

kaspersky

Kaspersky Endpoint Security for Windows 11.4.0

© 2021 AO Kaspersky Lab

Contents

[Часто задаваемые вопросы](#)

[Что нового](#)

[Kaspersky Endpoint Security для Windows](#)

[Комплект поставки](#)

[Аппаратные и программные требования](#)

[Сравнение функций программы в зависимости от типа операционной системы](#)

[Сравнение функций программы в зависимости от инструментов управления](#)

[Совместимость с другими программами "Лаборатории Касперского"](#)

[Установка и удаление программы](#)

[Развертывание через Kaspersky Security Center](#)

[Стандартная установка программы](#)

[Создание инсталляционного пакета](#)

[Обновление баз в инсталляционном пакете](#)

[Создание задачи удаленной установки](#)

[Локальная установка программы с помощью мастера](#)

[Установка программы из командной строки](#)

[Удаленная установка программы с помощью System Center Configuration Manager](#)

[Описание параметров установки в файле setup.ini](#)

[Изменение состава компонентов программы](#)

[Обновление предыдущей версии программы](#)

[Удаление программы](#)

[Удаление через Kaspersky Security Center](#)

[Удаление программы с помощью мастера](#)

[Удаление программы из командной строки](#)

[Лицензирование программы](#)

[О Лицензионном соглашении](#)

[О лицензии](#)

[О лицензионном сертификате](#)

[О подписке](#)

[О лицензионном ключе](#)

[О коде активации](#)

[О файле ключа](#)

[Активация программы](#)

[Активация программы через Kaspersky Security Center](#)

[Активация программы с помощью мастера активации программы](#)

[Активация программы с помощью командной строки](#)

[Просмотр информации о лицензии](#)

[Приобретение лицензии](#)

[Продление подписки](#)

[Предоставление данных](#)

[Начало работы](#)

[О плагине управления Kaspersky Endpoint Security для Windows](#)

[Особенности работы с плагинами управления разных версий](#)

[Интерфейс программы](#)

[Значок программы в области уведомлений](#)

[Упрощенный интерфейс программы](#)

[Настройка отображения интерфейса программы](#)

[Подготовка программы к работе](#)

[Управление политиками](#)

[Управление задачами](#)

[Настройка локальных параметров программы](#)

[Запуск и остановка Kaspersky Endpoint Security](#)

[Приостановка и возобновление защиты и контроля компьютера](#)

[Проверка компьютера](#)

[Запуск и остановка задачи проверки](#)

[Изменение уровня безопасности](#)

[Изменение действия над зараженными файлами](#)

[Формирование списка проверяемых объектов](#)

[Выбор типа проверяемых файлов](#)

[Оптимизация проверки файлов](#)

[Проверка составных файлов](#)

[Использование методов проверки](#)

[Использование технологий проверки](#)

[Выбор режима запуска для задачи проверки](#)

[Настройка запуска задачи проверки с правами другого пользователя](#)

[Проверка съемных дисков при подключении к компьютеру](#)

[Фоновая проверка](#)

[Обновление баз и модулей программы](#)

[Схемы обновления баз и модулей программы](#)

[Обновление с серверного хранилища](#)

[Обновление из папки общего доступа](#)

[Обновление с помощью Kaspersky Update Utility](#)

[Обновление в мобильном режиме](#)

[Использование прокси-сервера при обновлении](#)

[Запуск и остановка задачи обновления](#)

[Запуск задачи обновления с правами другого пользователя](#)

[Выбор режима запуска для задачи обновления](#)

[Добавление источника обновлений](#)

[Выбор региона сервера обновлений](#)

[Настройка обновления из папки общего доступа](#)

[Настройка обновления модулей программы](#)

[Настройка использования прокси-сервера](#)

[Откат последнего обновления](#)

[Работа с активными угрозами](#)

[Работа со списком активных угроз](#)

[Запуск задачи выборочной проверки файлов из списка активных угроз](#)

[Удаление записей из списка активных угроз](#)

[Проверка целостности программы](#)

[Защита компьютера](#)

[Kaspersky Security Network](#)

[О предоставлении данных при использовании Kaspersky Security Network](#)

[Включение и выключение использования Kaspersky Security Network](#)

[Включение и выключение облачного режима для компонентов защиты](#)

[Проверка подключения к Kaspersky Security Network](#)

[Проверка репутации файла в Kaspersky Security Network](#)

[Анализ поведения](#)

[Включение и выключение Анализа поведения](#)

[Выбор действия при обнаружении вредоносной активности программы](#)

[Защита папок общего доступа от внешнего шифрования](#)

[Включение и выключение защиты папок общего доступа от внешнего шифрования](#)

[Выбор действия при обнаружении внешнего шифрования папок общего доступа](#)

[Создание исключения для защиты папок общего доступа от внешнего шифрования](#)

[Настройка адресов исключений из защиты папок общего доступа от внешнего шифрования](#)

[Защита от эксплойтов](#)

[Включение и выключение Защиты от эксплойтов](#)

[Выбор действия при обнаружении эксплойта](#)

[Включение и выключение защиты памяти системных процессов](#)

[Предотвращение вторжений](#)

[Ограничения контроля аудио и видео устройств](#)

[Включение и выключение Предотвращения вторжений](#)

[Работа с группами доверия программ](#)

[Настройка параметров распределения программ по группам доверия](#)

[Изменение группы доверия](#)

[Выбор группы доверия для программ, запускаемых до Kaspersky Endpoint Security](#)

[Работа с правами программ](#)

[Изменение прав программ для групп доверия и для групп программ](#)

[Изменение прав программы](#)

[Выключение загрузки и обновления прав программ из базы Kaspersky Security Network](#)

[Выключение наследования ограничений родительского процесса](#)

[Исключение некоторых действий программ из прав программ](#)

[Удаление информации о неиспользуемых программах](#)

[Защита ресурсов операционной системы и персональных данных](#)

[Добавление категории защищаемых ресурсов](#)

[Добавление защищаемого ресурса](#)

[Выключение защиты ресурса](#)

[Откат вредоносных действий](#)

[Ограничения функциональности восстановления файлов](#)

[Включение и выключение Отката вредоносных действий](#)

[Защита от файловых угроз](#)

[Включение и выключение Защиты от файловых угроз](#)

[Автоматическая приостановка Защиты от файловых угроз](#)

[Изменение уровня безопасности](#)

[Изменение действия компонента Защита от файловых угроз над зараженными файлами](#)

[Формирование области защиты компонента Защита от файловых угроз](#)

[Использование эвристического анализа в работе компонента Защита от файловых угроз](#)

[Использование технологий проверки в работе компонента Защита от файловых угроз](#)

[Оптимизация проверки файлов](#)

[Проверка составных файлов](#)

[Изменение режима проверки файлов](#)

[Защита от веб-угроз](#)

[Включение и выключение Защиты от веб-угроз](#)

[Изменение уровня безопасности веб-трафика](#)

[Изменение действия над вредоносными объектами веб-трафика](#)

[Проверка компонентом Защита от веб-угроз ссылок по базам фишинговых и вредоносных веб-адресов](#)

[Использование эвристического анализа в работе компонента Защита от веб-угроз](#)

[Формирование списка доверенных веб-адресов](#)

[Защита от почтовых угроз](#)

[Включение и выключение Защиты от почтовых угроз](#)

[Изменение уровня безопасности почты](#)

[Изменение действия над зараженными сообщениями электронной почты](#)

[Формирование области защиты компонента Защита от почтовых угроз](#)

[Проверка составных файлов, вложенных в сообщения электронной почты](#)

[Фильтрация вложений в сообщениях электронной почты](#)

[Проверка почты в Microsoft Office Outlook](#)

[Настройка проверки почты в программе Outlook](#)

[Настройка проверки почты с помощью Kaspersky Security Center](#)

[Защита от сетевых угроз](#)

[Включение и выключение Защиты от сетевых угроз](#)

[Изменение параметров блокирования атакующего компьютера](#)

[Настройка адресов исключений из блокирования](#)

[Защита от атак типа MAC-спуфинг](#)

[Проверка защищенных соединений](#)

[Настройка параметров проверки защищенных соединений](#)

[Исключение защищенных соединений из проверки](#)

[Сетевой экран](#)

[Включение и выключение Сетевого экрана](#)

[Изменение статуса сетевого соединения](#)

[Работа с сетевыми пакетными правилами](#)

[Создание и изменение сетевого пакетного правила](#)

[Включение и выключение сетевого пакетного правила](#)

[Изменение действия Сетевого экрана для сетевого пакетного правила](#)

[Изменение приоритета сетевого пакетного правила](#)

[Работа с сетевыми правилами программ](#)

[Создание и изменение сетевого правила программ](#)

[Включение и выключение сетевого правила программ](#)

[Изменение действия Сетевого экрана для сетевого правила программ](#)

[Изменение приоритета сетевого правила программ](#)

[Мониторинг сети](#)

[Защита от атак BadUSB](#)

[Включение и выключение Защиты от атак BadUSB](#)

[Разрешение и запрещение использования экранной клавиатуры при авторизации](#)

[Авторизация клавиатуры](#)

[Поставщик AMSI-защиты](#)

[Включение и выключение Поставщика AMSI-защиты](#)

[Проверка составных файлов Поставщиком AMSI-защиты](#)

[Контроль компьютера](#)

[Контроль программ](#)

[Ограничения функциональности Контроля программ](#)

[Включение и выключение Контроля программ](#)

[Управление правилами Контроля программ](#)

[Получение информации о программах, которые установлены на компьютерах пользователей](#)

[Создание категорий программ](#)

[Добавление в категорию программ исполняемых файлов из папки Исполняемые файлы](#)

[Добавление в категорию программ исполняемых файлов, связанных с событиями](#)

[Добавление и изменение правила Контроля программ с помощью Kaspersky Security Center](#)

[Изменение статуса правила Контроля программ с помощью Kaspersky Security Center](#)

[Тестирование правил Контроля программ с помощью Kaspersky Security Center](#)

[Просмотр событий по результатам тестовой работы компонента Контроля программ](#)

[Просмотр отчета о запрещенных программах в тестовом режиме](#)

[Просмотр событий по результатам работы компонента Контроль программ](#)

[Просмотр отчета о запрещенных программах](#)

[Выбор режима Контроля программ](#)

[Действия с правилами Контроля программ](#)

[Добавление и изменение правила Контроля программ](#)

[Добавление условия срабатывания в правило Контроля программ](#)

[Изменение статуса правила Контроля программ](#)

[Тестирование правил Контроля программ](#)

[Правила формирования масок имен файлов или папок](#)

[Изменение шаблонов сообщений Контроля программ](#)

[Контроль устройств](#)

[Включение и выключение Контроля устройств](#)

[О правилах доступа](#)

[Изменение правила доступа к устройствам](#)

[Включение и выключение записи событий в журнал](#)

[Добавление сети Wi-Fi в список доверенных](#)

[Изменение правила доступа к шине подключения](#)

[Действия с доверенными устройствами](#)

[Добавление устройства в список доверенных из интерфейса программы](#)

[Добавление устройства в список доверенных из Kaspersky Security Center](#)

[Экспорт и импорт списка доверенных устройств](#)

[Получение доступа к заблокированному устройству](#)

[Онлайн-режим предоставления доступа](#)

[Офлайн-режим предоставления доступа](#)

[Изменение шаблонов сообщений Контроля устройств](#)

[Лучшие практики по внедрению режима белого списка](#)

[Настройка режима белого списка](#)

[Тестирование режима белого списка](#)

[Поддержка режима белого списка](#)

[Анти-Бриджинг](#)

[Включение и выключение Анти-Бриджинга](#)

[Изменение статуса правила установки соединений](#)

[Изменение приоритета правила установки соединений](#)

[Веб-Контроль](#)

[Включение и выключение Веб-Контроля](#)

[Действия с правилами доступа к веб-ресурсам](#)

[Добавление и изменение правила доступа к веб-ресурсам](#)

[Назначение приоритета правилам доступа к веб-ресурсам](#)

[Проверка работы правил доступа к веб-ресурсам](#)

[Включение и выключение правила доступа к веб-ресурсам](#)

[Миграция правил доступа к веб-ресурсам из предыдущих версий программы](#)

[Экспорт и импорт списка адресов веб-ресурсов](#)

[Мониторинг активности пользователей в интернете](#)

[Правила формирования масок адресов веб-ресурсов](#)

[Изменение шаблонов сообщений Веб-Контроля](#)

[Адаптивный контроль аномалий](#)

[Включение и выключение Адаптивного контроля аномалий](#)

[Включение и выключение правила Адаптивного контроля аномалий](#)

[Изменение действия при срабатывании правила Адаптивного контроля аномалий](#)

[Создание и изменение исключения для правила Адаптивного контроля аномалий](#)

[Удаление исключения для правила Адаптивного контроля аномалий](#)

[Импорт исключений для правил Адаптивного контроля аномалий](#)

[Экспорт исключений для правил Адаптивного контроля аномалий](#)

[Применение обновлений для правил Адаптивного контроля аномалий](#)

[Изменение шаблонов сообщений Адаптивного контроля аномалий](#)

[Просмотр отчетов Адаптивного контроля аномалий](#)

[Контроль сетевых портов](#)

[Включение контроля всех сетевых портов](#)

[Включение контроля портов для программ из списка, сформированного специалистами "Лаборатории Касперского"](#)

[Формирование списка контролируемых сетевых портов](#)

[Формирование списка программ, для которых контролируются все сетевые порты](#)

[Удаление данных](#)

[Защита паролем](#)

[Включение Защиты паролем](#)

[Предоставление разрешений для отдельных пользователей или групп](#)

[Использование временного пароля для предоставления разрешений](#)

[Особенности разрешений Защиты паролем](#)

[Доверенная зона](#)

[Создание исключения из проверки](#)

[Изменение исключения из проверки](#)

[Удаление исключения из проверки](#)

[Запуск и остановка работы исключения из проверки](#)

[Формирование списка доверенных программ](#)

[Включение и выключение действия правил доверенной зоны на программу из списка доверенных программ](#)

[Использование доверенного системного хранилища сертификатов](#)

[Работа с резервным хранилищем](#)

[Настройка максимального срока хранения файлов в резервном хранилище](#)

[Настройка максимального размера резервного хранилища](#)

[Восстановление файлов из резервного хранилища](#)

[Удаление резервных копий файлов из резервного хранилища](#)

[Служба уведомлений](#)

[Настройка параметров журналов событий](#)

[Настройка отображения и доставки уведомлений](#)

[Настройка отображения предупреждений о состоянии программы в области уведомлений](#)

[Работа с отчетами](#)

[Просмотр отчетов](#)

[Настройка максимального срока хранения отчетов](#)

[Настройка максимального размера файла отчета](#)

[Сохранение отчета в файл](#)

[Удаление информации из отчетов](#)

[Самозащита Kaspersky Endpoint Security](#)

[Включение и выключение механизма самозащиты](#)

[Включение и выключение поддержки AM-PPL](#)

[Включение и выключение механизма защиты от внешнего управления](#)

[Обеспечение работы программ удаленного администрирования](#)

[Производительность Kaspersky Endpoint Security и совместимость с другими программами](#)

[Выбор типов обнаруживаемых объектов](#)

[Включение и выключение технологии лечения активного заражения](#)

[Включение и выключение режима энергосбережения](#)

[Включение и выключение режима передачи ресурсов другим программам](#)

[Kaspersky Endpoint Agent](#)

[Создание и использование конфигурационного файла](#)

[Обмен сообщениями между пользователем и администратором](#)

[Шифрование данных](#)

[Ограничения функциональности шифрования](#)

[Смена длины ключа шифрования \(AES56 / AES256\)](#)

[Шифрование диска Kaspersky](#)

[Полнодисковое шифрование с помощью технологии Шифрование диска Kaspersky](#)

[Формирование списка жестких дисков для исключения из шифрования](#)

[Включение использования технологии единого входа \(SSO\)](#)

[Управление учетными записями Агента аутентификации](#)

[Использование токена и смарт-карты при работе с Агентом аутентификации](#)

[Расшифровка жестких дисков](#)

[Восстановление доступа к диску, защищенному технологией Шифрование диска Kaspersky](#)

[Обновление операционной системы](#)

[Устранение ошибок при обновлении функциональности шифрования](#)

[Выбор уровня трассировки Агента аутентификации](#)

[Изменение справочных текстов Агента аутентификации](#)

[Удаление объектов и данных, оставшихся после тестовой работы Агента аутентификации](#)

[Управление BitLocker](#)

[Запуск шифрования диска BitLocker](#)

[Расшифровка жесткого диска, защищенного BitLocker](#)

[Восстановление доступа к диску, защищенному BitLocker](#)

[Шифрование файлов на локальных дисках компьютера](#)

[Запуск шифрования файлов на локальных дисках компьютера](#)

[Формирование правил доступа программ к зашифрованным файлам](#)

[Шифрование файлов, создаваемых и изменяемых отдельными программами](#)

[Формирование правила расшифровки](#)

[Расшифровка файлов на локальных дисках компьютера](#)

[Создание зашифрованных архивов](#)

[Восстановление доступа к зашифрованным файлам](#)

[Восстановление доступа к зашифрованным данным в случае выхода из строя операционной системы](#)

[Изменение шаблонов сообщений для получения доступа к зашифрованным файлам](#)

[Шифрование съемных дисков](#)

[Запуск шифрования съемных дисков](#)

[Добавление правила шифрования для съемных дисков](#)
[Изменение правила шифрования для съемных дисков](#)
[Портативный режим для работы с зашифрованными файлами на съемных дисках](#)
[Расшифровка съемных дисков](#)
[Просмотр информации о шифровании данных](#)
[Просмотр статусов шифрования](#)
[Просмотр статистики шифрования на информационных панелях Kaspersky Security Center](#)
[Просмотр ошибок шифрования файлов на локальных дисках компьютера](#)
[Просмотр отчета о шифровании данных](#)
[Работа с зашифрованными устройствами при отсутствии доступа к ним](#)
[Восстановление данных с помощью утилиты восстановления FDERT](#)
[Создание диска аварийного восстановления операционной системы](#)
[Управление программой из командной строки](#)
[Команды AVP](#)
[SCAN. Антивирусная проверка](#)
[UPDATE. Обновление баз и модулей программы](#)
[ROLLBACK. Откат последнего обновления](#)
[TRACES. Трассировка](#)
[START. Запуск профиля](#)
[STOP. Остановка профиля](#)
[STATUS. Статус профиля](#)
[STATISTICS. Статистика выполнения профиля](#)
[RESTORE. Восстановление файлов](#)
[EXPORT. Экспорт параметров программы](#)
[IMPORT. Импорт параметров программы](#)
[ADDKEY. Применение файла ключа](#)
[LICENSE. Лицензирование](#)
[RENEW. Покупка лицензии](#)
[PBATESTRESET. Сбросить результаты проверки перед шифрованием диска](#)
[EXIT. Завершение работы программы](#)
[EXITPOLICY. Выключение политики](#)
[STARTPOLICY. Включение политики](#)
[DISABLE. Выключение защиты](#)
[SPYWARE. Обнаружение шпионского ПО](#)
[Команды KESCLI](#)
[Scan. Антивирусная проверка](#)
[GetScanState. Статус выполнения проверки](#)
[GetLastScanTime. Определения времени выполнения проверки](#)
[GetThreats. Получение данных об обнаруженных угрозах](#)
[UpdateDefinitions. Обновление баз и модулей программы](#)
[GetDefinitionState. Определение времени выполнения обновления](#)
[EnableRTP. Включение защиты](#)
[GetRealTimeProtectionState. Статус Защиты от файловых угроз](#)
[Version. Определение версии программы](#)
[Коды ошибок](#)
[Приложение. Профили программы](#)
[Управление программой через REST API](#)
[Установка программы с REST API](#)

[Работа с API](#)

[Источники информации о программе](#)

[Обращение в Службу технической поддержки](#)

[Способы получения технической поддержки](#)

[Техническая поддержка через Kaspersky CompanyAccount](#)

[Получение информации для Службы технической поддержки](#)

[О составе и хранении файлов трассировки](#)

[Трассировка работы программы](#)

[Трассировка производительности программы](#)

[Запись дампов](#)

[Защита файлов дампов и трассировок](#)

[Глоссарий](#)

[OLE-объект](#)

[Агент администрирования](#)

[Агент аутентификации](#)

[Активный ключ](#)

[Антивирусные базы](#)

[Архив](#)

[База вредоносных веб-адресов](#)

[База фишинговых веб-адресов](#)

[Группа администрирования](#)

[Доверенный платформенный модуль](#)

[Задача](#)

[Зараженный файл](#)

[Издатель сертификата](#)

[Лечение объектов](#)

[Лицензионный сертификат](#)

[Ложное срабатывание](#)

[Маска](#)

[Нормализованная форма адреса веб-ресурса](#)

[Область защиты](#)

[Область проверки](#)

[Портативный файловый менеджер](#)

[Резервный ключ](#)

[Приложения](#)

[Приложение 1. Параметры политики в Web Console и Cloud Console](#)

[Kaspersky Security Network](#)

[Анализ поведения](#)

[Защита от эксплойтов](#)

[Предотвращение вторжений](#)

[Откат вредоносных действий](#)

[Защита от файловых угроз](#)

[Защита от веб-угроз](#)

[Защита от почтовых угроз](#)

[Защита от сетевых угроз](#)

[Сетевой экран](#)

[Защита от атак BadUSB](#)

[Поставщик AMSI-защиты](#)

[Контроль программ](#)
[Контроль устройств](#)
[Веб-Контроль](#)
[Адаптивный контроль аномалий](#)
[Полнодисковое шифрование](#)
[Шифрование файлов](#)
[Шифрование съемных дисков](#)
[Шаблоны \(шифрование данных\)](#)
[Endpoint Sensor](#)
[Управление задачами](#)
[Проверка из контекстного меню](#)
[Проверка съемных дисков](#)
[Фоновая проверка](#)
[Параметры программы](#)
[Параметры сети](#)
[Исключения](#)
[Отчеты и хранение](#)
[Интерфейс](#)
[Приложение 2. Группы доверия программ](#)
[Приложение 3. Категории содержания веб-ресурсов](#)
[Приложение 4. Расширения файлов для быстрой проверки съемных дисков](#)
[Приложение 5. Типы файлов для фильтра вложений Защиты от почтовых угроз](#)
[Приложение 6. Сетевые параметры для взаимодействия с внешними службами](#)
[Информация о стороннем коде](#)
[Уведомления о товарных знаках](#)

Frequently asked questions



GENERAL

[On what computers can Kaspersky Endpoint Security operate?](#)

[What has changed since the last version?](#)

[With which other Kaspersky applications can Kaspersky Endpoint Security operate?](#)

[How can I conserve computer resources during operation of Kaspersky Endpoint Security?](#)



DEPLOYMENT

[How do I install Kaspersky Endpoint Security to all computers of an organization?](#)

[Which installation settings can be configured in the command line?](#)

[How do I remotely uninstall Kaspersky Endpoint Security?](#)



UPDATE

[What methods are available to update the databases?](#)

[What should I do if problems arise after an update?](#)

[How do I update databases outside of the corporate network?](#)

[Is it possible to use a proxy server for updates?](#)



SECURITY

[How does Kaspersky Endpoint Security scan email?](#)

[How do I exclude a trusted file from scans?](#)

[How do I protect a computer against viruses from flash drives?](#)

[How can I run a virus scan that is hidden from the user?](#)

[How do I temporarily pause the protection of Kaspersky Endpoint Security?](#)

[How do I restore a file that Kaspersky Endpoint Security erroneously deleted?](#)

[How do I protect Kaspersky Endpoint Security from being uninstalled by a user?](#)



INTERNET

[Does Kaspersky Endpoint Security scan encrypted connections \(HTTPS\)?](#)

[How do I allow users to connect only to trusted Wi-Fi networks?](#)

[How do I block social networks?](#)



APPLICATIONS

[How do I find out which applications are installed on a user's computer \(inventory\)?](#)

[How do I prevent computer games from running?](#)

[How do I verify that Application Control has been correctly configured?](#)

[How do I add an application to the trusted list?](#)



DEVICES

[How do I block the use of flash drives?](#)

[How do I add a device to the trusted list?](#)

[Is it possible to obtain access to a blocked device?](#)



ENCRYPTION

[Under which conditions is encryption impossible?](#)

[How do I use a password to restrict access to an archive?](#)

[Is it possible to use smart cards and tokens with encryption?](#)

[Is it possible to gain access to encrypted data if there is no connection with Kaspersky Security Center?](#)

[What should I do if the computer operating system fails but data remains encrypted?](#)



SUPPORT






[Where is the report file stored?](#)

[How do I create a trace file?](#)

[How do I enable dump writing?](#)

What's new

Kaspersky Endpoint Security 11.4.0 for Windows offers the following features and improvements:

1. New design of the [application icon in the taskbar notification area](#). The new  is now displayed instead of the old  icon. If the user is required to perform an action (for example, restart the computer after updating the application), the icon will change to . If the protection components of the application are disabled or have malfunctioned, the icon will change to  or . If you hover over the icon, Kaspersky Endpoint Security will display a description of the problem in computer protection.
2. Kaspersky Endpoint Agent, which is included in the distribution kit, has been updated to version 3.9. Kaspersky Endpoint Agent 3.9 supports integration with new Kaspersky solutions. For more information about integration with Kaspersky solutions, refer to [Kaspersky Endpoint Agent help](#).
3. Added the *Not supported by license* status for Kaspersky Endpoint Security components. You can view the status of components by clicking the **Protection components** button in the [main application window](#).
4. New events from [Exploit Prevention](#) have been added to [reports](#).
5. Drivers for [Kaspersky Disk Encryption technology](#) are now automatically added to the Windows Recovery Environment (WinRE) when drive encryption is started. The previous version of Kaspersky Endpoint Security added drivers when installing the application. Adding drivers to WinRE can improve the stability of the application when restoring the operating system on computers protected by Kaspersky Disk Encryption technology.

The Endpoint Sensor component has been removed from Kaspersky Endpoint Security. You can still configure Endpoint Sensor settings in a policy provided that Kaspersky Endpoint Security version 11.0.0 to 11.3.0 is installed on the computer.

Kaspersky Endpoint Security for Windows

Kaspersky Endpoint Security for Windows (hereinafter also referred to as Kaspersky Endpoint Security) provides comprehensive computer protection against various types of threats, network and phishing attacks.

Each type of threat is handled by a dedicated component. Components can be enabled or disabled independently, and their settings can be configured.

The following application components are control components:

- **Application Control.** This component keeps track of user attempts to start applications and regulates the startup of applications.
- **Device Control.** This component lets you configure flexible access restrictions to data storage devices (such as hard drives, removable drives, and CD/DVD disks), data transmission equipment (such as modems), equipment that converts information (such as printers), or interfaces for connecting devices to computers (such as USB, Bluetooth).
- **Web Control.** This component lets you set flexible restrictions on access to web resources for different user groups.
- **Adaptive Anomaly Control.** This component monitors and controls potentially harmful actions that are not typical of the protected computer.

The following application components are protection components:

- **Behavior Detection.** This component receives information about the actions of applications on your computer and provides this information to other components for more effective protection.
- **Exploit Prevention.** This component tracks executable files that are run by vulnerable applications. When there is an attempt to run an executable file from a vulnerable application that was not initiated by the user, Kaspersky Endpoint Security blocks this file from running.
- **Host Intrusion Prevention.** This component registers the actions of applications in the operating system and regulates application activity depending on the trust group of a particular application. A set of rules is specified for each group of applications. These rules regulate the access of applications to user data and to resources of the operating system. Such data includes user files in Documents folder, cookies, user activity log files and files, folders, and registry keys that contain settings and important information for the most frequently used applications.
- **Remediation Engine.** This component lets Kaspersky Endpoint Security roll back actions that have been performed by malware in the operating system.
- **File Threat Protection.** This component protects the file system of the computer from infection. The component starts immediately after Kaspersky Endpoint Security is launched; it continuously remains in computer RAM, and scans all files that are opened, saved, or started on the computer and on all connected storage devices. This component intercepts every attempt to access a file and scans the file for viruses and other threats.
- **Web Threat Protection.** This component scans traffic that arrives to the user computer via the HTTP and FTP protocols, and checks whether web addresses are malicious or phishing.
- **Mail Threat Protection.** This component scans incoming and outgoing email messages for viruses and other threats.
- **Network Threat Protection.** This component inspects inbound network traffic for activity that is typical of network attacks. Upon detecting an attempted network attack that targets your computer, Kaspersky

Endpoint Security blocks network activity from the attacking computer.

- **Firewall.** This component protects data that is stored on the computer and blocks most possible threats to the operating system while the computer is connected to the Internet or to a local area network.
- **BadUSB Attack Prevention.** This component prevents infected USB devices emulating a keyboard from connecting to the computer.
- **AMSI Protection Provider.** This component scans objects based on a request from third-party applications and notifies the requesting application about the scan result.

In addition to the real-time protection that the application components provide, we recommend that you regularly *scan the computer* for viruses and other threats. This helps to rule out the possibility of spreading malware that was not detected by protection components, for example, due to a low security level.

To keep computer protection up to date, you must *update the databases and modules* that the application uses. The application is updated automatically by default, but if necessary, you can update the databases and application modules manually.

The following tasks are provided in Kaspersky Endpoint Security:

- **Integrity Check.** Kaspersky Endpoint Security checks the application modules in the application installation folder for corruption or modifications. If an application module has an incorrect digital signature, the module is considered corrupt.
- **Full Scan.** Kaspersky Endpoint Security scans the operating system, including kernel memory, objects that are loaded at operation system startup, disk boot sectors, backup storage of the operating system, and all hard drives and removable drives.
- **Custom Scan.** Kaspersky Endpoint Security scans the objects that are selected by the user.
- **Critical Areas Scan.** Kaspersky Endpoint Security scans the kernel memory, objects that are loaded at operation system startup and disk boot sectors.
- **Update.** Kaspersky Endpoint Security downloads updated databases and application modules. Updating keeps the computer protected against the latest viruses and other threats.
- **Last update rollback.** Kaspersky Endpoint Security rolls back the last update of databases and modules. This lets you roll back the databases and application modules to their previous versions when necessary, for example, when the new database version contains an invalid signature that causes Kaspersky Endpoint Security to block a safe application.

Service functions of the application

Kaspersky Endpoint Security includes a number of service functions. Service functions are provided for keeping the application up to date, expand its functionality, and assist the user with operating the application.

- **Reports.** In the course of its operation, the application keeps a report on each application component. You can also use reports to track the results of completed tasks. The reports contain lists of events that occurred during Kaspersky Endpoint Security operation and all the operations that the application performs. In case of an incident, you can send reports to Kaspersky, where Technical Support specialists can look into the issue in more detail.
- **Data storage.** If the application detects infected files while scanning the computer for viruses and other threats, it blocks those files. Kaspersky Endpoint Security stores copies of disinfected and deleted files in

Backup. Kaspersky Endpoint Security moves files that are not processed for any reason to the *list of active threats*. You can scan files, restore files to their original folders, and empty the data storage.

- **Notification service.** The notification service helps the user to track the events that influence the computer protection status and Kaspersky Endpoint Security operation. Notifications can be displayed on the screen or sent by email.
- **Kaspersky Security Network.** User participation in Kaspersky Security Network enhances efficiency of computer protection through real-time use of information on the reputation of files, web resources, and software received from users worldwide.
- **License.** Purchasing a license unlocks full application functionality, provides access to application database and module updates, and support by phone or via email on issues related to installation, configuration, and use of the application.
- **Support.** All registered users of Kaspersky Endpoint Security can contact Technical Support specialists for assistance. You can send a request to Kaspersky Technical Support through the Kaspersky CompanyAccount portal or call Technical Support by phone.

If the application returns errors or hangs up during operation, it may be restarted automatically.

If the application encounters recurring errors that cause the application to crash, the application performs the following operations:

1. Disables control and protection functions (encryption functionality remains enabled).
2. Notifies the user that the functions have been disabled.
3. Attempts to restore the application to a functional state after updating anti-virus databases or applying application module updates.

Distribution kit

The distribution kit includes the following distribution packages:

- **Strong encryption (AES256)**
This distribution package contains cryptographic tools that implement the AES (Advanced Encryption Standard) encryption algorithm with an effective key length of 256 bits.
- **Lite encryption (AES56)**
This distribution package contains cryptographic tools that implement the AES encryption algorithm with an effective key length of 56 bits.

Each distribution package contains the following files:

kes_win.msi	Kaspersky Endpoint Security installation package.
setup_kes.exe	Files that are required for installing the application using any of the available methods.
kes_win.kud	File for creating installation packages for Kaspersky Endpoint Security .

<code>klcfginst.msi</code>	Kaspersky Endpoint Security Management Plug-in installation package for Kaspersky Security Center.
<code>bases.cab</code>	Update package files that are used during installation.
<code>cleaner.cab</code>	Files for removing incompatible software.
<code>incompatible.txt</code>	File that contains a list of incompatible software.
<code>ksn_<language_ID>.txt</code>	File where you can read through the terms of participation in Kaspersky Security Network.
<code>license.txt</code>	File where you can read through the End User License Agreement and the Privacy Policy.
<code>installer.ini</code>	File that contains the internal settings of the distribution kit.
<code>endpointagent.msi</code>	Installation package for Kaspersky Endpoint Agent, the application required for integration with other Kaspersky solutions (for example, Kaspersky Sandbox).

It is not recommended to change the values of these settings. If you want to change installation options, use the [setup.ini file](#).

Hardware and software requirements

To ensure proper operation of Kaspersky Endpoint Security, your computer must meet the following requirements:

Minimum general requirements:

- 2 GB of free disk space on the hard drive
- Processor with a clock speed of 1 GHz (that supports the SSE2 instruction set)
- RAM:
 - 1 GB for a 32-bit operating system
 - 2 GB for a 64-bit operating system

Supported operating systems for workstations:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 or later
- Windows 8 Professional / Enterprise

- Windows 8.1 Professional / Enterprise
- Windows 10 Home / Pro / Education / Enterprise

For details about support for the Microsoft Windows 10 operating system, please refer to the [Technical Support Knowledge Base](#).

Supported operating systems for servers:

- Windows Small Business Server 2011 Essentials / Standard (64-bit)

Microsoft Small Business Server 2011 Standard (64-bit) is supported only if Service Pack 1 for Microsoft Windows Server 2008 R2 is installed

- Windows MultiPoint Server 2011 (64-bit)
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 or later
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter
- Windows Server 2016 Essentials / Standard / Datacenter
- Windows Server 2019 Essentials / Standard / Datacenter

For details about support for the Microsoft Windows Server 2016 and Microsoft Windows Server 2019 operating systems, please refer to the [Technical Support Knowledge Base](#).

Supported virtual platforms:

- VMware Workstation 15
- VMware ESXi 6.7 U2
- Microsoft Hyper-V 2019 Server
- Citrix Hypervisor 8
- Citrix XenDesktop 7.18
- Citrix XenApp 7.18
- Citrix Provisioning Services 7.18

Kaspersky Endpoint Security supports operation with the following versions of Kaspersky Security Center:

- Kaspersky Security Center 11
- Kaspersky Security Center 12

- Kaspersky Security Center 12 Patch A
- Kaspersky Security Center 12 Patch B
- Kaspersky Security Center 13
- Kaspersky Security Center 13.1
- Kaspersky Security Center 13.2

For details about support for Kaspersky Security Center, please refer to the [Technical Support Knowledge Base](#).

Comparison of available application features depending on the type of operating system

The set of available Kaspersky Endpoint Security features depends on the type of operating system: workstation or server (see the table below).

