endpoint Security для Windows в конфигурации Endpoint Detection and Response Agent (EDR Agent) статусы *Предупреждение* и *Критический* для компонентов защиты и управления не отображаются.

  Актив может иметь один из следующих статусов:

  - **OK** (зеленый)

    Телеметрия отправляется, защита полностью работоспособна.

  - **Внимание** (желтый)

    Телеметрия отправляется.

    Возможные причины статуса **Предупреждение**:

    - По крайней мере, один из следующих компонентов EPP-программы на активе выключен или не установлен:

      - *Сетевой экран* – узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux или Kaspersky Security для виртуальных сред Легкий агент.

      - *Защита от сетевых угроз* – узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac.

      - *Защита от почтовых угроз* и *дополнительное расширение Microsoft Office Outlook* – узнайте, как включить или настроить эти компоненты в Kaspersky Endpoint Security для Windows.

      - *Защита от веб-угроз* – узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Security для Mac или Kaspersky Security для виртуальных сред Легкий агент.

      - *Самозащита продукта* – узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows или Kaspersky Security для виртуальных сред Легкий агент.

      - Антивирусные базы не обновлялись более 7 дней.

      Эти компоненты влияют на полноту отправляемой телеметрии. Если компонент выключен или отсутствует, Kaspersky Managed Detection and Response не отправляет события телеметрии, связанные с этим компонентом. Установленная EPP-программа может включать не все из перечисленных компонентов.

    - Срок действия конфигурационного файла KSN истекает. В приложении отображается срок действия. Рассмотрите возможность обновления конфигурационного файла KSN. Если вы продолжите работу с текущим конфигурационным файлом, статус изменится на **Критический** за несколько дней до истечения срока его действия.

    Статус **Предупреждение** применим к активам с установленным Kaspersky Endpoint Security для Windows 11 и выше, Kaspersky Endpoint Security для Linux 11.2 и выше, Kaspersky Endpoint Security для Mac 11.2 и выше, Kaspersky Security для виртуальных сред 5.2 Легкий агент и выше. Для активов с Kaspersky Endpoint Security для Windows в конфигурации Endpoint Detection and Response Agent (EDR Agent), этот статус не отображается.

  - **Критический** (красный)

Возможные причины статуса **Критический**:

- По крайней мере, один из следующих компонентов EPP-программы на активе выключен или не установлен:
  - *Мониторинг активности* или *Анализ поведения* – узнайте, как включить или настроить эти компоненты в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux или Kaspersky Security для виртуальных сред Легкий агент.
  - *Защита от файловых угроз*— узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Security для Mac или Kaspersky Security для виртуальных сред Легкий агент.

  Если какой-либо из этих компонентов выключен или отсутствует, Kaspersky Managed Detection and Response прекращает отправку телеметрии с актива. Установленная EPP-программа может включать не все из перечисленных компонентов.
- Конфигурационный файл KSN скоро истекает или уже истек. В приложении отображается срок действия. Рассмотрите возможность обновления конфигурационного файла KSN.

Этот статус применим к активам с установленным Kaspersky Endpoint Security для Windows 11 и выше, Kaspersky Endpoint Security для Linux 11.2 и выше, Kaspersky Endpoint Security для Mac 11.2 и выше, Kaspersky Security для виртуальных сред 5.2 Легкий агент и выше. Для активов с Kaspersky Endpoint Security для Windows в конфигурации Endpoint Detection and Response Agent (EDR Agent), этот статус не отображается.

- **Не в сети** (черный).

  Телеметрия не отправлялась более 7 дней (значение по умолчанию). Вы можете изменить количество дней отсутствия телеметрии, по истечении которых для актива будет отображаться статус **Не в сети** в разделе **Параметры**. Доступный диапазон: 2–29 дней.

  Если вы видите статус **Не в сети** для ваших активов:

  - Убедитесь, что компоненты EPP-программы, перечисленные в статусах **Предупреждение** и **Критический**, установлены и включены на активах.
  - Убедитесь, что Kaspersky Managed Detection and Response правильно развернут в вашей инфраструктуре.

  Статус **Не в сети** не применим к активам VDI (временным виртуальным машинам).

- **Отсутствует** (черный).

  Отсутствие телеметрии более 30 дней для физических активов или более 24 часов для VDI-активов (временных виртуальных машин).

  Если вы видите статус **Отсутствует** для ваших активов:

  - Убедитесь, что компоненты EPP-программы, перечисленные в статусах **Предупреждение** и **Критический**, установлены и включены на активах.
  - Убедитесь, что Kaspersky Managed Detection and Response правильно развернут в вашей инфраструктуре.

  Вы можете скрыть активы со статусом **Отсутствует** в списке активов, в отчетах и в данных, полученных через API-интерфейс.

2. Чтобы изменить количество активов, отображаемых на странице списка, выберите требуемое количество, нажав на ссылку **Записей на странице** в нижней части страницы.

   Можно выбрать отображение по 10, 20 или 50 активов на странице.

Вы можете скрыть активы со статусом **Отсутствует** в списке активов, установив флажок в разделе **Параметры**.

Для перехода по списку активов выберите номер страницы под списком. Для перехода между соседними страницами используйте кнопки **Назад** и **Вперед**.

По умолчанию список активов содержит активы, доступные в Консоли за последние 30 дней.

Чтобы изменить этот период:

1. Нажмите на значок воронки, расположенный над списком.
2. Справа в панели **Фильтр** выберите период в поле **Последнее появление**.
3. Нажмите на кнопку **Сохранить**.

Поиск активов можно выполнить, выбрав значок лупы, расположенный рядом со значком воронки над списком активов.

Фильтрация активов в Консоли MDR

Можно создавать фильтры и применять их к списку активов.

Чтобы создать фильтр для списка активов:

1. В Консоли MDR перейдите в разделу **Активы**.

   Откроется список активов.

2. Нажмите на значок воронки, расположенный над списком активов.

   Отобразится меню **Фильтр**.

   Параметры, доступные для фильтрации:

   - **Последнее появление**

     Момент, последнего появления актива в Консоли.

   - **Имя актива**

     Доступные имена активов.

     Имя актива – это сетевое имя компьютера.

   - **Тенант**

     Доступные названия тенантов.

     Чтобы просмотреть список активов, не назначенных ни одному из ваших тенантов, выберите значение **Не имеет тенантов**.

     Наряду с выбором значения **Не имеет тенантов** можно указать названия тенантов.

   - Статус.

     Статус отражает текущее состояние актива. Для активов со статусами *OK*, *Предупреждение* или *Критический* в приложении дополнительно перечислены проблемы (если были) за последние 72 часа.

     > Для активов с Kaspersky Endpoint Security для Windows в конфигурации Endpoint Detection and Response Agent (EDR Agent) статусы *Предупреждение* и *Критический* для компонентов защиты и управления не отображаются.

     Актив может иметь один из следующих статусов:

     - **OK** (зеленый)

       Телеметрия отправляется, защита полностью работоспособна.

     - **Внимание** (желтый)

       Телеметрия отправляется.

       Возможные причины статуса **Предупреждение**:

       - По крайней мере, один из следующих компонентов EPP-программы на активе выключен или не установлен:

         - *Сетевой экран* – узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux или Kaspersky Security для виртуальных сред Легкий агент.

         - *Защита от сетевых угроз* – узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac.

         - *Защита от почтовых угроз* и *дополнительное расширение Microsoft Office Outlook* – узнайте, как включить или настроить эти компоненты в Kaspersky Endpoint Security для Windows.

         - *Защита от веб-угроз* – узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Security для Mac или Kaspersky Security для виртуальных сред Легкий агент.

         - *Самозащита продукта* – узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows или Kaspersky Security для виртуальных сред Легкий агент.

         - Антивирусные базы не обновлялись более 7 дней.

         Эти компоненты влияют на полноту отправляемой телеметрии. Если компонент выключен или отсутствует, Kaspersky Managed Detection and Response не отправляет события телеметрии, связанные с этим компонентом. Установленная EPP-программа может включать не все из перечисленных компонентов.

       - Срок действия конфигурационного файла KSN истекает. В приложении отображается срок действия. Рассмотрите возможность обновления конфигурационного файла KSN. Если вы продолжите работу с текущим конфигурационным

файлом, статус изменится на **Критический** за несколько дней до истечения срока его действия.

Статус **Предупреждение** применим к активам с установленным Kaspersky Endpoint Security для Windows 11 и выше, Kaspersky Endpoint Security для Linux 11.2 и выше, Kaspersky Endpoint Security для Mac 11.2 и выше, Kaspersky Security для виртуальных сред 5.2 Легкий агент и выше. Для активов с Kaspersky Endpoint Security для Windows в конфигурации Endpoint Detection and Response Agent (EDR Agent), этот статус не отображается.

- **Критический** (красный)

  Возможные причины статуса **Критический**:

  - По крайней мере, один из следующих компонентов EPP-программы на активе выключен или не установлен:

    - *Мониторинг активности* или *Анализ поведения* – узнайте, как включить или настроить эти компоненты в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux или Kaspersky Security для виртуальных сред Легкий агент.

    - *Защита от файловых угроз*— узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Security для Mac или Kaspersky Security для виртуальных сред Легкий агент.

    Если какой-либо из этих компонентов выключен или отсутствует, Kaspersky Managed Detection and Response прекращает отправку телеметрии с актива. Установленная EPP-программа может включать не все из перечисленных компонентов.

  - Конфигурационный файл KSN скоро истекает или уже истек. В приложении отображается срок действия. Рассмотрите возможность обновления конфигурационного файла KSN.

  Этот статус применим к активам с установленным Kaspersky Endpoint Security для Windows 11 и выше, Kaspersky Endpoint Security для Linux 11.2 и выше, Kaspersky Endpoint Security для Mac 11.2 и выше, Kaspersky Security для виртуальных сред 5.2 Легкий агент и выше. Для активов с Kaspersky Endpoint Security для Windows в конфигурации Endpoint Detection and Response Agent (EDR Agent), этот статус не отображается.

- **Не в сети** (черный).

  Телеметрия не отправлялась более 7 дней (значение по умолчанию). Вы можете изменить количество дней отсутствия телеметрии, по истечении которых для актива будет отображаться статус **Не в сети** в разделе **Параметры**. Доступный диапазон: 2–29 дней.

  Если вы видите статус **Не в сети** для ваших активов:

  - Убедитесь, что компоненты EPP-программы, перечисленные в статусах **Предупреждение** и **Критический**, установлены и включены на активах.

  - Убедитесь, что Kaspersky Managed Detection and Response правильно развернут в вашей инфраструктуре.

  Статус **Не в сети** не применим к активам VDI (временным виртуальным машинам).

- **Отсутствует** (черный).

  Отсутствие телеметрии более 30 дней для физических активов или более 24 часов для VDI-активов (временных виртуальных машин).

  Если вы видите статус **Отсутствует** для ваших активов:

  - Убедитесь, что компоненты EPP-программы, перечисленные в статусах **Предупреждение** и **Критический**, установлены и включены на активах.

  - Убедитесь, что Kaspersky Managed Detection and Response правильно развернут в вашей инфраструктуре.

  Вы можете скрыть активы со статусом **Отсутствует** в списке активов, в отчетах и в данных, полученных через API-интерфейс.

- **Изоляция**

  Показывает, включена ли сетевая изоляция. Допустимые значения фильтра:

  - **Изолировано**

    Сетевая изоляция включена.

  - **Не изолировано**

    Сетевая изоляция отключена.

3. Нажмите на кнопку **Сохранить**, чтобы применить созданный фильтр.

После применения фильтра в списке отобразятся только активы, соответствующие заданным параметрам фильтрации.

Вы можете скрыть активы со статусом **Отсутствует** в списке активов, установив флажок в разделе **Параметры**.

Просмотр подробной информации об активах в Консоли MDR

Развернуть все | Свернуть все

Чтобы просмотреть подробную информацию об активах:

1. В окне Консоли MDR перейдите к пункту **Активы**.

   Откроется список активов.

2. Выберите строку с активом, данные о котором вы хотите просмотреть.

   Отобразится карточка актива. Карточка актива содержит две вкладки:

   - **Свойства** – общая информация об активе.
   - **Инциденты** – информация об инцидентах, связанных с активом.

   Общая информация на вкладке **Свойства** содержит следующие данные:

   - **Имя актива**

     Сетевое имя компьютера.

     По нажатию на **Имя актива** можно просмотреть информацию об активе в Kaspersky Security Center Web Console.

   - **Статус.**

     Статус отражает текущее состояние актива. Для активов со статусами *OK*, *Предупреждение* или *Критический* в приложении дополнительно перечислены проблемы (если были) за последние 72 часа.

     Для активов с Kaspersky Endpoint Security для Windows в конфигурации Endpoint Detection and Response Agent (EDR Agent) статусы *Предупреждение* и *Критический* для компонентов защиты и управления не отображаются.

     Актив может иметь один из следующих статусов:

     - **OK** (зеленый)

       Телеметрия отправляется, защита полностью работоспособна.

     - **Внимание** (желтый)

       Телеметрия отправляется.

       Возможные причины статуса **Предупреждение**:

       - По крайней мере, один из следующих компонентов EPP-программы на активе выключен или не установлен:

         - *Сетевой экран* – узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux или Kaspersky Security для виртуальных сред Легкий агент.
         - *Защита от сетевых угроз* – узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac.
         - *Защита от почтовых угроз* и *дополнительное расширение Microsoft Office Outlook* – узнайте, как включить или настроить эти компоненты в Kaspersky Endpoint Security для Windows.
         - *Защита от веб-угроз* – узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Security для Mac или Kaspersky Security для виртуальных сред Легкий агент.
         - *Самозащита продукта* – узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows или Kaspersky Security для виртуальных сред Легкий агент.
         - Антивирусные базы не обновлялись более 7 дней.

         Эти компоненты влияют на полноту отправляемой телеметрии. Если компонент выключен или отсутствует, Kaspersky Managed Detection and Response не отправляет события телеметрии, связанные с этим компонентом. Установленная EPP-программа может включать не все из перечисленных компонентов.

       - Срок действия конфигурационного файла KSN истекает. В приложении отображается срок действия. Рассмотрите возможность обновления конфигурационного файла KSN. Если вы продолжите работу с текущим конфигурационным файлом, статус изменится на **Критический** за несколько дней до истечения срока его действия.

Статус **Предупреждение** применим к активам с установленным Kaspersky Endpoint Security для Windows 11 и выше, Kaspersky Endpoint Security для Linux 11.2 и выше, Kaspersky Endpoint Security для Mac 11.2 и выше, Kaspersky Security для виртуальных сред 5.2 Легкий агент и выше. Для активов с Kaspersky Endpoint Security для Windows в конфигурации Endpoint Detection and Response Agent (EDR Agent), этот статус не отображается.

- **Критический** (красный)

  Возможные причины статуса **Критический**:

  - По крайней мере, один из следующих компонентов EPP-программы на активе выключен или не установлен:

    - *Мониторинг активности* или *Анализ поведения* – узнайте, как включить или настроить эти компоненты в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux или Kaspersky Security для виртуальных сред Легкий агент.

    - *Защита от файловых угроз*— узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Security для Mac или Kaspersky Security для виртуальных сред Легкий агент.

    Если какой-либо из этих компонентов выключен или отсутствует, Kaspersky Managed Detection and Response прекращает отправку телеметрии с актива. Установленная EPP-программа может включать не все из перечисленных компонентов.

  - Конфигурационный файл KSN скоро истекает или уже истек. В приложении отображается срок действия. Рассмотрите возможность обновления конфигурационного файла KSN.

  Этот статус применим к активам с установленным Kaspersky Endpoint Security для Windows 11 и выше, Kaspersky Endpoint Security для Linux 11.2 и выше, Kaspersky Endpoint Security для Mac 11.2 и выше, Kaspersky Security для виртуальных сред 5.2 Легкий агент и выше. Для активов с Kaspersky Endpoint Security для Windows в конфигурации Endpoint Detection and Response Agent (EDR Agent), этот статус не отображается.

- **Не в сети** (черный).

  Телеметрия не отправлялась более 7 дней (значение по умолчанию). Вы можете изменить количество дней отсутствия телеметрии, по истечении которых для актива будет отображаться статус **Не в сети** в разделе **Параметры**. Доступный диапазон: 2–29 дней.

  Если вы видите статус **Не в сети** для ваших активов:

  - Убедитесь, что компоненты EPP-программы, перечисленные в статусах **Предупреждение** и **Критический**, установлены и включены на активах.

  - Убедитесь, что Kaspersky Managed Detection and Response правильно развернут в вашей инфраструктуре.

  Статус **Не в сети** не применим к активам VDI (временным виртуальным машинам).

- **Отсутствует** (черный).

  Отсутствие телеметрии более 30 дней для физических активов или более 24 часов для VDI-активов (временных виртуальных машин).

  Если вы видите статус **Отсутствует** для ваших активов:

  - Убедитесь, что компоненты EPP-программы, перечисленные в статусах **Предупреждение** и **Критический**, установлены и включены на активах.

  - Убедитесь, что Kaspersky Managed Detection and Response правильно развернут в вашей инфраструктуре.

  Вы можете скрыть активы со статусом **Отсутствует** в списке активов, в отчетах и в данных, полученных через API-интерфейс.

- **IP-адрес**

  IP-адрес актива.

- Физический адрес

- **Тенант**

  Имя тенанта, если актив принадлежит одному из тенантов. Если актив не принадлежит ни одному из тенантов, поле остается пустым.