Comparison of Kaspersky Endpoint Security features

Feature	Workstation	Server
Advanced Threat Protection		
Kaspersky Security Network	✓	✓
Behavior Detection	✓	✓
Exploit Prevention	✓	✓
Host Intrusion Prevention	✓	–
Remediation Engine	✓	✓
Essential Threat Protection		
File Threat Protection	✓	✓
Web Threat Protection	✓	–
Mail Threat Protection	✓	–
Firewall	✓	✓
Network Threat Protection	✓	✓
BadUSB Attack Prevention	✓	✓
AMSI Protection Provider	✓	✓
Security Controls		
Application Control	✓	✓
Device Control	✓	–
Web Control	✓	–
Adaptive Anomaly Control	✓	–

Data Encryption		
Kaspersky Disk Encryption	✓	–
BitLocker Drive Encryption	✓	✓
File Level Encryption	✓	–
Encryption of removable drives	✓	–
Endpoint Agent	✓	✓

Comparison of application functions depending on the management tools

The set of functions available in Kaspersky Endpoint Security depends on the management tools (see the table below).

You can manage the application by using the following consoles of Kaspersky Security Center:

- Administration Console. Microsoft Management Console (MMC) snap-in installed on the administrator's workstation.
- Web Console. Component of Kaspersky Security Center that is installed on the Administration Server. You can work in the Web Console through a browser on any computer that has access to the Administration Server.

You can also manage the application by using the Kaspersky Security Center Cloud Console. The *Kaspersky Security Center Cloud Console* is the cloud version of Kaspersky Security Center. This means that the Administration Server and other components of Kaspersky Security Center are installed in the cloud infrastructure of Kaspersky. For details on managing the application through the Kaspersky Security Center Cloud Console, please refer to the [Kaspersky Security Center Cloud Console Help Guide](#).

Comparison of Kaspersky Endpoint Security features

Feature	Kaspersky Security Center		Kaspersky Security Center
	Administration Console	Web Console	Cloud Console
Advanced Threat Protection			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
Behavior Detection	✓	✓	✓
Exploit Prevention	✓	✓	✓
Host Intrusion Prevention	✓	✓	✓
Remediation Engine	✓	✓	✓
Essential Threat Protection			
File Threat Protection	✓	✓	✓
Web Threat Protection	✓	✓	✓
Mail Threat Protection	✓	✓	✓

Firewall	✓	✓	✓
Network Threat Protection	✓	✓	✓
BadUSB Attack Prevention	✓	✓	✓
AMSI Protection Provider	✓	✓	✓
Security Controls			
Application Control	✓	✓	✓
Device Control	✓	✓	✓
Web Control	✓	✓	✓
Adaptive Anomaly Control	✓	✓	–
Data Encryption			
Kaspersky Disk Encryption	✓	✓	–
BitLocker Drive Encryption	✓	✓	–
File Level Encryption	✓	✓	–
Encryption of removable drives	✓	✓	–
Endpoint Agent	✓	✓	✓
Tasks			
Add key	✓	✓	✓
Change application components	✓	✓	✓
Inventory	✓	✓	✓
Update	✓	✓	✓
Update rollback	✓	✓	✓
Virus scan	✓	✓	✓
Integrity check	✓	✓	–
Wipe Data	✓	✓	✓
Managing Authentication Agent accounts	✓	–	–

Compatibility with other Kaspersky applications

Prior to the installation, Kaspersky Endpoint Security checks the computer for the presence of Kaspersky applications.

Kaspersky Endpoint Security is incompatible with the following Kaspersky applications:

- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.

- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Kaspersky Anti Targeted Attack Platform (including the Endpoint Sensor component).
- Kaspersky Sandbox (including Kaspersky Endpoint Agent).
- Kaspersky Endpoint Detection and Response (including the Endpoint Sensor component).

If the Endpoint Agent component was installed on a computer using the deployment tools of other Kaspersky applications, the component will be automatically removed during installation of Kaspersky Endpoint Security. Kaspersky Endpoint Security may also include the Endpoint Sensor / Kaspersky Endpoint Agent component if you selected Endpoint Agent in the list of application components.

- Kaspersky Security for Virtualization Light Agent.
- Kaspersky Fraud Prevention for Endpoint.
- Kaspersky Security for Windows Server.
- Kaspersky Embedded Systems Security.

If Kaspersky applications from this list are installed on the computer, Kaspersky Endpoint Security removes these applications. Please wait for this process to finish before continuing installation of Kaspersky Endpoint Security.

Installing and removing the application

Kaspersky Endpoint Security can be installed on a computer in the following ways:

- locally, by using the [Setup Wizard](#).
- locally from the [command line](#).
- remotely through [Kaspersky Security Center 12](#).
- remotely through the Microsoft Windows Group Policy Management Editor (for more details, see [Microsoft Technical Support website](#)).
- remotely, by using the [System Center Configuration Manager](#).

You can configure the application installation settings in several ways. If you simultaneously use multiple methods for configuring the settings, Kaspersky Endpoint Security applies the settings with the highest priority. Kaspersky Endpoint Security uses the following order of priorities:

1. Settings received from the [setup.ini](#) file.
2. Settings received from the installer.ini file.
3. Settings received from the [command line](#).

We recommend closing all running applications before starting the installation of Kaspersky Endpoint Security (including remote installation).

Deployment through Kaspersky Security Center 12

Kaspersky Endpoint Security can be deployed on computers within a corporate network in several ways. You can choose the most suitable deployment scenario for your organization or combine several deployment scenarios at the same time. Kaspersky Security Center supports the following main deployment methods:

- Installing the application using the Protection Deployment Wizard.
[Standard installation method](#) is convenient if you are satisfied with the default settings of Kaspersky Endpoint Security and your organization has a simple infrastructure that does not require special configurations.

- Installing the application using the remote installation task.

Universal installation method, which allows to configure Kaspersky Endpoint Security settings and flexibly manage remote installation tasks. Installation of Kaspersky Endpoint Security consists of the following steps:

1. [Creating an installation package](#).
2. [Creating a remote installation task](#).

Kaspersky Security Center also supports other methods of installing Kaspersky Endpoint Security, such as deployment within an operating system image. For details about other deployment methods, refer to [Kaspersky Security Center Help](#).

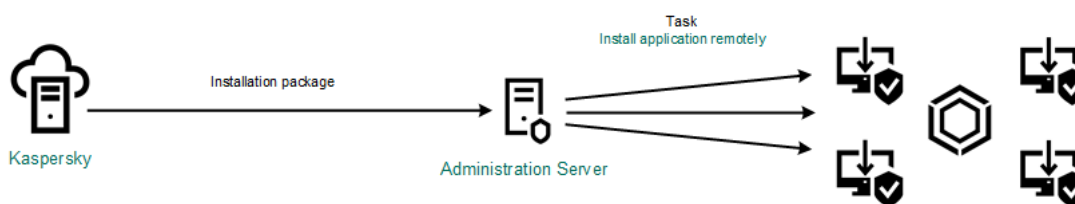
Standard installation of the application

Kaspersky Security Center provides a Protection Deployment Wizard for installing the application on corporate computers. The Protection Deployment Wizard includes the following main actions:

1. Selecting a Kaspersky Endpoint Security installation package.

An *installation package* is a set of files created for remote installation of a Kaspersky application via Kaspersky Security Center. The installation package contains a range of settings needed to install the application and get it running immediately after installation. The installation package is created using files with the .kpd and .kud extensions included in the application distribution kit. Kaspersky Endpoint Security installation package is common for all supported Windows versions and processor architecture types.

2. Creating the *Install application remotely* task of the Kaspersky Security Center Administration Server.



Kaspersky Endpoint Security deployment

[How to run the Protection Deployment Wizard in the Administration Console \(MMC\)](#) 

1. In the Administration Console, go to the folder **Administration Server** → **Additional** → **Remote installation**.

2. Click the **Deploy installation package on managed devices (workstations)** link.

This will start the Protection Deployment Wizard. Follow the instructions of the Wizard.

TCP ports 139 and 445, and UDP ports 137 and 138 must be opened on a client computer.

Step 1. Selecting an installation package

Select Kaspersky Endpoint Security installation package from the list. If the list does not contain the installation package for Kaspersky Endpoint Security, you can create the package in the Wizard.

You can configure the [installation package settings](#) in Kaspersky Security Center. For example, you can select the application components that will be installed to a computer.

Network Agent will also be installed together with Kaspersky Endpoint Security. *Network Agent* facilitates interaction between the Administration Server and a client computer. If Network Agent is already installed on the computer, it is not installed again.

Step 2. Selecting devices for installation

Select the computers for installing Kaspersky Endpoint Security. The following options are available:

- Assign the task to an administration group. In this case, the task is assigned to computers included in a previously created administration group.
- Select computers detected by the Administration Server in the network: *unassigned devices*. Network Agent is not installed on unassigned devices. In this case, the task is assigned to specific devices. The specific devices can include devices in administration groups as well as unassigned devices.
- Specify device addresses manually, or import addresses from a list. You can specify NetBIOS names, IP addresses, and IP subnets of devices to which you want to assign the task.

Step 3. Defining remote installation task settings

Configure the following additional application settings:

- **Force download of the installation package.** Select the method of application installation:
 - **Using Network Agent.** If Network Agent has not been installed on the computer, first Network Agent will be installed using the tools of the operating system. Then Kaspersky Endpoint Security is installed by the tools of Network Agent.
 - **Using operating system resources through distribution points.** The installation package is delivered to client computers using operating system resources via distribution points. You can select this option if there is at least one distribution point in the network. For more details about distribution points, refer to [Kaspersky Security Center Help](#).

- **Using operating system resources through Administration Server.** Files will be delivered to client computers by using operating system resources through the Administration Server. You can select this option if Network Agent is not installed on the client computer, but the client computer is in the same network as the Administration Server.
- **Behavior of devices managed by other Servers.** Select the Kaspersky Endpoint Security installation method. If the network has more than one Administration Server installed, these Administration Servers may see the same client computers. This may cause, for example, an application to be installed remotely on the same client computer several times through different Administration Servers, or other conflicts.
- **Do not install application if it is already installed.** Clear this check box if you want to install an earlier version of the application, for example.
- **Assign Network Agent installation in the Active Directory group policies.** Manually installing Network Agent using Active Directory resources. To install Network Agent, the remote installation task must be run with domain administrator privileges.

Step 4. Selecting a license key

Add a key to the installation package for activating the application. This step is optional. If the Administration Server contains a license key with automatic distribution functionality, the key will be automatically added later. You can also [activate the application](#) later by using the *Add key* task.

Step 5. Selecting the operating system restart setting

Select the action to be performed if a computer restart is required. Restart is not required when installing Kaspersky Endpoint Security. Restart is required only if you have to remove incompatible applications prior to installation. Restart may also be required when updating the application version.

Step 6. Removing incompatible applications before installing the application

Carefully read the list of incompatible applications and allow removal of these applications. If incompatible applications are installed on the computer, installation of Kaspersky Endpoint Security ends with an error.

Step 7. Selecting an account for accessing devices

Select the account for installing Network Agent using the tools of the operating system. In this case, administrator rights are required for computer access. You can add multiple accounts. If an account does not have sufficient rights, the Installation Wizard uses the next account. If you install Kaspersky Endpoint Security using Network Agent tools, you do not have to select an account.

Step 8. Starting the installation

Exit the Wizard. If required, select the **Do not run the task after the Remote Installation Wizard completes** check box. You can monitor the progress of the task in the task properties.

[How to start the Protection Deployment Wizard in the Web Console and Cloud Console](#) 

In Web Console main window, select **Device discovery and deployment** → **Deployment and assignment** → **Protection Deployment Wizard**.

This will start the Protection Deployment Wizard. Follow the instructions of the Wizard.

TCP ports 139 and 445, and UDP ports 137 and 138 must be opened on a client computer.

Step 1. Selecting an installation package

Select Kaspersky Endpoint Security installation package from the list. If the list does not contain the installation package for Kaspersky Endpoint Security, you can create the package in the Wizard. To create the installation package, you do not need to search for the distribution package and save it to computer memory. In Kaspersky Security Center, you can view the list of distribution packages residing on Kaspersky servers, and the installation package is created automatically. Kaspersky updates the list after the release of new versions of applications.

You can configure the [installation package settings](#) in Kaspersky Security Center. For example, you can select the application components that will be installed to a computer.

Step 2. Selecting a license key

Add a key to the installation package for activating the application. This step is optional. If the Administration Server contains a license key with automatic distribution functionality, the key will be automatically added later. You can also [activate the application](#) later by using the *Add key* task.

Step 3. Selecting a Network Agent

Select the version of Network Agent that will be installed together with Kaspersky Endpoint Security. *Network Agent* facilitates interaction between the Administration Server and a client computer. If Network Agent is already installed on the computer, it is not installed again.

Step 4. Selecting devices for installation

Select the computers for installing Kaspersky Endpoint Security. The following options are available:

- Assign the task to an administration group. In this case, the task is assigned to computers included in a previously created administration group.
- Select computers detected by the Administration Server in the network: *unassigned devices*. Network Agent is not installed on unassigned devices. In this case, the task is assigned to specific devices. The specific devices can include devices in administration groups as well as unassigned devices.
- Specify device addresses manually, or import addresses from a list. You can specify NetBIOS names, IP addresses, and IP subnets of devices to which you want to assign the task.

Step 5. Configuring advanced settings

Configure the following additional application settings:

- **Force download of the installation package.** Selecting the method of application installation:
 - **Using Network Agent.** If Network Agent has not been installed on the computer, first Network Agent will be installed using the tools of the operating system. Then Kaspersky Endpoint Security is installed by the tools of Network Agent.
 - **Using operating system resources through distribution points.** The installation package is delivered to client computers using operating system resources via distribution points. You can select this option if there is at least one distribution point in the network. For more details about distribution points, refer to [Kaspersky Security Center Help](#).
 - **Using operating system resources through Administration Server.** Files will be delivered to client computers by using operating system resources through the Administration Server. You can select this option if Network Agent is not installed on the client computer, but the client computer is in the same network as the Administration Server.
- **Do not install application if it is already installed.** Clear this check box if you want to install an earlier version of the application, for example.
- **Assign package installation in Active Directory group policies.** Kaspersky Endpoint Security is installed by means of Network Agent or manually by means of Active Directory. To install Network Agent, the remote installation task must be run with domain administrator privileges.

Step 6. Selecting the operating system restart setting

Select the action to be performed if a computer restart is required. Restart is not required when installing Kaspersky Endpoint Security. Restart is required only if you have to remove incompatible applications prior to installation. Restart may also be required when updating the application version.

Step 7. Removing incompatible applications before installing the application

Carefully read the list of incompatible applications and allow removal of these applications. If incompatible applications are installed on the computer, installation of Kaspersky Endpoint Security ends with an error.

Step 8. Assigning to an administration group

Select the administration group to which the computers will be moved after Network Agent is installed. Computers need to be moved to an administration group so that [policies](#) and [group tasks](#) can be applied. If a computer is already in any administration group, the computer will not be moved. If you do not select an administration group, computers will be added to the **Unassigned devices** group.

Step 9. Selecting an account for accessing devices

Select the account for installing Network Agent using the tools of the operating system. In this case, administrator rights are required for computer access. You can add multiple accounts. If an account does not have sufficient rights, the Installation Wizard uses the next account. If you install Kaspersky Endpoint Security using Network Agent tools, you do not have to select an account.

Step 10. Starting installation

Exit the Wizard. If necessary, select the **Run task after Wizard finishes** check box. You can monitor the progress of the task in the task properties.

Creating an installation package

An *installation package* is a set of files created for remote installation of a Kaspersky application via Kaspersky Security Center. The installation package contains a range of settings needed to install the application and get it running immediately after installation. The installation package is created using files with the .kpd and .kud extensions included in the application distribution kit. Kaspersky Endpoint Security installation package is common for all supported Windows versions and processor architecture types.

[How to create an installation package in the Administration Console \(MMC\)](#) 

1. In the Administration Console, go to the folder **Administration Server** → **Additional** → **Remote installation** → **Installation packages**.

This opens a list of installation packages that have been downloaded to Kaspersky Security Center.

2. Click the **Create installation package** button.

The New Package Wizard starts. Follow the instructions of the Wizard.

Step 1. Selecting the installation package type

Select the **Create installation package for Kaspersky application** option.

Step 2. Defining the installation package name

Enter the name of the installation package, for example, **Kaspersky Endpoint Security 11.4.0 for Windows**.

Step 3. Selecting the distribution package for installation

Click the **Browse** button and select the `kes_win.kud` file that is included in the [distribution kit](#).

If required, update the anti-virus databases in the installation package by using the **Copy updates from repository to installation package** check box.

Step 4. End User License Agreement and Privacy Policy

Read and accept the terms of the End User License Agreement and Privacy Policy.

The installation package will be created and added to Kaspersky Security Center. Using the installation package, you can install Kaspersky Endpoint Security on corporate network computers or update the application version. In the installation package settings, you can also select the application components and configure the application installation settings (see the table below). The installation package contains anti-virus databases from the Administration Server repository. You can [update the databases in the installation package](#) to reduce traffic consumption when updating the databases after installing Kaspersky Endpoint Security.

[How to create an installation package in the Web Console and Cloud Console](#) 

1. In Web Console main window, select **Device discovery and deployment** → **Deployment and assignment** → **Installation packages**.

This opens a list of installation packages that have been downloaded to Kaspersky Security Center.

2. Click the **Add** button.

The New Package Wizard starts. Follow the instructions of the Wizard.

Step 1. Selecting the installation package type

Select the **Create installation package for Kaspersky application** option.

The Wizard will create an installation package from the distribution package residing on Kaspersky servers. The list is updated automatically as new versions of applications are released. It is recommended to select this option for installation of Kaspersky Endpoint Security.

You can also create an installation package from a file.

Step 2. Installation packages

Select the Kaspersky Endpoint Security for Windows installation package. The installation package creation process starts. During creation of the installation package, you must accept the terms of the End User License Agreement and Privacy Policy.

The installation package will be created and added to Kaspersky Security Center. Using the installation package, you can install Kaspersky Endpoint Security on corporate network computers or update the application version. In the installation package settings, you can also select the application components and configure the application installation settings (see the table below). The installation package contains anti-virus databases from the Administration Server repository. You can [update the databases in the installation package](#) to reduce traffic consumption when updating the databases after installing Kaspersky Endpoint Security.

Installation package settings

Section	Description
Protection components	In this section, you can select the application components that will be available. You can change the set of application components at a later time by using the <i>Change application components</i> task. The BadUSB Attack Prevention component, Endpoint Agent component, and data encryption components are not installed by default. These components can be added in the installation package settings.
Installation options	<p>Add application location to environment variable %PATH%. You can add the installation path to the %PATH% variable for convenient use of the command line interface.</p> <p>Do not protect the installation process. Installation protection includes protection against replacement of the distribution package with malicious applications, blocking access to the installation folder of Kaspersky Endpoint Security, and blocking access to the system registry section containing application keys. However, if the application cannot be installed (for example, when performing remote installation with the help of Windows Remote Desktop), you are advised to disable protection of the installation process.</p> <p>Ensure compatibility with Citrix PVS. You can enable support of Citrix Provisioning Services to install Kaspersky Endpoint Security to a virtual machine.</p>

Path to application installation folder. You can change the installation path of Kaspersky Endpoint Security on a client computer. By default, the application is installed in the folder %ProgramFiles%\Kaspersky Lab\Kaspersky Endpoint Security for Windows.

Configuration file. You can upload a file that defines the settings of Kaspersky Endpoint Security. You can [create a configuration file in the local interface of the application](#).

Updating databases in the installation package

The installation package contains anti-virus databases from the Administration Server repository that are up to date when the installation package is created. After creating the installation package, you can update the anti-virus databases in the installation package. This lets you reduce traffic consumption when updating anti-virus databases after installing Kaspersky Endpoint Security.

To update the anti-virus databases in the Administration Server repository, use the *Download updates to the Administration Server repository* task of the Administration Server. For more information about updating the anti-virus databases in the Administration Server repository, please refer to the [Kaspersky Security Center Help Guide](#).

You can update the databases in the installation package only in the Administration Console and Kaspersky Security Center Web Console. It is not possible to update the databases in the installation package in the Kaspersky Security Center Cloud Console.

[How to update the anti-virus databases in the installation package through the Administration Console \(MMC\)](#)

1. In the Administration Console, go to the folder **Administration Server** → **Additional** → **Remote installation** → **Installation packages**.

This opens a list of installation packages that have been downloaded to Kaspersky Security Center.

2. Open the properties of the installation package.
3. In the **General** section, click the **Update databases** button.

As a result, the anti-virus databases in the installation package will be updated from the Administration Server repository. The bases .cab file that is included in the [distribution kit](#) will be replaced by the bases folder. The update package files will be inside the folder.

[How to update anti-virus databases in an installation package through the Web Console](#)

1. In Web Console main window, select **Device discovery and deployment** → **Deployment and assignment** → **Installation packages**.

This opens a list of installation packages downloaded to Web Console.

2. Click on the name of the Kaspersky Endpoint Security installation package in which you want to update the anti-virus databases.

The installation package properties window opens.

3. On the **General information** tab, click the **Update databases** link.

As a result, the anti-virus databases in the installation package will be updated from the Administration Server repository. The bases .cab file that is included in the [distribution kit](#) will be replaced by the bases folder. The update package files will be inside the folder.

Creating a remote installation task

The *Install application remotely* task is designed for remote installation of Kaspersky Endpoint Security. The *Install application remotely* task allows you to deploy the [installation package of the application](#) to all computers in the organization. Before deploying the installation package, you can [update the anti-virus databases](#) inside the package and select the available application components in the properties of the installation package.

[How to create a remote installation task in the Administration Console \(MMC\)](#) 

1. In the Administration Console, go to the folder **Administration Server** → **Tasks**.

The list of tasks opens.

2. Click the **New task** button.

The Task Wizard starts. Follow the instructions of the Wizard.

Step 1. Selecting task type

Select **Kaspersky Security Center Administration Server** → **Install application remotely**.

Step 2. Selecting an installation package

Select Kaspersky Endpoint Security installation package from the list. If the list does not contain the installation package for Kaspersky Endpoint Security, you can create the package in the Wizard.

You can configure the [installation package settings](#) in Kaspersky Security Center. For example, you can select the application components that will be installed to a computer.

Network Agent will also be installed together with Kaspersky Endpoint Security. *Network Agent* facilitates interaction between the Administration Server and a client computer. If Network Agent is already installed on the computer, it is not installed again.

Step 3. Additional

Select the Network Agent installation package. The selected version of Network Agent will be installed together with Kaspersky Endpoint Security.

Step 4. Settings

Configure the following additional application settings:

- **Force download of the installation package.** Select the method of application installation:
 - **Using Network Agent.** If Network Agent has not been installed on the computer, first Network Agent will be installed using the tools of the operating system. Then Kaspersky Endpoint Security is installed by the tools of Network Agent.
 - **Using operating system resources through distribution points.** The installation package is delivered to client computers using operating system resources via distribution points. You can select this option if there is at least one distribution point in the network. For more details about distribution points, refer to [Kaspersky Security Center Help](#).
 - **Using operating system resources through Administration Server.** Files will be delivered to client computers by using operating system resources through the Administration Server. You can select this option if Network Agent is not installed on the client computer, but the client computer is in the same network as the Administration Server.
- **Behavior of devices managed by other Servers.** Select the Kaspersky Endpoint Security installation method. If the network has more than one Administration Server installed, these Administration Servers

may see the same client computers. This may cause, for example, an application to be installed remotely on the same client computer several times through different Administration Servers, or other conflicts.

- **Do not install application if it is already installed.** Clear this check box if you want to install an earlier version of the application, for example.

Step 5. Selecting the operating system restart setting

Select the action to be performed if a computer restart is required. Restart is not required when installing Kaspersky Endpoint Security. Restart is required only if you have to remove incompatible applications prior to installation. Restart may also be required when updating the application version.

Step 6. Selecting the devices to which the task will be assigned

Select the computers for installing Kaspersky Endpoint Security. The following options are available:

- Assign the task to an administration group. In this case, the task is assigned to computers included in a previously created administration group.
- Select computers detected by the Administration Server in the network: *unassigned devices*. Network Agent is not installed on unassigned devices. In this case, the task is assigned to specific devices. The specific devices can include devices in administration groups as well as unassigned devices.
- Specify device addresses manually, or import addresses from a list. You can specify NetBIOS names, IP addresses, and IP subnets of devices to which you want to assign the task.

Step 7. Selecting the account to run the task

Select the account for installing Network Agent using the tools of the operating system. In this case, administrator rights are required for computer access. You can add multiple accounts. If an account does not have sufficient rights, the Installation Wizard uses the next account. If you install Kaspersky Endpoint Security using Network Agent tools, you do not have to select an account.



Step 8. Configuring a task start schedule

Configure a schedule for starting a task, for example, manually or when the computer is idle.

Step 9. Defining the task name

Enter a name for the task, for example, `Install Kaspersky Endpoint Security 11.4.0 for Windows`.

Step 10. Finishing task creation

Exit the Wizard. If necessary, select the **Run task after Wizard finishes** check box. You can monitor the progress of the task in the task properties. The application will be installed in silent mode. After installation, the  icon will be added to the notification area of the user's computer. If the icon looks like this , make sure that you [activated the application](#).

1. In the main window of Web Console, select **Devices** → **Tasks**.

The list of tasks opens.

2. Click the **Add** button.

The Task Wizard starts. Follow the instructions of the Wizard.

Step 1. Configuring general task settings

Configure the general task settings:

1. In the **Application** drop-down list, select **Kaspersky Security Center**.

2. In the **Task type** drop-down list, select **Install application remotely**.

3. In the **Task name** field, enter a brief description, such as **Installation of Kaspersky Endpoint Security for Managers**.

4. In the **Devices to which the task will be assigned** section, select the task scope.

Step 2. Selecting computers for installation

At this step, select the computers on which Kaspersky Endpoint Security will be installed according to the selected task scope option.

Step 3. Configuring an installation package

At this step configure the settings of the installation package:

1. Select the Kaspersky Endpoint Security for Windows (11.4.0) installation package.

2. Select the Network Agent installation package.

The selected version of Network Agent will be installed together with Kaspersky Endpoint Security. *Network Agent* facilitates interaction between the Administration Server and a client computer. If Network Agent is already installed on the computer, it is not installed again.

3. In the **Force download of the installation package** section, select the application installation method:

- **Using Network Agent.** If Network Agent has not been installed on the computer, first Network Agent will be installed using the tools of the operating system. Then Kaspersky Endpoint Security is installed by the tools of Network Agent.
- **Using operating system resources through distribution points.** The installation package is delivered to client computers using operating system resources via distribution points. You can select this option if there is at least one distribution point in the network. For more details about distribution points, refer to [Kaspersky Security Center Help](#).
- **Using operating system resources through Administration Server.** Files will be delivered to client computers by using operating system resources through the Administration Server. You can select this



option if Network Agent is not installed on the client computer, but the client computer is in the same network as the Administration Server.

4. In the **Maximum number of simultaneous downloads** field, set a limit on the number of installation package download requests sent to the Administration Server. A limit on the number of requests will help prevent the network from being overloaded.
5. In the **Number of installation attempts** field, set a limit on the number of attempts to install the application. If installation of Kaspersky Endpoint Security ends with an error, the task will automatically start the installation again.
6. If necessary, clear the **Do not install application if it is already installed** check box. It allows, for example, to install one of the previous versions of the application.
7. If necessary, clear the **Check the operating system version before installation** check box. This lets you avoid downloading an application distribution package if the operating system of the computer does not meet the software requirements. If you are sure that the operating system of the computer meets the software requirements, you can skip this verification.
8. If necessary, select the **Assign package installation in Active Directory group policies** check box. Kaspersky Endpoint Security is installed by means of Network Agent or manually by means of Active Directory. To install Network Agent, the remote installation task must be run with domain administrator privileges.
9. If necessary, select the **Offer users to quit running applications** check box. Installation of Kaspersky Endpoint Security takes up computer resources. For the convenience of the user, the Application Installation Wizard prompts you to close running applications before starting the installation. This helps prevent disruptions in the operation of other applications and prevents possible malfunctions of the computer.
10. In the **Behavior of devices managed by this Server** section, select the Kaspersky Endpoint Security installation method. If the network has more than one Administration Server installed, these Administration Servers may see the same client computers. This may cause, for example, an application to be installed remotely on the same client computer several times through different Administration Servers, or other conflicts.

Step 4. Selecting the account to run the task

Select the account for installing Network Agent using the tools of the operating system. In this case, administrator rights are required for computer access. You can add multiple accounts. If an account does not have sufficient rights, the Installation Wizard uses the next account. If you install Kaspersky Endpoint Security using Network Agent tools, you do not have to select an account.

Step 5. Completing task creation

Finish the wizard by clicking the **Finish** button. A new task will be displayed in the list of tasks. To run a task, select the check box opposite the task and click the **Start** button. The application will be installed in silent mode. After installation, the  icon will be added to the notification area of the user's computer. If the icon looks like this , make sure that you [activated the application](#).

Installing the application locally using the Wizard

The interface of the application Setup Wizard consists of a sequence of windows corresponding to the application installation steps.

To install the application or upgrade the application from a previous version using the Setup Wizard:

1. Copy the [distribution kit](#) folder to the user's computer.
2. Run setup_kes.exe.

The Setup Wizard starts.

Preparing for installation

Before installing Kaspersky Endpoint Security on a computer or upgrading it from a previous version, the following conditions are checked:

- Presence of installed incompatible software (the list of incompatible software is available in the incompatible.txt file that is included in the [distribution kit](#)).
- Whether or not the [hardware and software requirements](#) are met.
- Whether or not the user has the rights to install the software product.

If any one of the previous requirements is not met, a relevant notification is displayed on the screen.

If the computer meets the listed requirements, the Setup Wizard searches for Kaspersky applications that could lead to conflicts when running at the same time as the application being installed. If such applications are found, you are prompted to remove them manually.

If the detected applications include previous versions of Kaspersky Endpoint Security, all data that can be migrated (such as activation data and application settings) is retained and used during the installation of Kaspersky Endpoint Security 11.4.0 for Windows, and the previous version of the application is automatically removed. This applies to the following application versions:

- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 for Windows (build 10.2.6.3733).
- Kaspersky Endpoint Security 10 Service Pack 2 for Windows (build 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 for Windows (build 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 for Windows (build 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 for Windows (build 10.3.3.275).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 for Windows (build 10.3.3.304).
- Kaspersky Endpoint Security 11.0.0 for Windows (build 11.0.0.6499).
- Kaspersky Endpoint Security 11.0.1 for Windows (build 11.0.190).
- Kaspersky Endpoint Security 11.0.1 for Windows SF1 (build 11.0.190).
- Kaspersky Endpoint Security 11.1.0 for Windows (build 11.1.0.15919).
- Kaspersky Endpoint Security 11.1.1 for Windows (build 11.1.1.126).

- Kaspersky Endpoint Security 11.2.0 for Windows (build 11.2.0.2254).
- Kaspersky Endpoint Security 11.3.0 for Windows (build 11.3.0.773).

Kaspersky Endpoint Security components

During the installation process, you can select the components of Kaspersky Endpoint Security that you want to install. The File Threat Protection component is a mandatory component that must be installed. You cannot cancel its installation.

By default, all application components are selected for installation except the following components:

- [BadUSB Attack Prevention](#).
- [File Level Encryption](#).
- [Full Disk Encryption](#).
- [BitLocker Management](#).
- [Endpoint Agent](#). *Endpoint Agent* installs Kaspersky Endpoint Agent for interaction between the application and [Kaspersky solutions](#) for detecting advanced threats (for example, Kaspersky Sandbox).

You can [change the available application components after the application is installed](#). To do so, you need to run the Setup Wizard again and choose to change the available components.

Advanced settings

Protect the application installation process. Installation protection includes protection against replacement of the distribution package with malicious applications, blocking access to the installation folder of Kaspersky Endpoint Security, and blocking access to the system registry section containing application keys. However, if the application cannot be installed (for example, when performing remote installation with the help of Windows Remote Desktop), you are advised to disable protection of the installation process.

Ensure compatibility with Citrix PVS. You can enable support of Citrix Provisioning Services to install Kaspersky Endpoint Security to a virtual machine.

Add application location to environment variable %PATH%. You can add the installation path to the %PATH% variable for convenient [use of the command line interface](#).

Installing the application from the command line

Kaspersky Endpoint Security can be installed from the command line in one of the following modes:

- In interactive mode by using the Application Setup Wizard.
- In silent mode. After installation is started in silent mode, your involvement in the installation process is not required. To install the application in silent mode, use the /s and /qn keys.

Prior to installing the application in silent mode, please open and read the End User License Agreement and the text of the Privacy Policy. The End User License Agreement and the text of the Privacy Policy are included in the [Kaspersky Endpoint Security distribution kit](#). You may proceed to install the application only if you have fully read, understand, and accept the provisions and terms of the End User License Agreement, you understand and agree that your data will be processed and transmitted (including to third-party countries) in accordance with the Privacy Policy, and you have fully read and understand the Privacy Policy. If you do not accept the provisions and terms of the End User License Agreement and the Privacy Policy, please do not install or use Kaspersky Endpoint Security.

To install the application or upgrade a previous version of the application:

1. Run the command line interpreter (cmd.exe) as an administrator.
2. Go to the folder where the Kaspersky Endpoint Security distribution package is located.
3. Run the following command:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pALLOWREBOOT=1|0]
[/pSKIPPRODUCTCHECK=1|0] [/pSKIPPRODUCTUNINSTALL=1|0] [/pKLLOGIN=<user name>
/pKLPASSWD=<password> /pKLPASSWDAREA=<password scope>] [/pENABLETRACES=1|0
/pTRACESLEVEL=<tracing level>] [/s]
```

or

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0]
[ALLOWREBOOT=1|0] [SKIPPRODUCTCHECK=1|0] [SKIPPRODUCTUNINSTALL=1|0] [KLLOGIN=<user
name> KLPASSWD=<password> KLPASSWDAREA=<password scope>] [ENABLETRACES=1|0 TRACESLEVEL=
<tracing level>] [/qn]
```

<p>EULA=1</p>	<p>Acceptance of the terms of the End User License Agreement. The text of the License Agreement is included in the distribution kit of Kaspersky Endpoint Security.</p> <div data-bbox="588 1263 1493 1420" style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Accepting the terms of the End User License Agreement is necessary for installing the application or upgrading the application version.</p> </div>
<p>PRIVACYPOLICY=1</p>	<p>Acceptance of the Privacy Policy. The text of the Privacy Policy is included in the Kaspersky Endpoint Security distribution kit.</p> <div data-bbox="588 1592 1493 1718" style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>To install the application or upgrade the application version, you must accept the Privacy Policy.</p> </div>
<p>KSN</p>	<p>Agreement or refusal to participate in Kaspersky Security Network (KSN). If no value is set for this parameter, Kaspersky Endpoint Security will prompt to confirm your consent or refusal to participate in KSN when Kaspersky Endpoint Security is first started. Available values:</p> <ul style="list-style-type: none"> • 1 – agreement to participate in KSN. • 0 – refusal to participate in KSN (default value).