- Первое появление

- Последнее появление

- **Операционная система**

Операционная система актива.

- Приложения "Лаборатории Касперского", работающие с MDR
- **Домен**

На вкладке **Инциденты** отображается список инцидентов. В столбце **Идентификатор/Создан** содержится идентификатор и время создания инцидента. В столбце **Статус** отображается информация о статусе инцидента.

Статусы активов

Статус отражает текущее состояние актива. Для активов со статусами *OK*, *Предупреждение* или *Критический* в приложении дополнительно перечислены проблемы (если были) за последние 72 часа.

Для активов с Kaspersky Endpoint Security для Windows в конфигурации Endpoint Detection and Response Agent (EDR Agent) статусы *Предупреждение* и *Критический* для компонентов защиты и управления не отображаются.

Актив может иметь один из следующих статусов:

- **OK** (зеленый)

  Телеметрия отправляется, защита полностью работоспособна.

- **Внимание** (желтый)

  Телеметрия отправляется.

  Возможные причины статуса **Предупреждение**:

  - По крайней мере, один из следующих компонентов EPP-программы на активе выключен или не установлен:

    - *Сетевой экран* – узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux или Kaspersky Security для виртуальных сред Легкий агент.
    - *Защита от сетевых угроз* – узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac.
    - *Защита от почтовых угроз* и *дополнительное расширение Microsoft Office Outlook* – узнайте, как включить или настроить эти компоненты в Kaspersky Endpoint Security для Windows.
    - *Защита от веб-угроз* – узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Security для Mac или Kaspersky Security для виртуальных сред Легкий агент.
    - *Самозащита продукта* – узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows или Kaspersky Security для виртуальных сред Легкий агент.
    - Антивирусные базы не обновлялись более 7 дней.

    Эти компоненты влияют на полноту отправляемой телеметрии. Если компонент выключен или отсутствует, Kaspersky Managed Detection and Response не отправляет события телеметрии, связанные с этим компонентом. Установленная EPP-программа может включать не все из перечисленных компонентов.

  - Срок действия конфигурационного файла KSN истекает. В приложении отображается срок действия. Рассмотрите возможность обновления конфигурационного файла KSN. Если вы продолжите работу с текущим конфигурационным файлом, статус изменится на **Критический** за несколько дней до истечения срока его действия.

  Статус **Предупреждение** применим к активам с установленным Kaspersky Endpoint Security для Windows 11 и выше, Kaspersky Endpoint Security для Linux 11.2 и выше, Kaspersky Endpoint Security для Mac 11.2 и выше, Kaspersky Security для виртуальных сред 5.2 Легкий агент и выше. Для активов с Kaspersky Endpoint Security для Windows в конфигурации Endpoint Detection and Response Agent (EDR Agent), этот статус не отображается.

- **Критический** (красный)

  Возможные причины статуса **Критический**:

  - По крайней мере, один из следующих компонентов EPP-программы на активе выключен или не установлен:

    - *Мониторинг активности* или *Анализ поведения* – узнайте, как включить или настроить эти компоненты в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux или Kaspersky Security для виртуальных сред Легкий агент.
    - *Защита от файловых угроз*— узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Security для Mac или Kaspersky Security для виртуальных сред Легкий агент.

Если какой-либо из этих компонентов выключен или отсутствует, Kaspersky Managed Detection and Response прекращает отправку телеметрии с актива. Установленная EPP-программа может включать не все из перечисленных компонентов.

- Конфигурационный файл KSN скоро истекает или уже истек. В приложении отображается срок действия. Рассмотрите возможность обновления конфигурационного файла KSN.

Этот статус применим к активам с установленным Kaspersky Endpoint Security для Windows 11 и выше, Kaspersky Endpoint Security для Linux 11.2 и выше, Kaspersky Endpoint Security для Mac 11.2 и выше, Kaspersky Security для виртуальных сред 5.2 Легкий агент и выше. Для активов с Kaspersky Endpoint Security для Windows в конфигурации Endpoint Detection and Response Agent (EDR Agent), этот статус не отображается.

- **Не в сети** (черный).

  Телеметрия не отправлялась более 7 дней (значение по умолчанию). Вы можете изменить количество дней отсутствия телеметрии, по истечении которых для актива будет отображаться статус **Не в сети** в разделе **Параметры**. Доступный диапазон: 2–29 дней.

  Если вы видите статус **Не в сети** для ваших активов:

  - Убедитесь, что компоненты EPP-программы, перечисленные в статусах **Предупреждение** и **Критический**, установлены и включены на активах.
  - Убедитесь, что Kaspersky Managed Detection and Response правильно развернут в вашей инфраструктуре.

  Статус **Не в сети** не применим к активам VDI (временным виртуальным машинам).

- **Отсутствует** (черный).

  Отсутствие телеметрии более 30 дней для физических активов или более 24 часов для VDI-активов (временных виртуальных машин).

  Если вы видите статус **Отсутствует** для ваших активов:

  - Убедитесь, что компоненты EPP-программы, перечисленные в статусах **Предупреждение** и **Критический**, установлены и включены на активах.
  - Убедитесь, что Kaspersky Managed Detection and Response правильно развернут в вашей инфраструктуре.

  Вы можете скрыть активы со статусом **Отсутствует** в списке активов, в отчетах и в данных, полученных через API-интерфейс.

Проверка статуса активов в Kaspersky Security Center

Развернуть все | Свернуть все

Вы можете проверить статус активов с помощью функции Работоспособность MDR. Это позволит выяснить, какие активы защищены с помощью Kaspersky Managed Detection and Response и какие активы не отправляли телеметрию в течение указанного периода времени.

Для активов с Kaspersky Endpoint Security для Windows 12.3 и выше, работающих в конфигурации Endpoint Detection and Response Agent (EDR Agent), отображаемый статус в Консоли MDR не отражает фактический статус.

Чтобы проверить статус активов:

1. В разделе **MDR** в Kaspersky Security Center перейдите на вкладку **Работоспособность MDR**.
2. Перейдите на вкладку **Все когда-либо подключенные активы**.

   Отобразится список всех активов, которые хотя бы один раз отправляли телеметрию в Kaspersky Managed Detection and Response.

   Для каждого актива отображается следующая информация:

   - **Статус.**

     Статус отражает текущее состояние актива. Для активов со статусами *OK*, *Предупреждение* или *Критический* в приложении дополнительно перечислены проблемы (если были) за последние 72 часа.

     Для активов с Kaspersky Endpoint Security для Windows в конфигурации Endpoint Detection and Response Agent (EDR Agent) статусы *Предупреждение* и *Критический* для компонентов защиты и управления не отображаются.

     Актив может иметь один из следующих статусов:

     - **OK** (зеленый)

       Телеметрия отправляется, защита полностью работоспособна.

     - **Внимание** (желтый)

       Телеметрия отправляется.

       Возможные причины статуса **Предупреждение**:

- По крайней мере, один из следующих компонентов EPP-программы на активе выключен или не установлен:
  - *Сетевой экран* – узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux или Kaspersky Security для виртуальных сред Легкий агент.
  - *Защита от сетевых угроз* – узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Mac.
  - *Защита от почтовых угроз* и *дополнительное расширение Microsoft Office Outlook* – узнайте, как включить или настроить эти компоненты в Kaspersky Endpoint Security для Windows.
  - *Защита от веб-угроз* – узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Security для Mac или Kaspersky Security для виртуальных сред Легкий агент.
  - *Самозащита продукта* – узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows или Kaspersky Security для виртуальных сред Легкий агент.
  - Антивирусные базы не обновлялись более 7 дней.

  Эти компоненты влияют на полноту отправляемой телеметрии. Если компонент выключен или отсутствует, Kaspersky Managed Detection and Response не отправляет события телеметрии, связанные с этим компонентом. Установленная EPP-программа может включать не все из перечисленных компонентов.

- Срок действия конфигурационного файла KSN истекает. В приложении отображается срок действия. Рассмотрите возможность обновления конфигурационного файла KSN. Если вы продолжите работу с текущим конфигурационным файлом, статус изменится на **Критический** за несколько дней до истечения срока его действия.

Статус **Предупреждение** применим к активам с установленным Kaspersky Endpoint Security для Windows 11 и выше, Kaspersky Endpoint Security для Linux 11.2 и выше, Kaspersky Endpoint Security для Mac 11.2 и выше, Kaspersky Security для виртуальных сред 5.2 Легкий агент и выше. Для активов с Kaspersky Endpoint Security для Windows в конфигурации Endpoint Detection and Response Agent (EDR Agent), этот статус не отображается.

- **Критический** (красный)

  Возможные причины статуса **Критический**:

  - По крайней мере, один из следующих компонентов EPP-программы на активе выключен или не установлен:
    - *Мониторинг активности* или *Анализ поведения* – узнайте, как включить или настроить эти компоненты в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux или Kaspersky Security для виртуальных сред Легкий агент.
    - *Защита от файловых угроз*— узнайте, как включить или настроить этот компонент в Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Security для Mac или Kaspersky Security для виртуальных сред Легкий агент.

    Если какой-либо из этих компонентов выключен или отсутствует, Kaspersky Managed Detection and Response прекращает отправку телеметрии с актива. Установленная EPP-программа может включать не все из перечисленных компонентов.

  - Конфигурационный файл KSN скоро истекает или уже истек. В приложении отображается срок действия. Рассмотрите возможность обновления конфигурационного файла KSN.

  Этот статус применим к активам с установленным Kaspersky Endpoint Security для Windows 11 и выше, Kaspersky Endpoint Security для Linux 11.2 и выше, Kaspersky Endpoint Security для Mac 11.2 и выше, Kaspersky Security для виртуальных сред 5.2 Легкий агент и выше. Для активов с Kaspersky Endpoint Security для Windows в конфигурации Endpoint Detection and Response Agent (EDR Agent), этот статус не отображается.

- **Не в сети** (черный).

  Телеметрия не отправлялась более 7 дней (значение по умолчанию). Вы можете изменить количество дней отсутствия телеметрии, по истечении которых для актива будет отображаться статус **Не в сети** в разделе **Параметры**. Доступный диапазон: 2–29 дней.

  Если вы видите статус **Не в сети** для ваших активов:

  - Убедитесь, что компоненты EPP-программы, перечисленные в статусах **Предупреждение** и **Критический**, установлены и включены на активах.
  - Убедитесь, что Kaspersky Managed Detection and Response правильно развернут в вашей инфраструктуре.

  Статус **Не в сети** не применим к активам VDI (временным виртуальным машинам).

- **Отсутствует** (черный).

  Отсутствие телеметрии более 30 дней для физических активов или более 24 часов для VDI-активов (временных виртуальных машин).

  Если вы видите статус **Отсутствует** для ваших активов:

- Убедитесь, что компоненты EPP-программы, перечисленные в статусах **Предупреждение** и **Критический**, установлены и включены на активах.
- Убедитесь, что Kaspersky Managed Detection and Response правильно развернут в вашей инфраструктуре.

Вы можете скрыть активы со статусом **Отсутствует** в списке активов, в отчетах и в данных, полученных через API-интерфейс.

- **Имя актива**

  Сетевое имя компьютера.

  По нажатию на **Имя актива** можно просмотреть информацию об активе в Kaspersky Security Center Web Console.

- **Идентификатор актива**

  Уникальный идентификатор актива. Идентификатор актива автоматически формируется в Kaspersky Managed Detection and Response до первой отправки телеметрии активом.

- **Домен**

  Сетевой домен, которому принадлежит актив.

- **Версия ОС**

  Операционная система актива.

- **EPP-программы**

  Программы Endpoint Protection Platform (EPP), установленные на активе и настроенные для использования с Kaspersky Managed Detection and Response.

- **Интерфейсы**

  Количество доступных сетевых интерфейсов устройства.

- **Тенант**

  Имя тенанта, если актив принадлежит одному из тенантов. Если актив не принадлежит ни одному из тенантов, поле остается пустым.

- **Последнее появление**

  Количество дней с момента последнего появления актива в Консоли.

  Активы отсортированы в соответствии с этим значением в порядке убывания.

  По умолчанию отображаются активы, видимые в сети за последние 30 дней. Можно увеличить этот временной интервал, отфильтровав активы.

3. Для работы с этим списком используйте следующие параметры сортировки и фильтрации:

   - Нажмите на заголовок любого столбца, чтобы отсортировать список по выбранным значениям столбца.
   - Щелкните столбец **Статус** и выберите требуемые статусы. Список отфильтрован и отображаются только активы с выбранными статусами.
   - Щелкните значок фильтра ( ) и выберите период времени, чтобы просмотреть активы, последнее появление которых было в течение выбранного периода. Можно также указать произвольный период времени.
   - Нажмите на значок экспорта ( ) над списком активов, чтобы выполнить экспорт в CSV.
   - Используйте поле **Поиск** для поиска активов по имени.

Чтобы просмотреть активы, не отправляющие телеметрию:

1. В разделе **MDR** в Kaspersky Security Center перейдите на вкладку **Работоспособность MDR**.

2. Перейдите на вкладку **Активы со сбоем**.

   Отобразится список всех активов, которые хотя бы один раз отправляли телеметрию в Kaspersky Managed Detection and Response.

   Вы можете выбрать один из следующих периодов для отображения данных:

   - **Активы, не наблюдаемые за сутки**
   - **Активы, не наблюдаемые 7 дней**

   Для каждого актива отображается следующая информация:

   - **Имя актива**

     Сетевое имя компьютера.

     По нажатию на **Имя актива** можно просмотреть информацию об активе в Kaspersky Security Center Web Console.

   - **ОС**

     Операционная система актива.

   - **Версия ОС**

     Версия операционной системы актива.

   - **IP**

     IP-адрес актива.

   - **Домен**

     Сетевой домен, которому принадлежит актив.

3. При необходимости нажмите на значок экспорта ( ) над списком активов, чтобы выполнить экспорт в CSV.

Как избежать потери данных телеметрии от активов

Активы отправляют данные телеметрии в Kaspersky Managed Detection and Response для регистрации и анализа инцидентов безопасности в вашей инфраструктуре. Если вы видите, что в статусе актива есть потери телеметрии, убедитесь, что выполнены следующие инструкции:

1. Рекомендованные версии приложений "Лаборатории Касперского" установлены на ваши активы (см. столбец *Рекомендуемые версии и срок их поддержки* в подразделе *Совместимые версии приложений "Лаборатории Касперского"* раздела Аппаратные и программные требования).

2. Пропускная способность вашего сетевого канала соответствует характеристикам, приведенным в подразделе *Сетевые каналы* раздела Аппаратные и программные требования.

3. Ваш прокси-сервер KSN обеспечивает достаточную пропускную способность.

   Если есть проблемы с пропускной способностью прокси-сервера KSN, выключите прокси-сервер KSN в политике в KSC для принудительного подключения ресурсов к KSN напрямую:

   a. В главном меню Kaspersky Security Center перейдите в раздел **Устройства** → **Политики и профили политик**.

   b. Нажмите на политику Kaspersky Endpoint Security для Windows, Linux или Mac. Откроется окно свойств выбранной политики.

   c. В свойствах политики выберите **Параметры приложения** → **Продвинутая защита** → **Kaspersky Security Network**.

   d. Включите параметр **Использовать серверы KSN, если прокси-сервер KSN недоступен** (если это применимо для политики).

   e. Нажмите на кнопку **OK**.

4. Прокси-сервер KSN включен на стороне точки распространения в Kaspersky Security Center Cloud Console или Web Console для оптимизации загрузки сети.

5. Нагрузка на Сервер администрирования Kaspersky Security Center не превышает установленных ограничений.

6. Используется рекомендованная версия Kaspersky Security Center, указанная в разделе Аппаратные и программные требования, установлены последние доступные исправления и патчи.

Управление инцидентами

Инцидент – это действие, оцениваемое технологией обнаружения как критическое и требующее немедленной реакции со стороны решения. В этом разделе приведена информация об управлении существующими инцидентами и добавлении новых инцидентов.

С выходом версии 2.3.1 плагина MDR функции управления инцидентами удалены из раздела MDR в Kaspersky Security Center. Вы можете управлять инцидентами в Консоли MDR.

Если вы используете плагин MDR версии 2.3.0 или ниже, рекомендуется управлять инцидентами в MDR Web Console, так как функции управления инцидентами в Kaspersky Security Center с плагином MDR больше не разрабатываются.

Для управления инцидентами в Консоли MDR необходимо создать учетную запись Kaspersky и попросить администратора MDR (пользователя Консоли MDR с ролью **Администратор MDR**) пригласить вас в Консоль MDR, используя адрес электронной почты, который вы используете для вашей учетной записи Kaspersky.

Затем вы получите письмо с приглашением, содержащее ссылку на Консоль MDR.

Об инцидентах

Что такое инцидент

Инцидент в контексте информационной безопасности – это любое непредвиденное или нежелательное событие, которое может нарушить нормальную деятельность или безопасность информации.

Событие – это идентифицированные внешние признаки определенного состояния системы, сервиса или сети.

К основным критериям принятия решений в рамках Kaspersky MDR о том, что наблюдаемая активность является инцидентом, относится возможность принять эффективные меры по противодействию, предотвращению или уменьшению возможного ущерба от последствий этой активности. В таблице ниже приведены примеры возможных критериев инцидента и мер реагирования в зависимости от источника события.