	<p>The Kaspersky Endpoint Security distribution package is optimized for use with Kaspersky Security Network. If you opted not to participate in Kaspersky Security Network, you should update Kaspersky Endpoint Security immediately after the installation is complete.</p>
ALLOWREBOOT=1	<p>Automatic restart of the computer, if required after installation or upgrade of the application. If no value is set for this parameter, automatic computer restart is blocked.</p> <p>Restart is not required when installing Kaspersky Endpoint Security. Restart is required only if you have to remove incompatible applications prior to installation. Restart may also be required when updating the application version.</p>
SKIPPRODUCTCHECK=1	<p>Disabling checking for incompatible software. The list of incompatible software is available in the incompatible.txt file that is included in the distribution kit. If no value is set for this parameter and incompatible software is detected, the installation of Kaspersky Endpoint Security will be terminated.</p>
SKIPPRODUCTUNINSTALL=1	<p>Disable automatic removal of detected incompatible software. If no value is set for this parameter, Kaspersky Endpoint Security attempts to remove incompatible software.</p>
KLLOGIN	<p>Set the user name for accessing the features and settings of Kaspersky Endpoint Security (the Password protection component). The user name is set together with the KLPASSWD and KLPASSWDAREA parameters. The user name KLAdmin is used by default.</p>
KLPASSWD	<p>Specify a password for accessing Kaspersky Endpoint Security features and settings (the password is specified together with the KLLOGIN and KLPASSWDAREA parameters).</p> <p>If you specified a password but did not specify a user name with the KLLOGIN parameter, the KLAdmin user name is used by default.</p>
KLPASSWDAREA	<p>Specify the scope of the password for accessing Kaspersky Endpoint Security. When a user attempts to perform an action that is included in this scope, Kaspersky Endpoint Security prompts for the user's account credentials (KLLOGIN and KLPASSWD parameters). Use the ";" character to specify multiple values. Available values:</p> <ul style="list-style-type: none"> • SET – modifying application settings. • EXIT – exiting the application. • DISPROTECT – disabling protection components and stopping scan tasks. • DISPOLICY – disabling Kaspersky Security Center policy. • UNINST – removing the application from the computer. • DISCTRL – disabling control components. • REMOVELIC – removing the key. • REPORTS – viewing reports.

ENABLETRACES	<p>Enabling or disabling application traces. After Kaspersky Endpoint Security starts, it saves trace files in the folder %ProgramData%/Kaspersky Lab. Available values:</p> <ul style="list-style-type: none"> • 1 – traces are enabled. • 0 – traces are disabled (default value).
TRACESLEVEL	<p>Level of detail of traces. Available values:</p> <ul style="list-style-type: none"> • 100 (critical). Only messages about fatal errors. • 200 (high). Messages about all errors, including fatal errors. • 300 (diagnostic). Messages about all errors, as well as warnings. • 400 (important). All error messages, warnings, and additional information. • 500 (normal). Messages about all errors and warnings, as well as detailed information about the operation of the application in normal mode (default). • 600 (low). All messages.
AMPPL	<p>Enables or disables protection of the Kaspersky Endpoint Security processes using AM-PPL technology (Antimalware Protected Process Light). For more details about AM-PPL technology, please visit the Microsoft website.</p> <p>AM-PPL technology is available for Windows 10 version 1703 (RS2) or later, and Windows Server 2019 operating systems.</p> <p>Available values:</p> <ul style="list-style-type: none"> • 1 – protection of the Kaspersky Endpoint Security processes using AM-PPL technology is enabled. • 0 – protection of the Kaspersky Endpoint Security processes using AM-PPL technology is disabled.
RESTAPI	<p>Managing the application through the REST API. To manage the application through the REST API, you must specify the user name (RESTAPI_User parameter).</p> <p>Available values:</p> <ul style="list-style-type: none"> • 1 – management via REST API is allowed. • 0 – management via REST API is blocked (default value). To manage the application through the REST API, management using administrative systems must be allowed. To do so, set the AdminKitConnector=1 parameter. If you manage the application through the REST API, it is impossible to manage the application using the administration systems of Kaspersky.
RESTAPI_User	<p>User name of the Windows domain account used for managing the application through the REST API. Management of the application through the REST API is available only to this user. Enter the user name in</p>

	<p>the format <DOMAIN>\<UserName> (for example, RESTAPI_User=COMPANY\Administrator). You can select only one user to work with the REST API.</p> <p>Adding a user name is a prerequisite for managing the application through the REST API.</p>
RESTAPI_Port	Port used for managing the application through the REST API. Port 6782 is used by default.
ADMINKITCONNECTOR	<p>Application management using administration systems. Administration systems include, for example, Kaspersky Security Center. In addition to Kaspersky administration systems, you can use third-party solutions. Kaspersky Endpoint Security provides an API for this purpose.</p> <p>Available values:</p> <ul style="list-style-type: none"> • 1 – application management with the help of administration systems is allowed (default value). • 0 – application management is allowed only through the local interface.

Example:

```

setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pALLOWREBOOT=1

msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1
KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn

setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pENABLETRACES=1 /pTRACESLEVEL=600 /s

```

After Kaspersky Endpoint Security is installed, the trial license is activated unless you provided an activation code in the [setup.ini file](#). A trial license usually has a short term. When the trial license expires, all Kaspersky Endpoint Security features become disabled. To continue using the application, you need to activate the application with a commercial license by using the [Application Activation Wizard](#) or a [special command](#).

When installing the application or upgrading the application version in silent mode, use of the following files is supported:

- [setup.ini](#) – general settings for application installation
- [install.cfg](#) – settings of Kaspersky Endpoint Security operation
- setup.reg – registry keys

Registry keys from the setup.reg file are written to the registry only if the setup.reg value is set for the SetupReg parameter in the setup.ini file. The setup.reg file is generated by Kaspersky experts. It is not recommended to modify the contents of this file.

To apply settings from the setup.ini, install.cfg, and setup.reg files, place these files into the folder containing the Kaspersky Endpoint Security distribution package.

Remotely installing the application using System Center Configuration Manager

These instructions apply to System Center Configuration Manager 2012 R2.

To remotely install an application using System Center Configuration Manager:

1. Open the Configuration Manager console.
2. In the right part of the console, in the **App management** section, select **Packages**.
3. In the upper part of the console in the control panel, click the **Create package** button.

This starts the *New Package and Application Wizard*.

4. In the New Package and Application Wizard:

a. In the **Package** section:

- In the **Name** field, enter the name of the installation package.
- In the **Source folder** field, specify the path to the folder containing the distribution kit of Kaspersky Endpoint Security.

b. In the **Application type** section, select the **Standard application** option.

c. In the **Standard application** section:

- In the **Name** field, enter the unique name for the installation package (for example, the application name including the version).
- In the **Command line** field, specify the Kaspersky Endpoint Security installation options from the command line.
- Click the **Browse** button to specify the path to the executable file of the application.
- Make sure that the **Execution mode** list has the **Run with administrator rights** item selected.

d. In the **Requirements** section:

- Select the **Start another application first** check box if you want a different application to be started before installing Kaspersky Endpoint Security.
Select the application from the **Application** drop-down list or specify the path to the executable file of this application by clicking the **Browse** button.
- Select the **This application can be started only on the specified platforms** option in the **Platform requirements** section if you want the application to be installed only in the specified operating systems.
In the list below, select the check boxes opposite the operating systems in which Kaspersky Endpoint Security will be installed.

This step is optional.

e. In the **Summary** section, check all entered values of the settings and click **Next**.

The created installation package will appear in the **Packages** section in the list of available installation packages.

5. In the context menu of the installation package, select **Deploy**.

This starts the *Deployment Wizard*.

6. In the Deployment Wizard:

a. In the **General** section:

- In the **Software** field, enter the unique name of the installation package or select the installation package from the list by clicking the **Browse** button.
- In the **Collection** field, enter the name of the collection of computers on which the application will be installed, or select the collection by clicking the **Browse** button.

b. In the **Contains** section, add distribution points (for more detailed information, please refer to the help documentation for System Center Configuration Manager).

c. If required, specify the values of other settings in the Deployment Wizard. These settings are optional for remote installation of Kaspersky Endpoint Security.

d. In the **Summary** section, check all entered values of the settings and click **Next**.

After the Deployment Wizard finishes, a task will be created for remote installation of Kaspersky Endpoint Security.

Description of setup.ini file installation settings

The setup.ini file is used when installing the application from the command line or when using the Group Policy Editor of Microsoft Windows. To apply settings from the setup.ini file, place this file into the folder containing the Kaspersky Endpoint Security distribution package.



[DOWNLOAD THE SETUP.INI FILE](#)

The setup.ini file consists of the following sections:

- **[Setup]** – general settings of application installation.
- **[Components]** – selection of application components to be installed. If none of the components are specified, all components that are available for the operating system are installed. File Threat Protection is a mandatory component and is installed on the computer regardless of which settings are indicated in this section.
- **[Tasks]** – selection of tasks to be included in the list of Kaspersky Endpoint Security tasks. If no task is specified, all tasks are included in the task list of Kaspersky Endpoint Security.

The alternatives to the value 1 are the values **yes**, **on**, **enable**, and **enabled**.

The alternatives to the value 0 are the values **no**, **off**, **disable**, and **disabled**.

Section	Parameter	Description
[Setup]	InstallDir	Path to the application installation folder.
	ActivationCode	Kaspersky Endpoint Security activation code.
	EULA=1	<p>Acceptance of the terms of the End User License Agreement. The text of the License Agreement is included in the distribution kit of Kaspersky Endpoint Security.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Accepting the terms of the End User License Agreement is necessary for installing the application or upgrading the application version.</p> </div>
	PrivacyPolicy=1	<p>Acceptance of the Privacy Policy. The text of the Privacy Policy is included in the Kaspersky Endpoint Security distribution kit.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>To install the application or upgrade the application version, you must accept the Privacy Policy.</p> </div>
	KSN	<p>Agreement or refusal to participate in Kaspersky Security Network (KSN). If no value is set for this parameter, Kaspersky Endpoint Security will prompt to confirm your consent or refusal to participate in KSN when Kaspersky Endpoint Security is first started. Available values:</p> <ul style="list-style-type: none"> • 1 – agreement to participate in KSN. • 0 – refusal to participate in KSN (default value). The Kaspersky Endpoint Security distribution package is optimized for use with Kaspersky Security Network. If you opted not to participate in Kaspersky Security Network, you should update Kaspersky Endpoint Security immediately after the installation is complete.
	Login	<p>Set the user name for accessing the features and settings of Kaspersky Endpoint Security (the Password protection component). The user name is set together with the Password and PasswordArea parameters. The user name KAdmin is used by default.</p>
	Password	<p>Specify a password for accessing Kaspersky Endpoint Security features and settings (the password is specified together with the Login and PasswordArea parameters).</p> <p>If you specified a password but did not specify a user name with the Login parameter, the KAdmin user name is used by default.</p>
	PasswordArea	Specify the scope of the password for accessing

		<p>Kaspersky Endpoint Security. When a user attempts to perform an action that is included in this scope, Kaspersky Endpoint Security prompts for the user's account credentials (Login and Password parameters). Use the ";" character to specify multiple values. Available values:</p> <ul style="list-style-type: none"> • SET – modifying application settings. • EXIT – exiting the application. • DISPROTECT – disabling protection components and stopping scan tasks. • DISPOLICY – disabling Kaspersky Security Center policy. • UNINST – removing the application from the computer. • DISCTRL – disabling control components. • REMOVELIC – removing the key. • REPORTS – viewing reports.
	SelfProtection	<p>Enabling or disabling the application installation protection mechanism. Available values:</p> <ul style="list-style-type: none"> • 1 – the application installation protection mechanism is enabled (default value). • 0 – the application installation protection mechanism is disabled. <p>Installation protection includes protection against replacement of the distribution package with malicious applications, blocking access to the installation folder of Kaspersky Endpoint Security, and blocking access to the system registry section containing application keys. However, if the application cannot be installed (for example, when performing remote installation with the help of Windows Remote Desktop), you are advised to disable protection of the installation process.</p>
	Reboot=1	<p>Automatic restart of the computer, if required after installation or upgrade of the application. If no value is set for this parameter, automatic computer restart is blocked.</p> <p>Restart is not required when installing Kaspersky Endpoint Security. Restart is required only if you have to remove incompatible applications prior to installation. Restart may also be required when updating the application version.</p>
	AddEnvironment	<p>In the %PATH% system variable, add the path to</p>

		<p>executable files located in the Kaspersky Endpoint Security setup folder. Available values:</p> <ul style="list-style-type: none"> • 1 – the %PATH% system variable is supplemented with the path to executable files that are located in the Kaspersky Endpoint Security setup folder. • 0 – the %PATH% system variable is not supplemented with the path to executable files that are located in the Kaspersky Endpoint Security setup folder.
	AMPPL	<p>Enables or disables protection of the Kaspersky Endpoint Security processes using AM-PPL technology (Antimalware Protected Process Light). For more details about AM-PPL technology, please visit the Microsoft website.</p> <p>AM-PPL technology is available for Windows 10 version 1703 (RS2) or later, and Windows Server 2019 operating systems.</p> <p>Available values:</p> <ul style="list-style-type: none"> • 1 – protection of the Kaspersky Endpoint Security processes using AM-PPL technology is enabled. • 0 – protection of the Kaspersky Endpoint Security processes using AM-PPL technology is disabled.
	SetupReg	<p>Enable writing of registry keys from the setup.reg file to the registry. SetupReg: setup.reg parameter value.</p>
	EnableTraces	<p>Enabling or disabling application traces. After Kaspersky Endpoint Security starts, it saves trace files in the folder %ProgramData%/Kaspersky Lab. Available values:</p> <ul style="list-style-type: none"> • 1 – traces are enabled. • 0 – traces are disabled (default value).
	TracesLevel	<p>Level of detail of traces. Available values:</p> <ul style="list-style-type: none"> • 100 (critical). Only messages about fatal errors. • 200 (high). Messages about all errors, including fatal errors. • 300 (diagnostic). Messages about all errors, as well as warnings. • 400 (important). All error messages, warnings, and additional information. • 500 (normal). Messages about all errors and warnings, as well as detailed information about the operation of the application in normal mode (default). • 600 (low). All messages.

	RESTAPI	<p>Managing the application through the REST API. To manage the application through the REST API, you must specify the user name (RESTAPI_User parameter).</p> <p>Available values:</p> <ul style="list-style-type: none"> • 1 – management via REST API is allowed. • 0 – management via REST API is blocked (default value). <p>To manage the application through the REST API, management using administrative systems must be allowed. To do so, set the AdminKitConnector=1 parameter. If you manage the application through the REST API, it is impossible to manage the application using the administration systems of Kaspersky.</p>
	RESTAPI_User	<p>User name of the Windows domain account used for managing the application through the REST API. Management of the application through the REST API is available only to this user. Enter the user name in the format <DOMAIN>\<UserName> (for example, RESTAPI_User=COMPANY\Administrator). You can select only one user to work with the REST API.</p> <p>Adding a user name is a prerequisite for managing the application through the REST API.</p>
	RESTAPI_Port	<p>Port used for managing the application through the REST API. Port 6782 is used by default.</p>
[Components]	ALL	<p>Installation of all components. If the parameter value 1 is specified, all components will be installed regardless of the installation settings of individual components.</p>
	MailThreatProtection	<p>Mail Threat Protection.</p>
	WebThreatProtection	<p>Web Threat Protection.</p>
	AMSI	<p>AMSI Protection Provider.</p>
	HostIntrusionPrevention	<p>Host Intrusion Prevention.</p>
	BehaviorDetection	<p>Behavior Detection.</p>
	ExploitPrevention	<p>Exploit Prevention.</p>
	RemediationEngine	<p>Remediation Engine.</p>
	Firewall	<p>Firewall.</p>
	NetworkThreatProtection	<p>Network Threat Protection.</p>
	WebControl	<p>Web Control.</p>
	DeviceControl	<p>Device Control.</p>
	ApplicationControl	<p>Application Control.</p>
	AdaptiveAnomaliesControl	<p>Adaptive Anomaly Control.</p>
	FileEncryption	<p>File Level Encryption libraries.</p>

	DiskEncryption	Full Disk Encryption libraries.
	BadUSBAttackPrevention	BadUSB Attack Prevention.
	AntiAPT	Endpoint Agent. <i>Endpoint Agent</i> installs Kaspersky Endpoint Agent for interaction between the application and Kaspersky solutions for detecting advanced threats (for example, Kaspersky Sandbox).
	AdminKitConnector	Application management using administration systems. Administration systems include, for example, Kaspersky Security Center. In addition to Kaspersky administration systems, you can use third-party solutions. Kaspersky Endpoint Security provides an API for this purpose. Available values: <ul style="list-style-type: none"> • 1 – application management with the help of administration systems is allowed (default value). • 0 – application management is allowed only through the local interface.
[Tasks]	ScanMyComputer	Full Scan task. Available values: <ul style="list-style-type: none"> • 1 – the task is included in the list of Kaspersky Endpoint Security tasks. • 0 – the task is not included in the list of Kaspersky Endpoint Security tasks.
	ScanCritical	Critical Areas Scan task. Available values: <ul style="list-style-type: none"> • 1 – the task is included in the list of Kaspersky Endpoint Security tasks. • 0 – the task is not included in the list of Kaspersky Endpoint Security tasks.
	Updater	Update task. Available values: <ul style="list-style-type: none"> • 1 – the task is included in the list of Kaspersky Endpoint Security tasks. • 0 – the task is not included in the list of Kaspersky Endpoint Security tasks.

Change application components

During installation of the application, you can select the components that will be available. You can change the available application components in the following ways:

- Locally, by using the Setup Wizard.

Application components are changed by using the normal method for a Windows operating system, which is through the Control Panel. Run the Application Setup Wizard and select the option to change the application components that are available. Follow the instructions on the screen.

- Remotely through Kaspersky Security Center.

The *Change application components* task allows you to change the components of Kaspersky Endpoint Security after the application is installed.

Please take into account the following special considerations when changing the application components:

- On computers running Windows Server, you cannot [install all components of Kaspersky Endpoint Security](#) (for example, the Adaptive Anomaly Control component is not available).
- If the hard drives on your computer are protected by [Full Disk Encryption \(FDE\)](#), you cannot remove the Full Disk Encryption component. To remove the Full Disk Encryption component, decrypt all the hard drives of the computer.
- If the computer has [encrypted files \(FLE\)](#) or the user uses [encrypted removable drives \(FDE or FLE\)](#), it will be impossible to access the files and removable drives after the Data Encryption components are removed. You can access the files and removable drives by reinstalling the Data Encryption components.

[How to add or remove application components in the Administration Console \(MMC\)](#) 

1. In the Administration Console, go to the folder **Administration Server** → **Tasks**.

The list of tasks opens.

2. Click the **New task** button.

The Task Wizard starts. Follow the instructions of the Wizard.

Step 1. Selecting task type

Select **Kaspersky Endpoint Security for Windows (11.4.0)** → **Change application components**.

Step 2. Task settings for changing application components

Select the application components that will be available on the user's computer.

Select the **Remove incompatible third-party applications** check box. The list of incompatible applications can be viewed in `incompatible.txt`, which is included in the [distribution kit](#). If incompatible applications are installed on the computer, installation of Kaspersky Endpoint Security ends with an error.

If necessary, enable [password protection](#) for task performance:

1. Click the **Additional** button.

2. Select the **Use password for modifying the set of application components** check box.

3. Enter the KLAdmin user account credentials.

Step 3. Selecting the devices to which the task will be assigned

Select the computers on which the task will be performed. The following options are available:

- Assign the task to an administration group. In this case, the task is assigned to computers included in a previously created administration group.
- Select computers detected by the Administration Server in the network: *unassigned devices*. The specific devices can include devices in administration groups as well as unassigned devices.
- Specify device addresses manually, or import addresses from a list. You can specify NetBIOS names, IP addresses, and IP subnets of devices to which you want to assign the task.

Step 4. Configuring a task start schedule

Configure a schedule for starting a task, for example, manually or when the computer is idle.

Step 5. Defining the task name

Enter a name for the task, for example, `Add the Application Control component`.

Step 6. Completing task creation

Exit the Wizard. If necessary, select the **Run task after Wizard finishes** check box. You can monitor the progress of the task in the task properties.

As a result, the set of Kaspersky Endpoint Security components on users' computers will be changed in silent mode. The settings of available components will be displayed in the local interface of the application. The components that were not included in the application are disabled, and the settings of these components are not available.

[How to add or remove application components in the Web Console and Cloud Console](#) 

1. In the main window of Web Console, select **Devices** → **Tasks**.

The list of tasks opens.

2. Click the **Add** button.

The Task Wizard starts. Follow the instructions of the Wizard.

Step 1. Configuring general task settings

Configure the general task settings:

1. In the **Application** drop-down list, select **Kaspersky Endpoint Security for Windows (11.4.0)**.

2. In the **Task type** drop-down list, select **Change application components**.

3. In the **Task name** field, enter a brief description, for example, **Add the Application Control component**.

4. In the **Select devices to which the task will be assigned** section, select the task scope.

Step 2. Selecting the devices to which the task will be assigned

Select the computers on which the task will be performed. For example, select a separate administration group or build a selection.

Step 3. Completing task creation

Select the **Open task properties window after task creation** check box and finish the Wizard. In the task properties, select the **Application Settings** tab and select the application components that will be available.

If necessary, enable [password protection](#) for task performance:

1. In the **Advanced Settings** section, select the **Use password for modifying the set of application components** check box.

2. Enter the KAdmin user account credentials.

Save the changes and run the task.

As a result, the set of Kaspersky Endpoint Security components on users' computers will be changed in silent mode. The settings of available components will be displayed in the local interface of the application. The components that were not included in the application are disabled, and the settings of these components are not available.

Upgrading from a previous version of the application

When you update a previous version of the application to a newer version, consider the following:

- Kaspersky Endpoint Security 11.4.0 for Windows is compatible with Kaspersky Security Center 12.
- We recommend quitting all active applications before starting the update.
- If the computer has hard drives that are encrypted using [Full Disk Encryption \(FDE\)](#), then you need to decrypt all encrypted hard drives to upgrade Kaspersky Endpoint Security from version 10 to version 11.0.0 or later.

Before updating, Kaspersky Endpoint Security blocks the Full Disk Encryption functionality. If Full Disk Encryption could not be locked, the upgrade installation will not start. After updating the application, the Full Disk Encryption functionality will be restored.

Kaspersky Endpoint Security supports updates for the following versions of the application:

- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 for Windows (build 10.2.6.3733).
- Kaspersky Endpoint Security 10 Service Pack 2 for Windows (build 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 for Windows (build 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 for Windows (build 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 for Windows (build 10.3.3.275).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 for Windows (build 10.3.3.304).
- Kaspersky Endpoint Security 11.0.0 for Windows (build 11.0.0.6499).
- Kaspersky Endpoint Security 11.0.1 for Windows (build 11.0.1.90).
- Kaspersky Endpoint Security 11.0.1 for Windows SF1 (build 11.0.1.90).
- Kaspersky Endpoint Security 11.1.0 for Windows (build 11.1.0.15919).
- Kaspersky Endpoint Security 11.1.1 for Windows (build 11.1.1.126).
- Kaspersky Endpoint Security 11.2.0 for Windows (build 11.2.0.2254).
- Kaspersky Endpoint Security 11.3.0 for Windows (build 11.3.0.773).

When updating Kaspersky Endpoint Security 10 Service Pack 2 for Windows to Kaspersky Endpoint Security 11.4.0 for Windows, the files that were placed in Backup or Quarantine in the previous version of the application will be transferred to Backup in the new version of the application. For versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows, files that were placed in Backup and Quarantine in a previous version of the application are not migrated to the newer version.

Kaspersky Endpoint Security can be updated on the computer in the following ways:

- locally, by using the [Setup Wizard](#).
- locally from the [command line](#).
- remotely through [Kaspersky Security Center 12](#).

- remotely through the Microsoft Windows Group Policy Management Editor (for more details, see [Microsoft Technical Support website](#)).
- remotely, by using the [System Center Configuration Manager](#).

If the application that is deployed in the corporate network features a set of components other than the default set, updating the application through the Administration Console (MMC) is different from updating the application through the Web Console and Cloud Console. When you update Kaspersky Endpoint Security, consider the following:

- Kaspersky Security Center Web Console or Kaspersky Security Center Cloud Console.

If you created an installation package for the new version of the application with the default set of components, then the set of components on a user's computer will not be changed. To use Kaspersky Endpoint Security with the default set of components, you need to [open the installation package properties](#), change the set of components, then revert to the original set of components and save the changes.

- Kaspersky Security Center Administration Console (MMC).

The set of application components after the update will match the set of components in the installation package. That is, if the new version of the application has the default set of components, then, for example, BadUSB Attack Prevention will be removed from the computer, since this component is excluded from the default set. To continue using the application with the same set of components as before the update, select the required components in the [installation package settings](#).

Removing the application

Removing Kaspersky Endpoint Security leaves the computer and user data unprotected against threats.

Kaspersky Endpoint Security can be uninstalled from the computer in the following ways:

- locally, by using the [Setup Wizard](#);
- locally from the [command line](#);
- remotely, by using Kaspersky Security Center (refer to the [Kaspersky Security Center Help](#) for more information);
- remotely through the Microsoft Windows Group Policy Management Editor (for more details, see [Microsoft Technical Support website](#)).

Uninstalling through Kaspersky Security Center

You can remotely uninstall the application by using the *Uninstall application remotely* task. When performing the task, Kaspersky Endpoint Security downloads the application uninstall utility to the user's computer. After completing uninstallation of the application, the utility will be automatically removed.

[How to remove the application through the Administration Console \(MMC\)](#)

1. In the Administration Console, go to the folder **Administration Server** → **Tasks**.

The list of tasks opens.

2. Click the **New task** button.

The Task Wizard starts. Follow the instructions of the Wizard.

Step 1. Selecting task type

Select **Kaspersky Security Center Administration Server** → **Additional** → **Uninstall application remotely**.

Step 2. Selecting the application to be removed

Select **Uninstall application supported by Kaspersky Security Center**.

Step 3. Task settings for application uninstallation

Select **Kaspersky Endpoint Security for Windows (11.4.0)**.

Step 4. Uninstall utility settings

Configure the following additional application settings:

- **Force download of the uninstall utility.** Select the utility delivery method:
 - **Using Network Agent.** If Network Agent has not been installed on the computer, first Network Agent will be installed using the tools of the operating system. Kaspersky Endpoint Security is then uninstalled by the tools of Network Agent.
 - **Using Microsoft Windows resources by means of Administration Server.** The utility will be delivered to client computers by using operating system resources through the Administration Server. You can select this option if Network Agent is not installed on the client computer, but the client computer is in the same network as the Administration Server.
 - **Using operating system resources through distribution points.** The utility is delivered to client computers using operating system resources via distribution points. You can select this option if there is at least one distribution point in the network. For more details about distribution points, *refer to [Kaspersky Security Center Help](#)*.
- **Verify operating system version before downloading.** If necessary, clear this check box. This lets you avoid downloading the uninstall utility if the operating system of the computer does not meet the software requirements. If you are sure that the operating system of the computer meets the software requirements, you can skip this verification.

If the application uninstallation operation is [password protected](#), do the following:

1. Select the **Use uninstall password** check box.

2. Click the **Edit** button.

3. Enter the KLAdmin account password.

Step 5. Selecting the operating system restart setting

After uninstalling the application, a restart is required. Select the action that will be performed to restart the computer.

Step 6. Selecting the devices to which the task will be assigned

Select the computers on which the task will be performed. The following options are available:

- Assign the task to an administration group. In this case, the task is assigned to computers included in a previously created administration group.
- Select computers detected by the Administration Server in the network: *unassigned devices*. The specific devices can include devices in administration groups as well as unassigned devices.
- Specify device addresses manually, or import addresses from a list. You can specify NetBIOS names, IP addresses, and IP subnets of devices to which you want to assign the task.

Step 7. Selecting the account to run the task

Select the account for installing Network Agent using the tools of the operating system. In this case, administrator rights are required for computer access. You can add multiple accounts. If an account does not have sufficient rights, the Installation Wizard uses the next account. If you uninstall Kaspersky Endpoint Security using Network Agent tools, you do not have to select an account.

Step 8. Configuring a task start schedule

Configure a schedule for starting a task, for example, manually or when the computer is idle.

Step 9. Defining the task name

Enter a name for the task, for example, `Uninstall Kaspersky Endpoint Security 11.4.0`.

Step 10. Finishing task creation

Exit the Wizard. If necessary, select the **Run task after Wizard finishes** check box. You can monitor the progress of the task in the task properties.

The application will be uninstalled in silent mode.

[How to remove the application through the Web Console and Cloud Console](#) 

1. In the main window of Web Console, select **Devices** → **Tasks**.

The list of tasks opens.

2. Click the **Add** button.

The Task Wizard starts. Follow the instructions of the Wizard.

Step 1. Configuring general task settings

Configure the general task settings:

1. In the **Application** drop-down list, select **Kaspersky Security Center**.

2. In the **Task type** drop-down list, select **Uninstall application remotely**.

3. In the **Task name** field, enter a brief description, for example, **Uninstall Kaspersky Endpoint Security from Technical Support computers**.

4. In the **Select devices to which the task will be assigned** section, select the task scope.

Step 2. Selecting the devices to which the task will be assigned

Select the computers on which the task will be performed. For example, select a separate administration group or build a selection.

Step 3. Configuring application uninstallation settings

At this step, configure the application uninstallation settings:

1. Select **Remove managed application**.

2. Select **Kaspersky Endpoint Security for Windows (11.4.0)**.

3. **Force download of the uninstall utility**. Select the utility delivery method:

- **Using Network Agent**. If Network Agent has not been installed on the computer, first Network Agent will be installed using the tools of the operating system. Kaspersky Endpoint Security is then uninstalled by the tools of Network Agent.
- **Using Microsoft Windows resources by means of Administration Server**. The utility will be delivered to client computers by using operating system resources through the Administration Server. You can select this option if Network Agent is not installed on the client computer, but the client computer is in the same network as the Administration Server.
- **Using operating system resources through distribution points**. The utility is delivered to client computers using operating system resources via distribution points. You can select this option if there is at least one distribution point in the network. For more details about distribution points, *refer to [Kaspersky Security Center Help](#)*.

4. In the **Maximum number of simultaneous downloads** field, set a limit on the number of requests sent to the Administration Server to download the application uninstall utility. A limit on the number of requests will

help prevent the network from being overload.

5. In the **Number of uninstallation attempts** field, set a limit on the number of attempts to uninstall the application. If uninstallation of Kaspersky Endpoint Security ends with an error, the task will automatically start the uninstallation again.
6. If necessary, clear the **Check the operating system version before installation** check box. This lets you avoid downloading the uninstall utility if the operating system of the computer does not meet the software requirements. If you are sure that the operating system of the computer meets the software requirements, you can skip this verification.

Step 4. Selecting the account to run the task

Select the account for installing Network Agent using the tools of the operating system. In this case, administrator rights are required for computer access. You can add multiple accounts. If an account does not have sufficient rights, the Installation Wizard uses the next account. If you uninstall Kaspersky Endpoint Security using Network Agent tools, you do not have to select an account.

Step 5. Completing task creation

Finish the wizard by clicking the **Finish** button. A new task will be displayed in the list of tasks.

To run a task, select the check box opposite the task and click the **Start** button. The application will be uninstalled in silent mode. After uninstallation is complete, Kaspersky Endpoint Security shows a prompt to restart the computer.

If the application uninstallation operation is [password protected](#), enter the KLAdmin account password in the properties of the *Uninstall application remotely* task. Without the password, the task will not be performed.

To use the KLAdmin account password in the Uninstall application remotely task:

1. In the main window of Web Console, select **Devices** → **Tasks**.
The list of tasks opens.
2. Click the Kaspersky Security Center task **Uninstall application remotely**.
The task properties window opens.
3. Select the **Application settings** tab.
4. Select the **Use uninstall password** check box.
5. Enter the KLAdmin account password.
6. Click the **Save** button.

Uninstalling the application using the Wizard

Kaspersky Endpoint Security is removed using the normal method for a Windows operating system, which is through the Control Panel. The Setup Wizard starts. Follow the instructions on the screen.

You can specify which of the data that is used by the application you want to save for future use, during the next installation of the application (such as when upgrading to a newer version of the application). If you do not specify any data, the application will be completely removed.

You can save the following data:

- **Activation data**, which lets you avoid having to activate the application again. Kaspersky Endpoint Security automatically adds a license key if the license term has not expired prior to installation.
- **Backup files** – files that are scanned by the application and placed in Backup.

Backup files that are saved after removal of the application can be accessed only from the same version of the application that was used to save those files.

If you plan to use Backup objects after removal of the application, you must restore those objects before removing the application. However, Kaspersky experts do not recommend restoring objects from Backup because this may harm the computer.

- **Operational settings of the application** – values of application settings that are selected during application configuration.
- **Local storage of encryption keys** – data that provides access to files and drives that were encrypted before removal of the application. To ensure access to encrypted files and drives, make sure that you selected data encryption functionality when reinstalling Kaspersky Endpoint Security. No further action is required for access to previously encrypted files and drives.

Removing the application from the command line

Kaspersky Endpoint Security can be uninstalled from the command line in one of the following ways:

- In interactive mode by using the Application Setup Wizard.
- In silent mode. After uninstallation is started in silent mode, your involvement in the removal process is not required. To uninstall the application in silent mode, use the `/s` and `/qn` switches.

To uninstall the application in silent mode:

1. Run the command line interpreter (cmd.exe) as an administrator.
2. Go to the folder where the Kaspersky Endpoint Security distribution package is located.
3. Run the following command:

- If the removal process is not [password protected](#):
`setup_kes.exe /s /x`
or
`msiexec.exe /x <GUID> /qn`

<GUID> is the unique identifier of the application. You can find out the GUID of the application by using the following command:

```
wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber.
```

- If the removal process is [password protected](#):

```
setup_kes.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
```

or

```
msiexec.exe /x <GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
```

Example:

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin  
KLPASSWD=!Password1 /qn
```

Application licensing

This section provides information about general concepts related to application licensing.

About the End User License Agreement

The *End User License Agreement* is a binding agreement between you and AO Kaspersky Lab stipulating the terms on which you may use the application.

We recommend carefully reading the terms of the License Agreement before using the application.

You can view the terms of the License Agreement in the following ways:

- When [installing Kaspersky Endpoint Security in interactive mode](#).
- By reading the license.txt file. This document is included in the [application distribution kit](#) and is also located in the application installation folder %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Endpoint Security for Windows\Doc\

By confirming that you agree with the End User License Agreement when installing the application, you signify your acceptance of the terms of the End User License Agreement. If you do not accept the terms of the End User License Agreement, you must abort the installation.

About the license

A *license* is a time-limited right to use the application, granted under the End User License Agreement.

A valid license entitles you to the following kinds of services:

- Use of the application in accordance with the terms of the End User License Agreement
- Technical Support

The scope of services and application usage term depend on the type of license under which the application was activated.

The following license types are provided:

- *Trial* – a free license intended for trying out the application.

A trial license usually has a short term. When the trial license expires, all Kaspersky Endpoint Security features become disabled. To continue using the application, you must purchase a commercial license.

You can activate the application under a trial license only once.

- *Commercial* – a paid license that is provided when you purchase Kaspersky Endpoint Security.

Application functionality available under the commercial license depends on the choice of product. The selected product is indicated in the [License Certificate](#). Information on available products may be found at the [Kaspersky website](#).

When the commercial license expires, the application continues to work in limited functionality mode. You can use protection and control components and run a scan using the application databases that were installed before the license expired. The application also continues to encrypt files that had been modified and encrypted before license expiration, but does not encrypt new files. Use of Kaspersky Security Network is not available.

To continue using Kaspersky Endpoint Security in fully functional mode, you must renew your commercial license.

We recommend renewing the license before its expiration to ensure that your computer stays fully protected against threats.

About the license certificate

A *license certificate* is a document transferred to the user together with a key file or activation code.

The license certificate contains the following license information:

- License key or order number.
- Details of the user to whom the license is granted.
- Details of the application that can be activated using the license.
- Limitation on the number of licensed units (for example, the number of devices on which the application can be used under the license).
- License term start date.
- License expiration date or license term.
- License type.

About subscription

A *subscription for Kaspersky Endpoint Security* is a purchase order for the application with specific parameters (such as the subscription expiry date and number of devices protected). You can order a subscription for Kaspersky Endpoint Security from your service provider (such as your ISP). A subscription can be renewed manually or automatically, or you may cancel your subscription. You can manage your subscription on the website of the service provider.

Subscription can be limited (for one year, for example) or unlimited (without an expiry date). To keep Kaspersky Endpoint Security working after the limited subscription term expires, you need to renew your subscription. Unlimited subscription is renewed automatically if the vendor's services have been prepaid on time.

When a limited subscription expires, you may be provided a subscription renewal grace period during which the application continues to function. The availability and duration of such a grace period is decided by the service provider.

To use Kaspersky Endpoint Security under a subscription, you need to apply the [activation code](#) received from the service provider. After the activation code is applied, the active key is added. The active key determines the license for using the application under the subscription. It is not possible to add a reserve license key under a subscription.

Activation codes purchased under subscription may not be used to activate previous versions of Kaspersky Endpoint Security.

About license key

A *license key* is a sequence of bits that you can use to activate and then use the application in accordance with the terms of the End User License Agreement.

A [license certificate](#) is not provided for a key that is added under a subscription.

You can add a license key to the application by either applying a key file or entering an activation code.

The key can be blocked by Kaspersky if the terms of the End User License Agreement are violated. If the key has been blocked, you need to add a different key to continue using the application.

There are two types of keys: active and reserve.

An *active key* is a key that is currently used by the application. A trial or commercial license key can be added as the active key. The application cannot have more than one active key.

A *reserve key* is a key that entitles the user to use the application, but is not currently in use. At the expiry of the active key, a reserve key automatically becomes active. A reserve key can be added only if the active key is available.

A key for a trial license can be added only as an active key. It cannot be added as the reserve key. A trial license key cannot replace the active key to a commercial license.

If a key gets blacklisted, the application functionality defined by the [license under which the application has been activated](#) remains available for eight days. The application notifies that user that the key has been blacklisted. After eight days, application functionality becomes limited to the functionality level that is available after license expiry. You can use protection and control components and run a scan using the application databases that were installed before the license expired. The application also continues to encrypt files that had been modified and encrypted before license expiration, but does not encrypt new files. Use of Kaspersky Security Network is not available.

About activation code

An *activation code* is a unique sequence of 20 alphanumeric characters. You enter an activation code to add a license key that activates Kaspersky Endpoint Security. You receive an activation code at the email address you specified after purchasing Kaspersky Endpoint Security.

To activate the application with an activation code, Internet access is required to connect to Kaspersky activation servers.

When the application is activated using an activation code, the active key is added. A reserve license key can be added only by using an activation code and cannot be added using a key file.

If an activation code is lost after activating the application, you can restore the activation code. You may need an activation code, for example, to register a Kaspersky CompanyAccount. If the activation code was lost after the application activation, contact Kaspersky partner from whom you purchased the license.

About the key file

A *key file* is a file with the .key extension that you receive from Kaspersky. The purpose of a key file is to add a license key that activates the application.

You receive a key file at the email address that you provided when you purchased Kaspersky Endpoint Security or ordered the trial version of Kaspersky Endpoint Security.

You do not need to connect to Kaspersky activation servers in order to activate the application with a key file.

You can recover a key file if it has been accidentally deleted. You may need a key file to register a Kaspersky CompanyAccount, for example.

To recover a key file, do one of the following:

- Contact the license seller.
- Obtain a key file on the [Kaspersky website](#) based on your existing activation code.

When the application is activated using a key file, an active key is added. A reserve license key can be added only by using a key file and cannot be added using an activation code.

Activating the application

Activation is the process of activating a [license](#) that allows you to use a fully functional version of the application until the license expires. The application activation involves adding a [license key](#).

You can activate the application in one of the following ways:

- Locally from the application interface, by using the [Activation Wizard](#). You can add both the active key and the reserve key in this way.
- Remotely with the [Kaspersky Security Center software suite](#) by creating and then starting an add license key task. You can add both the active key and the reserve key in this way.
- Remotely by distributing key files and activation codes stored in the Kaspersky Security Center Administration Server key storage to client computers. For more details on distributing keys, *please refer to the [Kaspersky Security Center Help Guide](#)*. You can add both the active key and the reserve key in this way.

The activation code purchased under subscription is distributed in the first place.

- Using the [command line](#).

It may take some time for the application to be activated with an activation code (during either remote or non-interactive installation) due to load distribution across activation servers of Kaspersky. If you need to activate the application right away, you may interrupt the ongoing activation process and start activation using the Activation Wizard.

Activating the application through Kaspersky Security Center


You can activate the application remotely through Kaspersky Security Center in the following ways:

- Using the *Add key* task.
This method lets you add a key to a specific computer or to computers that are part of an administration group.
- By distributing a key stored on the Kaspersky Security Center Administration Server to the computers.
This method lets you automatically add a key to computers that are already connected to Kaspersky Security Center, and to new computers. To use this method, you need to first add the key to the Kaspersky Security Center Administration Server. For more details about adding keys to the Kaspersky Security Center Administration Server, please refer to [Kaspersky Security Center Help](#).

A trial version is provided for Kaspersky Security Center Cloud Console. The *trial version* is a special version of Kaspersky Security Center Cloud Console designed to familiarize a user with the features of the application. In this version, you can perform actions in a workspace for a period of 30 days. All managed applications are automatically run under a trial license for Kaspersky Security Center Cloud Console, including Kaspersky Endpoint Security. However, you cannot activate Kaspersky Endpoint Security using its own trial license when the trial license for Kaspersky Security Center Cloud Console expires. For detailed information about Kaspersky Security Center licensing, please refer to the [Kaspersky Security Center Cloud Console Help](#).

The trial version of Kaspersky Security Center Cloud Console does not allow you to subsequently switch to a commercial version. Any trial workspace will be automatically deleted with all its contents after the 30-day period expires.

You can monitor the use of licenses in the following ways:

- View the *Key usage report* for the organization's infrastructure (**Monitoring and reports** → **Reports**).
- View the statuses of computers on the **Devices** → **Managed devices** tab. If the application is not activated, the computer will have the  status and the **Application is not activated** status description.
- View license information in the computer properties.
- View the key properties (**Operations** → **Licensing**).

[How to activate the application in the Administration Console \(MMC\)](#)

1. In the Administration Console, go to the folder **Administration Server** → **Tasks**.

The list of tasks opens.

2. Click the **New task** button.

The Task Wizard starts. Follow the instructions of the Wizard.

Step 1. Selecting task type

Select **Kaspersky Endpoint Security for Windows (11.4.0)** → **Add Key**.

Step 2. Adding a key

Enter an [activation code](#) or select a [key file](#).

For more details about adding keys to the Kaspersky Security Center repository, please *refer to the [Kaspersky Security Center Help Guide](#)*.

Step 3. Selecting the devices to which the task will be assigned

Select the computers on which the task will be performed. The following options are available:

- Assign the task to an administration group. In this case, the task is assigned to computers included in a previously created administration group.
- Select computers detected by the Administration Server in the network: *unassigned devices*. The specific devices can include devices in administration groups as well as unassigned devices.
- Specify device addresses manually, or import addresses from a list. You can specify NetBIOS names, IP addresses, and IP subnets of devices to which you want to assign the task.


Step 4. Configuring a task start schedule

Configure a schedule for starting a task, for example, manually or when the computer is idle.

Step 5. Defining the task name

Enter a name for the task, such as **Activate Kaspersky Endpoint Security for Windows**.

Step 6. Completing task creation

Exit the Wizard. If necessary, select the **Run task after Wizard finishes** check box. You can monitor the progress of the task in the task properties. As a result, Kaspersky Endpoint Security will be activated on users' computers in silent mode (license status .

1. In the main window of Web Console, select **Devices** → **Tasks**.

The list of tasks opens.

2. Click the **Add** button.

The Task Wizard starts. Follow the instructions of the Wizard.

Step 1. Configuring general task settings

Configure the general task settings:

1. In the **Application** drop-down list, select **Kaspersky Endpoint Security for Windows (11.4.0)**.

2. In the **Task type** drop-down list, select **Add key**.

3. In the **Task name** field, enter a brief description, such as **Activation of Kaspersky Endpoint Security for Windows**.

4. In the **Select devices to which the task will be assigned** section, select the task scope. Click the **Next** button.

Step 2. Selecting the devices to which the task will be assigned

Select the computers on which the task will be performed. The following options are available:


- Assign the task to an administration group. In this case, the task is assigned to computers included in a previously created administration group.
- Select computers detected by the Administration Server in the network: *unassigned devices*. The specific devices can include devices in administration groups as well as unassigned devices.
- Specify device addresses manually, or import addresses from a list. You can specify NetBIOS names, IP addresses, and IP subnets of devices to which you want to assign the task.

Step 3. Selecting a license

Select the license that you want to use to activate the application. Click the **Next** button.

You can add keys to the Web Console (**Operations** → **Licensing**).

Step 4. Completing task creation

Finish the wizard by clicking the **Finish** button. A new task will be displayed in the list of tasks. To run a task, select the check box opposite the task and click the **Start** button. As a result, Kaspersky Endpoint Security will be activated on users' computers in silent mode (license status .

In the properties of the *Add key* task, you can add a reserve key to the computer. A *reserve key* becomes active when the active key expires or is deleted. The availability of a reserve key lets you avoid application functionality limitations when a license expires.

[How to automatically add a license key to computers through the Administration Console \(MMC\)](#)

1. In the Administration Console, go to the folder **Administration Server** → **Kaspersky licenses**.

A list of license keys opens.

2. Open the license key properties.

3. In the **General** section, select the **Automatically distributed license key** check box.

4. Save your changes.

As a result, the key will be automatically distributed to the appropriate computers. During automatic distribution of a key as an active or a reserve key, the licensing limit on the number of computers (set in the key properties) is taken into account. If the licensing limit is reached, distribution of this key to computers ceases automatically. You can view the number of computers to which the key has been added and other data in the key properties in the **Devices** section.

[How to automatically add a license key to computers through the Web Console and Cloud Console](#)

1. In Web Console main window, select the **Operations** → **Licensing** → **Kaspersky Licenses**.

A list of license keys opens.

2. Open the license key properties.

3. On the **General** tab, switch on the **Deploy key automatically** toggle button.

4. Save your changes.

As a result, the key will be automatically distributed to the appropriate computers. During automatic distribution of a key as an active or a reserve key, the licensing limit on the number of computers (set in the key properties) is taken into account. If the licensing limit is reached, distribution of this key to computers ceases automatically. You can view the number of computers to which the key has been added and other data in the key properties on the **Devices** tab.

Using the Activation Wizard to activate the application

To activate Kaspersky Endpoint Security by using the Activation Wizard:

1. Click the  /  button in the lower part of the main application window.

2. In the window that opens, click the **Activate the application under a new license** button.

The Application Activation Wizard starts. Follow the instructions of the Activation Wizard.

Activating the application from the command line

To activate the application from the command line,

type the following string in the command line:

```
avp.com license /add <activation code or key file> [/login=<user name> /password=<password>]
```

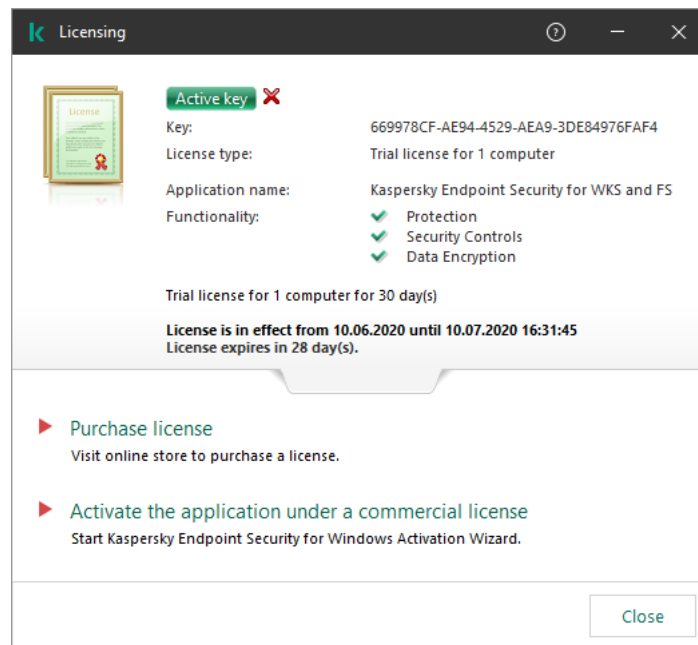
You need to enter the user account credentials (/login=<user name> /password=<password>) if [Password Protection is enabled](#).

Viewing license information

To view information about a license:

Click the  /  icon in the lower part of the main application window.

The **Licensing** window opens. This window displays information about the license (see figure below).



Licensing window

The following information is provided in the **Licensing** window:

- **Key status.** Several [keys](#) can be stored on a computer. There are two types of keys: active and reserve. The application cannot have more than one active key. A reserve key may become active only when the active key expires or after the key is deleted by using the **x** button.
- **Key.** A key is a unique alphanumeric sequence that is generated from an activation code or a key file.
- **License type.** The following [types of licenses](#) are available: trial and commercial.
- **Application name.** Full name of the purchased Kaspersky application.
- **Functionality.** Application features that are available under your license. Features may include Protection, Security Controls, Data Encryption, and others. The list of available features is also provided in the License Certificate.

- **Additional information about the license.** License type, number of computers that are covered by this license, license start date and expiration date and time (only for the active key).

License expiration time is displayed according to the time zone configured in the operating system.

In the Licensing window, you can also do one of the following:

- **Purchase license / Renew license.** Opens the Kaspersky online store website, where you can purchase or renew a license. To do so, please enter your company information and pay for the order.
- **Activate the application under a new license.** Starts the Application Activation Wizard. In this Wizard you can add a key using an activation code or a key file. The Application Activation Wizard allows you to add an active key and only one reserve key.

Purchasing a license

You may purchase a license after installing the application. On purchasing a license, you receive an activation code or a key file for activating the application.

To purchase a license:

1. In the main application window, click the  /  button.

The **Licensing** window opens.

2. In the **Licensing** window, do one of the following:

- If no keys have been added or a key for trial license has been added, click the **Purchase license** button.
- If the key for a commercial license is added, click the **Renew license** button.

A window will open with the website of the Kaspersky online store, where you can purchase a license.

Renewing subscription

When you use the application under subscription, Kaspersky Endpoint Security automatically contacts the activation server at specific intervals until your subscription expires.

If you use the application under unlimited subscription, Kaspersky Endpoint Security automatically checks the activation server for renewed keys in background mode. If a key is available on the activation server, the application adds it by replacing the previous key. In this way, unlimited subscription for Kaspersky Endpoint Security is renewed without user involvement.

If you are using the application under a limited subscription, on the expiration date of the subscription (or on the expiration date of the subscription renewal grace period), Kaspersky Endpoint Security notifies you about this and stops attempting to renew the subscription automatically. In this case, Kaspersky Endpoint Security behaves in the same way as it does when a [commercial license for the application expires](#): the application operates without updates and the Kaspersky Security Network is unavailable.

You can renew subscription on the website of the service provider.

You can update subscription status manually in the **Licensing** window. This may be required if the subscription has been renewed after the grace period and the application has not updated the subscription status automatically.

To visit the website of the service provider from the application interface:

1. In the main application window, click the  /  button.

The **Licensing** window opens.

2. In the **Licensing** window, click **Contact your subscription provider**.

Data provision

If an [activation code](#) is applied to activate Kaspersky Endpoint Security, you agree to periodically send Kaspersky the following information automatically for the purposes of verifying correct use of the application:

- type, version, and localization of Kaspersky Endpoint Security;
- versions of installed updates for Kaspersky Endpoint Security;
- ID of the computer and ID of the specific Kaspersky Endpoint Security installation on the computer;
- serial number and active key identifier;
- type, version and bit rate of the operating system, and name of the virtual environment (if Kaspersky Endpoint Security is installed in a virtual environment);
- IDs of Kaspersky Endpoint Security components that are active when the information is transmitted;

Kaspersky may also use this information to generate statistics on the dissemination and use of Kaspersky software.

By using an activation code, you agree to automatically transmit the data listed above. If you do not agree to transmit this information to Kaspersky, you should use a key file to activate Kaspersky Endpoint Security.

By accepting the terms of the End User License Agreement, you agree to automatically transmit the following information:

- When upgrading Kaspersky Endpoint Security:
 - version of Kaspersky Endpoint Security;
 - ID of Kaspersky Endpoint Security;
 - active key;
 - unique ID of the upgrade task start;
 - unique ID of the Kaspersky Endpoint Security installation.
- When following links from the Kaspersky Endpoint Security interface:
 - version of Kaspersky Endpoint Security;
 - version of the operating system;
 - Kaspersky Endpoint Security activation date;
 - license expiration date;
 - key creation date;
 - Kaspersky Endpoint Security installation date;
 - ID of Kaspersky Endpoint Security;
 - ID of the detected vulnerability in the operating system;

- ID of the last update installed for Kaspersky Endpoint Security;
- hash of the detected file with a threat, and the name of this threat according to the Kaspersky classification;
- Kaspersky Endpoint Security activation error category;
- Kaspersky Endpoint Security activation error code;
- number of days until key expiration;
- number of days that have elapsed since the key was added;
- number of days that have elapsed since the license expired;
- number of computers on which the active license is applied;
- active key;
- Kaspersky Endpoint Security license term;
- current status of the license;
- type of active license;
- application type;
- unique ID of the upgrade task start;
- unique ID of the Kaspersky Endpoint Security installation on the computer;
- Kaspersky Endpoint Security interface language.

Received information is protected by Kaspersky in accordance with the law and the requirements and applicable regulations of Kaspersky. Data is transmitted over encrypted communication channels.

Read the End User License Agreement and visit the [Kaspersky website](#) to learn more about how we receive, process, store, and destroy information about application usage after you accept the End User License Agreement and consent to the Kaspersky Security Network Statement. The license.txt and ksn_<language ID>.txt files contain the text of the End User License Agreement and Kaspersky Security Network Statement and are included in the application [distribution kit](#).

Getting started

After installing Kaspersky Endpoint Security, you can manage the application using the following interfaces:

- [Local application interface](#).
- Kaspersky Security Center Administration Console.
- Kaspersky Security Center 12 Web Console.
- Kaspersky Security Center Cloud Console.

Kaspersky Security Center Administration Console

Kaspersky Security Center lets you remotely install and uninstall, start and stop Kaspersky Endpoint Security, configure application settings, change the set of available application components, add keys, and start and stop update and scan tasks.

The application can be managed via Kaspersky Security Center using the Kaspersky Endpoint Security Management Plug-in.

For more details on managing the application through Kaspersky Security Center, *refer to the [Kaspersky Security Center Help](#)*.

Kaspersky Security Center 12 Web Console and Cloud Console

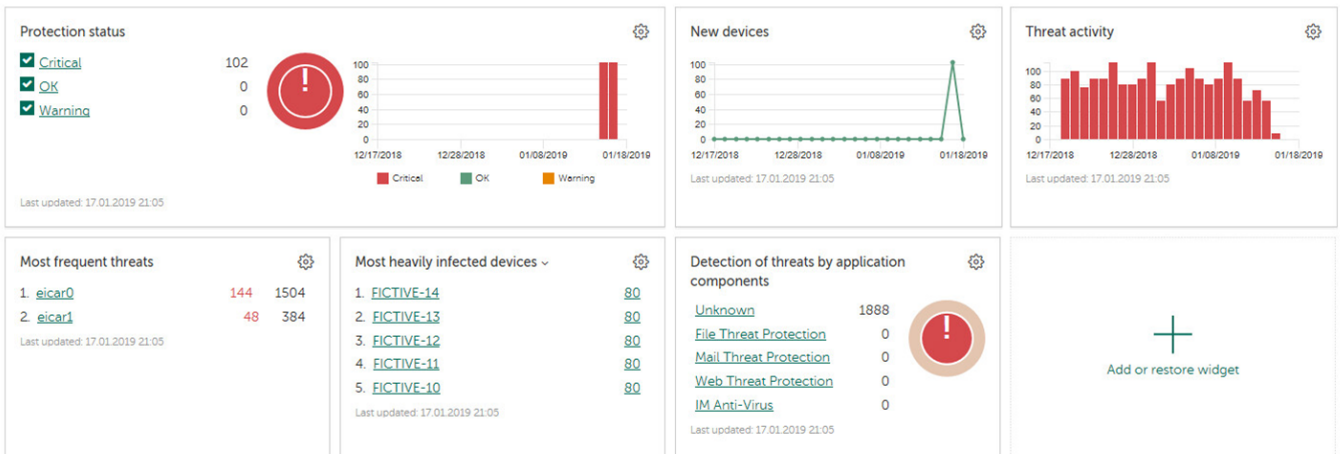
Kaspersky Security Center 12 Web Console (hereinafter also referred to as *Web Console*) is a web application intended for centrally performing the main tasks to manage and maintain the security system of an organization's network. Web Console is a Kaspersky Security Center component that provides a user interface. For detailed information about Kaspersky Security Center 12 Web Console, please *refer to the [Kaspersky Security Center Help](#)*.

Kaspersky Security Center Cloud Console (hereinafter also referred to as the "*Cloud Console*") is a cloud-based solution for protecting and managing an organization's network. For detailed information about Kaspersky Security Center Cloud Console, please refer to the [Kaspersky Security Center Cloud Console Help](#).

Web Console and Cloud Console let you do the following:

- Monitor the status of your organization's security system.
- Install Kaspersky applications on devices within your network.
- Manage installed applications.
- View reports on the security system status.

Management of Kaspersky Endpoint Security through the Web Console, Cloud Console, and Kaspersky Security Center Administration Console all provide different management capabilities. The [available components and tasks](#) also vary for the different Consoles.



Kaspersky Security Center 12 Web Console Interface

About the Kaspersky Endpoint Security for Windows Management Plug-in

The Kaspersky Endpoint Security for Windows Management Plug-in enables interaction between Kaspersky Endpoint Security and Kaspersky Security Center. The Management Plug-in lets you manage Kaspersky Endpoint Security by using [policies](#), [tasks](#), and [local application settings](#). Interaction with Kaspersky Security Center 12 Web Console is provided by the web plug-in.

The version of the Management Plug-in may differ from the version of Kaspersky Endpoint Security application installed on the client computer. If the installed version of the Management Plug-in has less functionality than the installed version of Kaspersky Endpoint Security, the settings of the missing functions are not regulated by the Management Plug-in. These settings can be modified by the user in the local interface of Kaspersky Endpoint Security.

The web plug-in is not installed by default in Kaspersky Security Center 12 Web Console. In contrast to the Management Plug-in for the Kaspersky Security Center Administration Console, which is installed on the administrator workstation, the web plug-in must be installed on a computer that has Kaspersky Security Center 12 Web Console installed. The functionality of the web plug-in is available to all administrators that have access to Web Console in a browser. You can view the list of installed web plug-ins in Web Console interface: **Console settings** → **Plug-ins**. For more details about the compatibility of web plug-in versions and Web Console, refer to [Kaspersky Security Center Help](#).

Installing the web plug-in

You can install the web plug-in as follows:

- Install web plug-in using Initial Configuration Wizard of Kaspersky Security Center 12 Web Console.

Web Console automatically prompts you to run the Initial Configuration Wizard when connecting Web Console to the Administration Server for the first time. You can also run the Initial Configuration Wizard in the Web Console interface (**Device discovery and deployment** → **Deployment and assignment** → **Initial Configuration Wizard**). The Initial Configuration Wizard can also check if the installed web plug-ins are up to date and download the necessary updates. For more details on the Initial Configuration Wizard for Kaspersky Security Center 12 Web Console, please refer to the [Kaspersky Security Center Help Guide](#).

- Install web plug-in using from the list of available distribution packages in Web Console.

To install the web plug-in, select the distribution package of the Kaspersky Endpoint Security web plug-in in the Web Console interface: **Console settings** → **Plug-ins**. The list of available distribution packages is updated automatically after new versions of Kaspersky applications are released.

- Download the distribution package to the Web Console from an external source.

To install the web plug-in, add the ZIP-archive of the distribution package for the Kaspersky Endpoint Security web plug-in in the Web Console interface: **Console settings** → **Plug-ins**. The distribution package of the web plug-in can be downloaded on the Kaspersky website, for example.

Updating the Management Plug-in

To update the Kaspersky Endpoint Security for Windows Management Plug-in, download the latest version of the plug-in (included in [distribution kit](#)) and run the plug-in installation wizard.

If a new version of the web plug-in becomes available, Web Console will display the notification *Updates are available for utilized plug-ins*. You can proceed to update the web plug-in version from this Web Console notification. You can also manually check for new web plug-in updates in the Web Console interface (**Console settings** → **Plug-ins**). The previous version of the web plug-in will be automatically removed during the update.

When the web plug-in is updated, already existing items (for example, policies or tasks) are saved. The new settings of items implementing new functions of Kaspersky Endpoint Security will appear in existing items and will have the default values.

You can update the web plug-in as follows:

- Update the web plug-in in the list of web plug-ins in online mode.

To update the web plug-in, you must select the distribution package of the Kaspersky Endpoint Security web plug-in in the Web Console interface (**Console settings** → **Plug-ins**). Web Console checks for available updates on Kaspersky servers and downloads the relevant updates.

- Update the web plug-in from a file.

To update the web plug-in, you must select the ZIP-archive of the distribution package for the Kaspersky Endpoint Security web plug-in in the Web Console interface: **Console settings** → **Plug-ins**. The distribution package of the web plug-in can be downloaded on the Kaspersky website, for example. You can update the Kaspersky Endpoint Security web plug-in only to a more recent version. The web plug-in cannot be updated to an older version.

If any item is opened (such as a policy or task), the web plug-in checks its compatibility information. If the version of the web plug-in is equal to or later than the version specified in the compatibility information, you can change the settings of this item. Otherwise, you cannot use the web plug-in to change the settings of the selected item. It is recommended to update the web plug-in.

Special considerations when working with different versions of management plug-ins

You can manage Kaspersky Endpoint Security via Kaspersky Security Center only if you have a Management Plug-in whose version is equal to or later than the version specified in the information regarding the compatibility of Kaspersky Endpoint Security with the Management Plug-in. You can view the minimum required version of the Management Plug-in in the installer.ini file included in the [distribution kit](#).

If any item is opened (such as a policy or task), the Management Plug-in checks its compatibility information. If the version of the Management Plug-in is equal to or later than the version specified in the compatibility information, you can change the settings of this item. Otherwise, you cannot use the Management Plug-in to change the settings of the selected item. It is recommended to upgrade the Management Plug-in.

Upgrading the Kaspersky Endpoint Security 10 for Windows Management Plug-in

If the Kaspersky Endpoint Security 10 for Windows Management Plug-in is installed in the Administration Console, please consider the following when installing the Kaspersky Endpoint Security 11 for Windows Management Plug-in:

- The Kaspersky Endpoint Security 10 for Windows Management Plug-in will not be removed, and will remain available for operation.
- The Kaspersky Endpoint Security 11 for Windows Management Plug-in does not support management of Kaspersky Endpoint Security 10 for Windows on users' computers.
- The Kaspersky Endpoint Security 11 for Windows Management Plug-in does not support items (for example, policies or tasks) that were created using the Kaspersky Endpoint Security 10 for Windows Management Plug-in.


If you removed the Kaspersky Endpoint Security 10 for Windows Management Plug-in and installed the Kaspersky Endpoint Security 11 for Windows Management Plug-in, you need to create new policies, tasks, etc. You can also install the Kaspersky Endpoint Security 11 for Windows Management Plug-in with the Kaspersky Endpoint Security 10 for Windows Management Plug-in to perform migration. After the migration is complete, remove the Kaspersky Endpoint Security 10 for Windows Management Plug-in.

Upgrading the Kaspersky Endpoint Security 11 for Windows Management Plug-in



If the Kaspersky Endpoint Security 11 for Windows Management Plug-in is installed in the Administration Console, please consider the following when installing a new version of the Kaspersky Endpoint Security 11 for Windows Management Plug-in:

- The previous version of the Kaspersky Endpoint Security 11 for Windows Management Plug-in will be removed.
- The new version of the Kaspersky Endpoint Security 11 for Windows Management Plug-in supports management of the previous version of Kaspersky Endpoint Security 11 for Windows on users' computers.
- You can use the new version of the Management Plug-in to change the settings in policies, tasks, and other items created by the previous version of the Management Plug-in.

- For new settings, the new version of the Management Plug-in assigns the default values when a policy, policy profile, or task are saved for the first time.

After the Management Plug-in is upgraded, it is recommended to check and save the values of the new settings in policies and policy profiles. If you do not do this, the new groups of Kaspersky Endpoint Security settings on the user's computer will take the default values and can be edited (the  attribute). It is recommended to check the settings starting with policies and policy profiles at the top level of the hierarchy. It is also recommended to use the user account that has access rights to all functional areas of Kaspersky Security Center.


To learn about the new capabilities of the application, please refer to the Release Notes or the [application help](#).




- If a new parameter has been added to a group of settings in the new version of the Management Plug-in, the previously defined status of the  /  attribute for this group of settings is not changed.

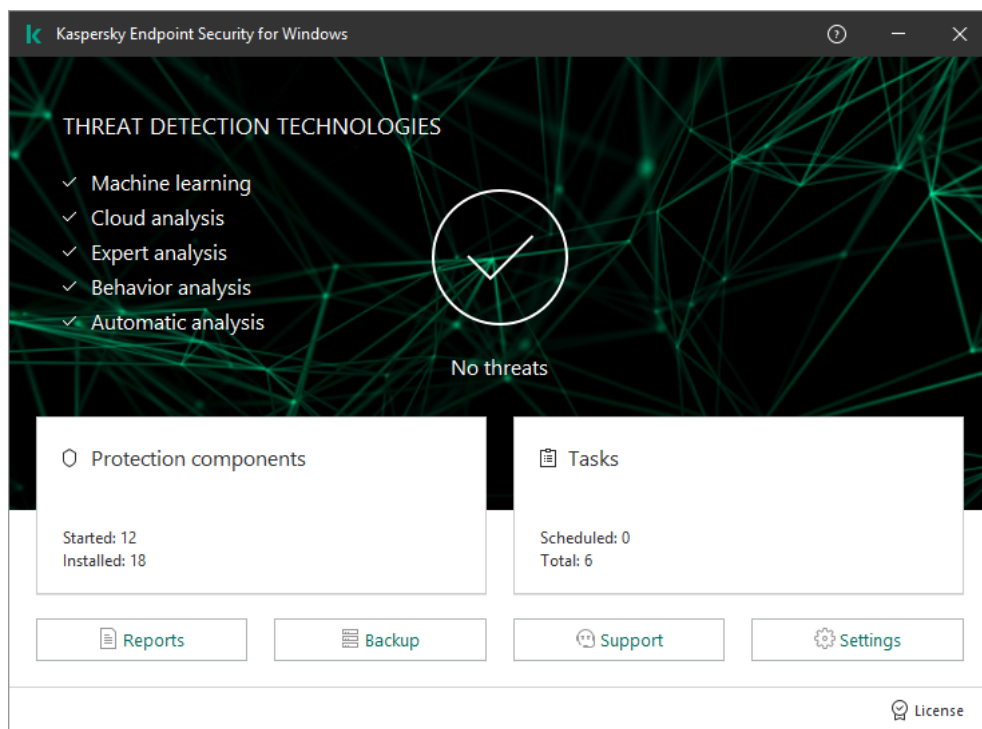
Application interface

The main window of Kaspersky Endpoint Security contains interface elements that provide access to the main functions of the application.

The main application window contains the following items:

- Link to **Kaspersky Endpoint Security for Windows**. Clicking this link opens the **About** window containing information about the application version.
- Button . Clicking this button takes you to the help system of Kaspersky Endpoint Security.
- **Threat detection technologies** section. The section contains the following information:
 - The left part of the section displays a list of threat detection technologies. The number of threats that were detected using the specific technology appears to the right of the name of each threat detection technology.
 - Depending on the presence of active threats, the center of the section displays one of the following captions:
 - **No threats**. If this caption is displayed, clicking the **Threat detection technologies** section opens the **Threat detection technologies** window, which provides a brief description of the threat detection technologies as well as the status and global statistics of the Kaspersky Security Network cloud service infrastructure.
 - **N active threats**. If this caption is displayed, clicking the **Threat detection technologies** section opens the **Active threats** window, which displays a list of events associated with infected files that were not processed for some reason.
- **Protection components** section. Clicking this section opens the **Protection components** window. In this window, you can view the operating status of installed components. From this window, you can also open a subsection in the **Settings** window containing the settings of any installed component except encryption components.

- **Tasks** section. Clicking this section opens the **Tasks** window. In this window, you can manage the operation of Kaspersky Endpoint Security tasks that are used to update application modules and databases, scan files for viruses and other malware, and run an integrity check.
- **Reports** button. Clicking this button opens the **Reports** window containing information about events that have occurred during operation of the application in general or its separate components, or during the performance of tasks.
- **Repositories** button. Clicking this button opens the **Backup** window. In this window, you can view a list of copies of infected files that the application has deleted.
- **Support** button. Clicking this button opens the **Support** window, which contains information on the operating system, the current version of Kaspersky Endpoint Security, and links to Kaspersky information resources.
- **Settings** button. Clicking this button opens the **Settings** window in which you can modify the default settings of the application.
- Button  /  / . Clicking this button opens the **Events** window that contains information about available updates as well as requests to access encrypted files and devices.
- **License** link. Clicking this link opens the **Licensing** window containing information about the current license.



Main application window





Application icon in the taskbar notification area

Immediately after installation of Kaspersky Endpoint Security, the application icon appears in the Microsoft Windows taskbar notification area.


The icon serves the following purposes:

- It indicates application activity.
- It acts as a shortcut to the context menu and main window of the application.

The following application icon statuses are provided for displaying application operating information:

- The  icon signifies that critically important protection components of the application are enabled. Kaspersky Endpoint Security will display a warning , if the user is required to perform an action, for example, restart the computer after updating the application.
- The  icon signifies that critically important protection components of the application are disabled or have malfunctioned. Protection components may malfunction, for example, if the license has expired or as a result of an application error. Kaspersky Endpoint Security will display a warning  with a description of the problem in computer protection.


The context menu of the application icon contains the following items:

- **Kaspersky Endpoint Security for Windows.** Opens the main application window. In this window, you can adjust the operation of application components and tasks, and view the statistics of processed files and detected threats.
- **Settings.** Opens the application settings window.
- **Pause protection and control / Resume protection and control.** Pause the operation of all protection and control components that are not marked by a lock () in the policy. Prior to performing this operation, it is recommended to disable the Kaspersky Security Center policy.

Prior to pausing the operation of protection and control components, the application requests the [password for accessing Kaspersky Endpoint Security](#) (account password or temporary password). You can then select the pause period: for a specific amount of time, until a restart, or upon user request.

This context menu item is available if [Password Protection is enabled](#). To resume the operation of protection and control components, select **Resume protection and control** in the context menu of the application.

Pausing the operation of protection and control components does not affect the performance of update and scan tasks. The application also continues using Kaspersky Security Network.

- **Disable policy / Enable policy.** Disables a Kaspersky Security Center policy on the computer. All Kaspersky Endpoint Security settings are available for configuration, including settings that have a closed lock in the policy (). If the policy is disabled, the application requests the [password for accessing Kaspersky Endpoint Security](#) (account password or temporary password). This context menu item is available if [Password Protection is enabled](#). To enable the policy, select **Enable policy** in the context menu of the application.
- **Support.** This opens the **Support** window containing information necessary for contacting Kaspersky Technical Support.
- **About.** This item opens an information window with application details.
- **Exit.** This item quits Kaspersky Endpoint Security. Clicking this context menu item causes the application to be unloaded from the computer RAM.

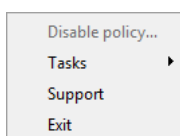


Application icon context menu

Simplified application interface

If a Kaspersky Security Center policy configured to [display the simplified application interface](#) is applied to a client computer on which Kaspersky Endpoint Security is installed, the main application window is not available on this client computer. Right-click to open the context menu of the Kaspersky Endpoint Security icon (see the figure below) containing the following items:

- **Disable policy / Enable policy.** Disables a Kaspersky Security Center policy on the computer. All Kaspersky Endpoint Security settings are available for configuration, including settings that have a closed lock in the policy (🔒). If the policy is disabled, the application requests the [password for accessing Kaspersky Endpoint Security](#) (account password or temporary password). This context menu item is available if [Password Protection is enabled](#). To enable the policy, select **Enable policy** in the context menu of the application.
- **Tasks.** Drop-down list containing the following items:
 - **Update.**
 - **Last update rollback.**
 - **Full Scan.**
 - **Custom Scan.**
 - **Critical Areas Scan.**
 - **Integrity Check.**
- **Support.** This opens the **Support** window containing information necessary for contacting Kaspersky Technical Support.
- **Exit.** This item quits Kaspersky Endpoint Security. Clicking this context menu item causes the application to be unloaded from the computer RAM.



Context menu of the application icon when displaying the simplified interface

Configuring the display of the application interface

You can configure the application interface display mode for a user. The user can interact with the application in the following ways:

- **With simplified interface.** On a client computer, the main application window is inaccessible, and only the [icon in the Windows notification area](#) is available. In the context menu of the icon, the user can [perform a limited number of operations with Kaspersky Endpoint Security](#). Kaspersky Endpoint Security also displays notifications above the application icon.
- **With full interface.** On a client computer, the main window of Kaspersky Endpoint Security and the [icon in the Windows notification area](#) are available. In the context menu of the icon, the user can perform operations with

Kaspersky Endpoint Security. Kaspersky Endpoint Security also displays notifications above the application icon.

- **No interface.** On a client computer, no signs of Kaspersky Endpoint Security operation are displayed. The [icon in the Windows notification area](#) and notifications are not available.

[How to configure the application interface display mode in the Administration Console \(MMC\)](#)

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **General Settings** → **Interface**.
6. In the **Interaction with user** section, do one of the following:
 - Select the **Display application interface** check box if you want the following interface elements to be displayed on the client computer:
 - Folder containing the application name in the **Start** menu
 - [Kaspersky Endpoint Security icon](#) in the Microsoft Windows taskbar notification area
 - Pop-up notifications
 - If this check box is selected, the user can view and, depending on the available rights, change application settings from the application interface.
 - Clear the **Display application interface** check box if you want to hide all signs of Kaspersky Endpoint Security on the client computer.
7. In the **Interaction with user** section, select the **Simplified application interface** check box if you want the [simplified application interface](#) to be displayed on a client computer that has Kaspersky Endpoint Security installed.

[How to configure the application interface display mode in the Web Console and Cloud Console](#)

1. In the main window of Web Console, select the **Devices** → **Policies and policy profiles** tab.
2. Click the name of the Kaspersky Endpoint Security policy for computers on which you want to enable support for portable mode.
The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General settings** → **Interface**.
5. In the **Interaction with user** section, configure how the application interface will be displayed:
 - **With simplified interface.** On a client computer, the main application window is inaccessible, and only the [icon in the Windows notification area](#) is available. In the context menu of the icon, the user can [perform a limited number of operations with Kaspersky Endpoint Security](#). Kaspersky Endpoint Security also displays notifications above the application icon.
 - **With full interface.** On a client computer, the main window of Kaspersky Endpoint Security and the [icon in the Windows notification area](#) are available. In the context menu of the icon, the user can perform operations with Kaspersky Endpoint Security. Kaspersky Endpoint Security also displays notifications above the application icon.
 - **No interface.** On a client computer, no signs of Kaspersky Endpoint Security operation are displayed. The [icon in the Windows notification area](#) and notifications are not available.
6. Click **OK**.

Getting started

After deploying the application on client computers, to work with Kaspersky Endpoint Security from Kaspersky Security Center Web Console you need to perform the following actions:

- Create and configure a policy.
You can use policies to apply identical Kaspersky Endpoint Security settings to all client computers within an administration group. The Initial Configuration Wizard of Kaspersky Security Center automatically creates a policy for Kaspersky Endpoint Security.
- Create the *Update* and *Virus Scan* tasks.
The *Update* task is required for keeping computer security up to date. When the task is performed, Kaspersky Endpoint Security [updates the anti-virus databases and application modules](#). The *Update* task is created automatically by the Initial Configuration Wizard of Kaspersky Security Center. To create the *Update* task, install the Kaspersky Endpoint Security for Windows web plug-in while running the Wizard.
The *Virus Scan* task is required for the timely detection of viruses and other malware. You need to manually create the *Virus Scan* task.

[How to create a Virus Scan task in the Administration Console \(MMC\)](#) 

1. In the Administration Console, go to the folder **Administration Server** → **Tasks**.

The list of tasks opens.

2. Click the **New task** button.

The Task Wizard starts. Follow the instructions of the Wizard.

Step 1. Selecting task type

Select **Kaspersky Endpoint Security for Windows (11.4.0)** → **Virus scan**.

Step 2. Scan scope

Create the list of objects that Kaspersky Endpoint Security will scan while performing a scan task.

Step 3. Kaspersky Endpoint Security action

Choose the action on threat detection:

- **Disinfect; delete if disinfection fails.** If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected files that are detected. If disinfection fails, Kaspersky Endpoint Security deletes the files.
- **Disinfect; inform if disinfection fails.** If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected files that are detected. If disinfection is not possible, Kaspersky Endpoint Security adds the information about the infected files that are detected to the list of active threats.
- **Inform.** If this option is selected, Kaspersky Endpoint Security adds the information about infected files to the list of active threats on detection of these files.
- **Run Advanced Disinfection immediately.** If the check box is selected, Kaspersky Endpoint Security uses the Advanced Disinfection technology to treat active threats during the scan.

Advanced disinfection technology is aimed at purging the operating system of malicious applications that have already started their processes in RAM and that prevent Kaspersky Endpoint Security from removing them by using other methods. The threat is neutralized as a result. While Advanced Disinfection is in progress, you are advised to refrain from starting new processes or editing the operating system registry. The advanced disinfection technology uses considerable operating system resources, which may slow down other applications. After the advanced disinfection is complete, Kaspersky Endpoint Security will restart the computer without asking the user for confirmation.

Configure the task run mode using the **Scan when the computer is idling** check box. This check box enables / disables the function that suspends the *Virus scan* task when computer resources are limited. Kaspersky Endpoint Security pauses the *Virus scan* task if the screensaver is off and the computer is unlocked.

Step 4. Selecting the devices to which the task will be assigned

Select the computers on which the task will be performed. The following options are available:

- Assign the task to an administration group. In this case, the task is assigned to computers included in a previously created administration group.
- Select computers detected by the Administration Server in the network: *unassigned devices*. The specific devices can include devices in administration groups as well as unassigned devices.
- Specify device addresses manually, or import addresses from a list. You can specify NetBIOS names, IP addresses, and IP subnets of devices to which you want to assign the task.

Step 5. Selecting the account to run the task

Select an account to run the *Virus Scan* task. By default, Kaspersky Endpoint Security starts the task with the rights of a local user account. If the scan scope includes network drives or other objects with restricted access, select a user account with the sufficient access rights.

Step 6. Configuring a task start schedule

Configure a schedule for starting a task, for example, manually or after anti-virus databases are downloaded to the repository.

Step 7. Defining the task name

Enter a name for the task, for example, `Daily full scan`.

Step 8. Completing task creation

Exit the Wizard. If necessary, select the **Run task after Wizard finishes** check box. You can monitor the progress of the task in the task properties. As a result, the Virus Scan task will be executed on the user computers in accordance to the specified schedule.

[How to create a Virus Scan task in the Web Console](#) 

1. In the main window of Web Console, select **Devices** → **Tasks**.

The list of tasks opens.

2. Click the **Add** button.

The Task Wizard starts.

3. Configure the task settings:

a. In the **Application** drop-down list, select **Kaspersky Endpoint Security for Windows (11.4.0)**.

b. In the **Task type** drop-down list, select **Virus Scan**.

c. In the **Task name** field, enter a brief description, for example, `Weekly scan`.

d. In the **Select devices to which the task will be assigned** section, select the task scope.

4. Select devices according to the selected task scope option. Click the **Next** button.

5. Finish the wizard by clicking the **Finish** button.

A new task will be displayed in the list of tasks.

6. To configure the task schedule, go to the task properties.

It is recommended to configure a schedule that runs the task at least once per week.

7. Select the check box next to the task.

8. Click the **Run** button.

You can monitor the status of the task, and the number of devices on which the task was completed successfully or completed with an error.

As a result, the Virus Scan task will be executed on the user computers in accordance to the specified schedule.

Managing policies

A *policy* is a collection of application settings that are defined for an administration group. You can configure multiple policies with different values for one application. An application can run under different settings for different administration groups. Each administration group can have its own policy for an application.

Policy settings are sent to client computers by Network Agent during *synchronization*. By default, the Administration Server performs synchronization immediately after policy settings are changed. UDP port 15000 on the client computer is used for synchronization. The Administration Server performs synchronization every 15 minutes by default. If synchronization fails after policy settings were changed, the next synchronization attempt will be performed according to the configured schedule.

Active and inactive policy

A policy is intended for a group of managed computers and can be active or inactive. The settings of an active policy are saved on client computers during synchronization. You cannot simultaneously apply multiple policies to one computer, therefore only one policy may be active in each group.



You can create an unlimited number of inactive policies. An inactive policy does not affect application settings on computers in the network. Inactive policies are intended as preparations for emergency situations, such as a virus attack. If there is an attack via flash drives, you can activate a policy that blocks access to flash drives. In this case, the active policy automatically becomes inactive.

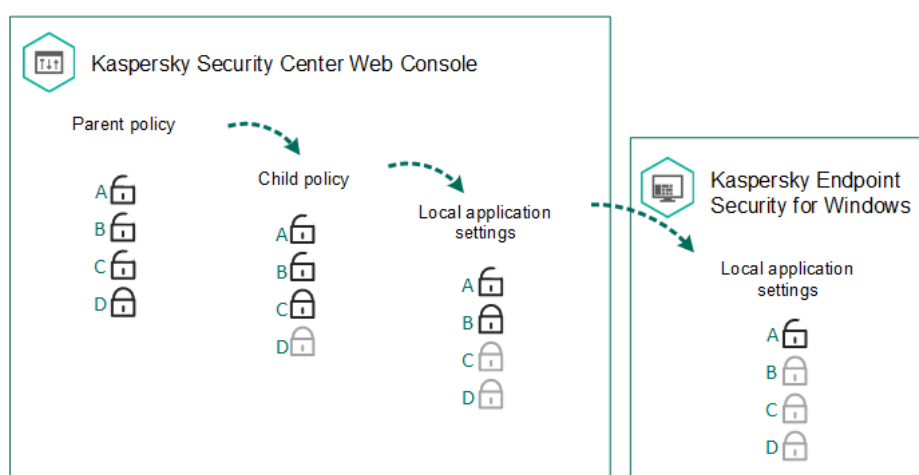
Out-of-office policy

An out-of-office policy is activated when a computer leaves the organization network perimeter.

Settings inheritance

Policies, like administration groups, are arranged in a hierarchy. By default, a child policy inherits settings from the parent policy. *Child policy* is a policy for nested hierarchy levels, that is a policy for nested administration groups and slave Administration Servers. You can disable the inheritance of settings from the parent policy.

Each policy setting has the  attribute, which indicates if the settings can be modified in the child policies or in the [local application settings](#). The  attribute is applicable only if inheritance of parent policy settings is enabled for the child policy. Out-of-office policies do not affect other policies through the hierarchy of administration groups.



Settings inheritance




The rights to access policy settings (read, write, execute) are specified for each user who has access to the Kaspersky Security Center Administration Server and separately for each functional scope of Kaspersky Endpoint Security. To configure the rights to access policy settings, go to the **Security** section of the properties window of the Kaspersky Security Center Administration Server.

Creating a policy

[How to create a policy in the Administration Console \(MMC\)](#) 

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, select the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Click the **New policy** button.
The Policy Wizard starts.
5. Follow the instructions of the Policy Wizard.

[How to create a policy in the Web Console and Cloud Console](#)

1. In the main window of Web Console, select **Devices** → **Policies and policy profiles**.
2. Click the **Add** button.
The Policy Wizard starts.
3. Select Kaspersky Endpoint Security and click **Next**.
4. Please read and accept the terms of the Kaspersky Security Network (KSN) Statement and click **Next**.
5. On the **General** tab, you can perform the following actions:
 - Change the policy name.
 - Select the policy status:
 - **Active**. After the next synchronization, the policy will be used as the active policy on the computer.
 - **Inactive**. Backup policy. If necessary, an inactive policy can be switched to active status.
 - **Out-of-office**. The policy is activated when a computer leaves the organization network perimeter.
 - Configure the inheritance of settings:
 - **Inherit settings from parent policy**. If this toggle button is switched on, the policy setting values are inherited from the top-level policy. Policy settings cannot be edited if  is set for the parent policy.
 - **Force inheritance of settings for child policies**. If the toggle button is on, the values of the policy settings are propagated to the child policies. In the properties of the child policy, the **Inherit parent policy settings** toggle button will be automatically switched on and cannot be switched off. Child policy settings are inherited from the parent policy, except for the settings marked with . Child policy settings cannot be edited if  is set for the parent policy.
6. On the **Application settings** tab, you can configure the [Kaspersky Endpoint Security policy settings](#).
7. Click the **Save** button.

As a result, Kaspersky Endpoint Security settings will be configured on client computers during the next synchronization. You can view information about the policy that is being applied to the computer in the Kaspersky Endpoint Security interface by clicking the **Support** button on the main screen (for example, the policy name). To do so, in the settings of the Network Agent policy, you need to enable the receipt of extended policy data. For more details about a Network Agent policy, please refer to the [Kaspersky Security Center Help Guide](#).

Security level indicator

The security level indicator is displayed in the top part of the **Properties: <Policy name>** window. The indicator can take one of the following values:

- **High protection level.** The indicator takes this value and turns green if all components from the following categories are enabled:
 - **Critical.** This category includes the following components:
 - File Threat Protection.
 - Behavior Detection.
 - Exploit Prevention.
 - Remediation Engine.
 - **Important.** This category includes the following components:
 - Kaspersky Security Network.
 - Web Threat Protection.
 - Mail Threat Protection.
 - Host Intrusion Prevention.
- **Medium protection level.** The indicator takes this value and turns yellow if one of the important components is disabled.
- **Low protection level.** The indicator takes this value and turns red in one of the following cases:
 - One or multiple critical components are disabled.
 - Two or more important components are disabled.

If the indicator has the **Medium protection level** or **Low protection level** value, a link that opens the **Recommended protection components** window appears to the right of the indicator. In this window, you can enable any of the recommended protection components.

Task management

You can create the following types of tasks to administer Kaspersky Endpoint Security through Kaspersky Security Center:

- Local tasks that are configured for an individual client computer.

- Group tasks that are configured for client computers within administration groups.
- Tasks for a selection of computers.

You can create any number of group tasks, tasks for a selection of computers, or local tasks. For more details about working with administration groups and selections of computers, *please refer to [Kaspersky Security Center Help](#)*.

Kaspersky Endpoint Security supports the following tasks:

- **[Virus Scan](#)**. Kaspersky Endpoint Security scans the computer areas specified in the task settings for viruses and other threats. The *Virus Scan* task is required for the operation of Kaspersky Endpoint Security and is created during the Initial Configuration Wizard. It is recommended to configure a schedule that runs the task at least once per week.
- **[Add key](#)**. Kaspersky Endpoint Security adds a key for activating applications, including an additional key. Before running the task, make sure that the number of computers, on which the task is to be executed, does not exceed the number of computers allowed by the license.
- **[Change application components](#)**. Kaspersky Endpoint Security installs or removes components on client computers according to the list of components specified in the task settings. The File Threat Protection component cannot be removed. The optimal set of Kaspersky Endpoint Security components helps to conserve computer resources.
- **[Inventory](#)**. Kaspersky Endpoint Security receives information about all application executable files that are stored on computers. The *Inventory* task is performed by the Application Control component. If the Application Control component is not installed, the task will end with an error.
- **[Update](#)**. Kaspersky Endpoint Security updates databases and application modules. The *Update* task is required for the operation of Kaspersky Endpoint Security and is created during the Initial Configuration Wizard. It is recommended to configure a schedule that runs the task at least once per day.
- **[Wipe data](#)**. Kaspersky Endpoint Security deletes files and folders from users' computers immediately or if there is no connection with Kaspersky Security Center for a long time.
- **[Update rollback](#)**. Kaspersky Endpoint Security rolls back the last update of databases and application modules. This may be necessary if, for example, new databases contain incorrect data that could cause Kaspersky Endpoint Security to block a safe application.
- **[Integrity check](#)**. Kaspersky Endpoint Security analyzes application files, checks files for corruption or modifications, and verifies the digital signatures of application files.
- **[Manage Authentication Agent accounts](#)**. Kaspersky Endpoint Security configures the Authentication Agent account settings. An Authentication Agent is needed for working with encrypted drives. Before the operating system is loaded, the user needs to complete authentication with the Agent.

Tasks are run on a computer only if [Kaspersky Endpoint Security is running](#).

Add a new task

[How to create a task in the Administration Console \(MMC\)](#)

1. Open the Kaspersky Security Center Administration Console.
2. Select the **Tasks** folder in the Administration Console tree.
3. Click the **New task** button.
The Task Wizard starts.
4. Follow the instructions of the Task Wizard.

[How to create a task in the Web Console and Cloud Console](#)

1. In the main window of Web Console, select **Devices** → **Tasks**.
The list of tasks opens.
2. Click the **Add** button.
The Task Wizard starts.
3. Configure the task settings:
 - a. In the **Application** drop-down list, select **Kaspersky Endpoint Security for Windows (11.4.0)**.
 - b. In the **Task type** drop-down list, select the task that you want to run on user computers.
 - c. In the **Task name** field, enter a brief description, for example, Update the application for accounting.
 - d. In the **Select devices to which the task will be assigned** section, select the task scope.
4. Select devices according to the selected task scope option. Click the **Next** button.
5. Finish the wizard by clicking the **Finish** button.

A new task will be displayed in the list of tasks. The task will have the default settings. To configure the task settings, you need to go to the task properties. To run a task, you need to select the check box opposite the task and click the **Start** button. After the task has started, you can pause the task and resume it later.

In the list of tasks, you can monitor the task results, which include the task status and the statistics for task performance on computers. You can also create a selection of events to monitor the completion of tasks (**Monitoring and reports** → **Event selections**). For more details on event selection, *please refer to the [Kaspersky Security Center Help Guide](#)*. Task execution results are also saved locally in Windows event log and in [Kaspersky Endpoint Security reports](#).

Task access control

The rights to access Kaspersky Endpoint Security tasks (read, write, execute) are defined for each user who has access to Kaspersky Security Center Administration Server, through the settings of access to functional areas of Kaspersky Endpoint Security. To configure access to the functional areas of Kaspersky Endpoint Security, go to the **Security** section of the properties window of Kaspersky Security Center Administration Server. For more details on task management through Kaspersky Security Center, *please refer to the [Kaspersky Security Center Help](#)*.

You can configure users' rights to access tasks using a policy (*task management mode*). For example, you can hide group tasks in the Kaspersky Endpoint Security interface.

[How to configure the task management mode in the Kaspersky Endpoint Security interface through the Administration Console \(MMC\)](#)

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Local Tasks** → **Task management** .
6. In the **Task management** section:
 - If you want to allow users to work with local tasks in the interface and command line of Kaspersky Endpoint Security, select the **Allow use of local tasks** check box.

If the check box is cleared, the functions of local tasks are stopped. In this mode, local tasks do not run according to schedule. Local tasks are also unavailable for starting and editing in the local interface of Kaspersky Endpoint Security, and when working with the command line.

- If you want to allow users to view the list of group tasks, select the **Allow group tasks to be displayed** check box.
 - If you want to allow users to modify the settings of group tasks, select the **Allow management of group tasks** check box.
7. Save your changes.


[How to configure the task management mode in the Kaspersky Endpoint Security interface through the Web Console](#)

1. In the main window of Web Console, select the **Devices** → **Policies and policy profiles** tab.
2. Click the name of the Kaspersky Endpoint Security policy for computers on which you want to enable support for portable mode.
The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Local tasks** → **Task management**.
5. Configure the task management mode (see the table below).
6. Click **OK**.
7. Confirm your changes by clicking **Save**.

Task management settings

Parameter	Description
Allow use of local tasks	<p>If the check box is selected, local tasks are displayed in the Kaspersky Endpoint Security local interface. When there are no additional policy restrictions, the user can configure and run tasks. However, configuring task run schedule remains unavailable for the user. The user can run tasks only manually.</p> <p>If the check box is cleared, use of local tasks is stopped. In this mode, local tasks do not run according to schedule. Tasks cannot be started or configured in the local interface of Kaspersky Endpoint Security, or when working with the command line.</p> <p>A user can still start a virus scan of a file or folder by selecting the Scan for viruses option in the context menu of the file or folder. The scan task is started with the default values of settings for the custom scan task.</p>