Примеры критериев обнаружения инцидентов и мер реагирования

Источник события	Возможные критерии инцидента	Возможные реагирования на инцидент
Конечное устройство	• Активная фаза атаки, которая не была предотвращена автоматически • Признаки вредоносного долговременного присутствия в системе • Признаки произошедших в прошлом инцидентов • Признаки активности внутреннего нарушителя на стороне клиента (также если атака была успешно предотвращена)	• Обнаружение проблем с помощью решений "Лаборатории Касперского", устанавливаемых на конечные устройства, и оценка эффективности автоматического реагирования (если это технически возможно) • Рекомендованные действия по реагированию вручную • Запрошенные действия по автоматическому реагированию • Рекомендации по повышению осведомленности пользователей об информационной безопасности
Конечное устройство + сеть	Событие безопасности от поддерживаемой технологии сетевого обнаружения, подтвержденное на конечном устройстве	• Обнаружение проблем с помощью решений "Лаборатории Касперского", установленных на конечных устройствах, а также решений "Лаборатории Касперского", контролирующих сетевой трафик, и оценка эффективности автоматического реагирования (если это технически возможно) • Рекомендованные действия по реагированию вручную • Запрошенные действия по автоматическому реагированию • Информирование клиента

Сценарии обнаружения инцидентов

Сценарий 1. Обнаружение инцидентов с помощью решения Kaspersky MDR

В этом сценарии инцидент информационной безопасности обнаружен в результате работы Kaspersky MDR. Инцидент регистрируется в системе отслеживания инцидентов автоматически. Приоритет инцидента по умолчанию можно изменить позже, но для этого потребуется указать причину изменения в соответствии с таблицей приоритетов инцидента (см. ниже). Kaspersky MDR обрабатывает зарегистрированные инциденты, чтобы оперативно получать информацию о состоянии ИТ-инфраструктуры клиента.

Если в результате анализа выявляются первопричины инцидента, клиенту предоставляются рекомендации по реагированию. Если информации для определения первопричины инцидента недостаточно, вся доступная информация и результаты анализа предоставляются клиенту для независимого исследования.

Сценарий 2. Обнаружение инцидентов клиентом (создание пользовательских инцидентов недоступно для некоторых типов коммерческой лицензии)

В этом сценарии инцидент информационной безопасности обнаружен клиентом независимо от работы Kaspersky MDR. Если инцидент требует обработки в Kaspersky MDR, клиент может зарегистрировать инцидент вручную и предоставить всю доступную информацию об обнаруженном инциденте с помощью функций Kaspersky MDR. Для приоритета инцидента установлено значение по умолчанию **Низкий**, если иное не указано клиентом при регистрации инцидента.

Дальнейшие этапы обработки инцидента аналогичны сценарию 1.

Уровни приоритета инцидентов

Приоритеты инцидентов и их описания

Приоритет инцидента	Описание
Высокий	Инциденты, которые, по мнению экспертов "Лаборатории Касперского", могут привести к серьезным сбоям в работе или несанкционированному доступу к активам клиентов, контролируемых Kaspersky MDR. Например, обнаружены следы целевой атаки или неизвестной угрозы, требующие дальнейшего расследования с помощью цифровых методов судебной экспертизы.
Средний	Инциденты, которые, по мнению экспертов "Лаборатории Касперского", могут повлиять на эффективность или производительность активов клиента, контролируемых Kaspersky MDR, или привести к единовременному повреждению данных.
Низкий	Инциденты, которые, по мнению экспертов "Лаборатории Касперского", не оказывают существенного влияния на эффективность работы клиентских активов, контролируемых Kaspersky MDR. Например, выявлено потенциально нежелательное программное обеспечение, такие как рекламные приложения или вредоносное ПО.

Приоритет инцидента по умолчанию – **Низкий**.

Целевые показатели предоставления решения

Целевое время реакции и целевой показатель предоставления Kaspersky MDR в зависимости от приоритета инцидента

Приоритет инцидента	Время реакции*	Целевой показатель**
Высокий	1 час	90%
Средний	4 часа	90%
Низкий	24 часа	90%

Инцидент считается решенным, если клиенту были предоставлены рекомендации по мерам реагирования.

*Время реакции – это время между обнаружением инцидента (время создания) и его публикацией в Консоли MDR (время обновления).

**Целевой показатель – процент инцидентов, у которых время реакции соответствует указанным в таблице значениям.

Просмотр и поиск инцидентов в Консоли MDR

Чтобы просмотреть список инцидентов:

1. В окне Консоли MDR выберите пункт меню **Инциденты**.

   Откроется список инцидентов. Каждая строка соответствует одному инциденту. Можно щелкнуть в любом месте строки, чтобы посмотреть информацию об инциденте.

   Над списком отображаются следующие атрибуты инцидента:

   - **ID/Создан** – числовой идентификатор инцидента в Консоли/дата создания инцидента.
   - **Статус** – один из следующих статусов инцидента:
     - **Открыт** – инцидент должен быть обработан службой безопасности.

- **Решен** – по инциденту было получено действие по реагированию от службы безопасности.
- **Ожидает решения** – обработка инцидента службой безопасности временно прекращена.
- **Закрыт** – инцидент обработан службой безопасности, и дополнительная работа над ним не требуется.

- **Сводная информация** – краткий комментарий к инциденту.
- **Тенант** – тенант, которому назначен инцидент.
- **Обновлен** – дата и время обновления инцидента.

  Инциденты будут отсортированы по времени обновления в порядке убывания.

  Вы можете добавлять или удалять атрибуты (столбцы) и изменять их порядок, нажав на значок шестеренки над списком.

2. Чтобы изменить количество инцидентов, отображаемых на странице списка, выберите требуемое количество, нажав на ссылку **Записей на странице** в нижней части страницы. Можно выбрать отображение по 10, 20 или 50 инцидентов на страницу.

Для перехода по списку инцидентов выберите номер страницы под списком. Для перехода между соседними страницами используйте кнопки **Назад** и **Вперед**.

Чтобы отфильтровать инциденты, нажмите на значок воронки над списком.

Поиск инцидентов можно выполнить, выбрав значок лупы, расположенный рядом со значком воронки над списком инцидентов.

Фильтрация инцидентов в Консоли MDR

Для просмотра конкретных инцидентов можно создавать фильтры и применять их к списку инцидентов.

Чтобы создать фильтр для списка инцидентов:

1. В Консоли MDR выберите раздел **Инциденты**.

   Откроется список инцидентов.

2. Нажмите на значок воронки, расположенный над списком инцидентов.

   Отобразится раздел **Фильтр**.

   Параметры, доступные для фильтрации:

   - **Создан**

     Время создания инцидента.

   - **Обновлен**

     Время обновления инцидента.

   - **Приоритет**

     Приоритет инцидента. Доступные приоритеты: Низкий, Средний и Высокий.

   - **Статус.**

     Статус инцидента.

   - **Решение**

     Разрешение инцидента.

   - **Активы**

     Доступные активы.

   - **Тенант**

     Доступные названия тенантов.

     Чтобы просмотреть список инцидентов, не назначенных ни одному из ваших тенантов, выберите значение **Тенант по умолчанию**.

     Наряду с выбором значения **Тенант по умолчанию** можно указать названия тенантов.

   - **Тактики**

     Доступная тактика MITRE реагирования на инцидент.

   - **Статусы реагирования**

     Показывать только инциденты с выбранными статусами соответствующих действий по реагированию.

3. Нажмите на кнопку **Сохранить**, чтобы применить созданный фильтр. Нажмите на кнопку **Очистить**, чтобы отменить созданный фильтр.

После применения фильтра в списке отобразятся только инциденты, соответствующие заданным параметрам фильтрации.

Создание пользовательских инцидентов в Консоли MDR

Развернуть все | Свернуть все

Создание пользовательских инцидентов недоступно для некоторых типов коммерческих лицензий.

Если вы считаете определенную активность в вашей инфраструктуре угрозой, но решение Kaspersky Managed Detection and Response не создало инцидент автоматически, вы можете добавить инцидент вручную.

Согласно условиям Соглашения об уровне обслуживания (SLA), количество создаваемых вручную инцидентов, которые могут обрабатываться службой безопасности, ограничено. Информация об ограничениях доступна на вкладке **Использование MDR** в Kaspersky Security Center. На этой вкладке можно отслеживать количество созданных вручную инцидентов за текущий период (например, за текущую неделю):

- Общее количество инцидентов, которые вы можете создать за текущий период. Эти инциденты должны обрабатываться службой безопасности в соответствии с Соглашением об уровне обслуживания. Вы можете создать больше инцидентов, чем предусмотрено соглашением MDR, но в этом случае не гарантируется соблюдение сроков обработки инцидентов, указанных в Соглашении об уровне обслуживания.
- Оставшееся количество инцидентов, которые вы можете создать за текущий период.

Чтобы добавить инцидент:

1. В окне Консоли MDR выберите пункт меню **Инциденты**.

   Откроется список инцидентов.

2. В верхней части окна нажмите на кнопку **Добавить**.

   Отобразится раздел добавления инцидента.

3. Заполните следующие поля:

   - **Общая информация**

     Краткий комментарий к инциденту.

   - **Описание**

     Подробная информация об инциденте в свободной форме. Поддерживается разметка

   - **Активы**

     Активы, скомпрометированные в результате инцидента. Для этого поля предлагаются активы, уже существующие в Консоли MDR и Kaspersky Security Center.

4. При необходимости заполните поле **Тенант**.

   Для поля **Тенант** можно выбрать существующие в Консоли тенанты или значение **Не имеет тенантов**.

5. Нажмите на кнопку **Отправить**.

   Раздел добавления инцидента будет скрыт.

Новый инцидент будет добавлен в список инцидентов в Консоли MDR. Можно просмотреть подробную информацию о созданном инциденте и действия по реагированию на инцидент.

Просмотр подробной информации об инцидентах в Консоли MDR

Чтобы просмотреть подробную информацию об инцидентах:

1. В окне Консоли MDR выберите пункт меню **Инциденты**.

   Откроется список инцидентов.

2. Выберите строку с инцидентом, данные о котором вы хотите просмотреть.

   Откроется страница с данными инцидента.

   В заголовке страницы отображается идентификатор инцидента. Под заголовком отображаются четыре вкладки:

   - **Общая информация.**

Общая информация об инциденте.

- **Действие по реагированию.**
  Информация о действиях по реагированию на инцидент.
- **Обсуждение.**
  Информация об обсуждении и файлах, связанных с инцидентом.
- **История.**
  Информация об изменениях инцидента.

Данные на вкладке **Общая информация** начинаются с краткой сводки инцидентов. Дополнительная информация в этом разделе включает:

- Приоритет инцидента.
- Статус инцидента.
- Решение по инциденту.
- Время создания и время обновления инцидента.
- Тактики MITRE.
- Техники MITRE.
- Технология обнаружения.

Под общей информацией об инциденте приведена следующая информация:

- Затронутые активы.
- Индикаторы компрометации активов.
- Индикаторы компрометации сети.

Данные на вкладке **Общая информация** завершаются описанием клиента и кнопкой **Закрыть инцидент**.

3. Если вам известно, что инцидент является дубликатом, или если вы не собираетесь его решать, нажмите на кнопку **Закрыть инцидент**.
4. На вкладке **Реагирование** отображается информация о действиях по реагированию.
   Информация на вкладке **Реагирование** представлена в виде списка. Список содержит следующие столбцы:
   - **Статус.**
   - **Идентификатор актива.**
   - **Тип.**
   - **Подробная информация.**
   - **Комментарий.**
   - **Изменен.**
   - **Время обновления.**
5. Чтобы добавить комментарий к инциденту:
   a. На вкладке **Обсуждение** на странице с информацией об инциденте введите комментарий в текстовом поле.
      Поддерживается разметка и прикрепленные файлы. Максимальный размер файла – 10 МБ.
   b. Нажмите на кнопку **Отправить**.
      Комментарий будет добавлен на вкладку **Обсуждение** на страницу с информацией об инциденте. Комментарий можно изменить или удалить в течение 10 минут после публикации.
6. На вкладке **История** можно просмотреть информацию об изменениях инцидента.
   Под заголовком имеется переключатель для отображения различных групп изменений:
   - **Все события.**
   - **Только инциденты.**

- **Только реагирование.**
- **Только обсуждение.**

Рядом с переключателем расположены следующие кнопки:

- Кнопка **Столбцы** со значком шестеренки позволяет выбрать столбцы для отображения на вкладке **История**.
- Кнопка **Фильтр** со значком воронки отображает изменения, относящиеся только к элементам, отмеченным установленными флажками.
- Кнопка **Поиск** со значком лупы отображает изменения, относящиеся только к введенным словам или символам.

Типы реагирования на инциденты

Развернуть все | Свернуть все

Аналитики MDR SOC исследуют инциденты и предлагают действия по реагированию, которые вы можете принять или отклонить. Это стандартный способ обработки инцидентов в Kaspersky Managed Detection and Response.

Однако вы можете создавать действия по реагированию вручную, используя функции Kaspersky Endpoint Detection и Response Optimum.

> В этой статье описаны только типы действий по реагированию на инциденты, предлагаемые аналитику SOC.

Каждое действие по реагированию может иметь набор параметров, представленных на вкладке **Реагирование** для инцидента.

Доступные типы действий по реагированию:

- **Получить файл**

  Копирование файла из вашей инфраструктуры в Kaspersky SOC. Если вы принимаете это действие по реагированию, указанный файл будет скопирован в Kaspersky SOC.

  Обратите внимание, что при этом типе действий могут передаваться файлы, содержащие личные и конфиденциальные данные.

  Допустимые параметры:

  - **Путь к зараженному файлу**

    Абсолютный путь к файлу. Например, `C:\\file.exe`.

  - **Максимальный размер файла**

    Максимальный размер файла в МБ.

    Если размер зараженного файла превышает указанное максимальное значение, выполнить действие по реагированию не удастся, но предлагаемое действие появится на вкладке **История** для инцидента.

- **Изолировать**

  Изоляция указанного актива от сети.

  > Если нужно срочно отключить сетевую изоляцию, обратитесь в службу технической поддержки или напишите запрос на вкладке **Обсуждение** инцидента.

  Допустимые параметры:

  - **Пароль для отключения изоляции**

    Пароль для отключения изоляции. Как только служба технической поддержки получит запрос на отключение сетевой изоляции, вам отправят информацию об использовании пароля.

  - **Идентификатор задачи**

    Уникальный идентификатор задачи, используемый совместно с **Паролем отключения изоляции** для отключения сетевой изоляции вручную.

  - **Данные пароля**

    Вы можете проверить действительность **Пароля**, сформировав на его основе производный ключ и сравнив полученное значение со значением параметра **Производный ключ**.

    - **Версия**

Цифровая версия правил создания пароля. Версия 1 означает, что для создания производного ключа применяются следующие параметры PBKDF2:

- Хеш-алгоритм HMACSHA256.
- 10000 итераций.
- Длина ключа – 32 байта.

- **Соль**

  Соль в шестнадцатеричном формате (HEX) для получения производного ключа с помощью PBKDF2.

- **Производный ключ**

  Производный ключ в шестнадцатеричном формате (HEX).

- **Срок изоляции актива**

  Время в секундах, по истечении которого изоляция будет отключена автоматически. Если значение времени не указано, применяется значение по умолчанию, равное семи дням. Максимальное значение – 2 678 400 секунд.

- **Правила исключения**

  Массив правил для настраиваемых портов, протоколов, IP-адресов и процессов, к которым не применяется изоляция.

  - **Направление**

    Направление трафика. Возможные значения: **Входящий**, **Исходящий**, **Оба**.

  - **Протокол**

    Номер протокола согласно спецификации IANA.

    Допустимые значения:

    - **1** (ICMP)
    - **6** (TCP)
    - **17** (UDP)
    - **58** (IPv6-ICMP)

  - **Диапазон удаленных портов**

    Диапазон удаленных портов, указанный в полях **С** и **По**.

  - **Удаленный IPv4-адрес**

    Удаленный IPv4-адрес или маска подсети.

  - **Удаленный IPv6-адрес**

    Удаленный IPv6-адрес или маска подсети.

  - **Диапазон локальных портов**

    Диапазон локальных портов, указанный в полях **С** и **По**.

  - **Локальный IPv4-адрес**

    Локальный IPv4-адрес или маска подсети.

  - **Локальный IPv6-адрес**

    Локальный IPv6-адрес или маска подсети.

  - **Процесс**

    Путь к образу процесса, указанный в поле **Образ** → **Путь**.

- **Отключить изоляцию**

  Отключение сетевой изоляции указанного актива.

- **Удалить ключ реестра**

  Удаление ключа реестра или ветки реестра на указанном активе.

  Допустимые параметры:

- **Ключ**

  Абсолютный путь ключа, который начинается с `HKEY_LOCAL_MACHINE` или `HKEY_USERS`. Например, `HKEY_LOCAL_MACHINE\\SYSTEM\\WebClient`.

  Если ключ является символической ссылкой, будет удален только этот ключ, а целевой ключ ссылки останется нетронутым.

- **Значение**

  Значение ключа.

  Если этот параметр не указан, ключ будет удален рекурсивно. Во время рекурсивного удаления каждый вложенный ключ, являющийся символической ссылкой, будет удален, а его целевой ключ останется нетронутым.

  Если значение ключа – пустая строка, значение по умолчанию будет удалено.

- **Дамп памяти**

  Создание дампа памяти и отправка его в Kaspersky SOC.

  Допустимые параметры:

  - **Тип дампа**

    Дамп памяти может быть одного из двух типов:

    - **Полный дамп памяти**

      Дамп всей памяти актива.