Allow group tasks to be displayed	<p>If the check box is selected, group tasks are displayed in the Kaspersky Endpoint Security local interface. The user can view the list of all tasks in the application interface.</p> <p>If the check box is cleared, Kaspersky Endpoint Security displays an empty task list.</p>
Allow management of group tasks	<p>If the check box is selected, users can start and stop group tasks specified in Kaspersky Security Center. Users can start and stop tasks in the application interface or in the simplified application interface.</p> <p>If the check box is cleared, Kaspersky Endpoint Security starts scheduled tasks automatically, or the administrator starts tasks manually in Kaspersky Security Center.</p>

Configuring local application settings

In Kaspersky Security Center, you can configure Kaspersky Endpoint Security settings on a particular computer. They are the *local application settings*. Some settings may be unaccessible for editing. These settings are locked by the  attribute in the [policy properties](#).

[How to configure the local application settings in the Administration Console \(MMC\)](#) 

1. Open the Kaspersky Security Center Administration Console.
 2. In the **Managed devices** folder of the Administration Console tree, open the folder with the name of the administration group to which the relevant client computer belongs.
 3. In the workspace, select the **Devices** tab.
 4. Select the computer for which you want to configure Kaspersky Endpoint Security settings.
 5. In the context menu of the client computer, select **Properties**.
A client computer properties window opens.
 6. In the client computer properties window, select the **Applications** section.
A list of Kaspersky applications that are installed on the client computer appears in the right part of the client computer properties window.
 7. Select Kaspersky Endpoint Security.
 8. Click the **Properties** button under the list of Kaspersky applications.
The **Kaspersky Endpoint Security for Windows application settings** window opens.
 9. In the **General Settings** section, configure the settings for Kaspersky Endpoint Security as well as the report and storage settings.
The other sections of the **Kaspersky Endpoint Security for Windows application settings** window are the same as in the standard sections of Kaspersky Security Center. A description of these sections is provided in the Kaspersky Security Center Help.
- If an application is subject to a policy that prohibits changes to specific settings, you will not be able to edit them while configuring application settings in the **General Settings** section.
10. To save your changes, in the **Kaspersky Endpoint Security for Windows application settings** window, click **OK**.

[How to configure the local application settings in the Web Console and Cloud Console](#) 

1. In the main window of Web Console, select **Devices** → **Managed devices**.
2. Select the computer for which you want to configure local application settings.
This opens the computer properties.
3. Select the **Applications** tab.
4. Click **Kaspersky Endpoint Security for Windows**.
This opens the local application settings.
5. Select the **Application settings** tab.
6. Configure the local application settings.
7. Local application settings are the same as [policy settings](#), except for encryption settings.

Starting and stopping Kaspersky Endpoint Security

After installing Kaspersky Endpoint Security to a user's computer, the application is started automatically. By default, Kaspersky Endpoint Security is started after operating system startup. It is not possible to configure automatic startup of the application in the operating system settings.

Downloading Kaspersky Endpoint Security anti-virus databases after the operating system starts can take up to two minutes depending on the capabilities of the computer. During this time, the level of computer protection is reduced. The downloading of anti-virus databases when Kaspersky Endpoint Security is started on an already started operating system does not cause a reduction in the level of computer protection.

[How to configure the startup of Kaspersky Endpoint Security in the Administration Console \(MMC\)](#)

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **General Settings** → **Application Settings**.
6. Use the **Start Kaspersky Endpoint Security for Windows on computer startup** check box to configure the application startup.
7. To save changes, click the **Save** button.

[How to configure the startup of Kaspersky Endpoint Security in the Web Console](#)

1. In the main window of Web Console, select **Devices** → **Policies and policy profiles**.
2. Click the name of Kaspersky Endpoint Security policy for the computers for which you want to configure the startup of the application.
The policy properties window opens.
3. Select the **Application settings** tab.
4. Select the **General settings** section.
5. Click the **Application settings** link.
6. Use the **Start Kaspersky Endpoint Security for Windows on computer startup** check box to configure the application startup.
7. Click **OK**.
8. Confirm your changes by clicking **Save**.



[How to configure the startup of Kaspersky Endpoint Security in the application interface](#)

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Application Settings**.
3. Use the **Start Kaspersky Endpoint Security for Windows on computer startup** check box to configure the application startup.
4. To save changes, click the **Save** button.

Kaspersky experts recommend against manually stopping Kaspersky Endpoint Security because doing so exposes the computer and your personal data to threats. If necessary, you can [pause computer protection](#) for as long as you need to, without stopping the application.

You can monitor the application status by using the **Protection Status** widget.

[How to start or stop Kaspersky Endpoint Security in the Administration Console \(MMC\)](#)

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder of the Administration Console tree, open the folder with the name of the administration group to which the relevant client computer belongs.
3. In the workspace, select the **Devices** tab.
4. Select the computer on which you want to start or stop the application.
5. Right-click to display the context menu of the client computer and select **Properties**.
6. In the client computer properties window, select the **Applications** section.
A list of Kaspersky applications that are installed on the client computer appears in the right part of the client computer properties window.
7. Select Kaspersky Endpoint Security.
8. Do the following:
 - To start the application, click the  button to the right of the list of Kaspersky applications.
 - To stop the application, click the  button to the right of the list of Kaspersky applications.

[How to start or stop Kaspersky Endpoint Security in the Web Console](#)

1. In the main window of Web Console, select **Devices** → **Managed devices**.
2. Click the name of the computer on which you want to start or stop Kaspersky Endpoint Security.
The computer properties window opens.
3. Select the **Applications** tab.
4. Select the check box opposite **Kaspersky Endpoint Security for Windows**.
5. Click the **Start** or **Stop** button.

[How to start or stop Kaspersky Endpoint Security from the command line](#)

To stop the application from the command line, [enable external management of system services](#).



The file `klpsm.exe`, which is included in the Kaspersky Endpoint Security distribution kit, is used to start or stop the application from the command line.

1. Run the command line interpreter (`cmd.exe`) as an administrator.
2. Go to the folder where the Kaspersky Endpoint Security executable file is located.
3. To start the application from the command line, enter `klpsm.exe start_avp_service`.
4. To stop the application from the command line, enter `klpsm.exe stop_avp_service`.

Pausing and resuming computer protection and control

Pausing computer protection and control means disabling all protection and control components of Kaspersky Endpoint Security for some time.

The application status is displayed using the [application icon in the taskbar notification area](#).

- The  icon signifies that computer protection and control are paused.
- The  icon signifies that computer protection and control are enabled.

Pausing or resuming computer protection and control does not affect scan or update tasks.

If any network connections are already established when you pause or resume computer protection and control, a notification about the termination of these network connections is displayed.

To pause computer protection and control:

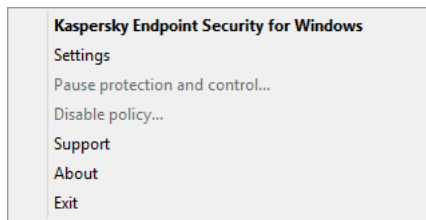
1. Right-click to bring up the context menu of the application icon that is in the taskbar notification area.
2. In the context menu, select **Pause protection and control** (see figure below).

This context menu item is available if [Password Protection is enabled](#).

3. Select one of the following options:

- **Pause for the specified time** – computer protection and control will resume after the amount of time that is specified in the drop-down list below.
- **Pause until restart** – computer protection and control will resume after you quit and reopen the application or restart the operating system. Automatic startup of the application must be enabled to use this option.
- **Pause** – computer protection and control will resume when you decide to re-enable them.

Kaspersky Endpoint Security will pause the operation of all protection and control components that are not marked by a lock (🔒) in the policy. Prior to performing this operation, it is recommended to disable the Kaspersky Security Center policy.



Application icon context menu

To resume computer protection and control:

1. Right-click to bring up the context menu of the application icon that is in the taskbar notification area.
2. In the context menu, select **Resume protection and control**.

You can resume computer protection and control at any time, regardless of the computer protection and control pause option that you selected previously.

Scanning the computer

A virus scan is vital to computer security. Regularly run virus scans to rule out the possibility of spreading malware that is undetected by protection components due to a low security level setting or for other reasons.

Kaspersky Endpoint Security does not scan files whose contents are located in OneDrive cloud storage, and creates log entries stating that these files have not been scanned.

Full Scan

A thorough scan of the entire computer. Kaspersky Endpoint Security scans the following objects:

- Kernel memory.
- Objects that are loaded at startup of the operating system.
- Boot sectors
- Operating system backup.
- All hard and removable drives

Kaspersky experts recommend that you do not change the scan scope of the *Full Scan* task.

To conserve computer resources, it is recommended to run a background scan task instead of a full scan task. This will not affect the security level of the computer.

Critical Areas Scan

By default, Kaspersky Endpoint Security scans the kernel memory, running processes, and disk boot sectors.

Kaspersky experts recommend that you do not change the scan scope of the *Critical Areas Scan* task.

Custom Scan

Kaspersky Endpoint Security scans the objects that are selected by the user. You can scan any object from the following list:

- Kernel memory.
- Objects that are loaded at startup of the operating system.
- Operating system backup.
- Outlook mailbox.

- Hard, removable, and network drives.
- Any selected file.

Background scan

Background scan is a scan mode of Kaspersky Endpoint Security that does not display notifications for the user. Background scan requires less computer resources than other types of scans (such as a full scan). In this mode, Kaspersky Endpoint Security scans startup objects, kernel memory, and the system partition.

Integrity check

Kaspersky Endpoint Security checks the application modules for corruption or modifications.

Starting or stopping a scan task

Regardless of the selected scan task run mode, you can start or stop a scan task at any time.

To start or stop a scan task:

1. In the main application window, click the **Tasks** button.
2. In the window that opens, select a scan task.
3. Do one of the following:
 - Click the **Start** button if you want to run the scan task.
The task progress status that is displayed under the name of this scan task changes to *Running*.
 - If you want to stop the scan task, select **Stop** in the context menu.
The task progress status that is displayed under the name of this scan task changes to *Stopped*.

To start or stop a scan task when the simplified application interface is displayed:

1. Right-click to bring up the context menu of the application icon that is in the taskbar notification area.
2. In the **Tasks** drop-down list in the context menu, do one of the following:
 - select a non-running scan task to start it
 - select a running scan task to stop it
 - select a paused scan task to resume or restart it

Changing the security level

To perform scan tasks, Kaspersky Endpoint Security uses various combinations of settings. These combinations of settings saved in the application are called *security levels*. There are three preset security levels: **High**, **Recommended**, and **Low**. The **Recommended** security level settings are considered to be optimal. They are recommended by Kaspersky experts. You can select one of the preset security levels or manually configure security level settings. If you change the security level settings, you can always revert back to the recommended security level settings.

To change a security level:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Tasks** → **Full Scan**, **Critical Areas Scan**, or **Custom Scan**.
3. In the **Security level** section, do one of the following:
 - If you want to apply one of the preset security levels (**High**, **Recommended**, or **Low**), select it with the slider.
 - If you want to configure a custom security level, click the **Settings** button and specify the settings in the appearing window with the name of the scan task.
After you configure a custom security level, the name of the security level in the **Security level** section changes to **Custom**.
 - If you want to change the security level to **Recommended**, click the **By default** button.
4. To save changes, click the **Save** button.

Changing the action to take on infected files

By default, on detection of infected files, Kaspersky Endpoint Security tries to disinfect them, or deletes them if disinfection is not possible.

To change the action to take on infected files:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Tasks** → **Full scan**, **Critical Areas Scan**, **Custom scan**, or **Scan from Context Menu**.
3. In the **Action on threat detection** section, select one of the following options:
 - Select the **Disinfect; delete if disinfection fails** check box if you want Kaspersky Endpoint Security to try to disinfect them, or delete them if disinfection is not possible.
 - Select the **Disinfect; inform if disinfection fails** check box if you want Kaspersky Endpoint Security to try to disinfect them, and inform you if disinfection is not possible.
 - Select the **Inform** check box if you want Kaspersky Endpoint Security to inform you when infected files are detected.

On detection of infected files that are part of the Windows Store application, Kaspersky Endpoint Security applies the **Delete** action.

4. To save changes, click the **Save** button.

Generating a list of objects to scan

To generate a list of objects to scan:

1. In the main application window, click the **Settings** button.
 2. In the application settings window, select **Tasks** → **Full scan**, **Critical Areas Scan**, **Custom scan**, or **Scan from Context Menu**.
 3. Click the **Scan scope** button.
The **Scan scope** window opens.
 4. If you want to add a new object to the scan scope:
 - a. Click the **Add** button.
The **Select scan scope** window opens.
 - b. Select the object and click **Add**.
All objects that are selected in the **Select scan scope** window are displayed in the **Scan scope** list.
 - c. Click **OK**.
 5. If you want to change the path to an object in the scan scope:
 - a. Select the object in the scan scope.
 - b. Click the **Edit** button.
The **Select scan scope** window opens.
 - c. Enter the new path to the object in the scan scope.
 - d. Click **OK**.
- You cannot remove or edit objects that are included in the default scan scope.
6. If you want to remove an object from the scan scope:
 - a. Select the object that you want to remove from the scan scope.
To select multiple objects, select them while holding down the **CTRL** key.
 - b. Click the **Delete** button.
A window for confirming deletion opens.
 - c. Click **Yes** in the removal confirmation window.

You cannot remove or edit objects that are included in the default scan scope.

7. To exclude an object from the scan scope, clear the check box next to the object in the **Scan scope** window. The object remains in the list of objects in the scan scope, but it is not scanned when the scan task runs.
8. Save your changes.

Selecting the type of files to scan

When selecting the type of files to scan, consider the following:

1. There is a low probability of introducing malicious code into files of certain formats and its subsequent activation (for example, TXT format). At the same time, there are file formats that contain executable code (such as .exe, .dll). The executable code may also be contained in files of formats that are not intended for this purpose (for example, the DOC format). The risk of intrusion and activation of malicious code in such files is high.
2. An intruder may send a virus or another malicious application to your computer in an executable file that has been renamed with the .txt extension. If you select scanning of files by extension, the application skips this file during scanning. If scanning of files by format is selected, the File Threat Protection component analyzes the file header regardless of the extension. If this analysis reveals that the file has the format of an executable file (for example, EXE), the application scans it.

To select the type of files to scan:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Tasks** → **Full scan**, **Critical Areas Scan**, **Custom scan**, or **Scan from Context Menu**.
3. In the **Security level** section, click the **Settings** button.
A window with the name of the selected scan task opens.
4. In the window with the name of the selected scan task, select the **Scope** tab.
5. In the **File types** section, specify the type of files that you want to scan when the selected scan task runs:
 - If you want to scan all files, select **All files**.
 - If you want to scan files of formats which are the most vulnerable to infection, select **Files scanned by format**.
 - If you want to scan files with extensions that are typically the most vulnerable to infection, select **Files scanned by extension**.
6. Save your changes.

Optimizing file scanning

You can optimize file scanning: reduce scan time and increase the operating speed of Kaspersky Endpoint Security. This can be achieved by scanning only new files and those files that have been modified since the previous scan. This mode applies both to simple and to compound files. You can also set a limit for scanning a single file. When the specified time interval expires, Kaspersky Endpoint Security excludes the file from the current scan (except archives and objects that include several files).

You can also enable the use of the iChecker and iSwift technologies. The iChecker and iSwift technologies optimize the speed of scanning files, by excluding files that have not been modified since the most recent scan.

To optimize file scanning:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Tasks** → **Full scan**, **Critical Areas Scan**, **Custom scan**, or **Scan from Context Menu**.
3. In the **Security level** section, click the **Settings** button.
A window with the name of the selected scan task opens.
4. In the window that opens, select the **Scope** tab.
5. In the **Scan optimization** section, perform the following actions:
 - Select the **Scan only new and changed files** check box.
 - Select the **Skip files that are scanned for longer than** check box and specify the scan duration for a single file (in seconds).
6. Save your changes.

Scanning compound files

A common technique of concealing viruses and other malware is to implant them in compound files, such as archives or databases. To detect viruses and other malware that are hidden in this way, the compound file must be unpacked, which may slow down scanning. You can limit the types of compound files to be scanned and thereby speed up scanning.

To configure scanning of compound files:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Tasks** → **Full Scan**, **Critical Areas Scan**, or **Custom Scan**.
3. In the **Security level** section, click the **Settings** button.
A window with the name of the selected scan task opens.
4. In the window that opens, select the **Scope** tab.
5. In the **Scan of compound files** section, specify which compound files you want to scan: archives, installation packages, files in office formats, files in mail formats, and password-protected archives.

6. If the **Scan only new and changed files** check box is cleared in the **Scan optimization** section, click the **all / new** link next to the name of the compound file type if you want to specify for each type of compound file whether to scan all files of this type or only new files of this type.

This link changes its value when it is clicked.

If the **Scan only new and changed files** check box is selected, only new files are scanned.

7. Click the **Additional** button.

The **Compound files** window opens.

8. In the **Size limit** section, do one of the following:

- If you do not want to unpack large compound files, select the **Do not unpack large compound files** check box and specify the required value in the **Maximum file size** field.
- If you want to unpack large compound files regardless of their size, clear the **Do not unpack large compound files** check box.

Kaspersky Endpoint Security scans large files that are extracted from archives, regardless of whether the **Do not unpack large compound files** check box is selected.

9. Save your changes.

Using scan methods

Kaspersky Endpoint Security uses a scanning technique called Machine learning and signature analysis. During signature analysis, Kaspersky Endpoint Security matches the detected object with records in its database. Based on the recommendations of Kaspersky experts, machine learning and signature analysis is always enabled.

To increase the effectiveness of protection, you can use heuristic analysis. During heuristic analysis, Kaspersky Endpoint Security analyzes the activity of objects in the operating system. Heuristic analysis can detect malicious objects for which there are currently no records in the Kaspersky Endpoint Security database.

To use scan methods:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Tasks** → **Full scan**, **Critical Areas Scan**, **Custom scan**, or **Scan from Context Menu**.
3. In the **Security level** section, click the **Settings** button.
A window with the name of the selected scan task opens.
4. In the window that opens, select the **Additional** tab.
5. If you want the application to use heuristic analysis when running the scan task, select the **Heuristic analysis** check box in the **Scan methods** block. Then use the slider to set the heuristic analysis level: **Light scan**, **Medium scan**, or **Deep scan**.
6. Save your changes.

Using scan technologies

To use scan technologies:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Tasks** → **Full scan**, **Critical Areas Scan**, **Custom scan**, or **Scan from Context Menu**.
3. In the **Security level** section, click the **Settings** button.
A window with the name of the selected scan task opens.
4. In the window that opens, select the **Additional** tab.
5. In the **Scan technologies** section, select the check boxes next to the names of technologies that you want to use during the scan.
6. Save your changes.

Selecting the run mode for the scan task

If it is impossible to run the scan task for any reason (for example, the computer is off at that time), you can configure the skipped task to be run automatically as soon as this becomes possible.

You can postpone the scan task start after application startup if you have selected the **By schedule** update task run mode and the Kaspersky Endpoint Security startup time matches the scan task run schedule. The scan task can only be run after the specified time interval elapses after the startup of Kaspersky Endpoint Security.

To select the scan task run mode:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Tasks** → **Full Scan**, **Critical Areas Scan**, or **Custom Scan**.
3. Click the **Run mode** button.
A window with the properties of the selected task opens on the **Run mode** tab.
4. In the **Run mode** section, select the task run mode: **Manually** or **By schedule**.
5. If you selected the **By schedule** option, specify the schedule settings. To do so:
 - a. In the **Frequency** drop-down list, select the task run frequency (**Minutes**, **Hours**, **Days**, **Every week**, **At a specified time**, **Every month**, or **After application startup**, **After every update**).
 - b. Depending on the selected frequency, configure advanced settings that specify the task run schedule.
 - c. If you want Kaspersky Endpoint Security to start skipped scan tasks as soon as possible, select the **Run skipped tasks** check box.

If **Minutes**, **Hours**, **After application startup** or **After every update** item is selected in the **Frequency** drop-down list, the **Run skipped tasks** check box is unavailable.

- d. If you want Kaspersky Endpoint Security to suspend a task when computer resources are limited, select the **Run only when the computer is idling** check box. Kaspersky Endpoint Security starts the scan task if the computer is locked.

This schedule option helps to conserve computer resources.

6. Save your changes.

Starting a scan task under the account of a different user

By default, a scan task is run with the permissions of the account under which the user logged in to the operating system. However, you may need to run a scan task under a different user account. You can specify a user who has the appropriate rights in the settings of the scan task and run the scan task under this user's account.

To configure the start of a scan task under a different user account:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Tasks** → **Full Scan**, **Critical Areas Scan**, or **Custom Scan**.
3. Click the **Run mode** button.

This opens a window with the properties of the selected task on the **Run mode** tab.

4. On the **Run mode** tab, in the **User** section, select the **Run task as** check box.
5. In the **Name** field, enter the name of the user account whose rights are necessary for starting the scan task.
6. In the **Password** field, enter the password of the user whose rights are necessary for starting the scan task.
7. Save your changes.

Scanning removable drives when they are connected to the computer

Kaspersky Endpoint Security scans all files that you run or copy, even if the file is located on a removable drive (File Threat Protection component). To prevent the spread of viruses and other malware, you can configure automatic scans of removable drives when they are connected to the computer. Kaspersky Endpoint Security automatically attempts to disinfect all infected files that are detected. If disinfection fails, Kaspersky Endpoint Security deletes the files. The component keeps a computer secure by running scans that implement machine learning, heuristic analysis (high level), signature analysis, and iSwift and iChecker technologies. It is not possible to optimize removable drive scans. In other words, you cannot enable scanning of only new and modified files or limit the scan time. Kaspersky Endpoint Security scans all files from the scan scope every time a removable drive is connected.

To configure scanning of removable drives when they are connected:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Tasks** → **Removable drives scan**.

3. In the **Action on connection of a removable drive** drop-down list, select the required action:

- **Do not scan.**
- **Detailed Scan**

In this mode, Kaspersky Endpoint Security scans all files located on the removable drive, including files embedded within compound objects, archives, distribution packages, and files in office formats. Kaspersky Endpoint Security does not scan files in mail formats or password-protected archives.

- **Quick Scan**

In this mode, Kaspersky Endpoint Security scans only [potentially infectable files](#), and does not unpack compound objects.

4. Do one of the following:

- If you want Kaspersky Endpoint Security to scan only those removable drives whose size does not exceed a specified value, select the **Maximum removable drive size** check box and specify the value (in megabytes) in the neighboring field.
- If you want Kaspersky Endpoint Security to scan all removable drives, clear the **Maximum removable drive size** check box.

5. Do one of the following:

- If you want Kaspersky Endpoint Security to display the removable drive scan progress in a separate window, select the **Show scan progress** check box.
In the removable drive scan window, the user can stop the scan. To make removable drive scans mandatory and prevent the user from stopping a scan, select the **Block the stopping of the scan task** check box.
- If you want Kaspersky Endpoint Security to run a removable drive scan in the background, clear the **Show scan progress** check box.

6. To save changes, click the **Save** button.

Background scan

Background scan is a scan mode of Kaspersky Endpoint Security that does not display notifications for the user. Background scan requires less computer resources than other types of scans (such as a full scan). In this mode, Kaspersky Endpoint Security scans startup objects, kernel memory, and the system partition. A background scan is started in the following cases:

- After an anti-virus database update.
- 30 minutes after Kaspersky Endpoint Security is started.
- Every six hours.
- When the computer is idling for five minutes or more.

Background scan when the computer is idling is interrupted when any of the following conditions are true:

- The computer went into active mode.

If the background scan has not been run for more than ten days, the scan is not interrupted.

- The computer (laptop) has switched to battery mode.

When performing a background scan, Kaspersky Endpoint Security does not scan files whose contents are located in OneDrive cloud storage.

To enable background scans of the computer:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Tasks** → **Background scan**.
3. Select the **Scan when the computer is idling** check box.
4. To save changes, click the **Save** button.

Updating databases and application software modules

Updating the databases and application modules of Kaspersky Endpoint Security ensures up-to-date protection on your computer. New viruses and other types of malware appear worldwide on a daily basis. Kaspersky Endpoint Security databases contain information about threats and ways of neutralizing them. To detect threats quickly, you are urged to regularly update the databases and application modules.

Regular updates require a license in effect. If there is no current license, you will be able to perform an update only once.

The main update source for Kaspersky Endpoint Security is Kaspersky update servers.

Your computer must be connected to the Internet to successfully download the update package from Kaspersky update servers. By default, the Internet connection settings are determined automatically. If you use a proxy server, you need to [adjust the connection settings](#).

Updates are downloaded over the HTTPS protocol. They may also be downloaded over the HTTP protocol when it is impossible to download updates over the HTTPS protocol.

While performing an update, the following objects are downloaded and installed on your computer:

- Kaspersky Endpoint Security databases. Computer protection is provided using databases that contain signatures of viruses and other threats and information on ways to neutralize them. Protection components use this information when searching for and neutralizing infected files on your computer. The databases are constantly updated with records of new threats and methods for counteracting them. Therefore, we recommend that you update the databases regularly.

In addition to the Kaspersky Endpoint Security databases, the network drivers that enable the application's components to intercept network traffic are updated.

- Application modules. In addition to the databases of Kaspersky Endpoint Security, you can also update the application modules. Updating the application modules fixes vulnerabilities in Kaspersky Endpoint Security, adds new functions, or enhances existing functions.

While updating, the application modules and databases on your computer are compared against the up-to-date version at the update source. If your current databases and application modules differ from their respective up-to-date versions, the missing portion of the updates is installed on your computer.

Context help files can be updated together with application module updates.

If the databases are obsolete, the update package may be large, which may cause additional Internet traffic (up to several dozen MB).

Information about the current status of Kaspersky Endpoint Security databases is displayed in the **Update** section in the **Tasks** window.

Information on update results and on all events that occur during the performance of the update task is logged in the [Kaspersky Endpoint Security report](#).

Database and application module update scenarios

Updating the databases and application modules of Kaspersky Endpoint Security ensures up-to-date protection on your computer. New viruses and other types of malware appear worldwide on a daily basis. Kaspersky Endpoint Security databases contain information about threats and ways of neutralizing them. To detect threats quickly, you are urged to regularly update the databases and application modules.

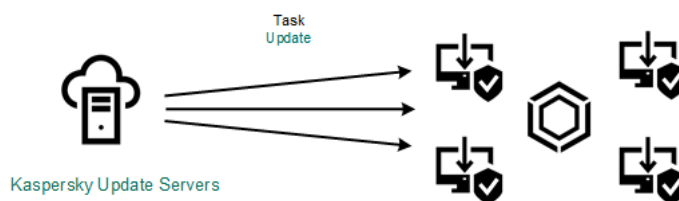
The following objects are updated on users' computers:

- Anti-virus databases. Anti-virus databases include databases of malware signatures, description of network attacks, databases of malicious and phishing web addresses, databases of banners, spam databases, and other data.
- Application modules. Module updates are intended for eliminating vulnerabilities in the application and to improve computer protection methods. Module updates may change the behavior of application components and add new capabilities.

Kaspersky Endpoint Security supports the following scenarios for updating databases and application modules:

- Update from Kaspersky servers.

Kaspersky update servers are located in various countries throughout the world. This ensures high reliability of updates. If an update cannot be performed from one server, Kaspersky Endpoint Security switches over to the next server.



Update from Kaspersky servers.

- Centralized update.

Centralized update reduces external Internet traffic, and provides for convenient monitoring of the update.

Centralized update consists of the following steps:

1. Download the update package to a repository within the organization's network.

The update package is downloaded to the repository by the Administration Server task named *Download updates to Administration Server repository*.

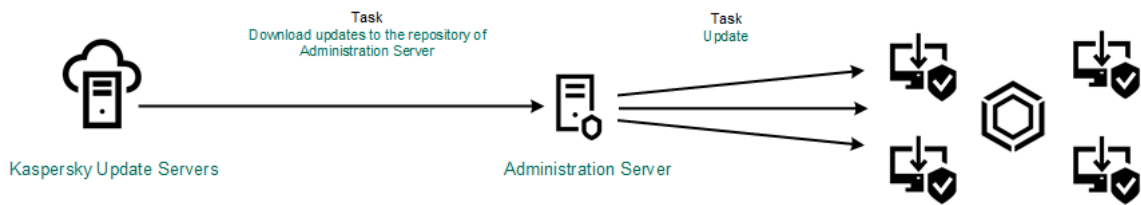
2. Download the update package to a shared folder (optional).

You can download the update package to a shared folder by using the following methods:

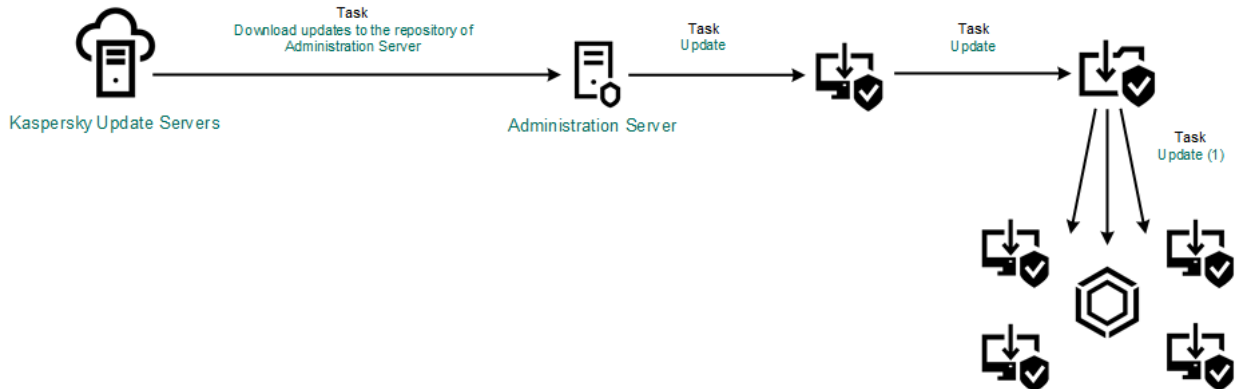
- Using Kaspersky Endpoint Security *Update* task. The task is intended for one of the computers in the local company network.
- Using the Kaspersky Update Utility. For detailed information about using Kaspersky Update Utility, refer to [Kaspersky Knowledge Base](#).

3. Distribute the update package to client computers.

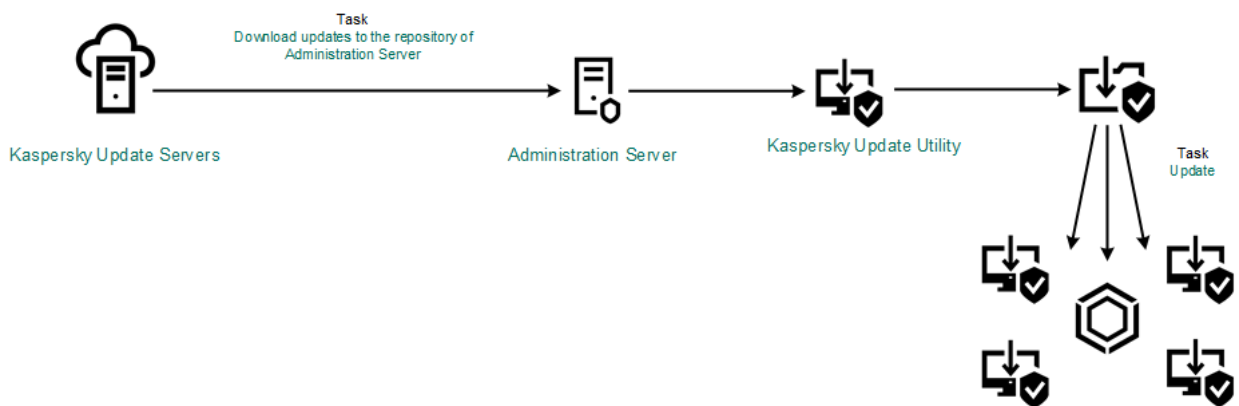
The update package is distributed to client computers by the Kaspersky Endpoint Security *Update* task. You can create an unlimited number of update tasks for each administration group.



Updating from a server repository



Updating from a shared folder



Updating using Kaspersky Update Utility

For the Web Console, the default list of update sources contains the Kaspersky Security Center Administration Server and Kaspersky update servers. For the Kaspersky Security Center Cloud Console, the default list of update sources contains distribution points and Kaspersky update servers. For more details about distribution points, refer to *Kaspersky Security Center Cloud Console Help*. You can add other update sources to the list. You can specify HTTP/FTP servers and shared folders as update sources. If an update cannot be performed from an update source, Kaspersky Endpoint Security switches over to the next one.

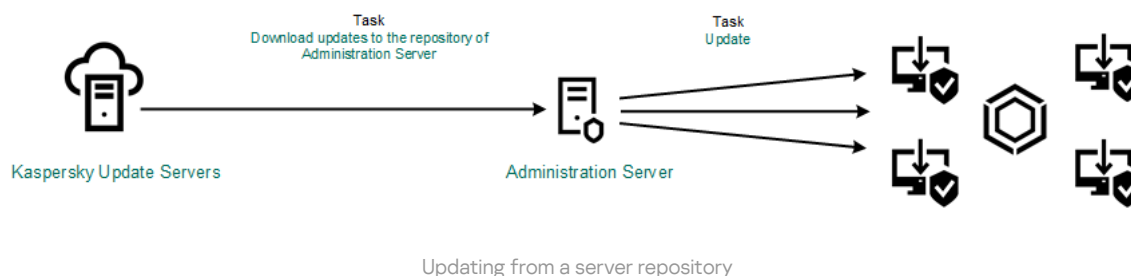
Updates are downloaded from Kaspersky update servers or from other FTP- or HTTP servers over standard network protocols. If connection to a proxy server is required for accessing the update source, [specify the proxy server settings in Kaspersky Endpoint Security policy settings](#).

Updating from a server repository

To conserve Internet traffic, you can configure updates of databases and application modules on computers of the organization's LAN from a server repository. For this purpose, Kaspersky Security Center must download an update package to the repository (FTP- or HTTP server, network or local folder) from Kaspersky update servers. Other computers on the organization's LAN will be able to receive the update package from the server repository.

Configuring database and application module updates from a server repository consists of the following steps:

1. Configure download of an update package to the Administration Server repository (*Download updates to Administration Server repository* task).
2. Configure database and application module updates from the specified server repository to the remaining computers on the organization's LAN (*Update* task).



To configure download of an update package to the server repository:

1. In the main window of Web Console, select **Devices** → **Tasks**.

The list of tasks opens.

2. Select the **Download updates to the repository** Administration Server task.

The task properties window opens.

The *Download updates to the repository* Administration Server task is created automatically by the Initial Configuration Wizard of Kaspersky Security Center 12 Web Console, and this task may only have one single instance.

3. Select the **Application settings** tab.

4. In the **Other settings** section, click **Configure**.

5. In the **Update storage folder** field, specify the address of FTP- or HTTP server, network folder or local folder where Kaspersky Security Center copies the update package received from Kaspersky update servers.

The following path format is used for update source:

- For an FTP or HTTP server, enter its web address or IP address.
For example, `http://dn1-01.geo.kaspersky.com/` or `93.191.13.103`.
For an FTP server, you can specify the authentication settings within the address in the following format:
`ftp://<user name>:<password>@<node>:<port>`.
- For a network folder, enter the UNC path.
For example, `\\ Server\Share\Update distribution`.
- For a local folder, enter the full path to that folder.
For example, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

6. Save your changes.

To configure Kaspersky Endpoint Security update from the specified server storage:

1. In the main window of Web Console, select **Devices** → **Tasks**.

The list of tasks opens.

2. Click the **Update** task for Kaspersky Endpoint Security.

The task properties window opens.

The *Update* task is created automatically by the Initial Configuration Wizard of Kaspersky Security Center. To create the *Update* task, install the Kaspersky Endpoint Security for Windows web plug-in while running the Wizard.

3. Select the **Application settings** tab → **Local mode**.

4. In the list of update sources, click the **Add** button.

5. In the **Source** field, specify the address of the FTP- or HTTP server, network folder or local folder where Kaspersky Security Center will copy the update package received from Kaspersky servers.

The address of the update source must match the address you specified in the **Folder for storing updates** field when you configured download of updates to the server storage (see *the instruction above*).

6. In the **Status** section select **Enabled**.

7. Click **OK**.

8. Configure the priorities of update sources by using the **Move up** and **Move down** buttons.

9. Click the **Save** button.

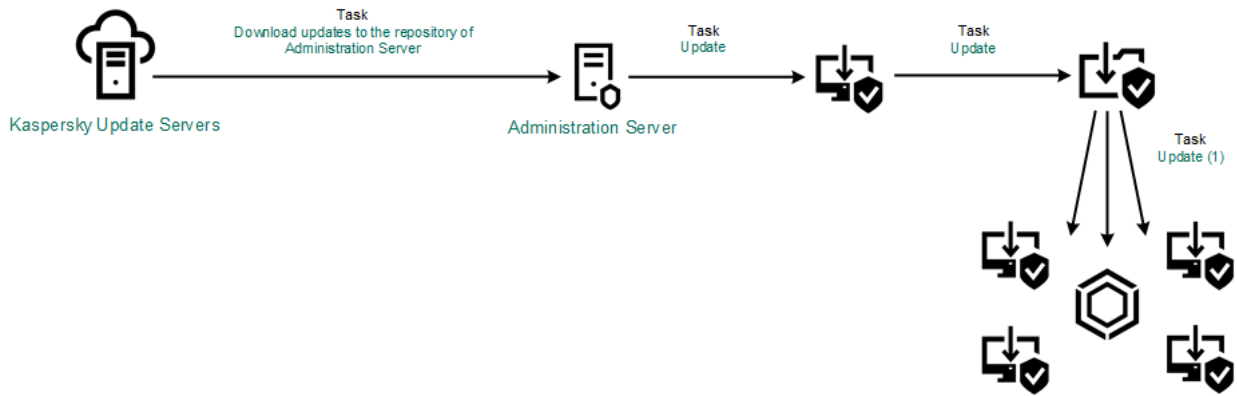
If an update cannot be performed from the first update source, Kaspersky Endpoint Security automatically switches over to the next source.

Updating from a shared folder

To conserve Internet traffic, you can configure updates of databases and application modules on computers of the organization's LAN from a shared folder. For this purpose, one of the computers on the organization's LAN must receive update packages from the Kaspersky Security Center Administration Server or from Kaspersky update servers and then copy the received update package to the shared folder. Other computers on the organization's LAN will be able to receive the update package from this shared folder.

Configuring database and application module updates from a shared folder consists of the following steps:

1. [Configuring database and application module updates from a server repository](#).
2. Enabling the copying of an update package to a shared folder on one of the computers on the local area network.
3. Configure database and application module updates from the specified shared folder to the remaining computers on the organization's LAN.



Updating from a shared folder

To enable copying of the update package to the shared folder:

1. In the main window of Web Console, select **Devices** → **Tasks**.

The list of tasks opens.

2. Click the **Update** task for Kaspersky Endpoint Security.

The task properties window opens.

The *Update* task is created automatically by the Initial Configuration Wizard of Kaspersky Security Center. To create the *Update* task, install the Kaspersky Endpoint Security for Windows web plug-in while running the Wizard.

3. Select the **Application settings** tab → **Local mode**.

4. Configure the sources of updates.

The sources of updates can be Kaspersky update servers, Kaspersky Security Center Administration Server, other FTP- or HTTP servers, local folders, or network folders.

5. Select the **Copy updates to folder** check box.

6. In the **Path** field, enter the UNC path to the shared folder (for example, \\Server\Share\Update distribution).

If the field is left blank, Kaspersky Endpoint Security will copy the update package to the folder C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\.

7. Click the **Save** button.

The *Update* task must be assigned for one computer that will serve as the source of updates.

To configure updates from a shared folder:

1. In the main window of Web Console, select **Devices** → **Tasks**.

The list of tasks opens.

2. Click the **Add** button.

The Task Wizard starts.

3. Configure the task settings:

- a. In the **Application** drop-down list, select **Kaspersky Endpoint Security for Windows (11.4.0)**.
- b. In the **Task type** drop-down list, select **Update**.
- c. In the **Task name** field, enter a brief description, for example, `Update from shared folder`.
- d. In the **Select devices to which the task will be assigned** section, select the task scope.

The *Update* task must be assigned to the computers of the organization's LAN, except the computer that serves as the update source.

4. Select devices according to the selected task scope option and click **Next**.
5. Finish the wizard by clicking the **Create** button.
A new task will be displayed in the table of tasks.
6. Click the newly created *Update* task.
The task properties window opens.
7. Go to the **Application settings** section.
8. Select the **Local mode** tab.
9. In the **Update source** section, click the **Add** button.
10. In the **Source** field, enter the path to the shared folder.

The source address must match the address that you previously specified in the **Path** field when you configured copying of the update package to the shared folder (see the *instructions above*).

11. Click **OK**.
12. Configure the priorities of update sources by using the **Move up** and **Move down** buttons.
13. Click the **Save** button.

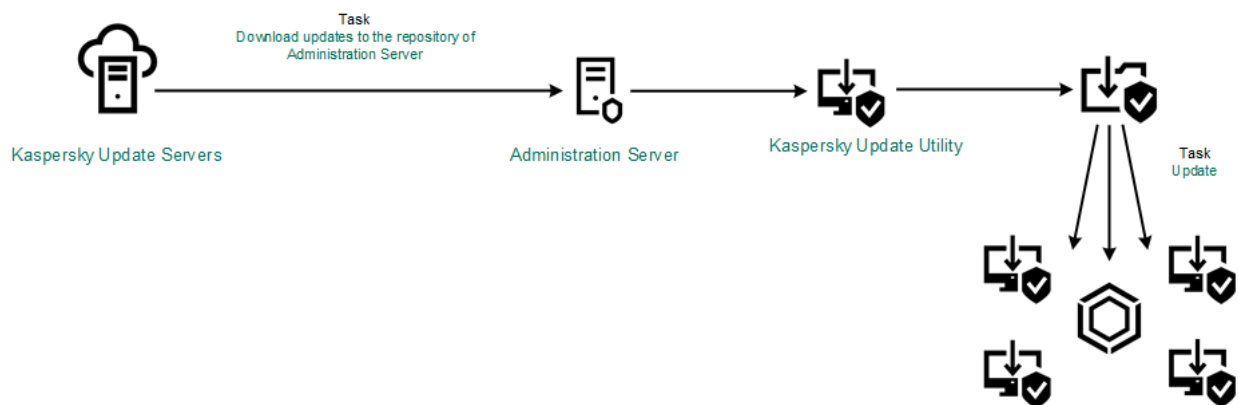
Updating using Kaspersky Update Utility

To conserve Internet traffic, you can configure updates of databases and application modules on computers of the organization's LAN from a shared folder using the Kaspersky Update Utility. For this purpose, one of the computers on the organization's LAN must receive update packages from the Kaspersky Security Center Administration Server or from Kaspersky update servers and then copy the received update packages to the shared folder using the utility. Other computers on the organization's LAN will be able to receive the update package from this shared folder.

Configuring database and application module updates from a shared folder consists of the following steps:

1. [Configuring database and application module updates from a server repository](#).
2. Install the Kaspersky Update Utility on one of the computers of the organization's LAN.

3. Configure copying of the update package to the shared folder in the Kaspersky Update Utility settings.
4. Configure database and application module updates from the specified shared folder to the remaining computers on the organization's LAN.



Updating using Kaspersky Update Utility

You can download the Kaspersky Update Utility distribution package from the [Kaspersky Technical Support website](#). After installing the utility, select the update source (for example, the Administration Server repository) and the shared folder to which the Kaspersky Update Utility will copy update packages. For detailed information about using Kaspersky Update Utility, refer to [Kaspersky Knowledge Base](#).

To configure updates from a shared folder:

1. In the main window of Web Console, select **Devices** → **Tasks**.

The list of tasks opens.

2. Click the **Update** task for Kaspersky Endpoint Security.

The task properties window opens.

The *Update* task is created automatically by the Initial Configuration Wizard of Kaspersky Security Center. To create the *Update* task, install the Kaspersky Endpoint Security for Windows web plug-in while running the Wizard.

3. Select the **Application settings** tab → **Local mode**.

4. In the list of update sources, click the **Add** button.

5. In the **Source** field, enter the UNC path to the shared folder (for example, \\Server\Share\Update distribution).

The source address must match the address indicated in the Kaspersky Update Utility settings.

6. Click **OK**.

7. Configure the priorities of update sources by using the **Move up** and **Move down** buttons.

8. Click the **Save** button.

Updating in mobile mode

Mobile mode is the mode of Kaspersky Endpoint Security operation, when a computer leaves the organization network perimeter (*offline computer*). For more details about working with offline computers and out-of-office users, refer to [Kaspersky Security Center Help](#).

An offline computer outside of the organization's network cannot connect to the Administration Server to update databases and application modules. By default, only Kaspersky update servers are used as update source for updating databases and application modules in mobile mode. The use of a proxy server to connect to the Internet is determined by a special [out-of-office policy](#). The out-of-office policy must be created separately. When Kaspersky Endpoint Security is switched to mobile mode, the update task is started every two hours.

To configure the update settings for mobile mode:

1. In the main window of Web Console, select **Devices** → **Tasks**.

The list of tasks opens.

2. Click the **Update** task for Kaspersky Endpoint Security.

The task properties window opens.

The *Update* task is created automatically by the Initial Configuration Wizard of Kaspersky Security Center. To create the *Update* task, install the Kaspersky Endpoint Security for Windows web plug-in while running the Wizard.

Select the **Application settings** tab → **Mobile mode**.

3. Configure the sources of updates. The sources of updates can be Kaspersky update servers, other FTP- and HTTP servers, local folders, or network folders.

4. Click the **Save** button.

As a result, the databases and application modules will be updated on user computers when they switch to mobile mode.

Using a proxy server for updates

You may be required to specify proxy server settings to download database and application module updates from the update source. If there are multiple update sources, proxy server settings are applied for all sources. If a proxy server is not needed for some update sources, you can disable use of a proxy server in the policy properties. Kaspersky Endpoint Security will also use a proxy server to access Kaspersky Security Network and activation servers.

To configure a connection to update sources through a proxy server:

1. In the main window of Web Console, click .

The Administration Server properties window opens.

2. Go to the **Internet access settings** section.

3. Select the **Use proxy server** check box.

4. Configure the proxy server connection settings: proxy server address, port, and authentication settings (user name and password).

5. Click the **Save** button.

To disable use of a proxy server for a specific administration group:

1. In the main window of Web Console, select the **Devices** → **Policies and policy profiles** tab.
2. Click the name of the Kaspersky Endpoint Security policy for computers on which you want to disable use of a proxy server.
The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to the **General settings** → **Network settings** section.
5. In the **Proxy Server Settings** section, select **Do not use proxy server**.
6. Click **OK**.
7. Confirm your changes by clicking **Save**.

Starting and stopping an update task

Regardless of the selected update task run mode, you can start or stop a Kaspersky Endpoint Security update task at any time.

To start or stop an update task:

1. In the main application window, click the **Tasks** button.
2. Click the section with the name of the update task.
The selected section is expanded.
3. Do one of the following:
 - If you want to start the update task, select **Start** from the menu.
The task progress status that is displayed under the name of the update task changes to *Running*.
 - If you want to stop the update task, select **Stop** from the menu.
The task progress status that is displayed under the name of the update task changes to *Stopped*.

To start or stop the update task when the [simplified application interface](#) is displayed:

1. Right-click to bring up the context menu of the application icon that is in the taskbar notification area.
2. In the **Tasks** drop-down list in the context menu, do one of the following:
 - select a non-running update task to start it
 - select a running update task to stop it
 - select a paused update task to resume or restart it

Starting an update task under the rights of a different user account