    - **Дамп процесса**

      Дамп указанного процесса.

  - **Максимальный размер файла**

    Максимальный размер файла дампа в формате ZIP в МБ. Значение по умолчанию – 100 МБ.

  - **Процесс**

    Идентификатор процесса и сведения об образе.

    - **Образ**

      - **Путь**

        Абсолютный путь к файлу. Например, `%systemroot%\\system32\\svchost.exe.`

      - **SHA-256**

        Контрольная сумма SHA256 в шестнадцатеричном формате (HEX).

      - **MD5**

        Контрольная сумма MD5 в шестнадцатеричном формате (HEX).

    - **Уникальный идентификатор**

      Уникальный идентификатор процесса.

  - **Ограничение на количество процессов**

    Максимальное количество процессов, которые могут содержаться в файле дампа.

- **Прервать процесс**

  Прервать процесс на указанном активе с помощью Kaspersky Endpoint Security для Windows. Прервать процесс можно указав его имя или идентификатор процесса (PID).

- **Запустить скрипт**

  Запускает скрипт на указанном активе с помощью Kaspersky Endpoint Security для Windows.

  Чтобы это действие по реагированию сработало, на активе должен быть установлен компонент PowerShell. Вы можете просмотреть запускаемый скрипт и его описание в Консоли MDR.

- **Поместить файл на карантин**

Помещает потенциально опасный файл в специальное локальное хранилище. Файлы в этом хранилище хранятся в зашифрованном виде и не угрожают безопасности устройства. В запросе подтверждения указывается актив, путь к файлу и хеш файла (MD5 или SHA256).

- **Восстановить файл из карантина**

  Восстанавливает ранее помещенный на карантин файл в исходное местоположение. Если в исходном местоположении есть файл с таким же именем, восстановление не выполняется.

Обработка реагирования на инциденты в Консоли MDR

Вы можете просматривать, принимать и отклонять действия по реагированию на инциденты.

Чтобы просмотреть действия по реагированию на инцидент:

1. В окне Консоли MDR выберите пункт меню **Инциденты**.

   Откроется список инцидентов.

2. Выберите строку с инцидентом, данные о котором вы хотите просмотреть.

   Откроется страница с данными инцидента.

3. На странице инцидента перейдите на вкладку **Реагирование**.

   Откроется список действий по реагированию на инцидент.

   Каждая строка соответствует одному действию. В списке отображается следующая информация о действии по реагированию на инцидент:

   - **Статус.**

     Статус задачи.

   - **Идентификатор актива.**

     Идентификатор актива для выполняемой задачи.

   - **Тип.**

     Тип объекта, который формирует действие по реагированию.

   - **Параметры**

     Локальный путь в конкретной операционной системе для получения файла действия по реагированию и ожидаемый размера файла в МБ. Максимальный размер файла – 10 МБ.

   - **Комментарий.**

     Последний комментарий к действию по реагированию.

   - **Изменен.**

     Имя пользователя, который последним изменил описание действия по реагированию.

Чтобы просмотреть описание действия по реагированию, нажмите на соответствующую строку.

Чтобы принять или отклонить действие по реагированию на инцидент:

1. В окне Консоли выберите пункт меню **Инциденты**.

   Откроется список инцидентов.

2. Выберите строку с инцидентом, данные о котором вы хотите просмотреть.

   Откроется страница с данными инцидента.

3. На странице инцидента перейдите на вкладку **Реагирование**.

   Откроется список действий по реагированию на инцидент.

4. Выберите действие по реагированию, которое вы хотите принять или отклонить, установив флажок в соответствующей строке.

   Вы также можете выбрать несколько действия по реагированию, установив соответствующие флажки слева. Чтобы выбрать все действия по реагированию, установите флажок в левой части заголовка таблицы задач.

5. Чтобы принять или отклонить действие по реагированию или реагирование, нажмите на кнопку **Принять** или **Отклонить** под списком действий. Появится окно для ввода комментариев. Введите свой комментарий и нажмите на кнопку **Отправить**.

   Вы также можете нажать на действие по реагированию на вкладке **Реагирования**, чтобы проверить его информацию и принять или отклонить его на появившейся боковой панели. Чтобы отклонить действие по реагированию, вы должны ввести свой комментарий в поле в боковой панели.

Статус действия по реагированию будет изменен.

Автоматическое подтверждение действий по реагированию в Консоли MDR

Вы можете включить автоподтверждение предложенных действий по реагированию. В этом случае действия, предлагаемые в рамках действий по реагированию, например, удаление зараженного файла, будут выполняться автоматически. Если эта функция выключена, меры, предлагаемые в действиях по реагированию, необходимо принять или отклонить вручную.

Если вы используете тенанты, вы можете включить автоподтверждение действий по реагированию для всех тенантов или только для выбранных тенантов. Если вы не используете тенанты, включите или выключите эту функцию для своей текущей организации.

Чтобы включить автоподтверждение действий по реагированию:

1. В окне Консоли MDR выберите пункт меню **Параметры**.
2. Откройте вкладку **Инциденты**.
3. Выберите один из следующих параметров:
   - **Включено для всех тенантов.**

     При выборе этого параметра автоподтверждение действий по реагированию включается как для существующих, так и для новых созданных тенантов.
   - **Включено для выбранных ниже тенантов.**

     Выберите тенанты, для которых вы хотите включить автоподтверждение действий по реагированию. Для новых созданных тенантов автоподтверждение действий по реагированию по умолчанию выключено.
4. Нажмите на кнопку **Сохранить**.

Автоподтверждение действий по реагированию включено, и действия, предлагаемые в действиях по реагированию, будут выполняться автоматически для всех тенантов или для выбранных тенантов. Вы можете выключить эту функцию в любое время.

Права доступа для просмотра или изменения параметров автоподтверждения

Роли пользователей Kaspersky Managed Detection and Response имеют следующие права доступа к параметрам автоподтверждения:

Операция	Администратор MDR	Старший специалист по безопасности.	Специалист по безопасности.
Право доступа к вкладке **Инциденты**	✓	✓	—
Изменять текущий выбранный параметр	✓	—	—
Просматривать текущий выбранный параметр	✓	✓	—
Включать автоподтверждение для всех тенантов	✓	—	—
Включать автоподтверждение для определенных тенантов	✓	✓ (только для тенантов, к которым у пользователя есть доступ)	—
Просматривать параметры автоподтверждения определенного тенанта	✓	✓ (только для тенантов, к которым у пользователя есть доступ)	—

Закрытие инцидентов в Консоли MDR

Закрыть инцидент можно, если известно, что инцидент является дубликатом или вы не планируете его решать. В остальных случаях нельзя закрывать инциденты, поскольку их должны решать аналитики MDR SOC. Аналитики MDR SOC решают инцидент в случае применения рекомендованных ими мер в рамках этого инцидента. Решенный инцидент автоматически закрывается через 72 часа.

Чтобы закрыть инцидент:

1. В окне Консоли MDR выберите пункт меню **Инциденты**.

   Откроется список инцидентов.
2. Выберите строку с инцидентом, данные о котором вы хотите просмотреть.

   Откроется страница с данными инцидента.
3. На вкладке **Общая информация** нажмите на кнопку **Закрыть инцидент** в нижней части окна.

Кнопка **Закрыть инцидент** отсутствует для инцидентов со статусом **Закрыт**.

Отобразится раздел **Закрытие инцидентов**.

4. В поле **Причина закрытия инцидента** укажите дополнительную информацию, которую вы хотите передать аналитикам Kaspersky Managed Detection and Response SOC. Например, можно подробно описать, почему вы считаете этот инцидент стандартной ситуацией, не угрожающей вашей инфраструктуре. Это поле можно оставить пустым.

5. Под полем с комментарием выберите вариант **Верное срабатывание** или **Ложное срабатывание**, в зависимости от причины закрытия.

   Выберите вариант **Верное срабатывание**, если решение Kaspersky Managed Detection and Response обнаружило угрозу, но вы не хотите, чтобы аналитики MDR SOC расследовали и решали инцидент.

   Выберите вариант **Ложное срабатывание**, если решение Kaspersky Managed Detection and Response приняло неопасную активность за угрозу. Kaspersky Managed Detection and Response использует эту информацию для улучшения алгоритмов автоматического обнаружения.

6. В нижней части раздела нажмите на кнопку **Закрыть**.

   Раздел **Закрытие инцидентов** будет скрыт.

Инцидент будет закрыт. Теперь Kaspersky Managed Detection and Response не будет выполнять никаких действий в отношении этого инцидента.

Использование функций Kaspersky Endpoint Detection and Response Optimum

Решение Kaspersky Endpoint Detection and Response Optimum предоставляет набор функций для реагирования на инциденты (далее также реагирование EDR), которые можно запускать и настраивать вручную.

- Сетевая изоляция.
- Перемещать файлы на Карантин.
- Отправлять файлы в Cloud Sandbox.
- Удалять файлы.
- Запускать сканирование критических областей.
- Поиск IOC.
- Запрещать запуск.
- Запускать процесс.
- Завершать процесс.
- Получать файлы.

Вы можете найти более подробную информацию об этих реагированиях EDR в справке Kaspersky Endpoint Detection and Response Optimum.

Описанные в этом разделе реагирования EDR доступны для активов с Kaspersky Endpoint Security для Windows 11.7 и выше. Если на своих активах вы используете Kaspersky Endpoint Security для Windows 11.6 или более раннюю версию, для работы с реагированиями EDR на этих активах должен быть установлен Kaspersky Endpoint Agent.

Чтобы активировать функции Kaspersky Endpoint Detection and Response Optimum, вам необходимо добавить на свои активы один из следующих лицензионных ключей с помощью Kaspersky Security Center:

- Kaspersky Endpoint Detection and Response Optimum
- Надстройка Kaspersky Endpoint Detection and Response Optimum

Для управления действиями по реагированию на обнаружение EDR в Kaspersky Security Center перейдите в раздел **Мониторинг и отчеты** → **Обнаружения**.

.

Мультитенантность

Развернуть все | Свернуть все

Мультитенантность – это механизм, позволяющий стать поставщиком услуг Kaspersky Managed Detection and Response для других организаций. Если у вас есть учетная запись MDR, вы можете использовать ее для создания тенантов.

Ваша учетная запись в Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console должна иметь роль со следующими правами доступа: **Доступ к инцидентам** и **Управление тенантами**, чтобы вы могли просматривать, добавлять, изменять и удалять тенанты в разделе **MDR** в Kaspersky Security Center.

Чтобы стать поставщиком услуг MDR, необходим доступ к инфраструктуре тенантов, поскольку это позволит выполнять сценарии развертывания.

Все тенанты являются независимыми и изолированными, то есть данные одного тенанта не доступны другим тенантам.

Только пользователи с назначенной ролью администратора MDR могут добавлять, изменять и удалять тенанты в Консоли MDR.

В рамках учетной записи MDR можно создать до 100 тенантов. Для каждого тенанта имеются следующие параметры:

- **Статус**

  Один из следующих статусов тенанта:

  - **Активен**

    Тенант может использовать Kaspersky Managed Detection and Response.

  - **Неактивен**

    Тенант не может использовать Kaspersky Managed Detection and Response.

    Вы можете установить неактивный статус вручную в карточке тенанта. Также неактивный статус устанавливается автоматически в конце срока действия тенанта.

- **Имя тенанта**

  Произвольное удобочитаемое название тенанта, указанное при создании или изменении тенанта. Название тенанта может содержать латинские буквы, цифры и специальные символы. Оно не должно быть длиннее 100 символов.

- **Описание**

  Информация в свободной форме, указанная при создании или изменении тенанта. Описание может содержать латинские буквы, цифры и специальные символы. Оно не должно быть длиннее 2000 символов.

- **Количество активов**

  Количество активов, назначенных вручную при создании или изменении тенанта. Количество активов не должно превышать количество, указанное в строке под этим полем. При попытке указать большее число появится ошибка, а кнопка **Сохранить** в нижней части раздела станет неактивной. Количество активов обычно равно количеству компьютеров в инфраструктуре тенанта, но это не является обязательным требованием.

- **Срок действия**

  Продолжительность "жизни" тенанта указывается вручную при создании или изменении тенанта. Дата прекращения действия не может совпадать или быть позже даты прекращения действия лицензии MDR.

Просмотр тенантов в Kaspersky Security Center

Развернуть все | Свернуть все

С помощью списка тенантов можно выполнять просмотр доступных тенантов.

Ваша учетная запись в Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console должна иметь роль со следующими правами доступа: **Доступ к инцидентам** и **Управление тенантами**, чтобы вы могли просматривать, добавлять, изменять и удалять тенанты в разделе **MDR** в Kaspersky Security Center.

Чтобы просмотреть список тенантов:

1. В разделе **MDR** в Kaspersky Security Center перейдите на вкладку **Тенанты**.

   Отобразится список **Тенанты**. Каждая строка соответствует одному тенанту. Можно щелкнуть в любом месте строки, чтобы посмотреть информацию о тенанте.

2. Над списком отображаются следующие атрибуты тенанта:

- Name

  Произвольное удобочитаемое название тенанта, указанное при создании или изменении тенанта. Название тенанта может содержать латинские буквы, цифры и специальные символы. Оно не должно быть длиннее 100 символов.

- Статус

  Один из следующих статусов тенанта:

  - **Активен**

    Тенант может использовать Kaspersky Managed Detection and Response.

  - **Неактивен**

    Тенант не может использовать Kaspersky Managed Detection and Response.

    Вы можете установить неактивный статус вручную в карточке тенанта. Также неактивный статус устанавливается автоматически в конце срока действия тенанта.

- Количество активов

  Количество активов, назначенных вручную при создании или изменении тенанта. Количество активов не должно превышать количество, указанное в строке под этим полем. При попытке указать большее число появится ошибка, а кнопка **Сохранить** в нижней части раздела станет неактивной. Количество активов обычно равно количеству компьютеров в инфраструктуре тенанта, но это не является обязательным требованием.

- Описание

  Информация в свободной форме, указанная при создании или изменении тенанта. Описание может содержать латинские буквы, цифры и специальные символы. Оно не должно быть длиннее 2000 символов.

- Создан

  Дата создания тенанта.

- Дата окончания срока действия

  Дата окончания срока действия тенанта.

  Тенанты отсортированы по дате окончания срока действия в порядке убывания.

Вы также можете просматривать тенанты в Консоли MDR.

Просмотр тенантов в Консоли MDR

Развернуть все | Свернуть все

Чтобы просмотреть список тенантов:

1. В окне Консоли MDR выберите пункт меню **Параметры**.

2. Перейдите на вкладку **Тенанты**.

   Отобразится список **Тенанты**. Каждая строка соответствует одному тенанту. Можно щелкнуть в любом месте строки, чтобы посмотреть информацию о тенанте.

3. Над списком отображаются следующие атрибуты тенанта:

- Name

  Произвольное удобочитаемое название тенанта, указанное при создании или изменении тенанта. Название тенанта может содержать латинские буквы, цифры и специальные символы. Оно не должно быть длиннее 100 символов.

- Статус

Один из следующих статусов тенанта:

- **Активен**

  Тенант может использовать Kaspersky Managed Detection and Response.

- **Неактивен**

  Тенант не может использовать Kaspersky Managed Detection and Response.

  Вы можете установить неактивный статус вручную в карточке тенанта. Также неактивный статус устанавливается автоматически в конце срока действия тенанта.

- Количество активов

  Количество активов, назначенных вручную при создании или изменении тенанта. Количество активов не должно превышать количество, указанное в строке под этим полем. При попытке указать большее число появится ошибка, а кнопка **Сохранить** в нижней части раздела станет неактивной. Количество активов обычно равно количеству компьютеров в инфраструктуре тенанта, но это не является обязательным требованием.

- Описание

  Информация в свободной форме, указанная при создании или изменении тенанта. Описание может содержать латинские буквы, цифры и специальные символы. Оно не должно быть длиннее 2000 символов.

- Создан

  Дата создания тенанта.

- Дата окончания срока действия

  Дата окончания срока действия тенанта.

  Тенанты отсортированы по дате окончания срока действия в порядке убывания.

Просмотр параметров тенанта в Kaspersky Security Center

Развернуть все | Свернуть все

Параметры каждого тенанта можно просмотреть в вашей учетной записи.

Ваша учетная запись в Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console должна иметь роль со следующими правами доступа: **Доступ к инцидентам** и **Управление тенантами**, чтобы вы могли просматривать, добавлять, изменять и удалять тенанты в разделе **MDR** в Kaspersky Security Center.

Чтобы просмотреть параметры тенанта:

1. В разделе **MDR** в Kaspersky Security Center перейдите на вкладку **Тенанты**.

   Отобразится список **Тенанты**. Каждая строка соответствует одному тенанту. Можно щелкнуть в любом месте строки, чтобы посмотреть информацию о тенанте.

2. Выберите строку с тенантом, данные о котором вы хотите просмотреть.

   Отобразится раздел **Параметры тенанта**.

   Первым параметром является переключатель **Активный**, показывающий, активен ли тенант. При необходимости можно изменить положение переключателя **Активный**. Далее отображаются следующие поля:

   - Name

     Произвольное удобочитаемое название тенанта, указанное при создании или изменении тенанта. Название тенанта может содержать латинские буквы, цифры и специальные символы. Оно не должно быть длиннее 100 символов.

   - Описание

     Информация в свободной форме, указанная при создании или изменении тенанта. Описание может содержать латинские буквы, цифры и специальные символы. Оно не должно быть длиннее 2000 символов.

- **Количество активов**

  Количество активов, назначенных вручную при создании или изменении тенанта. Количество активов не должно превышать количество, указанное в строке под этим полем. При попытке указать большее число появится ошибка, а кнопка **Сохранить** в нижней части раздела станет неактивной. Количество активов обычно равно количеству компьютеров в инфраструктуре тенанта, но это не является обязательным требованием.

- **Продолжительность "жизни" тенанта**

  Продолжительность "жизни" тенанта указывается вручную при создании или изменении тенанта. Дата прекращения действия не может совпадать или быть позже даты прекращения действия лицензии MDR.

3. В нижней части раздела **Параметры тенанта** нажмите на кнопку **Закрыть**, чтобы закрыть раздел.

Вы также можете просматривать параметры тенанта в Консоли MDR.

Просмотр параметров тенанта в Консоли MDR

Развернуть все | Свернуть все

Чтобы просмотреть параметры тенанта:

1. В окне Консоли MDR перейдите к пункту **Параметры**.

2. Перейдите на вкладку **Тенанты**.

   Отобразится список **Тенанты**. Каждая строка соответствует одному тенанту. Можно щелкнуть в любом месте строки, чтобы посмотреть информацию о тенанте.

3. Выберите строку с тенантом, данные о котором вы хотите просмотреть.

   Отобразится раздел **Параметры тенанта**.

   Первым параметром является переключатель **Активный**, показывающий, активен ли тенант. При необходимости можно изменить положение переключателя **Активный**. Далее отображаются следующие поля:

   - **Имя тенанта**

     Произвольное удобочитаемое название тенанта, указанное при создании или изменении тенанта. Название тенанта может содержать латинские буквы, цифры и специальные символы. Оно не должно быть длиннее 100 символов.

   - **Описание**

     Информация в свободной форме, указанная при создании или изменении тенанта. Описание может содержать латинские буквы, цифры и специальные символы. Оно не должно быть длиннее 2000 символов.

   - **Количество активов**

     Количество активов, назначенных вручную при создании или изменении тенанта. Количество активов не должно превышать количество, указанное в строке под этим полем. При попытке указать большее число появится ошибка, а кнопка **Сохранить** в нижней части раздела станет неактивной. Количество активов обычно равно количеству компьютеров в инфраструктуре тенанта, но это не является обязательным требованием.

   - **Срок действия**

     Продолжительность "жизни" тенанта указывается вручную при создании или изменении тенанта. Дата прекращения действия не может совпадать или быть позже даты прекращения действия лицензии MDR.

4. В нижней части раздела **Параметры тенанта** нажмите на кнопку **Отмена**, чтобы закрыть раздел.

Изменение параметров тенанта в Kaspersky Security Center

Параметры тенантов можно изменить в вашей учетной записи.

Ваша учетная запись в Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console должна иметь роль со следующими правами доступа: **Доступ к инцидентам** и **Управление тенантами**, чтобы вы могли просматривать, добавлять, изменять и удалять тенанты в разделе **MDR** в Kaspersky Security Center.

Чтобы изменить параметры тенанта:

1. В разделе **MDR** в Kaspersky Security Center перейдите на вкладку **Тенанты**.

   Отобразится список **Тенанты**. Каждая строка соответствует одному тенанту. Можно щелкнуть в любом месте строки, чтобы посмотреть информацию о тенанте.

2. Выберите строку с тенантом, параметры которого вы хотите изменить.

   Отобразится раздел **Параметры тенанта**.

3. При необходимости измените положение переключателя **Активный**.

4. При необходимости измените значения полей.

5. В нижней части раздела **Параметры тенанта** нажмите на кнопку **Сохранить**.

   Раздел **Параметры тенанта** будет скрыт. После нажатия на кнопку **Сохранить** Kaspersky Managed Detection and Response сформирует новый файл конфигурации MDR, соответствующий обновленным параметрам тенанта.

6. В списке **Тенанты** выберите строку с измененным тенантом.

   Отобразится раздел **Параметры тенанта**.

7. Перейдите по ссылке **Развернуть файл**.

   Отобразится список групп администрирования.

8. Выберите группы администрирования, активы из которых требуется добавить к тенанту. Конфигурационный файл BLOB тенанта будет применен к политикам выбранных групп администрирования.

9. Нажмите на кнопку **Далее**.

   Kaspersky Managed Detection and Response применяет конфигурационный файл BLOB тенанта к политикам выбранных групп администрирования.

   Если не удается автоматически применить конфигурационный файл BLOB тенанта к отдельным группам администрирования, нажмите на ссылку **Скачать файл**, чтобы скачать конфигурационный файл MDR, а затем примените конфигурационный файл BLOB тенанта к политикам вручную.

10. В нижней части раздела **Параметры тенанта** нажмите на кнопку **Отмена**, чтобы закрыть раздел.

Выполнено изменение параметров тенанта. Обновленные параметры будут применены к активам выбранных групп администрирования.

Вы также можете изменять параметры тенанта в Консоли MDR.

Изменение параметров тенанта в Консоли MDR

Добавлять, настраивать и удалять тенанты могут только пользователи с ролью Администратор MDR.

Чтобы изменить параметры тенанта:

1. Откройте Консоль MDR.

2. В Консоли MDR, в разделе **Параметры** перейдите на вкладку **Тенанты**.

   Отобразится список **Тенанты**. Каждая строка соответствует одному тенанту. Можно щелкнуть в любом месте строки, чтобы посмотреть информацию о тенанте.

3. Выберите строку с тенантом, параметры которого вы хотите изменить.

   Отобразится раздел **Параметры тенанта**.

4. При необходимости измените положение переключателя **Активный**.

5. При необходимости измените значения полей.

6. В нижней части раздела **Параметры тенанта** нажмите на кнопку **Сохранить**.

   Раздел **Параметры тенанта** будет скрыт. После нажатия на кнопку **Сохранить** Kaspersky Managed Detection and Response сформирует новый файл конфигурации MDR, соответствующий обновленным параметрам тенанта.

7. В списке **Тенанты** выберите строку с измененным тенантом.

Отобразится раздел **Параметры тенанта**. В нижней части раздела расположены две кнопки для скачивания файла конфигурации MDR для развертывания тенанта:

- **Файл для активов с KEA**

  Файл используется при развертывании приложений "Лаборатории Касперского" с использованием Kaspersky Endpoint Agent.

- **Файл для активов без KEA**

  Файл используется при развертывании Kaspersky Endpoint Security без использования Kaspersky Endpoint Agent.

8. Нажмите на кнопку **Файл для активов с KEA** или **Файл для активов без KEA**, чтобы скачать новый конфигурационный файл MDR.

9. В нижней части раздела **Параметры тенанта** нажмите на кнопку **Отмена**, чтобы закрыть раздел.

Выполнено изменение параметров тенанта. Теперь, чтобы применить измененные параметры, необходимо развернуть новый файл конфигурации MDR на активах тенанта.

Добавление тенантов в Kaspersky Security Center

Развернуть все | Свернуть все

Если вы хотите стать поставщиком услуг Kaspersky Managed Detection and Response для другой организации, необходимо добавить нового тенанта в вашу учетную запись.

Ваша учетная запись в Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console должна иметь роль со следующими правами доступа: **Доступ к инцидентам** и **Управление тенантами**, чтобы вы могли просматривать, добавлять, изменять и удалять тенанты в разделе **MDR** в Kaspersky Security Center.

Чтобы добавить тенант:

1. В разделе **MDR** в Kaspersky Security Center перейдите на вкладку **Тенанты**.

   Отобразится список **Тенанты**.

2. В верхней части окна нажмите на значок плюс (+).

   Отобразится раздел **Параметры тенанта**.

3. При необходимости измените положение переключателя **Активный**.

   По умолчанию переключатель установлен в положение **Активный**.

4. Заполните следующие поля:

   - Name

     Произвольное удобочитаемое название тенанта, указанное при создании или изменении тенанта. Название тенанта может содержать латинские буквы, цифры и специальные символы. Оно не должно быть длиннее 100 символов.

   - Описание

     Информация в свободной форме, указанная при создании или изменении тенанта. Описание может содержать латинские буквы, цифры и специальные символы. Оно не должно быть длиннее 2000 символов.

   - Количество активов

     Количество активов, назначенных вручную при создании или изменении тенанта. Количество активов не должно превышать количество, указанное в строке под этим полем. При попытке указать большее число появится ошибка, а кнопка **Сохранить** в нижней части раздела станет неактивной. Количество активов обычно равно количеству компьютеров в инфраструктуре тенанта, но это не является обязательным требованием.

   - Продолжительность "жизни" тенанта

     Продолжительность "жизни" тенанта указывается вручную при создании или изменении тенанта. Дата прекращения действия не может совпадать или быть позже даты прекращения действия лицензии MDR.

5. В нижней части раздела **Параметры тенанта** нажмите на кнопку **Сохранить.**

   Раздел **Параметры тенанта** будет скрыт. После нажатия на кнопку **Сохранить** Kaspersky Managed Detection and Response сформирует файл конфигурации MDR для нового тенанта.

6. В списке **Тенанты** выберите строку с новым тенантом.

   Отобразится раздел **Параметры тенанта**.

7. Перейдите по ссылке **Развернуть файл**.

   Отобразится список групп администрирования.

8. Выберите группы администрирования, активы из которых требуется добавить к тенанту. Конфигурационный файл BLOB тенанта будет применен к политикам выбранных групп администрирования.

9. Нажмите на кнопку **Далее**.

   Kaspersky Managed Detection and Response применяет конфигурационный файл BLOB тенанта к политикам выбранных групп администрирования.

   BLOB-объект тенанта может быть применен автоматически только к тем группам администрирования, в которых есть политики для Kaspersky Endpoint Agent. Если не удается автоматически применить конфигурационный файл BLOB тенанта к отдельным группам администрирования, нажмите на ссылку **Скачать файл**, чтобы скачать конфигурационный файл MDR, а затем примените конфигурационный файл BLOB тенанта к политикам вручную.

10. В нижней части раздела **Параметры тенанта** нажмите на кнопку **Отмена**, чтобы закрыть раздел.

Новый тенант будет добавлен.

Новые тенанты можно также добавлять в Консоли MDR.

Добавление тенантов в Консоли MDR

Развернуть все | Свернуть все

Добавлять, настраивать и удалять тенанты могут только пользователи с ролью Администратор MDR.

Чтобы добавить тенант:

1. В окне Консоли MDR выберите пункт меню **Параметры**.

2. Перейдите на вкладку **Тенанты**.

   Отобразится список **Тенанты**.

3. В верхней части окна нажмите на кнопку **Добавить**.

   Отобразится раздел **Параметры тенанта**.

4. При необходимости измените положение переключателя **Активный**.

   По умолчанию переключатель установлен в положение **Активный**.

5. Заполните следующие поля:

   - **Имя тенанта**

     Произвольное удобочитаемое название тенанта, указанное при создании или изменении тенанта. Название тенанта может содержать латинские буквы, цифры и специальные символы. Оно не должно быть длиннее 100 символов.

   - **Описание**

     Информация в свободной форме, указанная при создании или изменении тенанта. Описание может содержать латинские буквы, цифры и специальные символы. Оно не должно быть длиннее 2000 символов.

   - **Количество активов**

     Количество активов, назначенных вручную при создании или изменении тенанта. Количество активов не должно превышать количество, указанное в строке под этим полем. При попытке указать большее число появится ошибка, а кнопка **Сохранить** в нижней части раздела станет неактивной. Количество активов обычно равно количеству компьютеров в инфраструктуре тенанта, но это не является обязательным требованием.

   - **Срок действия**

     Продолжительность "жизни" тенанта указывается вручную при создании или изменении тенанта. Дата прекращения действия не может совпадать или быть позже даты прекращения действия лицензии MDR.

6. В нижней части раздела **Параметры тенанта** нажмите на кнопку **Сохранить.**

   Раздел **Параметры тенанта** будет скрыт. После нажатия на кнопку **Сохранить** Kaspersky Managed Detection and Response сформирует файл конфигурации MDR для нового тенанта.

7. В списке **Тенанты** выберите строку с новым тенантом.

   Отобразится раздел **Параметры тенанта**. В нижней части раздела расположены две кнопки для скачивания файла конфигурации MDR для развертывания тенанта:

   - **Файл для активов с KEA**

     Файл используется при развертывании приложений "Лаборатории Касперского" с использованием Kaspersky Endpoint Agent.

   - **Файл для активов без KEA**

     Файл используется при развертывании Kaspersky Endpoint Security без использования Kaspersky Endpoint Agent.

8. Нажмите на кнопку **Файл для активов с KEA** или **Файл для активов без KEA**, чтобы скачать новый конфигурационный файл MDR.

9. В нижней части раздела **Параметры тенанта** нажмите на кнопку **Отмена**, чтобы закрыть раздел.

Новый тенант будет добавлен. Теперь можно развернуть скачанный конфигурационный файл MDR на активах тенанта.

Обратите внимание, что тенанты, созданные в Консоли MDR, недоступны в разделе **MDR** в Kaspersky Security Center. Для работы с этими тенантами используйте Консоль MDR.

Удаление тенантов в Kaspersky Security Center

При удалении тенанта, содержащего некоторые активы, все его активы отключаются от решения MDR. Перед удалением тенанта переместите все его активы в тенант по умолчанию или в новый тенант.

Ваша учетная запись в Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console должна иметь роль со следующими правами доступа: **Доступ к инцидентам** и **Управление тенантами**, чтобы вы могли просматривать, добавлять, изменять и удалять тенанты в разделе **MDR** в Kaspersky Security Center.

Чтобы удалить тенант:

1. В разделе **MDR** в Kaspersky Security Center перейдите на вкладку **Тенанты**.

   Отобразится список **Тенанты**.

2. В списке **Тенанты** наведите указатель мыши на тенанта, которого вы хотите удалить, и щелкните по значку корзины (🗑) в правой части строки.

3. Подтвердите удаление.

Выбранный тенант будет удален.

Тенанты можно также удалять в Консоли MDR.

Удаление тенантов в Консоли MDR

При удалении тенанта, содержащего некоторые активы, все его активы отключаются от решения MDR. Перед удалением тенанта переместите все его активы в тенант по умолчанию или в новый тенант.

Добавлять, настраивать и удалять тенанты могут только пользователи с ролью Администратор MDR.

Чтобы удалить тенанта:

1. В окне Консоли MDR перейдите к пункту **Параметры**.

2. Перейдите на вкладку **Тенанты**.

   Отобразится список **Тенанты**.

3. В списке тенантов наведите курсор мыши на тенант, который вы хотите удалить, и нажмите кнопку **Удалить тенант** со значком корзины, расположенную справа.

Появится окно **Подтвердите удаление тенанта.**

4. Нажмите кнопку **Удалить**, чтобы удалить тенант.

Обратите внимание, что тенанты, созданные в Консоли MDR, недоступны в разделе **MDR** в Kaspersky Security Center. Для работы с этими тенантами используйте Консоль MDR.

Перемещение активов от корневого тенанта к новому тенанту

При удалении тенанта, содержащего некоторые активы, все его активы перестают отправлять данные телеметрии решению MDR. Перед удалением тенанта переместите все его активы в корневой тенант или в новый тенант.

Ваша учетная запись в Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console должна иметь роль со следующими правами доступа: **Доступ к инцидентам** и **Управление тенантами**, чтобы вы могли просматривать, добавлять, изменять и удалять тенанты в разделе **MDR** в Kaspersky Security Center.

Чтобы переместить активы новому тенанту:

1. В разделе **MDR** в Kaspersky Security Center создайте тенант. Позже вы добавите активы этому тенанту.

   При создании тенанта скачивается файл конфигурации MDR.

2. Создайте новую группу администрирования в Kaspersky Security Center Web Console.

3. Добавьте активы, которые вы хотите назначить новому тенанту, в созданную группу администрирования.

4. Создайте политику для Kaspersky Endpoint Agent или EPP-программы для созданной группы администрирования.

5. Примените файл конфигурации MDR к созданной политике.

   Подробную информацию о различных сценариях развертывания см. в разделе Развертывание Kaspersky Managed Detection and Response.

После применения политики к активам группы администрирования они будут переназначены от тенанта по умолчанию новому созданному тенанту.

Чтобы переместить активы корневому тенанту:

1. Загрузите конфигурационный файл MDR для корневого тенанта:

   - В Консоли MDR (https://mdr.kaspersky.com/guide), перейдите на страницу **Начало работы** и перейдите по **ссылке конфигурационного файла MDR (включая BLOB-файл)** или **по ссылке конфигурационного файла MDR (включая BAT-файл)**.

   - В Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console перейдите в раздел **MDR** > **Начало работы** и нажмите на ссылку **Скачать**.

2. Создайте новую группу администрирования в Kaspersky Security Center Web Console.

3. Добавьте активы, которые вы хотите назначить новому тенанту, в созданную группу администрирования.

4. Создайте политику для Kaspersky Endpoint Agent или EPP-программы для созданной группы администрирования.

5. Примените файл конфигурации MDR к созданной политике.

После применения политики к активам группы администрирования они будут переназначены от тенанта по умолчанию новому созданному тенанту.

Разграничение прав доступа к тенантам

Эта процедура относится только к Kaspersky Security Center. В Консоли MDR доступ к тенантам можно настроить при приглашении или изменении пользователей.