By default, the Kaspersky Endpoint Security update task is started on behalf of the user whose account you have used to log in to the operating system. However, Kaspersky Endpoint Security may be updated from an update source that the user cannot access due to a lack of required rights (for example, from a shared folder that contains an update package) or an update source for which proxy server authentication is not configured. In the Kaspersky Endpoint Security settings, you can specify a user that has such rights and start the Kaspersky Endpoint Security update task under that user account.

To start an update task under a different user account:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Tasks** → **Update**.
3. In the **Run mode and update source** section, click the **Run mode** button.
The **Run mode** tab opens in the **Update** window.
4. On the **Run mode** tab, in the **User** section, select the **Run task as** check box.
5. In the **Name** field, enter the name of the user account whose rights are necessary for accessing the update source.
6. In the **Password** field, enter the password of the user whose rights are necessary for accessing the update source.
7. Save your changes.

Selecting the update task run mode

If it is not possible to run the update task for any reason (for example, the computer is not on at that time), you can configure the skipped task to be start automatically as soon as this becomes possible.

You can postpone starting the update task after the application starts if you select the **By schedule** update task run mode, and if the start time of Kaspersky Endpoint Security matches the update task start schedule. The update task can only be run after the specified time interval elapses after the startup of Kaspersky Endpoint Security.

To select the update task run mode:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Tasks** → **Update**.
3. Click the **Run mode** button.
The **Run mode** tab opens in the **Update** window.
4. In the **Run mode** section, select one of the following options for starting an update task:
 - If you want Kaspersky Endpoint Security to run the update task depending on whether or not an update package is available from the update source, select **Automatically**. The frequency of checks by Kaspersky Endpoint Security for update packages increases during virus outbreaks and is less at other times.
 - If you want to start an update task manually, select **Manually**.

- If you want to configure a startup schedule for the update task, select **By schedule**.

5. Do one of the following:

- If you have selected the **Automatically** or **Manually** option, go to step 6 in the instructions.
- If you have selected the **By schedule** option, specify the settings of the update task run schedule. To do so:
 - a. In the **Frequency** drop-down list, specify when to start the update task. Select one of the following options: **Minutes**, **Hours**, **Days**, **Every week**, **At a specified time**, **Every month**, or **After application startup**.
 - b. Depending on the item that is selected from the **Frequency** drop-down list, specify values for the settings that define the startup time of the update task.
 - c. In the **Postpone running after application startup for** field, specify the time interval by which the start of the update task is postponed after the startup of Kaspersky Endpoint Security.

If the **After application startup** item is selected from the **Frequency** drop-down list, the **Postpone running after application startup for** field is not available.

- d. If you want Kaspersky Endpoint Security to run skipped update tasks as soon as possible, select the **Run skipped tasks** check box.

If **Hours**, **Minutes** or **After application startup** is selected from the **Frequency** drop-down list, the **Run skipped tasks** check box is unavailable.

6. Save your changes.

Adding an update source

An *update source* is a resource that contains updates for databases and application modules of Kaspersky Endpoint Security.

Update sources include the Kaspersky Security Center server, Kaspersky update servers, and network or local folders.

The default list of update sources includes Kaspersky Security Center and Kaspersky update servers. You can add other update sources to the list. You can specify HTTP/FTP servers and shared folders as update sources.

Kaspersky Endpoint Security does not support updates from HTTPS servers unless they are Kaspersky's update servers.

If several resources are selected as update sources, Kaspersky Endpoint Security tries to connect to them one after another, starting from the top of the list, and performs the update task by retrieving the update package from the first available source.

To add an update source:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Tasks** → **Update**.
3. In the **Run mode and update source** section, click the **Update source** button.
4. On the **Source** tab, click the **Add** button.
5. In the window that opens, specify the address of the FTP or HTTP server, network folder or local folder that contains the update package.

The following path format is used for update source:

- For an FTP or HTTP server, enter its web address or IP address.
For example, `http://dn1-01.geo.kaspersky.com/` or `93.191.13.103`.
For an FTP server, you can specify the authentication settings within the address in the following format:
`ftp://<user name>:<password>@<node>:<port>`.
- For a network folder, enter the UNC path.
For example, `\\ Server\Share\Update distribution`.
- For a local folder, enter the full path to that folder.
For example, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

6. Save your changes.

Selecting the update server region

If you use Kaspersky update servers as an update source, you can select the location of the Kaspersky update server that is used to download the update package. Kaspersky update servers are located in several countries. Using the nearest Kaspersky update servers helps to reduce the time that is spent on retrieving an update package.

By default, the application uses information about the current region from the operating system's registry.

To select the update server region:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Tasks** → **Update**.
3. In the **Run mode and update source** section, click the **Update source** button.
4. On the **Source** tab, in the **Regional settings** section, choose **Select from the list**.
5. In the drop-down list, select the country that is nearest to your current location.
6. Save your changes.

Configuring updates from a shared folder

To conserve Internet traffic, you can configure updates of databases and application modules on computers of the organization's LAN from a shared folder. For this purpose, one of the computers on the organization's LAN must receive update packages from the Kaspersky Security Center Administration Server or from Kaspersky update servers and then copy the received update package to the shared folder. Other computers on the organization's LAN will be able to receive the update package from this shared folder.

Configuring database and application module updates from a shared folder consists of the following steps:

1. Enabling the copying of an update package to a shared folder on one of the computers on the local area network.
2. Configure database and application module updates from the specified shared folder to the remaining computers on the organization's LAN.

To enable copying of the update package to the shared folder:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Tasks** → **Update**.
3. In the **Additional** section, select the **Copy updates to folder** check box.
4. Enter the UNC path to the shared folder (for example, \\Server\Share\Update distribution).
5. Click the **Save** button.

To configure updates from a shared folder:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Tasks** → **Update**.
3. In the **Run mode and update source** section, click the **Update source** button.
4. On the **Source** tab, click the **Add** button.
5. In the window that opens, enter the path to the shared folder.

The source address must match the address that you previously specified when you configured copying of the update package to the shared folder (see the *instructions above*).

6. Click **OK**.
7. Configure the priorities of update sources by using the **Move up** and **Move down** buttons.
8. Save your changes.

Configuring application module updates

To configure application module updates:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Tasks** → **Update**.
3. In the **Additional** section, do one of the following:
 - Select the **Download updates of application modules** check box if you want the application to include application module updates in the update packages.
 - Otherwise, clear the **Download updates of application modules** check box.
4. If the **Download updates of application modules** check box was selected at the previous step, specify the conditions under which the application will install the application module updates:
 - Select the **Install critical and approved updates** option if you want the application to install critical updates of application modules automatically, and other updates after their installation is approved, locally via the application interface or using Kaspersky Security Center.
 - Select the **Install only approved updates** option if you want the application to install application module updates after their installation is approved, locally via the application interface or using Kaspersky Security Center.
5. To save changes, click the **Save** button.

Configuring proxy server use

To configure proxy server settings:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Network settings**.
3. In the **Proxy server** section, click the **Settings** button.
4. In the **Proxy Server Settings** window, select the **Use proxy server** check box.
5. Select one of the following options for determining the proxy server address:
 - **Automatically detect proxy server address.**
This option is selected by default.
 - **Use specified proxy server address and port.**
6. If you selected the **Use specified proxy server address and port** option, specify values in the **Address** and **Port** fields.

7. If you want to enable authentication on the proxy server, select the **Set user name and password for authentication** check box and specify values in the following fields:

- **User name.**

Field for entering the user name that is used for authentication on the proxy server.

- **Password.**

Field for entering the user password that is used for authentication on the proxy server.

8. If you want to disable proxy server use when [updating databases and application modules](#) from a shared folder, select the **Bypass proxy server for local addresses** check box.

9. Save your changes.

Last update rollback

After the databases and application modules are updated for the first time, the function of rolling back the databases and application modules to their previous versions becomes available.

Each time that a user starts the update process, Kaspersky Endpoint Security creates a backup copy of the current databases and application modules. This lets you roll back the databases and application modules to their previous versions when necessary. Rolling back the last update is useful, for example, when the new database version contains an invalid signature that causes Kaspersky Endpoint Security to block a safe application.

To roll back the last update:

1. Click the **Tasks** button located in the lower part of the main application window.

The **Tasks** window opens.

2. Click the section with the name of the update rollback task.

The selected section is expanded.

3. Click the **Start** button.

This starts the rollback task.

The task progress status that is displayed under the name of the rollback task changes to *Running*.

To start or stop a rollback task when the [simplified application interface](#) is displayed:

1. Right-click to bring up the context menu of the application icon that is in the taskbar notification area.

2. In the **Tasks** drop-down list in the context menu, do one of the following:

- Select a non-running rollback task to start it.
- Select a running rollback task to stop it.
- Select a paused rollback task to resume or restart it.

Working with active threats

Kaspersky Endpoint Security logs information about files that it has not processed for some reason. This information is recorded in the form of events in the list of active threats.

An infected file is considered *processed* if Kaspersky Endpoint Security performs one of the following actions on this file according to the specified application settings while scanning the computer for viruses and other threats:

- Disinfect.
- Remove.
- Delete if disinfection fails.

Kaspersky Endpoint Security moves the file to the list of active threats if, for any reason, Kaspersky Endpoint Security failed to perform an action on this file according to the specified application settings while scanning the computer for viruses and other threats.

This situation is possible in the following cases:

- The scanned file is unavailable (for example, it is located on a network drive or on a removable drive without write privileges).
- The action that is selected in the **Action on threat detection** section for scan tasks is **Inform**, and the user selects the **Skip** action when a notification about the infected file is displayed.

You can do one of the following:

- Manually start a Custom Scan task for files in the list of active threats after updating databases and application modules. File status may change after the scan.
- [Remove records from the list of active threats.](#)

Working with the list of active threats

The list of active threats is presented as a table of events related to infected files that were not processed for some reason.

You can perform the following actions with files from the list of active threats:

- View the list of active threats
- Scan active threats from the list using the current version of Kaspersky Endpoint Security databases and modules
- Restore files from the list of active threats to their original folders or to a different folder of your choice (when the original folder cannot be written to)
- Remove files from the list of active threats
- Open the folder where the file was initially located from the list of active threats

You can also perform the following actions while managing data in the table:

- Filter active threats based on column values or custom filter conditions.
- Use the active threat search function.
- Sort active threats.
- Change the order and arrangement of columns that are shown in the list of active threats.
- Group active threats.

If necessary, you can copy information about selected active threats to the clipboard.

Start custom scan task for files from the list of active threats

You can manually start a custom scan task for infected files that for some reason were not processed. You can start the scan if, for example, the last scan was interrupted for some reason or if you want to rescan files from the list of active threats after the latest update of databases and application modules.

To start a Custom Scan of files from the list of active threats:

1. In the main application window, click the <...> **active threats** section.
The **Active threats** window opens.
2. In the table in the **Active threats** window, select one or several records associated with files that you want to scan.
To select multiple entries, select them while holding down the **CTRL** key.
3. Start the Custom Scan task in one of the following ways:
 - Click the **Rescan** button.
 - Right-click to bring up the context menu and select **Rescan**.

Deleting records from the list of active threats

To delete records from the list active threats:

1. In the main application window, click the <...> **active threats** section.
The **Active threats** window opens.
2. In the table in the **Active threats** window select one or more records you want to delete from the list of active threats.
To select multiple entries, select them while holding down the **CTRL** key.
3. Delete the records in one of the following ways:
 - Click the **Delete** button.
 - Right-click to open the context menu and select **Delete**.

Checking the integrity of application

Kaspersky Endpoint Security checks the application files in the application installation folder for corruption or modifications. For example, if an application library has an incorrect digital signature, the library is considered corrupt. The *Integrity check* task is intended for scanning application files. Run the *Integrity check* task if Kaspersky Endpoint Security detected a malicious object but did not neutralize it.

You can create the *Integrity Check* task both in the Kaspersky Security Center 12 Web Console and in the Administration Console. It is not possible to create a task in the Kaspersky Security Center Cloud Console.

[How to run an application integrity check through the Administration Console \(MMC\)](#) 

1. In the Administration Console, go to the folder **Administration Server** → **Tasks**.

The list of tasks opens.

2. Click the **New task** button.

The Task Wizard starts. Follow the instructions of the Wizard.

Step 1. Selecting task type

Select **Kaspersky Endpoint Security for Windows (11.4.0)** → **Integrity check**.

Step 2. Selecting the devices to which the task will be assigned

Select the computers on which the task will be performed. The following options are available:

- Assign the task to an administration group. In this case, the task is assigned to computers included in a previously created administration group.
- Select computers detected by the Administration Server in the network: *unassigned devices*. The specific devices can include devices in administration groups as well as unassigned devices.
- Specify device addresses manually, or import addresses from a list. You can specify NetBIOS names, IP addresses, and IP subnets of devices to which you want to assign the task.

Step 3. Configuring a task start schedule

Configure a schedule for starting a task, for example, manually or when a virus outbreak is detected.

Step 4. Defining the task name

Enter a name for the task, for example, `Integrity check after the computer was infected`.

Step 5. Completing task creation

Exit the Wizard. If necessary, select the **Run task after Wizard finishes** check box. You can monitor the progress of the task in the task properties. As a result, Kaspersky Endpoint Security will check the integrity of the application. You can also configure an application integrity check schedule in the task properties.

[How to run an application integrity check through the Web Console](#) 

1. In the main window of Web Console, select **Devices** → **Tasks**.

The list of tasks opens.

2. Click the **Add** button.

The Task Wizard starts.

3. Configure the task settings:

a. In the **Application** drop-down list, select **Kaspersky Endpoint Security for Windows (11.4.0)**.

b. In the **Task type** drop-down list, select **Integrity check**.

c. In the **Task name** field, enter a brief description, for example, **Check the integrity of the application after a computer infection**.

d. In the **Select devices to which the task will be assigned** section, select the task scope.

4. Select devices according to the selected task scope option. Click the **Next** button.

5. Finish the wizard by clicking the **Finish** button.

A new task will be displayed in the list of tasks.

6. Select the check box next to the task.

As a result, Kaspersky Endpoint Security will check the integrity of the application. You can also configure an application integrity check schedule in the task properties.

Application integrity breaches may occur in the following cases:

- A malicious object modified files of Kaspersky Endpoint Security. In this case, perform the procedure for restoring Kaspersky Endpoint Security using the tools of the operating system. After restoration, run a full scan of the computer and repeat the integrity check.
- The digital signature expired. In this case, update Kaspersky Endpoint Security.

Computer protection

Kaspersky Security Network

To protect your computer more effectively, Kaspersky Endpoint Security uses data that is received from users around the globe. Kaspersky Security Network is designed for obtaining this data.

Kaspersky Security Network (KSN) is an infrastructure of cloud services providing access to the online Kaspersky Knowledge Base that contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky Endpoint Security to new threats, improves the performance of some protection components, and reduces the likelihood of false positives. If you are participating in Kaspersky Security Network, KSN services provide Kaspersky Endpoint Security with information about the category and reputation of scanned files, as well as information about the reputation of scanned web addresses.

Use of Kaspersky Security Network is voluntary. The application prompts you to use KSN during initial configuration of the application. Users can begin or discontinue participation in KSN at any time.

For more detailed information about sending Kaspersky statistical information that is generated during participation in KSN, and about the storage and destruction of such information, please refer to the Kaspersky Security Network Statement and the [Kaspersky website](#). The ksn_<language ID>.txt file with the text of the Kaspersky Security Network Statement is included in the application [distribution kit](#).

To reduce the load on KSN servers, Kaspersky experts may release application updates that temporarily disable or partly restrict requests to Kaspersky Security Network. In this case, the status of the connection to KSN in the local interface of the application is *Enabled with restrictions*.

KSN Infrastructure

Kaspersky Endpoint Security supports the following KSN infrastructural solutions:

- *Global KSN* is the solution that is used by most Kaspersky applications. KSN participants receive information from Kaspersky Security Network and send Kaspersky information about objects detected on the user's computer to be analyzed additionally by Kaspersky analysts and to be included in the reputation and statistical databases of Kaspersky Security Network.
- *Private KSN* is a solution that enables users of computers hosting Kaspersky Endpoint Security or other Kaspersky applications to obtain access to reputation databases of Kaspersky Security Network, and to other statistical data without sending data to KSN from their own computers. Private KSN is designed for corporate customers who are unable to participate in Kaspersky Security Network for any of the following reasons:
 - Local workstations are not connected to the Internet.
 - Transmission of any data outside the country or outside the corporate LAN is prohibited by law or restricted by corporate security policies.

By default, Kaspersky Security Center uses Global KSN. You can configure the use of Private KSN in the Administration Console (MMC) and Kaspersky Security Center 12 Web Console. It is not possible to configure the use of Private KSN in the Kaspersky Security Center Cloud Console.

For more details about Private KSN, please refer to the *documentation on Kaspersky Private Security Network*.

KSN Proxy

User computers managed by Kaspersky Security Center Administration Server can interact with KSN via the KSN Proxy service.

The KSN Proxy service provides the following capabilities:

- The user's computer can query KSN and submit information to KSN even without direct access to the Internet.
- The KSN Proxy service caches processed data, thereby reducing the load on the external network communication channel and speeding up receipt of the information that is requested by the user's computer.

For more details on the KSN Proxy service, please refer to the [Kaspersky Security Center Help Guide](#).

About data provision when using Kaspersky Security Network

By accepting the Kaspersky Security Network Statement, you agree to automatically transmit the following information:

- If the **Kaspersky Security Network** check box is selected and the **Extended KSN mode** check box is cleared, the application sends the following information:
 - information about KSN configuration updates: identifier of the active configuration, identifier of the configuration received, error code of the configuration update;
 - information about files and URL addresses to be scanned: checksums of the scanned file (MD5, SHA2-256, SHA1) and file patterns (MD5), the size of the pattern, type of the detected threat and its name according to Rightholder's classification, identifier for the anti-virus databases, URL address for which the reputation is being requested, as well as the referrer URL address, the connection's protocol identifier and the number of the port being used;
 - ID of the scan task during which the threat was detected;
 - information about digital certificates being used needed to verify their authenticity: the checksums (SHA256) of the certificate used to sign the scanned object and the certificate's public key;
 - identifier of the Software component performing the scan;
 - IDs of the anti-virus databases and of the records in these anti-virus databases;
 - information about the Rightholder's Software: type and full version of Kaspersky Endpoint Security, version of the protocol used to connect to Kaspersky services;
 - information about activation of the Software on the Computer: signed header of the ticket from the activation service (identifier of the regional activation center, checksum of the activation code, checksum of the ticket, ticket creation date, unique identifier of the ticket, ticket version, license status, start/end date and time of ticket validity, unique identifier of the license, license version), identifier of the certificate used to sign the ticket header, checksum (MD5) of the key file.
- If the **Extended KSN mode** check box is selected in addition to the **Kaspersky Security Network** check box, the application sends the following information in addition to the information listed above:

- information about the results of categorization of the requested web-resources, which contains the processed URL and IP address of the host, the version of the Software's component that performed the categorization, the method of categorization and set of the categories defined for the web-resource;
- information about the software installed on the Computer: names of the software applications and software vendors, registry keys and their values, information about files of the installed software components (checksums (MD5, SHA2-256, SHA1), name, path to the file on the Computer, size, version and the digital signature);
- information about the state of the Computer anti-virus protection: the versions and the release timestamps of the anti-virus databases being used, identifier of the task that performs scanning;
- information about files being downloaded by the End User: the URL and IP addresses of the download and the download pages, download protocol identifier and connection port number, the status of the URLs as malicious or not, file's attributes, size and checksums (MD5, SHA2-256, SHA1), information about the process that downloaded the file (checksums (MD5, SHA2-256, SHA1), creation/build date and time, autoplay status, attributes, names of packers, information about signatures, executable file flag, format identifier, and entropy), file name and its path on the Computer, the file's digital signature and timestamp of its generation, the URL address where detection occurred, the script's number on the page that appears to be suspicious or harmful, information about HTTP requests generated and the response to them;
- information about the running applications and their modules: data about processes running on the system (process ID (PID), process name, information about the account the process was started from, the application and command that started the process, the sign of trusted program or process, the full path to the process's files and their checksums (MD5, SHA2-256, SHA1), and the starting command line, level of the process's integrity, a description of the product that the process belongs to (the name of the product and information about the publisher), as well as digital certificates being used and information needed to verify their authenticity or information about the absence of a file's digital signature), and information about the modules loaded into the processes (their names, sizes, types, creation dates, attributes, checksums (MD5, SHA2-256, SHA1), the paths to them on the Computer), PE-file header information, names of packers (if the file was packed);
- information about all potentially malicious objects and activities: name of the detected object and full path to the object on the computer, checksums of processed files (MD5, SHA2-256, SHA1), detection date and time, names and sizes of infected files and paths to them, path template code, executable file flag, indicator of whether the object is a container, names of the packer (if the file was packed), file type code, file format ID, list of actions performed by malware and the decision made by the software and user in response to them, IDs of the anti-virus databases and of the records in these anti-virus databases that were used to make the decision, indicator of a potentially malicious object, the name of the detected threat according to the Rightholder's classification, the level of danger, the detection status and detection method, reason for inclusion into the analyzed context and sequence number of the file in the context, checksums (MD5, SHA2-256, SHA1), the name and attributes of the executable file of the application through which the infected message or link was transmitted, depersonalized IP addresses (IPv4 and IPv6) of the host of the blocked object, file entropy, file autorun indicator, time when the file was first detected in the system, the number of times the file has been run since the last statistics were sent, information about the name, checksums (MD5, SHA256, SHA1) and size of the mail client through which the malicious object was received, ID of the software task that performed the scan, indicator of whether the file reputation or signature was checked, file processing result, checksum (MD5) of the pattern collected for the object, the size of the pattern in bytes, and the technical specifications of the applied detection technologies;
- information about scanned objects: the assigned trust group to which and/or from which the file has been placed, the reason the file was placed in that category, category identifier, information about the source of the categories and the version of the category database, the file's trusted certificate flag, name of the file's vendor, file version, name and version of the software application which includes the file;
- information about vulnerabilities detected: the vulnerability ID in the database of vulnerabilities, the vulnerability danger class;

- information about emulation of the executable file: file size and its checksums (MD5, SHA2-256, SHA1), the version of the emulation component, emulation depth, an array of properties of logical blocks and functions within logical blocks obtained during the emulation, data from the executable file's PE headers;
- information about network attacks: the IP addresses of the attacking computer (IPv4 and IPv6), the number of the port on the Computer that the network attack is directed at, identifier of the protocol of the IP packet containing the attack, the attack's target (organization name, website), flag for the reaction to the attack, the attack's weight, trust level;
- information about attacks associated with spoofed network resources, the DNS and IP addresses (IPv4 and IPv6) of visited websites;
- DNS and IP addresses (IPv4 or IPv6) of the requested web resource, information about the file and web client accessing the web resource, the name, size and checksums (MD5, SHA2-256, SHA1) of the file, full path to the file and path template code, the result of checking its digital signature, and its status in KSN;
- information about rollback of malware actions: data on the file whose activity was rolled back (name of the file, full path to the file, its size and checksums (MD5, SHA2-256, SHA1)), data on successful and unsuccessful actions to delete, rename and copy files and restore the values in the registry (names of registry keys and their values), and information about system files modified by malware, before and after rollback;
- information about the exclusions set for the Adaptive anomaly control component: the ID and status of the rule that was triggered, the action performed by the Software when the rule was triggered, the type of user account under which the process or the thread performs suspicious activity, as well as about the process which was subject to suspicious activity (script ID or process file name, full path to the process file, path template code, check sums (MD5, SHA2-256, SHA1) of the process file); information about the object that performed the suspicious actions as well as about the object that was subject to the suspicious actions (registry key name or file name, full path to the file, path template code, and the checksums (MD5, SHA2-256, SHA1) of the file);
- information about loaded software modules: name, size and checksums (MD5, SHA2-256, SHA1) of the module file, full path to it and the path template code, digital signature settings of the module file, data and time of signature creation, name of the subject and organization that signed the module file, ID of the process in which the module was loaded, name of the module supplier, and the sequence number of the module in the loading queue;
- information about the quality of Software interaction with the KSN services: start and end date and time of the period when the statistics were generated, information about the quality of requests and connection to each of the KSN services used (KSN service ID, number of successful requests, number of requests with responses from cache, number of unsuccessful requests (network problems, KSN being disabled in the Software settings, incorrect routing), time spread of the successful requests, time spread of the cancelled requests, time spread of the requests with exceeded time limit, number of connections to KSN taken from cache, number of successful connections to KSN, number of unsuccessful connections to KSN, number of successful transactions, number of unsuccessful transactions, time spread of the successful connections to KSN, time spread of the unsuccessful connections to KSN, time spread of the successful transactions, time spread of the unsuccessful transactions);
- if a potentially malicious object is detected, information is provided about data in the processes' memory: elements of the system object hierarchy (ObjectManager), data in UEFI BIOS memory, names of registry keys and their values;
- information about events in the systems logs: the event's timestamp, the name of the log in which the event was found, type and category of the event, name of the event's source and the event's description;
- information about network connections: version and checksums (MD5, SHA2-256, SHA1) of the file from which process was started that opened the port, the path to the process's file and its digital signature, local

and remote IP addresses, numbers of local and remote connection ports, connection state, timestamp of the port's opening;

- information about the date of installation and activation of the Software on the Computer: identifier of the partner from whom the license was purchased, license serial number, the unique ID of the software installation on the computer, the type and ID of the application with which the update is performed, and the ID of the update task, information about installed Software components and their operation state;
- information about the set of all installed updates, and the set of most recently installed/removed updates, the type of event that caused the update information to be sent, duration since the installation of last update, information about any currently installed anti-virus databases;
- information about software operation on the computer: data on CPU usage, data on memory usage (Private Bytes, Non-Paged Pool, Paged Pool), number of active threads in the software process and pending threads, and the duration of software operation prior to the error;
- number of software dumps and system dumps (BSOD) since the Software was installed and since the time of the last update, the identifier and version of the Software module that crashed, the memory stack in the Software's process, and information about the anti-virus databases at the time of the crash;
- data on the system dump (BSOD): a flag indicating the occurrence of the BSOD on the Computer, the name of the driver that caused the BSOD, the address and memory stack in the driver, a flag indicating the duration of the OS session before the BSOD occurred, memory stack of driver that crashed, type of stored memory dump, flag for the OS session before BSOD lasted more than 10 minutes, unique identifier of the dump, timestamp of the BSOD;
- information about errors or performance problems that occurred during operation of the Software components: the status ID of the Software, error type, code and cause as well of the time when the error occurred, the IDs of the component, module and process of the product in which the error occurred, the ID of the task or update category during which the error occurred, logs of drivers used by the Software (error code, module name, name of the source file and the line where the error occurred);
- information about updates of anti-virus databases and Software components: the name, date and time of index files downloaded during the last update and being downloaded during the current update;
- information about abnormal termination of the Software operation: the creation timestamp of the dump, its type, the type of event that caused the abnormal termination of the Software operation (unexpected power-off, third-party application crash), date and time of the unexpected power-off;
- information about the compatibility of Software drivers with hardware and Software: information about OS properties that restrict the functionality of Software components (Secure Boot, KPTI, WHQL Enforce, BitLocker, Case Sensitivity), type of download Software installed (UEFI, BIOS), Trusted Platform Module (TPM) identifier, TPM specification version, information about the CPU installed on the Computer, operating mode and parameters of Code Integrity and Device Guard, operating mode of drivers and reason for use of the current mode, version of Software drivers, software and hardware virtualization support status of the Computer;
- information about third-party applications that caused the error: their name, version and localization, the error code and information about the error from the system log of applications, the address of the error and memory stack of the third-party application, a flag indicating the occurrence of the error in the Software component, the length of time the third-party application was in operation before the error occurred, checksums (MD5, SHA2-256, SHA1) of the application process image, in which the error occurred, path to the application process image and template code of the path, information from the system log with a description of the error associated with the application, information about the application module, in which an error occurred (exception identifier, crash memory address as an offset in the application module, name and version of the module, identifier of the application crash in the Rightholder's plug-in and memory stack of the crash, duration of the application session before crash);

- version of the Software updater component, number of crashes of the updater component while running update tasks over the lifetime of the component, ID of the update task type, number of failed attempts of the updater component to complete update tasks;
- information about the operation of the Software system monitoring components: full versions of the components, date and time when the components were started, code of the event that overflowed the event queue and number of such events, the total number of queue overflow events, information about the file of the process of the initiator of the event (file name and its path on the Computer, template code of the file path, checksums (MD5, SHA2-256, SHA1) of the process associated with the file, file version), identifier of the event interception that occurred, the full version of the interception filter, identifier of the type of the intercepted event, size of the event queue and the number of events between the first event in the queue and the current event, number of overdue events in the queue, information about the file of the process of the initiator of the current event (file name and its path on the Computer, template code of the file path, checksums (MD5, SHA2-256, SHA1) of the process associated with the file), duration of the event processing, maximum duration of the event processing, probability of sending statistics, information about OS events for which the processing time limit was exceeded (date and time of the event, number of repeated initializations of anti-virus databases, date and time of the last repeated initialization of anti-virus databases after their update, event processing delay time for each system monitoring component, number of queued events, number of processed events, number of delayed events of the current type, total delay time for the events of the current type, total delay time for all events);
- information from the Windows event tracing tool (Event Tracing for Windows, ETW) in the event of Software performance problems, suppliers of SysConfig / SysConfigEx / WinSATAssessment events from Microsoft: information about the Computer (model, manufacturer, form factor of the housing, version), information about Windows performance metrics (WinSAT assessments, Windows performance index), domain name, information about physical and logical processors (number of physical and logical processors, manufacturer, model, stepping level, number of cores, clock frequency, CPUID, cache characteristics, logic processor characteristics, indicators of supported modes and instructions), information about RAM modules (type, form factor, manufacturer, model, capacity, granularity of memory allocation), information about network interfaces (IP and MAC addresses, name, description, configuration of network interfaces, breakdown of number and size of network packages by type, speed of network exchange, breakdown of number of network errors by type), configuration of IDE controller, IP addresses of DNS servers, information about the video card (model, description, manufacturer, compatibility, video memory capacity, screen permission, number of bits per pixel, BIOS version), information about plug-and-play devices (name, description, device identifier [PnP, ACPI], information about disks and storage devices (number of disks or flash drives, manufacturer, model, disk capacity, number of cylinders, number of tracks per cylinder, number of sectors per track, sector capacity, cache characteristics, sequential number, number of partitions, configuration of SCSI controller), information about logical disks (sequential number, partition capacity, volume capacity, volume letter, partition type, file system type, number of clusters, cluster size, number of sectors per cluster, number of empty and occupied clusters, letter of bootable volume, offset address of partition in relation to the start of the disk), information about BIOS motherboard (manufacturer, release date, version), information about motherboard (manufacturer, model, type), information about physical memory (shared and free capacity), information about operating system services (name, description, status, tag, information about processes [name and PID]), energy consumption parameters for the Computer, configuration of interrupt controller, path to Windows system folders (Windows and System32), information about the OS (version, build, release date, name, type, installation date), size of page file, information about monitors (number, manufacturer, screen permission, resolution capacity, type), information about video card driver (manufacturer, release date, version);
- information from ETW, suppliers of EventTrace / EventMetadata events from Microsoft: information on the sequence of system events (type, time, date, time zone), metadata about the file with trace results (name, structure, trace parameters, breakdown of number of trace operations by type), information about the OS (name, type, version, build, release date, start time);
- information from ETW, suppliers of Process / Microsoft Windows Kernel Process / Microsoft Windows Kernel Processor Power events from Microsoft: information about started and completed processes (name, PID, start parameters, command line, return code, power management parameters, start and completion time, access token type, SID, SessionID, number of descriptors installed), information about changes in

thread priorities (TID, priority, time), information about disk operations of the process (type, time, capacity, number), history of changes to the structure and capacity of usable memory processes;

- information from ETW, suppliers of StackWalk / Perfinfo events from Microsoft: information about performance counters (performance of individual code sections, sequence of function calls, PID, TID, addresses and attributes of ISRs and DPCs);
- information from ETW, supplier of KernelTraceControl-ImageID events from Microsoft: information on executable files and dynamic libraries (name, image size, full path), information on PDB files (name, identifier), VERSIONINFO resource data for executable files (name, description, creator, localization, application version and identifier, file version and identifier);
- information from ETW, suppliers of FileIo / DiskIo / Image / Windows Kernel Disk events from Microsoft: information on file and disk operations (type, capacity, start time, completion time, duration, completion status, PID, TID, driver function call addresses, I/O Request Packet (IRP), Windows file object attributes), information about files involved in file and disk operations (name, version, size, full path, attributes, offset, image checksum, open and access options);
- information from ETW, supplier of PageFault events from Microsoft: information on memory page access errors (address, time, capacity, PID, TID, attributes of Windows file object, memory allocation parameters);
- information from ETW, supplier of Thread events from Microsoft: information on thread creation/completion, information on threads started (PID, TID, size of stack, priorities and allocation of CPU resources, I/O resources, memory pages between threads, stack address, address of init function, address of Thread Environment Block (TEB), Windows service tag);
- information from ETW, supplier of Microsoft Windows Kernel Memory events from Microsoft: information about memory management operations (completion status, time, quantity, PID), memory allocation structure (type, capacity, SessionID, PID);
- information about Software operation in the event of performance problems: Software installation identifier, type and value of drop in performance, information about the sequence of events within the Software (time, time zone, type, completion status, Software component identifier, Software operating scenario identifier, TID, PID, function call addresses), information about network connections to be checked (URL, direction of the connection, size of network package), information about PDB files (name, identifier, image size of executable file), information about files to be checked (name, full path, checksum), Software performance monitoring parameters;
- information about the last unsuccessful OS restart: the number of unsuccessful restarts since OS installation, data on the system dump (code and parameters of an error, name, version and checksum (CRC32) of the module that caused an error in the OS operation, error address as an offset in the module, checksums (MD5, SHA2-256, SHA1) of the system dump);
- information to verify authenticity of digital certificates being used to sign files: the certificate's fingerprint, the checksum algorithm, the certificate's public key and serial number, the name of the issuer of the certificate, the result of certificate validation and the certificate's database identifier;
- information about the process executing the attack on the Software's self-defense: the name and size of the process file, its checksums (MD5, SHA2-256, SHA1), the full path to the process file and the template code of the file path, the creation/build timestamps, executable file flag, attributes of the process file, information about the certificate used to sign the process file, code of the account used to launch the process, ID of operations performed to access the process, type of resource with which the operation is performed (process, file, registry object, FindWindow search function), name of resource with which the operation is performed, flag indicating success of the operation, the status of the file of the process and its signature according to the KSN;
- information about the Rightholder's Software: its localization language and operation state, versions of the installed Software components and their operation state, information about the installed updates, the value

of the TARGET filter;

- information about hardware installed on the Computer: type, name, model name, firmware version, parameters of built-in and connected devices, the unique identifier of the Computer with the installed Software;
- information about the versions of the operating system and installed updates, the word size, edition and parameters of the OS run mode, version and checksums (MD5, SHA2-256, SHA1) of the OS kernel file, and OS startup date and time;
- executable and non-executable files or their parts, including trusted files;
- portions of the Computer's RAM;
- sectors involved in the process of booting the OS;
- network traffic data packets;
- web pages and emails containing suspicious and malicious objects;
- description of the classes and instances of classes of the WMI repository;
- application activity reports: the name, size and version of the file being sent, its description and checksums (MD5, SHA2-256, SHA1), file format identifier, the name of the file's vendor, the product name to which the file belongs, full path on the Computer, template code of the file path, the creation and modification timestamps of the file; start and end date/time of the validity period of the certificate (if the file has a digital signature), the date and the time of the signature, the name of the issuer of the certificate, information about the certificate holder, the fingerprint, the certificate's public key and appropriate algorithms, and the certificate's serial number; the name of the account from which the process is running; checksums (MD5, SHA2-256, SHA1) of the name of the Computer on which the process is running; titles of the process windows; identifier for the anti-virus databases, name of the detected threat according to Rightholder's classification; data about the installed license, its identifier, type and expiration date; local time of the Computer at the moment of the provision of information; names and paths of the files that were accessed by the process; names of registry keys and their values that were accessed by the process; URL and IP addresses that were accessed by the process; URL and IP addresses from which the running file was downloaded.

Enabling and disabling use of Kaspersky Security Network

To enable or disable use of Kaspersky Security Network:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Kaspersky Security Network**.
3. Select the **Kaspersky Security Network** check box if you want Kaspersky Endpoint Security to use information about the reputation of files, web resources, and applications received from Kaspersky Security Network databases.

Kaspersky Endpoint Security will display the Kaspersky Security Network Statement. Please read and accept the terms of the Kaspersky Security Network (KSN) Statement if you agree to them.