Может потребоваться разграничить права доступа пользователей Kaspersky Security Center к тенантам. Это гарантирует, что пользователи Kaspersky Security Center смогут просматривать активы и инциденты, относящиеся только к указанным тенантам. Это достигается за счет создания отдельного виртуального Сервера администрирования для каждого тенанта, к которому требуется ограничить доступ.

Чтобы настроить виртуальный Сервер администрирования для тенанта:

1. В консоли MDR создайте токен обновления и сохраните последовательность символов токена в буфер обмена.

При создании токена обновления укажите тенант, к которому требуется предоставить доступ.

2. В Kaspersky Security Center Web Console создайте виртуальный Сервер администрирования и укажите его администраторов.

3. В Kaspersky Security Center Web Console выполните вход с правами администратора на созданный виртуальный Сервер администрирования, указанный на предыдущем шаге.

   На экране авторизации нажмите на кнопку **Дополнительные параметры**. Появится поле **Виртуальный Сервер администрирования**.

4. Перейдите в раздел **Мониторинг и отчеты** → **MDR**.

   Откроется раздел **MDR**.

5. На вкладке **Начало работы** добавьте токен, созданный на первом шаге, в поле **Вставить токен** в нижней части окна.

6. Нажмите на кнопку **Применить** в нижней части окна.

С этого момента только администратор, выполнивший вход на созданном виртуальном Сервере администрирования, сможет видеть активы и инциденты, связанные с указанным тенантом.

Управление решением с помощью REST API

Эта функция доступна в версиях MDR Expert, MDR Advanced (доступна только в некоторых регионах) и MDR Prime (доступна только в некоторых регионах). Сравнение лицензионных решений приведено в этом разделе.

Для доступа к REST API в Kaspersky Security Center, ваша учетная запись Kaspersky Security Center Web Console должна иметь следующие разрешения: доступ к инцидентам и доступ к REST API.

Для некоторых типов коммерческой лицензии в Консоли MDR можно будет только сгенерировать токен обновления, чтобы использовать его для настройки параметров плагина MDR, без доступа к REST API в Kaspersky Security Center.

Kaspersky Managed Detection and Response позволяет программно получать, создавать и обновлять объекты MDR с помощью REST API. REST API работает по протоколу HTTP и состоит из набора методов запросов/действий по реагированию. Другими словами, решением Kaspersky Managed Detection and Response можно управлять с помощью стороннего решения, а не только через консоль MDR.

Чтобы начать работу с REST API, необходимо создать токен обновления и токен доступа.

ОТКРЫТЬ СПРАВКУ ПО REST API

Сценарий: авторизация на основе токенов

В этом сценарии описано, как выполнить авторизацию на основе токенов для работы с REST API.

Предварительные требования

Убедитесь, что у вас есть учетная запись MDR, которой назначена одна из следующих ролей.

- Роль Администратор MDR.
- Настраиваемая роль со следующими правами доступа (применимо только для Kaspersky Security Center):
  - Доступ к инцидентам
  - Доступ к REST API

Шаги

Авторизация на основе токенов состоит из следующих шагов:

1. **Создание токена обновления в Консоли MDR**

   Токен обновления необходим для создания токена доступа. Токен обновления действителен в течение 24 часов. Токен обновления можно использовать только один раз.

2. **Создание токена доступа с помощью REST API**

Токен доступа необходим для работы с REST API. Токен доступа действителен в течение 1 часа. Токен доступа можно использовать несколько раз в течение срока его действия.

При создании токена доступа REST API формирует новый токен обновления и добавляет его в действие по реагированию. После истечении срока действия токена доступа можно создать новый токен доступа с использованием последнего токена обновления, сформированного с помощью API.

Токен обновления, сформированный с помощью API, действителен в течение 7 дней.

Результаты

По завершении этого сценария вы сможете начать работу с REST API, отправляя запросы с токеном доступа.

Создание API-подключения в Kaspersky Security Center

Развернуть все | Свернуть все

При создании нового API-подключения формируется токен обновления. *Токен обновления* – это уникальная последовательность букв, цифр и символов. После создания токен обновления позволяет создать токен доступа.

Чтобы создать API-подключение:

1. В разделе **MDR** в Kaspersky Security Center перейдите на вкладку **API**.

   Появится список **API-подключения**.

2. В верхней части окна нажмите на значок плюс (+).

   Появится раздел **Добавить новое API-подключение**.

3. Укажите следующие параметры:

   - **Название подключения**

     Название подключения может содержать латинские буквы, цифры и специальные символы. Название подключения указывается как `author_name` в реагированиях REST API и отображается как имя автора комментария на вкладке **Обсуждение** для инцидента.

   - **Права доступа**

     Выберите, какие права доступа необходимо предоставить для выполнения действий через HTTP API:

     - **Полный доступ + API и тенанты**

       Права доступа роли Администратора MDR. Администратор MDR – это суперпользователь, имеющий доступ ко всем функциям Kaspersky Managed Detection and Response, предоставляемым в рамках лицензии. Администратор MDR может предоставить доступ к источникам данных клиентов другим пользователям. При активации Kaspersky Managed Detection and Response вы автоматически становитесь администратором MDR, поэтому для активации рекомендуется использовать корпоративный адрес электронной почты вместо личного. Создание администратора MDR с использованием личного адреса электронной почты может создать угрозу безопасности, например, кражу учетной записи администратора MDR.

       В Kaspersky Security Center этой роли соответствуют следующие права доступа:

Функциональная область	Разрешать	Запретить
Доступ к инцидентам	✓	—
Параметры автоподтверждения	✓	—
Управление действиями по реагированию	✓	—
Управление тенантами	✓	—
Сводная информация по инцидентам	✓	—
Доступ к REST API	✓	—

     - **Доступ к инцидентам, управлению действиями по реагированию и параметрам автоподтверждения**

       Права доступа для роли Старший специалист по безопасности. Старший специалист по безопасности – это сотрудник, имеющий доступ к функциям Kaspersky Managed Detection and Response, предоставляемым в рамках лицензии, но не имеющий доступа к REST API. Старший специалист по безопасности имеет право принимать и отклонять действия по реагированию.

       В Kaspersky Security Center этой роли соответствуют следующие права доступа:

Функциональная область	Разрешать	Запретить
Доступ к инцидентам	✓	—

Параметры автоподтверждения	✓	—
Управление действиями по реагированию	✓	—
Управление тенантами	—	✓
Сводная информация по инцидентам	—	✓
Доступ к REST API	—	✓

- **Доступ к инцидентам**

Права доступа для роли Специалист по безопасности. Специалист по безопасности – это сотрудник, имеющий доступ к функциям Kaspersky Managed Detection and Response, предоставляемым в рамках лицензии, но не имеющий доступа к REST API. Специалист по безопасности не имеет права принимать и отклонять действия по реагированию.

В Kaspersky Security Center этой роли соответствуют следующие права доступа:

Функциональная область	Разрешать	Запретить
Доступ к инцидентам	✓	—
Параметры автоподтверждения	—	✓
Управление действиями по реагированию	—	✓
Управление тенантами	—	✓
Сводная информация по инцидентам	—	✓
Доступ к REST API	—	✓

- **Тенант**

  При необходимости выберите одно или несколько значений в раскрывающемся списке **Тенант**.

  Пользователь может просматривать только активы и инциденты, связанные с указанными тенантами.

4. Нажмите на кнопку **Создать**.

   Появится поле **Токен JWT**.

5. Нажмите на кнопку **Закрыть**.

   Новое API-подключение появится в списке **API-подключения**. Теперь можно использовать токен обновления для создания токена доступа.

Вы также можете создать API-подключения в Консоли MDR.

Создание API-подключения в Консоли MDR

Развернуть все | Свернуть все

Токен обновления – это уникальная последовательность букв, цифр и символов. После создания токен обновления позволяет создать токен доступа.

Чтобы создать токен обновления:

1. В окне Консоли MDR выберите пункт меню **Параметры**.

2. Перейдите на вкладку **API**.

   Отобразится список **Все токены**.

3. В верхней части окна нажмите на кнопку **Добавить**.

   Отобразится раздел **Создать токен**.

4. Укажите следующие параметры:

   - **Название подключения**

     Название токена.

     Название токена может содержать латинские буквы, цифры и специальные символы. Название токена указывается как `author_name` в реагированиях REST API и отображается как имя автора комментария на вкладке **Обсуждение** для инцидента.

     Для некоторых типов коммерческой лицензии это единственное доступное поле при создании токена обновления.

- **Роль пользователя**

  Роль пользователя для указания разрешений, предоставляемых для выполнения действий через HTTP API.

  Доступны следующие роли пользователей:

  - Администратор MDR

    Суперпользователь, имеющий доступ ко всем функциям Kaspersky Managed Detection and Response, предоставляемым в рамках лицензии. Администратор MDR может предоставить доступ к источникам данных клиентов другим пользователям. При активации Kaspersky Managed Detection and Response вы автоматически становитесь администратором MDR, поэтому для активации рекомендуется использовать корпоративный адрес электронной почты вместо личного. Создание учетной записи администратора MDR с использованием личного адреса электронной почты может создать угрозу безопасности, например, кражу учетной записи администратора MDR.

    В Kaspersky Security Center этой роли соответствуют следующие права доступа:

Функциональная область	Разрешать	Запретить
Доступ к инцидентам	✓	—
Параметры автоподтверждения	✓	—
Управление действиями по реагированию	✓	—
Управление тенантами	✓	—
Сводная информация по инцидентам	✓	—
Доступ к REST API	✓	—

  - Старший специалист по безопасности.

    Сотрудник, имеющий доступ к функциям Kaspersky Managed Detection and Response, предоставляемым в рамках лицензии, но не имеющий доступа к REST API. Старший специалист по безопасности имеет право принимать и отклонять действия по реагированию.

    В Kaspersky Security Center этой роли соответствуют следующие права доступа:

Функциональная область	Разрешать	Запретить
Доступ к инцидентам	✓	—
Параметры автоподтверждения	✓	—
Управление действиями по реагированию	✓	—
Управление тенантами	—	✓
Сводная информация по инцидентам	—	✓
Доступ к REST API	—	✓

  - Специалист по безопасности.

    Сотрудник, имеющий доступ к функциям Kaspersky Managed Detection and Response, предоставляемым в рамках лицензии, но не имеющий доступа к REST API. Специалист по безопасности не имеет права принимать и отклонять действия по реагированию.

    В Kaspersky Security Center этой роли соответствуют следующие права доступа:

Функциональная область	Разрешать	Запретить
Доступ к инцидентам	✓	—
Параметры автоподтверждения	—	✓
Управление действиями по реагированию	—	✓
Управление тенантами	—	✓
Сводная информация по инцидентам	—	✓
Доступ к REST API	—	✓

- **Тенант**

При необходимости выберите одно или несколько значений в раскрывающемся списке **Тенант**.

В Консоли можно выбрать существующие тенанты или значение **Не имеет тенантов**.

Пользователь может просматривать только активы и инциденты, связанные с указанными тенантами. Пользователь может просмотреть активы и инциденты, не назначенные ни одному тенанту, если выбрано значение **Не имеет тенантов**.

Наряду с выбором значения **Не имеет тенантов** можно указать названия тенантов.

5. В нижней части раздела нажмите на кнопку **Создать**.

   Раздел **Создать токен** будет заменен на раздел **Данные токена**.

6. Нажмите на кнопку **Закрыть** в нижней части раздела **Данные токена**.

   Созданный токен обновления появится в списке **Все токены**. Теперь можно использовать этот токен обновления для создания токена доступа.

Изменение API-подключения в Kaspersky Security Center

Вы можете изменять существующие API-подключения.

Чтобы изменить API-подключение:

1. В разделе **MDR** в Kaspersky Security Center перейдите на вкладку **API**.

   Появится список **API-подключения**.

2. Выберите API-подключение, которое вы хотите изменить.

   Появится раздел, содержащий информацию о подключении.

3. Измените параметры подключения.

4. Нажмите на кнопку **Сохранить**.

Новые параметры выбранного API-подключения будут сохранены.

Изменение API-подключения в Консоли MDR

Вы можете изменять существующие API-подключения.

Чтобы изменить API-подключение:

1. В Консоли MDR перейдите на вкладку **API**.

   Отобразится список **Все токены**.

2. Выберите токен API-подключения, который вы хотите изменить.

   Появится раздел, содержащий информацию о подключении.

3. Измените параметры подключения.

4. Нажмите на кнопку **Сохранить**.

Новые параметры выбранного API-подключения будут сохранены.

Создание токена доступа в Kaspersky Security Center

Токен доступа – это уникальная последовательность символов (букв, цифр и символов), позволяющая использовать методы REST API.

Чтобы создать токен доступа:

1. В разделе **MDR** в Kaspersky Security Center перейдите на вкладку **API**.

   Появится список **API-подключения**.

2. Выберите подключение со статусом **Ожидает активации**.

   Появится раздел, содержащий информацию о подключении.

3. В поле **Токен JWT** нажмите на кнопку **Обновить**.

   Отобразится токен обновления.

4. Выделите и сохраните значение поля **Идентификатор клиента**.

5. Выделите и скопируйте последовательность символов токена в буфер обмена.

6. Отправьте запрос POST на конечную точку `/session/confirm`.

Замените {client_id} и {refresh_token} значениями, выбранными и сохраненными на предыдущих шагах.

Пример (Python):

```
#####################################################
# Общая часть
#####################################################

import time
import datetime
import requests
import jwt

# Сертификат необходим для аутентификации внешнего ресурса.
# Вы можете скачать сертификат с https://mdr.kaspersky.com.
# Сохраните сертификат на свой диск и добавьте путь к сертификату в переменной:
VERIFY_CERT_PATH = "C:\\tools\\DigiCert Global Root G2.crt"

# MDR REST API URL:
API_URL = "https://mdr.kaspersky.com/api/v1"

# Ваш идентификатор клиента и ваши токены.
# Подробнее о получении идентификатора и токенов см. в справке https://support.kaspersky.com/MDR/ru-RU/258285.htm.
CLIENT_ID = "9ed43ed54sAmpleIdf349323951f" # (Вставьте ваше значение)
REFRESH_TOKEN = "ReFrEsHToKeN"  # (Вставьте ваше значение)
ACCESS_TOKEN = "AcCeSsToKeN"  # (Вставьте ваше значение)


#####################################################
# Получение токена доступа и токена обновления для следующего обновления токена доступа
#####################################################

if REFRESH_TOKEN:
    refresh_token_exp = jwt.decode(REFRESH_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"REFRESH_TOKEN дата и время истечения срока действия :
{datetime.datetime.fromtimestamp(refresh_token_exp)}")
    if refresh_token_exp > time.time():
        print("REFRESH_TOKEN действительный ")
    else:
        print(
            " Вам нужно обновить REFRESH_TOKEN . Возьмите его из Консоли MDR (https://support.kaspersky.com/MDR/ru-
RU/258285.htm). "
        )
        exit()
else:
    print(
        " Вам нужно заполнить значение REFRESH_TOKEN. Возьмите его из Консоли MDR
(https://support.kaspersky.com/MDR/ru-RU/258285.htm). "
    )
    exit()

# Проверьте наличие и срок действия токена доступа.
need_update_access_token = False
if ACCESS_TOKEN:
    access_token_exp = jwt.decode(ACCESS_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"ACCESS_TOKEN дата и время истечения срока действия:
{datetime.datetime.fromtimestamp(access_token_exp)}")
    if access_token_exp > time.time():
        print("ACCESS_TOKEN действительный ")
    else:
        need_update_access_token = True
else:
    need_update_access_token = True

# При необходимости обновите токен доступа и токен обновления для следующего обновления токена доступа.
access_token = ACCESS_TOKEN
if need_update_access_token:
    request_body = {"refresh_token": REFRESH_TOKEN}
    result = requests.post(url=f"{API_URL}/{CLIENT_ID}/session/confirm", json=request_body,
verify=VERIFY_CERT_PATH)
    result_json = result.json()

    if "error" in result_json:
        print(result_json)
        exit()
```

```
    # Необходимо сохранить токен обновления, чтобы получить следующий токен доступа после истечения срока действия
текущего токена доступа
    refresh_token = result_json["refresh_token"]
    print(
        f' !!! Ваш новый REFRESH_TOKEN для следующего запроса ACCESS_TOKEN (замените значение REFRESH_TOKEN
значением) : "{refresh_token}"'
    )

    # Требуется новый токен доступа для получения данных
    access_token = result_json["access_token"]
    print(f' !!! Ваш новый ACCESS_TOKEN (замените значение ACCESS_TOKEN значением): "{access_token}"')

# Токен доступа добавлен в заголовок запроса.
headers = {"Authorization": f"Bearer {access_token}"}
```

Пример (Shell):

```
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/session/confirm -H "Content-Type: application/json" -d
'{"refresh_token": "{refresh_token}"}'
```

REST API отправляет действие по реагированию с токеном доступа и новым токеном обновления:

```
{
"access_token": "SamPLET346yoKEnSamPLEToK25EnSamPLEToK35EnS",
"refresh_token": "tOKenSaMPlet259OKenS123aMPle926tOKenSaMPle"
}
```

Теперь можно отправлять запросы в REST API, используя токен доступа. Для каждого запроса к REST API требуется токен доступа; в ответ на запрос без токена доступа возвращается только ошибка авторизации.

Вы также можете создать токен доступа в Консоли MDR.

Создание токена доступа в Консоли MDR

Чтобы создать токен доступа:

1. В окне Консоли MDR выберите пункт меню **Параметры**.
2. Перейдите на вкладку **API**.

   Отобразится список **Все токены**. Каждая строка соответствует одному токену. Можно щелкнуть в любом месте строки, чтобы посмотреть информацию о токене.
3. Выберите токен со статусом **Ожидает активации**.

   Отобразится раздел **Данные токена**.
4. В поле **Токен JWT** нажмите на кнопку **Обновить**.

   Отобразится токен обновления.
5. Выделите и сохраните значение поля **Идентификатор клиента**.
6. Выделите и скопируйте последовательность символов токена в буфер обмена.
7. Отправьте запрос POST на конечную точку `/session/confirm` (см. пример ниже).

   Замените `{client_id}` и `{refresh_token}` значениями, выбранными и сохраненными на предыдущих шагах.

Пример (Python):

```
#####################################################
# Общая часть
#####################################################

import time
import datetime
import requests
import jwt

# Сертификат необходим для аутентификации внешнего ресурса.
# Вы можете скачать сертификат с https://mdr.kaspersky.com.
# Сохраните сертификат на свой диск и добавьте путь к сертификату в переменной:
```

```
VERIFY_CERT_PATH = "C:\\tools\\DigiCert Global Root G2.crt"

# MDR REST API URL:
API_URL = "https://mdr.kaspersky.com/api/v1"

# Ваш идентификатор клиента и ваши токены.
# Подробнее о получении идентификатора и токенов см. в справке https://support.kaspersky.com/MDR/ru-RU/258285.htm.
CLIENT_ID = "9ed43ed54sAmpleIdf349323951f" # (Вставьте ваше значение)
REFRESH_TOKEN = "ReFrEsHToKeN"  # (Вставьте ваше значение)
ACCESS_TOKEN = "AcCeSsToKeN"  # (Вставьте ваше значение)


#####################################################
# Получение токена доступа и токена обновления для следующего обновления токена доступа
#####################################################

if REFRESH_TOKEN:
    refresh_token_exp = jwt.decode(REFRESH_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"REFRESH_TOKEN дата и время истечения срока действия:
{datetime.datetime.fromtimestamp(refresh_token_exp)}")
    if refresh_token_exp > time.time():
        print("REFRESH_TOKEN действительный")
    else:
        print(
            "Вам нужно обновить REFRESH_TOKEN. Возьмите его из Консоли MDR (https://support.kaspersky.com/MDR/ru-
RU/258285.htm)."
        )
        exit()
else:
    print(
        "Вам нужно заполнить значение REFRESH_TOKEN. Возьмите его из Консоли MDR
(https://support.kaspersky.com/MDR/ru-RU/258285.htm)."
    )
    exit()

# Проверьте наличие и срок действия токена доступа.
need_update_access_token = False
if ACCESS_TOKEN:
    access_token_exp = jwt.decode(ACCESS_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"ACCESS_TOKEN дата и время истечения срока действия:
{datetime.datetime.fromtimestamp(access_token_exp)}")
    if access_token_exp > time.time():
        print("ACCESS_TOKEN действительный")
    else:
        need_update_access_token = True
else:
    need_update_access_token = True

# При необходимости обновите токен доступа и токен обновления для следующего обновления токена доступа.
access_token = ACCESS_TOKEN
if need_update_access_token:
    request_body = {"refresh_token": REFRESH_TOKEN}
    result = requests.post(url=f"{API_URL}/{CLIENT_ID}/session/confirm", json=request_body,
verify=VERIFY_CERT_PATH)
    result_json = result.json()

    if "error" in result_json:
        print(result_json)
        exit()

    # Необходимо сохранить токен обновления, чтобы получить следующий токен доступа после истечения срока действия
текущего токена доступа
    refresh_token = result_json["refresh_token"]
    print(
        f'!!! Ваш новый REFRESH_TOKEN для следующего запроса ACCESS_TOKEN (замените значение REFRESH_TOKEN
значением): "{refresh_token}"'
    )

    # Требуется новый токен доступа для получения данных
    access_token = result_json["access_token"]
    print(f'!!! Ваш новый ACCESS_TOKEN (замените значение ACCESS_TOKEN значением): "{access_token}"')

# Токен доступа добавлен в заголовок запроса.
headers = {"Authorization": f"Bearer {access_token}"}
```

Пример (Shell):

```
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/session/confirm -H "Content-Type: application/json" -d
'{"refresh_token": "{refresh_token}"}'
```

REST API отправляет действие по реагированию с токеном доступа и новым токеном обновления:

```
{
"access_token": "SamPLET346yoKEnSamPLEToK25EnSamPLEToK35EnS",
"refresh_token": "tOKenSaMPlet259OKenS123aMPle926tOKenSaMPle"
}
```

Теперь можно отправлять запросы в REST API, используя токен доступа. Для каждого запроса к REST API требуется токен доступа; в ответ на запрос без токена доступа возвращается только ошибка авторизации.

Работа с REST API

Работа с MDR с помощью REST API включает получение, создание и обновление активов, инцидентов, действий по реагированию и пользователей.

ОТКРЫТЬ СПРАВКУ ПО REST API

Для методов REST API требуется значение `client_id`. Вы можете получить значение `client_id` в разделе **Информации о токене** любого токена обновления в Консоли MDR.

Ниже приведены примеры скриптов для Python и Shell, демонстрирующие основные возможности REST API:

- Определение пути к сертификату, веб-адреса REST API, идентификатора клиента и токенов.
- Получение токена доступа и токена обновления для следующего обновления токена доступа.
- Получение номера актива.
- Получение списка активов или подробной информации об активах.
- Получение количества инцидентов, списка инцидентов или деталей инцидента.
- Получение списка действий по реагированию на инцидент.
- Подтверждение и отклонение действий по реагированию или обновление списка действий по реагированию.
- Получение списка комментариев для указанного инцидента или создание комментария для указанного инцидента.

Пример (Python):

```
#####################################################
# Общая часть
#####################################################

import time
import datetime
import requests
import jwt

# Сертификат необходим для аутентификации внешнего ресурса.
# Вы можете скачать сертификат с https://mdr.kaspersky.com.
# Сохраните сертификат на свой диск и добавьте путь к сертификату в переменной:
VERIFY_CERT_PATH = "C:\\tools\\DigiCert Global Root G2.crt"

# веб-адрес MDR REST API:
API_URL = "https://mdr.kaspersky.com/api/v1"

# Ваш идентификатор клиента и ваши токены.
# Подробнее о получении идентификатора и токенов см. в справке https://support.kaspersky.com/MDR/ru-RU/258285.htm.
CLIENT_ID = "9ed43ed54sAmpleIdf349323951f"  # ( Вставьте ваше значение )
REFRESH_TOKEN = "ReFrEsHToKeN"  # ( Вставьте ваше значение )
ACCESS_TOKEN = "AcCeSsToKeN"  # ( Вставьте ваше значение )


#####################################################
# Получение токена доступа и токена обновления для следующего обновления токена доступа
#####################################################
```

```
if REFRESH_TOKEN:
    refresh_token_exp = jwt.decode(REFRESH_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"REFRESH_TOKEN дата и время истечения срока действия:
{datetime.datetime.fromtimestamp(refresh_token_exp)}")
    if refresh_token_exp > time.time():
        print("REFRESH_TOKEN действительный ")
    else:
        print(
            " Вам нужно обновить REFRESH_TOKEN . Возьмите его из Консоли MDR (https://support.kaspersky.com/MDR/ru-
RU/258285.htm). "
        )
        exit()
else:
    print(
        " Вам нужно заполнить значение REFRESH_TOKEN value. Возьмите его из Консоли MDR
(https://support.kaspersky.com/MDR/ru-RU/258285.htm). "
    )
    exit()

# Проверьте наличие и срок действия токена доступа.
need_update_access_token = False
if ACCESS_TOKEN:
    access_token_exp = jwt.decode(ACCESS_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"ACCESS_TOKEN дата и время истечения срока действия:
{datetime.datetime.fromtimestamp(access_token_exp)}")
    if access_token_exp > time.time():
        print("ACCESS_TOKEN действительный ")
    else:
        need_update_access_token = True
else:
    need_update_access_token = True

# При необходимости обновите токен доступа и токен обновления для следующего обновления токена доступа.
access_token = ACCESS_TOKEN
if need_update_access_token:
    request_body = {"refresh_token": REFRESH_TOKEN}
    result = requests.post(url=f"{API_URL}/{CLIENT_ID}/session/confirm", json=request_body,
verify=VERIFY_CERT_PATH)
    result_json = result.json()

    if "error" in result_json:
        print(result_json)
        exit()

    # Необходимо сохранить токен обновления, чтобы получить следующий токен доступа после истечения срока действия
текущего токена доступа
    refresh_token = result_json["refresh_token"]
    print(
        f'!!! Ваш новый REFRESH_TOKEN для следующего запроса ACCESS_TOKEN (замените значение REFRESH_TOKEN
значением) : "{refresh_token}"'
    )

    # Требуется новый токен доступа для получения данных
    access_token = result_json["access_token"]
    print(f'!!! Ваш новый ACCESS_TOKEN (замените значение ACCESS_TOKEN значением): "{access_token}"')

# Токен доступа добавлен в заголовок запроса.
headers = {"Authorization": f"Bearer {access_token}"}


#####################################################
# Получить количество активов
#####################################################

# Дата и время в миллисекундах с 1970-01-01T00:00:00Z
request_body = {
    "max_last_seen": int(time.time())
    * 1000,  # Ограничение максимального времени последнего появления актива от текущего временем
    "min_last_seen": 1639311132000,  # Ограничение минимального времени последнего появления актива с константой –
воскресенье, 12 декабря 2021 г, 12:12:12 (GMT)
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/assets/count", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())
```

```
#####################################################
# Получить список активов
#####################################################

request_body = {
    # Параметры поиска:
    "max_last_seen": int(time.time())
    * 1000,  # Ограничение максимального времени последнего появления актива от текущего временем
    "min_last_seen": 1639311132000,  # Ограничение минимального времени последнего появления актива с константой –
воскресенье, 12 декабря 2021 г, 12:12:12 (GMT)
    "domain": "",
    "host_names": ["MA-MDR-KES-S", "SIN-MDR-KSC"],  # (Вставьте ваше значение) Список имен устройств
    "is_isolated": False,
    "network_interface": "10.70.104.1",
    "os_version": "Windows",  # Актив должен содержать указанную строку в названии операционной системы
    "product": "",
    "search_phrase": "mdr",  # Фраза для поиска по содержимому поля: "host_name", "domain",
"installed_product_info", "network_interfaces", "os_version"
    "statuses": ["OK", "ABSENT"],  # Поиск объектов с текущими перечисленными статусами
    # Варианты отображения результатов поиска:
    "sort": "first_seen:asc",  # Сортировка результатов по времени первого появления. В случае постраничного
получения результатов необходимо указать поле для сортировки, которое не будет меняться от запроса к запросу,
например "first_seen" (не указывайте поля, значения которых постоянно меняются, например поле "last_seen"; это
может привести к неверным результатам).
    "page_size": 100,  # Активов на странице – 100
    "page": 1,  # Получить первую страницу результатов поиска
    "version": 2,  # Версия решения
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/assets/list", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())


#####################################################
# Получить информацию об активе
#####################################################

request_body = {
    "asset_id": "0xFA6A68CC9A9415963DE841048A3BE929",  # (Вставьте ваше значение) Идентификатор актива
    "version": 2,  # Версия решения
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/assets/details", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
).json()
print(result)


#####################################################
# Получить количество инцидентов
#####################################################

request_body = {
    "max_update_time": int(time.time())
    * 1000,  # Ограничить максимальное время последнего обновления инцидента текущим временем
    "min_update_time": 1639311132000,  # Ограничение минимального времени для последнего обновления инцидента
константой – воскресенье, 12 декабря 2021 г, 12:12:12 PM (GMT)
    "affected_hosts": [
        "MA-MDR-KES-S:0xFA6A68CC9A94145456E841048A3BE929"
    ],  # (Вставьте ваше значение) Список устройств в формате "host_name:asset_id" format
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/incidents/count", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())


#####################################################
# Получить список инцидентов
#####################################################

request_body = {
    # Параметры поиска:
    "max_creation_time": int(time.time())
    * 1000,  # Ограничить максимальное время создания инцидента текущим временем
    "min_creation_time": 1639311132000,  # Ограничение минимального времени создания инцидента константой –
воскресенье, 12 декабря 2021 г, 12:12:12 PM (GMT)
    "asset_ids": [
```

```
        "0xFA6A68CC9A9415963DE841048A3BE929"
    ],  # (Вставьте ваше значение) Список активов, для которых получаем инциденты
    "priorities": ["HIGH"],
    "resolutions": ["True positive"],
    "response_statuses": ["Confirmed"],
    "response_types": ["hash"],
    "statuses": ["Closed"],
    # Параметры для предоставления результатов
    "markdown_to_html": True,  # Результаты в формате HTML. Если значение равно "False", результаты имеют формат
Markdown.
    "sort": "creation_time:asc",  # Сортировать результаты по дате и времени создания инцидента. В случае
постраничного получения результатов необходимо указать поле для сортировки, которое не будет меняться от запроса к
запросу, например creation_time (не указывайте поля, значения которых постоянно меняются, например поле
"update_time"; это может привести к неверным результатам).
    "page_size": 100,  # Инцидентов на странице – 100
    "page": 1,  # Получить первую страницу результатов поиска
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/incidents/list", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())


#####################################################
# Получить детали инцидента
#####################################################

request_body = {
    "incident_id": "60gWG4UBMUGN-LWUuv1m",  # Вставьте ваше значение) Идентификатор инцидента
    "markdown_to_html": True,  # Результаты в формате HTML. Если значение равно "False", результаты имеют формат
Markdown.
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/incidents/details", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())


#####################################################
# Получить список действий по реагированию на инцидент
#####################################################

request_body = {
    "incident_id": "60gWG4UBMUGN-LWUuv1m",  # Вставьте ваше значение) Идентификатор инцидента
    "page_size": 10,  # Действий по реагированию на странице – 10
    "page": 1,  # Получить первую страницу результатов поиска
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/responses/list", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())


#####################################################
# Подтвердите действие по реагированию
#####################################################

request_body = {
    "response_id": "CEgYG4UBMUGN-LWULP7W",  # (Вставьте ваше значение) Идентификатор действия по реагированию
    "comment": "comment_text",  # Комментарий, который нужно добавить к действию по реагированию
    "status": "Confirmed",  # Новый статус действия по реагированию – "Confirmed"
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/response/update", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())


#####################################################
# Отклонить действие по реагированию
#####################################################

request_body = {
    "response_id": "CEgYG4UBMUGN-LWULP7W",  # (Вставьте ваше значение) Идентификатор действия по реагированию
    "comment": "comment_text",  # Комментарий, который нужно добавить к действию по реагированию
    "status": "Declined",  # Новый статус действия по реагированию – "Declined"
}
result = requests.post(
```

```
    url=f"{API_URL}/{CLIENT_ID}/response/update", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())


##################################################
# Обновить список действий по реагированию
##################################################

request_body = {
    "responses_ids": [
        "CEgYG4UBMUGN-LWULP7W",
        "2ESl6IgB4cAOUyXBb5IB",
    ],  # (Вставьте ваше значение) Идентификаторы действий по реагированию
    "comment": "comment_text",  # Комментарий, который нужно добавить к реагированию
    "status": "Confirmed",  # Новый статус действий по реагированию – "Confirmed"
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/responses/update", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())
```

Пример (Shell):

```
# Получение токена доступа и нового токена обновления
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/session/confirm -H "Content-Type: application/json" -d
'{"refresh_token": "{refresh_token}"}'
# Пример ответа. Далее вам нужно использовать access_token для получения данных и refresh_token для получения
нового токена доступа и токена обновления.
{
"access_token": "SamPLET346yoKEnSamPLEToK25EnSamPLEToK35EnS",
"refresh_token": "tOKenSaMPlet259OKenS123aMPle926tOKenSaMPle"
}

# Получить количество активов
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/assets/count -H "Content-Type: application/json" -H
"Authorization: Bearer {access_token}" -d '{"max_last_seen": 1704103200000, "min_last_seen": 1704762000000}'

# Получить список активов
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/assets/list -H "Content-Type: application/json" -H
"Authorization: Bearer {access_token}" -d '{"max_last_seen": 1704103200000, "min_last_seen": 1704762000000,
"domain": "", "host_names": ["MA-MDR-KES-S","SIN-MDR-KSC"], "is_isolated": false, "network_interface":
"10.70.104.1", "os_version": "Windows", "product": "", "search_phrase": "mdr", "statuses": ["OK","ABSENT"],
"sort": "first_seen:asc", "page_size": 100, "page": 1, "version": 2}'

# Получить информацию об активе
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/assets/details -H "Content-Type: application/json" -H
"Authorization: Bearer {access_token}" -d '{"asset_id": "0xFA6A68CC9A9415963DE841048A3BE929", "version": 2}'

# Получить количество инцидентов
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/incidents/count -H "Content-Type: application/json" -H
"Authorization: Bearer {access_token}" -d '{"max_update_time": 1704103200000, "min_update_time": 1704762000000,
"affected_hosts": ["MA-MDR-KES-S:0xFA6A68CC9A9415963DE841048A3BE929"]}'

# Получить список инцидентов
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/incidents/list -H "Content-Type: application/json" -H
"Authorization: Bearer {access_token}" -d '{"max_creation_time": 1704103200000, "min_creation_time":
1704762000000, "asset_ids": ["0xFA6A68CC9A9415963DE841048A3BE929"], "priorities": ["HIGH"], "resolutions": ["True
positive"], "response_statuses": ["Confirmed"], "response_types": ["hash"], "statuses": ["Closed"],
"markdown_to_html": true, "sort": "creation_time:asc", "page_size": 100, "page": 1}'

# Получить сведения об инциденте
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/incidents/details -H "Content-Type: application/json" -H
"Authorization: Bearer {access_token}" -d '{"incident_id": "60gWG4UBMUGN-LWUuv1m", "markdown_to_html": true}'

# Получить список действий по реагированию на инцидент
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/responses/list -H "Content-Type: application/json" -H
"Authorization: Bearer {access_token}" -d '{"incident_id": "60gWG4UBMUGN-LWUuv1m", "page_size": 10, "page": 1}'

# Обновить действие по реагированию
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/response/update -H "Content-Type: application/json" -H
"Authorization: Bearer {access_token}" -d '{"response_id": "CEgYG4UBMUGN-LWULP7W", "comment": "comment_text",
"status": "Confirmed"}'

# Обновить список действий по реагированию
```

```
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/responses/update -H "Content-Type: application/json" -H
"Authorization: Bearer {access_token}" -d '{"responses_ids": ["CEgYG4UBMUGN-LWULP7W", "2ESl6IgB4cAOUyXBb5IB"],
"comment": "comment_text", "status": "Confirmed"}'
```

Пример ответа REST API с токеном доступа и новым токеном обновления:

```
{
"access_token": "SamPLET346yoKEnSamPLEToK25EnSamPLEToK35EnS",
"refresh_token": "tOKenSaMPlet259OKenS123aMPle926tOKenSaMPle"
}
```

Пример ответа REST API со структурой и значениями комментариев:

```
[{
  "comment_id": "bfu6TiNghqp",
  "author_name": "Иван Иванов",
  "text": "<p> Первый комментарий. </p>",
  "creation_time": 1601295428640
}, {
  "comment_id": "bfu6TiNghqt",
  "author_name": "Мария Ивановна",
  "text": "<p> Второй комментарий. </p>",
  "creation_time": 1601295433441
}]
```

Пример ответа REST API, если REST API создает комментарий и отправляет действие по реагированию с деталями комментария:

```
{
  "comment_id": "AXTej0Qi4bfu6TiNgmvT",
  "author_name": "Название токена",
  "text": " Это новый комментарий, созданный с помощью REST API. ",
  "creation_time": 1601461748122
}
```

Отзыв обновления токена в Kaspersky Security Center

Вы можете отозвать токены обновления из API-подключений, находящихся в состоянии *Активно* или *Простой*.

Чтобы отозвать токен обновления:

1. В разделе **MDR** в Kaspersky Security Center перейдите на вкладку **API**.

   Появится список **API-подключения**.

2. Выберите API-подключение, для которого вы хотите отозвать токен обновления.

   Появится раздел, содержащий информацию о подключении.

3. Нажмите на кнопку **Отозвать**.

Токен обновления будет отозван.

Удаление API-подключения в Kaspersky Security Center

Вы можете удалить существующие API-подключения.

Чтобы удалить API-подключение:

1. В разделе **MDR** в Kaspersky Security Center перейдите на вкладку **API**.

   Появится список **API-подключения**.

2. Наведите указатель мыши на API-подключение, которое вы хотите удалить, и щелкните по значку корзины (🗑) в правой части строки.

Выбранное API-подключение будет удалено.

Удаление API-подключения в Консоли MDR

Вы можете изменять существующие API-подключения.

Чтобы изменить API-подключение:

1. В Консоли MDR перейдите на вкладку **API**.

   Отобразится список **Все токены**.

2. Наведите указатель мыши на API-подключение, которое вы хотите удалить, и щелкните по значку корзины (🗑) в правой части строки.

Выбранное API-подключение будет удалено.

Известные проблемы

Kaspersky Managed Detection and Response имеет ряд ограничений, не критичных для работы приложения:

- Если вы клонируете виртуальный или физический актив с Kaspersky Endpoint Security для Linux, который уже подключен к решению MDR, данные телеметрии из клонированных активов передаются некорректно. Для этих клонированных активов удалите Kaspersky Endpoint Security для Linux, удалите файл install_id в папке /var/opt/kaspersky/epagent/ и переустановите Kaspersky Endpoint Security для Linux.
- Для активов с Kaspersky Endpoint Security для Windows в конфигурации Endpoint Detection and Response Agent (EDR Agent) статусы *Предупреждение* и *Критический* для компонентов защиты и управления не отображаются.
- Вы не можете использовать возможности Kaspersky Endpoint Detection and Response Optimum для активов с Kaspersky Endpoint Security для Windows в конфигурации EDR Agent.
- **Приложения "Лаборатории Касперского", которые работают с разделом MDR** карточки актива в Консоли MDR, могут содержать устаревшие EPP-программы, которые больше не используются для работы с Kaspersky Managed Detection and Response. Это происходит, когда на активе устаревшая EPP-программа заменяется новой. Для этих устаревших приложений в поле **Последнее появление** указана старая дата, а для новой EPP-программы в поле **Последнее появление** указана более новая дата.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации Kaspersky Managed Detection and Response или в других источниках информации о решении, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании решения Kaspersky Managed Detection and Response.

"Лаборатория Касперского" обеспечивает поддержку решения Kaspersky Managed Detection and Response в течение его жизненного цикла (см. таблицу поддерживаемых приложений). Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Посетить веб-сайт Службы технической поддержки
- Отправить запрос в Службу технической поддержки с портала Kaspersky CompanyAccount

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов и хранить их историю.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;

- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки.

Источники информации о решении

На странице Kaspersky Managed Detection and Response можно ознакомиться с общей информацией о решении, его функциях и особенностях.

Глоссарий

Endpoint Protection Platform (EPP)

Интегрированная система комплексной защиты конечных устройств (например, мобильных устройств, компьютеров или ноутбуков), включающая различные технологии безопасности. Примером решения Endpoint Protection Platform является Kaspersky Endpoint Security для бизнеса.

EPP-программа

Программа, входящая в состав системы защиты конечных устройств (Endpoint Protection Platform или EPP). EPP-программы устанавливаются на конечные устройства в ИТ-инфраструктуре организации (например, на мобильные устройства, компьютеры или ноутбуки). Примером EPP-программы является Kaspersky Endpoint Security для Windows в составе EPP-решения Kaspersky Endpoint Security для бизнеса.

IOC

Индикатор компрометации (англ. indicator of compromise, IOC) является свидетельством нарушения системы безопасности на устройстве.

Актив

Устройство с установленной EPP-программой от "Лаборатории Касперского" (например, Kaspersky Endpoint Security для Windows).

Действие по реагированию

Действие по реагированию на инцидент – это структурированная методология обработки инцидентов и нарушений системы безопасности и киберугроз.

Инцидент

Действие, оцениваемое технологией обнаружения как критическое и требующее немедленной реакции со стороны Kaspersky Managed Detection and Response.

Тактика MITRE

Цель, которую хотел достичь злоумышленник во время кибератаки на инфраструктуру клиента.

Телеметрия

Данные, отправляемые с активов в Kaspersky Managed Detection and Response.

Тенант

Тенант – это организация, которой предоставляется решение Kaspersky Managed Detection and Response.

Техника MITRE

Метод, используемый злоумышленником для выполнения вредоносных действий во время кибератаки на инфраструктуру клиента. Каждая тактика MITRE содержит набор техник MITRE.

Информация о стороннем коде

При разработке решения использовался сторонний код.

Для получения информации о стороннем коде, используемом в консоли Kaspersky Managed Detection and Response, обратитесь в службу поддержки Kaspersky Managed Detection and Response.

Информация о стороннем коде, используемом в плагине MDR, содержится в файле legal_notices.txt.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Apple, Mac, macOS и Safari – товарные знаки Apple Inc.

Amazon AWS, Amazon Web Services являются товарными знаками Amazon.com, Inc. или аффилированных лиц компании.

Active Directory, Internet Explorer, Microsoft, Microsoft Edge, Outlook, PowerShell, Windows PowerShell, Windows и Windows Server – являются товарными знаками группы компаний Microsoft.

Mozilla и Firefox – товарные знаки Mozilla Foundation, зарегистрированные в США и других странах.

Google, Google Chrome – товарные знаки Google LLC.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

Настройка параметров аудита для работы с Kaspersky Managed Detection and Response

Развернуть все | Свернуть все

Для стабильной работы и максимальной эффективности Kaspersky Managed Detection and Response рекомендуется настроить параметры аудита следующим образом:

- **Настройка политики аудита событий Windows**

Чтобы повысить эффективность работы Kaspersky Managed Detection and Response, необходимо настроить политику аудита событий Windows на активах.

Чтобы настроить политику аудита событий Windows:

1. В Windows нажмите сочетание клавиш **Win+R**, чтобы открыть окно **Выполнить**.
2. В поле **Открыть** введите `gpedit.msc,` и нажмите на клавишу **Enter** или на кнопку **OK**. Откроется окно **Редактор локальной групповой политики**.
3. В дереве консоли выберите **Конфигурация компьютера** → **Конфигурация Windows** → **Параметры безопасности** → **Конфигурация расширенной политики аудита** → **Политики аудита системы – Объект локальной групповой политики**.
4. Выберите узел **Вход в учетные записи.** В правой части окна укажите следующие значения:

Подкатегория	События аудита
Аудит проверки учетных данных	Успех и Отказ
Аудит службы аутентификации Kerberos	Успех и Отказ
Аудит операций с билетами службы Kerberos	Успех и Отказ

5. Выберите узел **Управление учетными записями.** В правой части окна укажите следующие значения:

Подкатегория	События аудита
Аудит управления учетными записями компьютеров	Успех и Отказ
Аудит управления группами безопасности	Успех
Аудит управления учетными записями пользователей	Успех и Отказ

6. Выберите узел **Доступ к службе каталогов (DS)**. В правой части окна укажите следующие значения:

Подкатегория	События аудита
Аудит доступа к службе каталогов	Успех и Отказ
Аудит изменений службы каталогов	Успех и Отказ

7. Выберите узел **Вход/выход**. В правой части окна укажите следующие значения:

Подкатегория	События аудита
Аудит блокировки учетных записей	Ошибка
Аудит входа в систему	Успех и Отказ
Аудит специального входа в систему	Успех и Отказ

8. Выберите узел **Доступ к объектам**. В правой части окна укажите следующие значения:

Подкатегория	События аудита
Аудит служб по сертификации	Успех и Отказ
Аудит общих папок	Успех
Аудит подключения платформы фильтрации	Успех

Аудит других событий доступа к объектам	Успех

9. Выберите узел **Изменение политики**. В правой части окна укажите следующие значения:

Подкатегория	События аудита
Аудит изменения политики	Успех
Аудит изменения политики на уровне правил MPSSVC	Успех

10. Выберите узел **Использование прав**. В правой части окна укажите следующее значение:

Подкатегория	События аудита
Аудит использования прав, затрагивающих конфиденциальные данные	Успех

11. Выберите узел **Система**. В правой части окна укажите следующие значения:

Подкатегория	События аудита
Аудит изменения состояния безопасности	Успех
Аудит расширения системы безопасности	Успех

12. В дереве консоли выберите **Конфигурация компьютера** → **Административные шаблоны** → **Компоненты Windows** → **Windows PowerShell**. В правой части окна укажите следующее значение:

Подкатегория	События аудита
Включить регистрацию блоков сценариев PowerShell	Включено

13. Закройте окно **Редактор локальной групповой политики**.

    Все изменения сохранятся автоматически.

Будет настроена политика аудита событий Windows для работы с Kaspersky Managed Detection and Response.

- Настройка аудита объектов Active Directory

Чтобы повысить эффективность работы Kaspersky Managed Detection and Response, необходимо настроить параметры аудита на контроллерах доменов Windows.

Чтобы настроить аудит для объектов Active Directory:

1. В контроллере домена Windows нажмите сочетание клавиш **Win+R**, чтобы открыть окно **Выполнить**.
2. В поле **Открыть** введите `dsa.msc` и нажмите на клавишу **Enter** или на кнопку **OK**. Откроется окно **Пользователи и компьютеры Active Directory**.
3. В дереве консоли нажмите правой кнопкой мыши в поле <доменное имя> и выберите **Найти**. Откроется окно **Поиск пользователей, контактов и групп**.
4. Введите **Администратор** в поле **Имя** и нажмите на кнопку **Найти**.
5. В области **Результаты поиска** нажмите правой кнопкой мыши объект **Администратор** и выберите **Свойства** → **Безопасность** → **Дополнительно** и перейдите на вкладку **Аудит**.
6. Нажмите на кнопку **Добавить**, чтобы открыть окно **Аудит для администратора**. Нажмите на кнопку **Выбрать участника**, введите `Все`, нажмите на кнопку **Проверить имена** и **OK**.
7. В окне **Аудит записи для администратора** установите флажки **Список содержимого**, **Чтение разрешений**, **Смена разрешений**, **Смена владельца**, **Чтение всех свойств** и **Запись всех свойств**.
8. Нажмите **OK** → **Применить** → **OK**.

   Аудит для объекта **Администратора** Active Directory теперь настроен для использования с Kaspersky Managed Detection and Response.
9. Выполните те же действия для следующих используемых по умолчанию объектов Active Directory, а также для важных пользователей и групп домена, которые существуют и включены в вашей системе:

- **Администраторы**
- **Группа с разрешением репликации паролей RODC**
- **Издатели сертификатов**

- **Клонируемые контроллеры домена**
- **Запрещенная группа репликации паролей RODC**
- **DnsAdmins**
- **DnsUpdateProxy**
- **Администраторы домена**
- **Компьютеры домена**
- **Контроллеры домена**
- **Администраторы предприятия**
- **Администраторы ключей предприятия**
- **Корпоративные контроллеры домена только для чтения**
- **Владельцы и создатели групповой политики**
- **Администраторы ключей**
- **krbtgt**
- **Защищенные пользователи**
- **Серверы RAS и IAS**
- **Контроллеры домена только для чтения**
- **Администраторы схемы**

- Настройка аудита служб сертификации Active Directory, шаблонов сертификатов и объектов сертификатов

Чтобы повысить эффективность Kaspersky Managed Detection and Response, необходимо настроить параметры аудита **служб сертификации Active Directory**, шаблонов и объектов сертификатов на узлах с включенными **службами сертификации Active Directory**.

*Чтобы настроить аудит **служб сертификации Active Directory**:*

1. Нажмите сочетание клавиш **Win+R**, чтобы открыть окно **Выполнить**.
2. В поле **Открыть** введите `cmd` и нажмите клавишу **Enter** или кнопку **OK**. Откроется окно **командной строки**.
3. Чтобы настроить параметры аудита центра сертификации, введите следующие команды и нажмите Enter:
   ```
   certutil -setreg CA\AuditFilter 127
   certutil -setreg policy\EditFlags +EDITF_AUDITCERTTEMPLATELOAD
   ```
4. Чтобы перезапустить **службу сертификации**, введите следующую команду и нажмите Enter:
   ```
   net stop certsvc && net start certsvc
   ```

Чтобы настроить аудит безопасности для шаблонов сертификатов:

1. Нажмите сочетание клавиш **Win+R**, чтобы открыть окно **Выполнить**.
2. В поле **Открыть** введите `adsiedit.msc` и нажмите на клавишу **Enter** или на кнопку **OK**.
3. Нажмите правой кнопкой мыши **ADSI Edit** и выберите **Подключиться к**.
4. В разделе **Точка подключения** выберите **Конфигурация** в поле **Выбор известного контекста именования**.
5. Дважды щелкните **Конфигурация/Схема** на панели слева.
6. Выберите папку **CN=Configuration,DC=...** → **CN=Services** → **CN=Public Key Services** → **CN=Certificate Templates**.
7. Нажмите правой кнопкой мыши на папку **CN=Certificate Templates**, выберите **Свойства** и откройте вкладку **Безопасность**.
8. Нажмите на кнопку **Дополнительно** и выберите вкладку **Аудит**.

9. Нажмите на кнопку **Все** субъекты, установите флажки **Запись всех свойств**, **Удаление**, **Смена разрешений**, **Смена владельца**, **Все проверенные операции записи** и нажмите **OK**.

Чтобы настроить аудит безопасности объекта NTAuthCertificates:

1. В поле **Открыть** введите `adsiedit.msc,` и нажмите на клавишу **`Enter`** или на кнопку **OK**.
2. Нажмите правой кнопкой мыши **ADSI Edit** и выберите **Подключиться к**.
3. В разделе **Точка подключения** выберите **Конфигурация** в поле **Выбор известного контекста именования**.
4. Дважды щелкните **Конфигурация/Схема** на панели слева.
5. Выберите папку **CN=Configuration,DC=...** → **CN=Services** → **CN=Public Key Services** → **CN=NTAuthCertificates**.
6. Нажмите правой кнопкой мыши на папку **CN=NTAuthCertificates**, выберите **Свойства** и откройте вкладку **Безопасность**.
7. Нажмите на кнопку **Дополнительно** и выберите вкладку **Аудит**.
8. Нажмите на кнопку **Все** субъекты, установите флажки **Запись всех свойств**, **Удаление**, **Смена разрешений**, **Смена владельца**, **Все проверенные операции записи** и нажмите **OK**.

Ознакомительное видео

Посмотрите видео, чтобы узнать больше об основных функциях решения MDR.

Ознакомительное видео

Посмотрите видео, чтобы узнать больше об основных функциях решения MDR.