By default, Kaspersky Endpoint Security uses the Extended KSN mode. *Extended KSN mode* is a mode in which Kaspersky Endpoint Security sends [additional data](#) to Kaspersky.

4. If required, clear the **Enable Extended KSN mode** check box.

5. Save your changes.

Enabling and disabling cloud mode for protection components

When using Kaspersky Private Security Network, cloud mode functionality is available starting with Kaspersky Private Security Network version 3.0.

To enable or disable cloud mode for protection components:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Kaspersky Security Network**.
3. Do one of the following:

- Select the **Enable cloud mode for protection components** check box.

If the check box is selected, Kaspersky Endpoint Security uses the light version of anti-virus databases, which reduces the load on operating system resources.

Kaspersky Endpoint Security downloads the light version of anti-virus databases during the next update after the check box was selected.

If the light version of anti-virus databases is not available for use, Kaspersky Endpoint Security automatically switches to the premium version of anti-virus databases.

- Clear the **Enable cloud mode for protection components** check box.

If the check box is cleared, Kaspersky Endpoint Security uses the full version of anti-virus databases.

Kaspersky Endpoint Security downloads the full version of anti-virus databases during the next update after the check box was cleared.

This check box is available if the **Kaspersky Security Network** check box is selected.

4. Save your changes.

Checking the connection to Kaspersky Security Network

To check the connection to Kaspersky Security Network:

1. In the main application window, click the **Threat detection technologies** section.

The following information about Kaspersky Security Network performance appears in the lower part of the **Threat detection technologies** window:

- One of the following status values of Kaspersky Endpoint Security connection to Kaspersky Security Network appears under the **Kaspersky Security Network (KSN)** line:
 - *Enabled. Available.*
This status means that Kaspersky Security Network is being used in Kaspersky Endpoint Security operations and KSN servers are available.
 - *Enabled. Not available.*
This status means that Kaspersky Security Network is being used in Kaspersky Endpoint Security operations and KSN servers are unavailable.
 - *Disabled.*
This status means that Kaspersky Security Network is not being used in Kaspersky Endpoint Security operations.
- The lines **Whitelisted objects**, **Blacklisted objects**, and **Threats neutralized in the last 24 hours** display global statistics of the infrastructure of Kaspersky Security Network cloud services.
- The **Last synchronization** line shows the date and time of the most recent synchronization of Kaspersky Endpoint Security with KSN servers.

The application receives KSN usage statistics when the **Threat detection technologies** window is opened. The global statistics of the Kaspersky Security Network cloud service infrastructure and the **Last synchronization** line are not refreshed in real time.

If the time that has elapsed since the last synchronization with KSN servers exceeds 15 minutes or shows the *Unknown* status, the status of the Kaspersky Endpoint Security connection to Kaspersky Security Network takes the *Enabled value. Not available*.

A connection to Kaspersky Security Network servers may be absent due to the following reasons:

- The computer is not connected to the Internet.
- Application is not activated.
- License expired.
- License key issues have been identified (for example, the key has been blacklisted).

If the connection with Kaspersky Security Network servers cannot be restored, it is recommended to contact Technical Support or your service provider.

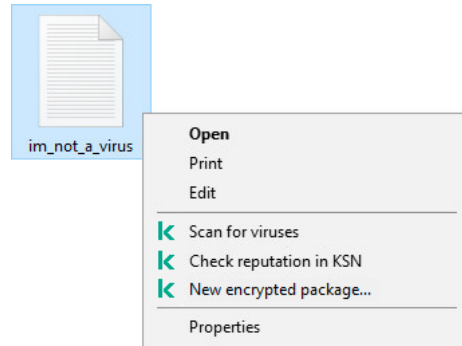
Checking the reputation of a file in Kaspersky Security Network

If you are doubtful of the security of a file, you can check its reputation in Kaspersky Security Network.

You can check the reputation of a file if you have accepted the terms of the [Kaspersky Security Network Statement](#).

To check the reputation of a file in Kaspersky Security Network:


Open the file context menu and select the **Check reputation in KSN** option (see the figure below).





File context menu

Kaspersky Endpoint Security displays the file reputation:

 **Trusted.** Most users of Kaspersky Security Network have confirmed that the file is trusted.

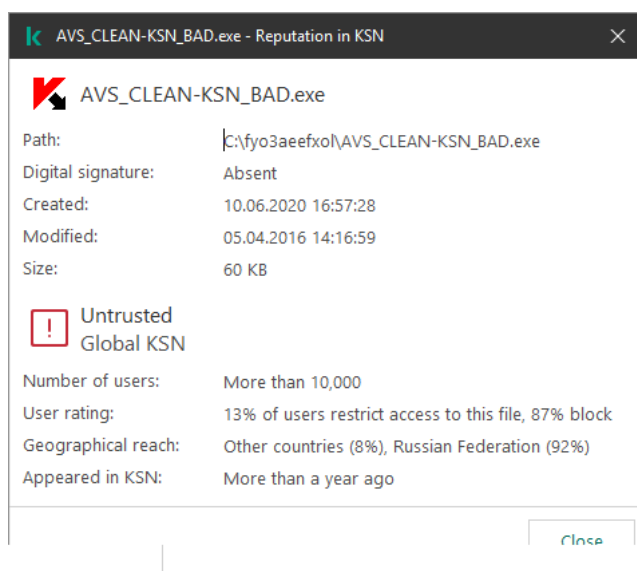
 **Legitimate software that could be exploited to harm your computer or personal data.** Although they do not have any malicious functions, such applications can be exploited by intruders. For details on legitimate software that could be used by criminals to harm the computer or personal data of a user, please visit the website of the [Kaspersky IT Encyclopedia](#). You can [add these applications to the trusted list](#).

 **Untrusted.** A virus or other application that [poses a threat](#).

 **Unknown.** Kaspersky Security Network does not have any information about the file. You can scan a file using anti-virus databases (the **Scan for viruses** option in the context menu).

Kaspersky Endpoint Security displays the KSN solution that was used to determine the reputation of the file: *Global KSN* or *Private KSN*.

Kaspersky Endpoint Security also displays additional information about the file (see the figure below).



Reputation of a file in Kaspersky Security Network

Behavior Detection

The Behavior Detection component receives data on the actions of applications on your computer and provides this information to other protection components to improve their performance.

The Behavior Detection component utilizes Behavior Stream Signatures (BSS) for applications. If application activity matches a behavior stream signature, Kaspersky Endpoint Security performs the selected responsive action. Kaspersky Endpoint Security functionality based on behavior stream signatures provides proactive defense for the computer.

Enabling and disabling Behavior Detection

By default, Behavior Detection is enabled and runs in the mode recommended by Kaspersky experts. You can disable Behavior Detection if necessary.

It is not recommended to disable Behavior Detection unless absolutely necessary because doing so would reduce the effectiveness of the protection components. The protection components may request data collected by the Behavior Detection component to detect threats.

To enable or disable Behavior Detection:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Behavior Detection**.
3. Do one of the following:
 - Select the **Behavior Detection** check box if you want Kaspersky Endpoint Security to use behavior stream signatures to analyze application activity in the operating system.
 - Clear the **Behavior Detection** check box if you do not want Kaspersky Endpoint Security to use behavior stream signatures to analyze application activity in the operating system.

4. Save your changes.

Selecting the action to take on detecting malware activity

In order to choose what to do if an application engages in malicious activity, perform the following steps:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Behavior Detection**.
3. Select the necessary action in the **On detecting malware activity** drop-down list:
 - **Delete file.**
If this item is selected, on detecting malicious activity Kaspersky Endpoint Security deletes the executable file of the malicious application and creates a backup copy of the file in Backup.
 - **Terminate the program.**
If this item is selected, on detecting malicious activity Kaspersky Endpoint Security terminates this application.
 - **Inform.**
If this item is selected and malware activity of an application is detected, Kaspersky Endpoint Security adds information about the malware activity of the application to the list of active threats.

4. Save your changes.

Protection of shared folders against external encryption

The component monitors operations performed only with those files that are stored on mass storage devices with the NTFS file system and that are not encrypted with EFS.

Protection of shared folders against external encryption provides for analysis of activity in shared folders. If this activity matches a behavior stream signature that is typical for external encryption, Kaspersky Endpoint Security performs the selected action.

By default, protection of shared folders against external encryption is disabled.

After Kaspersky Endpoint Security is installed, the protection of shared folders against external encryption will be limited until the computer is restarted.

Enabling and disabling protection of shared folders against external encryption

After Kaspersky Endpoint Security is installed, the protection of shared folders against external encryption will be limited until the computer is restarted.

To enable or disable protection of shared folders against external encryption:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Behavior Detection**.
3. In the **Protection of shared folders against external encryption** section, do one of the following:
 - Select the **Enable protection of shared folders against external encryption** check box if you want Kaspersky Endpoint Security to analyze activity that is typical for external encryption.
 - Clear the **Enable protection of shared folders against external encryption** check box if you do not want Kaspersky Endpoint Security to analyze activity that is typical for external encryption.
4. Save your changes.

Selecting the action to take on detection of external encryption of shared folders

To select the action to take on detection of external encryption of shared folders:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Behavior Detection**.
3. In the **Protection of shared folders against external encryption** section, in the **On detection of external encryption of shared folders** drop-down list, select the necessary action:

- **Block connection.**

If this option is selected and Kaspersky Endpoint Security detects an attempt to modify files in shared folders, it performs the following actions:

- Blocks network activity of the computer attempting the modification.
- Creates backup copies of files that are being modified.
- Adds an entry to [local application interface reports](#).
- Sends information about the detected malicious activity to Kaspersky Security Center.

Also, if the [Remediation Engine component is enabled](#), the modified files are restored from backup copies.

If you selected **Block connection**, you can specify the duration (in minutes) that the network connection will be blocked in the **Block connection for N minutes** field.

- **Inform.**

If this option is selected, on detecting an attempt to modify files in shared folders, Kaspersky Endpoint Security adds a record to [local application interface reports](#), adds a record to [list of active threats](#) and sends to Kaspersky Security Center information about detection of malicious activity.

4. Save your changes.

Creating an exclusion for protection of shared folders against external encryption

Excluding a folder can reduce the amount of false positives if your organization uses data encryption when exchanging files using shared folders. For example, Behavior Detection can raise false positives when the user works with files with the ENC extension in a shared folder. Such activity matches a behavioral pattern that is typical for external encryption. If you have encrypted files in a shared folder to protect data, add that folder to exclusions.

[How to create an exclusion for protection of shared folders using the Administration Console \(MMC\)](#) 

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **General settings** → **Exclusions**.
6. In the **Scan exclusions and trusted applications** block, click the **Settings** button.
7. In the window that opens, select the **Scan exclusions** tab.
This opens a window containing a list of exclusions.
8. Select the **Merge values when inheriting** check box if you want to create a consolidated list of exclusions for all computers in the company. The lists of exclusions in the parent and child policies will be merged. The lists will be merged provided that merging values when inheriting is enabled. Exclusions from the parent policy are displayed in child policies in a read-only view. Changing or deleting exclusions of the parent policy is not possible.
9. Select the **Allow use of local trusted applications** check box if you want to enable the user to create a local list of exclusions. This way, a user can create their own local list of exclusions in addition to the general list of exclusions generated in the policy. An administrator can use Kaspersky Security Center to view, add, edit, or delete list items in the computer properties.
If the check box is cleared, the user can access only the general list of exclusions generated in the policy. If a local list was generated, after this functionality is disabled Kaspersky Endpoint Security continues excluding the listed files from scans.
10. Click **Add**.
11. In the **Properties** block, select the **File or folder** check box.
12. Click the **select file or folder** link in the **Scan exclusion description (click underlined items to edit them)** block to open the **Name of file or folder** window.
13. Click **Browse** and select the shared folder.

You can also manually enter the path. Kaspersky Endpoint Security supports the * and ? characters when entering a mask:

- The * (asterisk) character, which takes the place of any set of characters, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:**.txt will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.
- Two consecutive * characters take the place of any set of characters (including an empty set) in the file or folder name, including the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\Folder***.txt will include all paths to files with the TXT extension located in folders nested within the Folder, except the Folder itself. The mask must include at least one nesting level. The mask C:***.txt is not a valid mask.
- The ? (question mark) character, which takes the place of any single character, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the

mask C:\Folder\???.txt will include paths to all files residing in the folder named Folder that have the TXT extension and a name consisting of three characters.

14. If necessary, in the **Comment** field, enter a brief comment on the scan exclusion that you are creating.
15. Click the **any** link in the **Scan exclusion description (click underlined items to edit them)** block to activate the **select components** link.
16. Click the **select components** link to open the **Protection components** window.
17. Select the check box next to the **Behavior Detection** component.
18. Save your changes.

[How to create an exclusion for protection of shared folders using the Web Console and Cloud Console](#) 

1. In the main window of the Web Console, select **Devices** → **Policies & Profiles**.
2. Click the name of the Kaspersky Endpoint Security policy.
The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General settings** → **Exclusions**.
5. In the **Scan exclusions and trusted applications** block, click the **Scan exclusions** link.
6. Select the **Merge values when inheriting** check box if you want to create a consolidated list of exclusions for all computers in the company. The lists of exclusions in the parent and child policies will be merged. The lists will be merged provided that merging values when inheriting is enabled. Exclusions from the parent policy are displayed in child policies in a read-only view. Changing or deleting exclusions of the parent policy is not possible.
7. Select the **Allow use of local trusted applications** check box if you want to enable the user to create a local list of exclusions. This way, a user can create their own local list of exclusions in addition to the general list of exclusions generated in the policy. An administrator can use Kaspersky Security Center to view, add, edit, or delete list items in the computer properties.

If the check box is cleared, the user can access only the general list of exclusions generated in the policy. If a local list was generated, after this functionality is disabled Kaspersky Endpoint Security continues excluding the listed files from scans.
8. Click the **Add** button.
9. Select how you want to add the exclusion **File or folder**.
10. Click **Browse** and select the shared folder.

You can also manually enter the path. Kaspersky Endpoint Security supports the * and ? characters when entering a mask:
 - The * (asterisk) character, which takes the place of any set of characters, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:**.txt will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.
 - Two consecutive * characters take the place of any set of characters (including an empty set) in the file or folder name, including the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\Folder***.txt will include all paths to files with the TXT extension located in folders nested within the Folder, except the Folder itself. The mask must include at least one nesting level. The mask C:***.txt is not a valid mask.
 - The ? (question mark) character, which takes the place of any single character, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\Folder\???.txt will include paths to all files residing in the folder named Folder that have the TXT extension and a name consisting of three characters.
11. In the **Protection components** block, select the **Behavior Detection** component.
12. If necessary, in the **Comment** field, enter a brief comment on the scan exclusion that you are creating.
13. Select the **Active** status for the exclusion.

You can use the toggle to [stop an exclusion](#) at any time.

14. Save your changes.

[How to create an exclusion for protection of shared folders in the application interface](#)

1. In the main application window, click the  icon_settings button.

2. In the application settings window, select **General settings** → **Threats and Exclusions**.

3. In the **Exclusions** block, click the **Manage exclusions** link.

4. Click **Add**.

5. Click **Browse** and select the shared folder.

You can also manually enter the path. Kaspersky Endpoint Security supports the * and ? characters when entering a mask:

- The * (asterisk) character, which takes the place of any set of characters, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:**.txt will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.
- Two consecutive * characters take the place of any set of characters (including an empty set) in the file or folder name, including the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\Folder***.txt will include all paths to files with the TXT extension located in folders nested within the Folder, except the Folder itself. The mask must include at least one nesting level. The mask C:***.txt is not a valid mask.
- The ? (question mark) character, which takes the place of any single character, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\Folder\???.txt will include paths to all files residing in the folder named Folder that have the TXT extension and a name consisting of three characters.

6. In the **Protection components** block, select the **Behavior Detection** component.

7. If necessary, in the **Comment** field, enter a brief comment on the scan exclusion that you are creating.

8. Select the **Active** status for the exclusion.

You can use the toggle to [stop an exclusion](#) at any time.

9. Save your changes.

Configuring addresses of exclusions from protection of shared folders against external encryption

The Audit Logon service must be enabled to enable exclusions of addresses from protection of shared folders against external encryption. By default, the Audit Logon service is disabled (for detailed information about enabling the Audit Logon service, please visit the Microsoft website).

The functionality for excluding addresses from shared folder protection does not work on a remote computer if the remote computer was turned on before Kaspersky Endpoint Security was started. You can restart this remote computer after Kaspersky Endpoint Security is started to ensure that the functionality for excluding addresses from shared folder protection works on this remote computer.

To exclude remote computers that perform external encryption of shared folders:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Behavior Detection**.
3. In the **Protection of shared folders against external encryption** section, click the **Exclusions** button.
The **Exclusions** window opens.
4. Do one of the following:
 - If you want to add an IP address or computer name to the list of exclusions, click the **Add** button.
 - If you want to edit an IP address or computer name, select it in the list of exclusions and click the **Edit** button.The **Computer** window opens.
5. Enter the IP address or name of the computer from which external encryption attempts must not be handled.
6. Save your changes.

Exploit Prevention

The Exploit Prevention component detects program code that takes advantage of vulnerabilities on the computer to exploit administrator privileges or to perform malicious activities. For example, exploits can utilize a buffer overflow attack. To do so, the exploit sends a large amount of data to a vulnerable application. When processing this data, the vulnerable application executes malicious code. As a result of this attack, the exploit can start an unauthorized installation of malware.

When there is an attempt to run an executable file from a vulnerable application that was not performed by the user, Kaspersky Endpoint Security blocks this file from running or notifies the user.

Enabling and disabling Exploit Prevention

By default, Exploit Prevention is enabled and runs in the mode recommended by Kaspersky experts. You can disable Exploit Prevention if necessary.

To enable or disable Exploit Prevention:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Exploit Prevention**.
3. Do one of the following:
 - Select the **Exploit Prevention** check box if you want Kaspersky Endpoint Security to monitor executable files that are run by vulnerable applications.
If Kaspersky Endpoint Security detects that an executable file from a vulnerable application was run by something other than the user, Kaspersky Endpoint Security will perform the action that is selected in the **On detecting exploit** drop-down list.
 - Clear the **Exploit Prevention** check box if you do not want Kaspersky Endpoint Security to monitor executable files that are run by vulnerable applications.
4. Save your changes.

Selecting an action to take when an exploit is detected

By default, on detection of an exploit, Kaspersky Endpoint Security blocks operations attempted by the exploit.

To choose an action to be taken when an exploit is detected:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Exploit Prevention**.
3. Select the necessary action in the **On detecting exploit** drop-down list:
 - **Block operation.**
If this item is selected, on detecting an exploit, Kaspersky Endpoint Security blocks the operations of this exploit and makes a log entry with information about this exploit.
 - **Inform.**
If this item is selected, when Kaspersky Endpoint Security detects an exploit it logs an entry containing information about the exploit and adds information about this exploit to the list of active threats.
4. Save your changes.

Enabling and disabling system processes memory protection

By default, protection of system process memory is enabled.

To enable or disable system process memory protection:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Exploit Prevention**.
3. Do one of the following:

- In the **System processes memory protection** section, select the **Enable system process memory protection** check box if you want Kaspersky Endpoint Security to block external processes that attempt to access system processes.
- In the **System processes memory protection** section, clear the **Enable system process memory protection** check box, if you do not want Kaspersky Endpoint Security to block external processes that attempt to access system processes.

4. Save your changes.

Host Intrusion Prevention

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Windows for workstations. This component is unavailable if Kaspersky Endpoint Security is installed on a computer that runs on Windows for servers.

The Host Intrusion Prevention component prevents applications from performing actions that may be dangerous for the operating system, and ensures control over access to operating system resources and personal data. The component provides computer protection with the help of anti-virus databases and the Kaspersky Security Network cloud service.

The component controls the operation of applications by using *application rights*. Application rights include the following access parameters:

- Access to operating system resources (for example, automatic startup options, registry keys)
- Access to personal data (such as files and applications)

Network activity of applications is controlled by the [Firewall](#) using *network rules*.

During the first startup of the application, the Host Intrusion Prevention component performs the following actions:

1. Checks the security of the application using downloaded anti-virus databases.
2. Checks the security of the application in Kaspersky Security Network.

You are advised to [participate in Kaspersky Security Network](#) to help the Host Intrusion Prevention component work more effectively.

3. Puts the application in one of the *trust groups*: Trusted, Low Restricted, High Restricted, Untrusted.

A [trust group defines the rights](#) used by Kaspersky Endpoint Security when controlling network activity of applications. Kaspersky Endpoint Security places an application in a trust group depending on the level of danger that this application may pose to the computer.

Kaspersky Endpoint Security places an application in a trust group for the Firewall and Host Intrusion Prevention components. You cannot change the trust group only for the Firewall or Host Intrusion Prevention.

If you refused to participate in KSN or there is no network, Kaspersky Endpoint Security places the application in a trust group depending on the [settings of the Host Intrusion Prevention component](#). After receiving the reputation of the application from KSN, the trust group can be changed automatically.

4. Blocks application actions depending on the trust group. For example, applications from the High Restricted trust group are denied access to the operating system modules.

The next time the application is started, Kaspersky Endpoint Security checks the integrity of the application. If the application is unchanged, the component uses the current application rights for it. If the application has been modified, Kaspersky Endpoint Security analyzes the application as if it were being started for the first time.

Limitations of audio and video device control

About audio stream protection

Audio stream protection has the following special considerations:

- The Host Intrusion Prevention component must be enabled for this functionality to work.
- If the application started receiving the audio stream before the Host Intrusion Prevention component was started, Kaspersky Endpoint Security allows the application to receive the audio stream and does not show any notifications.
- If you moved the application to the **Untrusted** group or **High Restricted** group after the application began receiving the audio stream, Kaspersky Endpoint Security allows the application to receive the audio stream and does not show any notifications.
- After the settings for the application's access to sound recording devices have been changed (for example, if the application has been blocked from receiving the audio stream in the Host Intrusion Prevention settings window), this application must be restarted to stop it from receiving the audio stream.
- Control of access to the audio stream from sound recording devices does not depend on an application's webcam access settings.
- Kaspersky Endpoint Security protects access to only built-in microphones and external microphones. Other audio streaming devices are not supported.
- Kaspersky Endpoint Security cannot guarantee the protection of an audio stream from such devices as DSLR cameras, portable video cameras, and action cameras.

Special considerations for the operation of audio and video devices during installation and upgrade of Kaspersky Endpoint Security

When you run audio and video recording or playback applications for the first time since installation of Kaspersky Endpoint Security, audio and video playback or recording may be interrupted. This is necessary in order to enable the functionality that controls access to sound recording devices by applications. The system service that controls audio hardware will be restarted when Kaspersky Endpoint Security is run for the first time.

About access to webcams by applications

Webcam access protection functionality has the following special considerations and limitations:

- The application controls video and still images derived from the processing of webcam data.
- The application controls the audio stream if it is part of the video stream received from the webcam.
- The application controls only webcams connected via USB or IEEE1394 that are displayed as **Imaging Devices** in the Windows Device Manager.

Supported webcams

Kaspersky Endpoint Security supports the following webcams:

- Logitech HD Webcam C270
- Logitech HD Webcam C310
- Logitech Webcam C210
- Logitech Webcam Pro 9000
- Logitech HD Webcam C525
- Microsoft LifeCam VX-1000
- Microsoft LifeCam VX-2000
- Microsoft LifeCam VX-3000
- Microsoft LifeCam VX-800
- Microsoft LifeCam Cinema

Kaspersky cannot guarantee support for webcams that are not specified in this list.

Enabling and disabling Host Intrusion Prevention

By default, the Host Intrusion Prevention component is enabled and runs in the mode recommended by Kaspersky experts. You can disable the Host Intrusion Prevention component if necessary.

To enable or disable the Host Intrusion Prevention component:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. In the right part of the window, do one of the following:
 - Select the **Host Intrusion Prevention** check box if you want to enable the Host Intrusion Prevention component.
 - Clear the **Host Intrusion Prevention** check box if you want to disable the Host Intrusion Prevention component.

4. Save your changes.

Managing application trust groups

When each application is started for the first time, the Host Intrusion Prevention component checks the security of the application and places the application into one of the [trust groups](#).

At the first stage of the application scan, Kaspersky Endpoint Security searches the internal database of known applications for a matching entry and at the same time sends a request to the Kaspersky Security Network database (if an Internet connection is available). Based on the results of the search in the internal database and the Kaspersky Security Network database, the application is placed into a trust group. Each time the application is subsequently started, Kaspersky Endpoint Security sends a new query to the KSN database and places the application into a different trust group if the reputation of the application in the KSN database has changed.

You can select a trust group to which Kaspersky Endpoint Security automatically assigns all unknown applications. Applications that were started before Kaspersky Endpoint Security are automatically moved to the trust group specified in the [Select trust group](#) window.

For applications that were started before Kaspersky Endpoint Security, only network activity is controlled. Control is performed according to the network rules set in the Firewall settings.

Configuring the settings for assigning applications to trust groups

If participation in Kaspersky Security Network is enabled, Kaspersky Endpoint Security sends KSN a query about the reputation of an application each time the application is started. Based on the received response, the application may be moved to a trust group that is different from the one specified in the Host Intrusion Prevention component settings.

Kaspersky Endpoint Security always places applications signed by Microsoft certificates or Kaspersky certificates into the Trusted group.

To configure the settings for placement of applications in trust groups:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. If you want to automatically place digitally signed applications from trusted vendors in the Trusted group, select the **Trust applications that have a digital signature** check box.

Trusted vendors are those software vendors that are included in the trusted group by Kaspersky. You can also [add vendor certificate to the trusted system certificate store manually](#).

4. To move all unknown applications to a specified trust group, select the required trust group from the **If a trust group cannot be defined, automatically move applications to** drop-down list.

For security reasons, the **Trusted** group is not included in the values of the **If trust group cannot be defined, automatically move applications to** setting.

5. Save your changes.

Modifying a trust group

When an application is first started, Kaspersky Endpoint Security automatically places the application in a trust group. You can move the application to another trust group manually, if necessary.

Kaspersky specialists do not recommend moving applications from the automatically assigned trust group to a different trust group. Instead, you can [modify rights for an individual application](#) if necessary.

To change the trust group to which an application has been automatically assigned by Kaspersky Endpoint Security when first started:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. Click the **Applications** button.
This opens the **Application rights** tab in the **Host Intrusion Prevention** window.
4. Select the required application on the **Application rights** tab.
5. Do one of the following:
 - Right-click to display the context menu of the application. In the context menu of the application, select **Move to group** <γρουπ ναμε>.
 - To open the context menu, click the **Trusted** / **Low Restricted** / **High Restricted** / **Untrusted** link. In the context menu, select the required trust group.
6. Save your changes.

Selecting a trust group for applications started before Kaspersky Endpoint Security

For applications that were started before Kaspersky Endpoint Security, only network activity is controlled. Control is performed according to the network rules set in the Firewall settings. To specify which network rules must be applied to network activity monitoring for such applications, you must select a trust group.

To select the trust group for applications started before Kaspersky Endpoint Security:

1. In the main application window, click the **Settings** button.

2. In the application settings window, select **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. Click the **Edit** button.
This opens the **Select trust group** window.
4. Select the necessary trust group.
5. Save your changes.

Managing application rights

By default, application activity is controlled by application rights that are defined for the trust group to which Kaspersky Endpoint Security assigned the application on first launch. If necessary, you can edit the application rights for an entire trust group, for an individual application, or a group of applications that are within a trust group.

Application rights that are defined for individual applications or groups of applications within a trust group have a higher priority than application rights that are defined for a trust group. In other words, if the settings of the application rights for an individual application or a group of applications within a trust group differ from the settings of application rights for the trust group, the Host Intrusion Prevention component controls the activity of the application or the group of applications within the trust group according to the application rights that are defined for the application or the group of applications.

Changing application rights for trust groups and groups of applications

The optimal application rights for different trust groups are created by default. The settings of rights for application groups that are in a trust group inherit values from the settings of the trust group rights. You can edit the preset rights of trust groups and rights of application groups.

To edit the rights of a trust group or the rights of an application group:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. Click the **Applications** button.
This opens the **Application rights** tab in the **Host Intrusion Prevention** window.
4. Select the necessary trust group or application group.
5. From the context menu of a trust group or of a group of applications, select **Group rights**.
The **Group rights** window opens.
6. In the **Group rights** window, do one of the following:
 - To edit trust group rights or application group rights that govern the rights of the trust group or application group to access the operating system registry, user files, and application settings, select the **Files and system registry** tab.
 - To edit trust group rights or application group rights that govern the rights of the trust group or application group to access operating system processes and objects, select the **Rights** tab.

7. For the required resource, in the column of the corresponding action, right-click to open the context menu.
8. From the context menu, select the required item.

- **Inherit.**
- **Allow.**
- **Block.**
- **Log events.**

If you are editing trust group control rules, the **Inherit** item is not available.

9. Save your changes.

Modifying application rights

By default, the settings of rights for applications that belong to an application group or trust group inherit the values of settings of trust group rights. You can edit the settings of application rights.

To edit application rights:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. Click the **Applications** button.
This opens the **Application rights** tab in the **Host Intrusion Prevention** window.
4. Select the necessary application.
5. Do one of the following:
 - From the context menu of the application, select **Application rights**.
 - Click the **Additional** button in the lower-right corner of the **Application rights** tab.

The **Application rights** window opens.

6. In the **Application rights** window, do one of the following:
 - If you want to edit application rights that govern the rights of the application to access the operating system registry, user files, and application settings, select the **Files and system registry** tab.
 - To edit application rights that define the rights of the application to access operating system processes and objects, select the **Rights** tab.
7. For the required resource, in the column of the corresponding action, right-click to open the context menu.
8. From the context menu, select the required item.

- **Inherit.**
- **Allow.**
- **Block.**
- **Log events.**

9. Save your changes.

Disabling downloads and updates of application rights from the Kaspersky Security Network database

By default, when new information about an application is detected in the Kaspersky Security Network database, Kaspersky Endpoint Security applies the rights downloaded from the KSN database for this application. You can then manually edit the application rights.

If an application was not in the Kaspersky Security Network database when started for the first time, but information about it was added to the database later, by default Kaspersky Endpoint Security automatically updates the rights for this application.

You can disable downloads of application rights from the Kaspersky Security Network database and automatic updates of rights for previously unknown applications.

To disable downloads and updates of application rights from the Kaspersky Security Network database:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. Clear the **Update rights for previously unknown applications from KSN database** check box.
4. Save your changes.

Disabling the inheritance of restrictions from the parent process

Application startup may be initiated either by the user or by another running application. When application startup is initiated by another application, a startup sequence is created, which consists of parent and child processes.

When an application attempts to obtain access to a protected resource, the Host Intrusion Prevention analyzes all parent processes of the application to determine whether these processes have rights to access the protected resource. The minimum priority rights are then applied: when comparing the access rights of the application to those of the parent process, the access rights with a minimum priority are applied to the application's activity.

The priority of access rights is as follows:

1. **Allow.** This access right has the highest priority.
2. **Block.** This access right has the lowest priority.

This mechanism prevents a non-trusted application or an application with restricted rights from using a trusted application to perform actions that require certain privileges.

If the activity of an application is blocked due to the lack of rights that are granted to a parent process, you can edit these rights or disable the inheritance of restrictions from the parent process.

To disable the inheritance of restrictions from the parent process:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. Click the **Applications** button.
This opens the **Application rights** tab in the **Host Intrusion Prevention** window.
4. Select the necessary application.
5. From the context menu of the application, select **Application rights**.
The **Application rights** window opens.
6. In the **Application rights** window, select the **Exclusions** tab.
7. Select the **Do not inherit restrictions of the parent process (application)** check box.
8. Save your changes.

Excluding specific application actions from application rights

To exclude specific application actions from application rights:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. Click the **Applications** button.
This opens the **Application rights** tab in the **Host Intrusion Prevention** window.
4. Select the necessary application.
5. From the context menu of the application, select **Application rights**.
The **Application rights** window opens.
6. Select the **Exclusions** tab.
7. Select check boxes next to application actions that do not need to be monitored.
8. Save your changes.

Deleting information about unused applications

Kaspersky Endpoint Security uses application rights to control the activities of applications. Application rights are determined by their trust group. Kaspersky Endpoint Security puts an application into a trust group the first time the application is started. You can [manually change the trust group of an application](#). You can also [manually configure the rights of an individual application](#). Kaspersky Endpoint Security stores the following information about an application: trust group of the application, and rights of the application.

Kaspersky Endpoint Security automatically deletes information about unused applications to save computer resources. Kaspersky Endpoint Security deletes application information according to the following rules:

- If the trust group and rights of an application were determined automatically, Kaspersky Endpoint Security deletes information about this application after 30 days. It is not possible to change the storage term for application information or turn off automatic deletion.
- If you manually put an application into a trust group or configured its access rights, Kaspersky Endpoint Security deletes information about this application after 60 days (default storage term). You can change the storage term for application information, or turn off automatic deletion (see the instructions below).

When you start an application whose information has been deleted, Kaspersky Endpoint Security analyzes the application as if it were starting for the first time.

To configure automatic deletion of information about unused applications:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. Do one of the following:
 - If you want to configure automatic deletion, select the **Delete rights for applications that are not started for more than N days** check box and specify the necessary number of days.
Information about the applications that you manually put into a trust group or whose access rights you manually configured will be deleted by Kaspersky Endpoint Security after the defined number of days. Information about applications whose trust group and application rights were automatically determined will also be deleted by Kaspersky Endpoint Security after 30 days.
 - If you want to turn off automatic deletion, clear the **Delete rights for applications that are not started for more than N days** check box.
Information about the applications that you manually put into a trust group or whose access rights you manually configured will be stored by Kaspersky Endpoint Security indefinitely, without any storage term limits. Kaspersky Endpoint Security will only delete information about applications whose trust group and application rights were automatically determined after 30 days.
4. Save your changes.

Protecting operating system resources and identity data

The Host Intrusion Prevention component manages the rights of applications to take actions on various categories of operating system resources and personal data.

Kaspersky specialists have established preset categories of protected resources. You cannot edit or delete the preset categories of protected resources or the protected resources that are within these categories.

You can perform the following actions:

- Add a new category of protected resources.
- Add a new protected resource.
- Disable protection of a resource.

Adding a category of protected resources

To add a new category of protected resources:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. Click the **Resources** button.
This opens the **Protected resources** tab in the **Host Intrusion Prevention** window.
4. In the left part of the **Protected resources** tab, select a section or category of protected resources to which you want to add a new category of protected resources.
5. Click the **Add** button and in the drop-down list select **Category**.
The **Category of protected resources** window opens.
6. In the **Category of protected resources** window that opens, enter a name for the new category of protected resources.
7. Save your changes.

Adding a protected resource

To add a protected resource:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. Click the **Resources** button.
This opens the **Protected resources** tab in the **Host Intrusion Prevention** window.
4. In the left part of the **Protected resources** tab, select a category of protected resources to which you want to add a new protected resource.
5. Click the **Add** button and in the drop-down list select the type of resource that you want to add:
 - **File or folder.**
 - **Registry key.**

The **Protected resource** window opens.

6. In the **Protected resource** window, enter the name of the protected resource in the **Name** field.
7. Click the **Browse** button.
8. In the window that opens, specify the necessary settings depending on the type of protected resource that you want to add. Click **OK**.
9. Save your changes.

Disabling resource protection

To disable resource protection:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. In the right part of the window, click the **Resources** button.
This opens the **Protected resources** tab in the **Host Intrusion Prevention** window.
4. Do one of the following:
 - In the left part of the tab, in the list of protected resources, select the resource for which you want to disable protection and clear the check box next to its name.
 - Click **Exclusions** and do the following:
 - a. In the **Exclusions** window, click the **Add** button. In the drop-down list, select the type of resource that you want to add to the list of exclusions from protection by the Host Intrusion Prevention component: **File or folder** or **Registry key**.
The **Protected resource** window opens.
 - b. In the **Protected resource** window, enter the name of the protected resource in the **Name** field.
 - c. Click the **Browse** button.
 - d. In the window that opens, specify the necessary settings depending on the type of protected resource that you want to add to the list of exclusions from protection by the Host Intrusion Prevention component.
 - e. Click **OK**.
 - f. In the **Protected resource** window, click **OK**.
A new item appears in the list of resources that are excluded from protection by the Host Intrusion Prevention component.
 - g. In the **Exclusions** window, click **OK**.
5. Save your changes.

Remediation Engine

The Remediation Engine lets Kaspersky Endpoint Security roll back actions that have been performed by malware in the operating system.

When rolling back malware activity in the operating system, Kaspersky Endpoint Security handles the following types of malware activity:

- **File activity**

Kaspersky Endpoint Security performs the following actions:

- Deletes executable files that were created by malware (on all media except network drives).
- Deletes executable files that were created by programs that have been infiltrated by malware.
- Restores files that have been modified or deleted by malware.

The file recovery feature has a [number of limitations](#).

- **Registry activity**

Kaspersky Endpoint Security performs the following actions:

- Deletes registry keys that were created by malware.
- Does not restore registry keys that have been modified or deleted by malware.

- **System activity**

Kaspersky Endpoint Security performs the following actions:

- Terminates processes that have been initiated by malware.
- Terminates processes into which a malicious application has penetrated.
- Does not resume processes that have been halted by malware.

- **Network activity**

Kaspersky Endpoint Security performs the following actions:

- Blocks the network activity of malware.
- Blocks the network activity of processes that have been infiltrated by malware.

A rollback of malware actions can be started by the [File Threat Protection](#) or [Behavior Detection](#) component, or during a [virus scan](#).

Rolling back malware operations affects a strictly defined set of data. Rollback has no adverse effects on the operating system or on the integrity of your computer data.

File recovery limitations

The file recovery feature has the following limitations:

- The application restores files only on devices that have the NTFS or FAT32 file system.
- The application can restore files with the following extensions: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xslm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.
- It is not possible to restore files residing on network drives or on rewritable CD/DVD discs.
- It is not possible to restore files that were encrypted with the Encryption File System (EFS). For more details on EFS operation, please visit the [Microsoft website](#).
- The application does not monitor modifications to files performed by processes at the level of the operating system kernel.
- The application does not monitor modifications made to files over a network interface (for example, if a file is stored in a shared folder and a process is started remotely from another computer).

Enabling and disabling Remediation Engine

To enable or disable Remediation Engine:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Advanced Threat Protection** → **Remediation Engine**.
3. If you want Kaspersky Endpoint Security to roll back actions that were performed by malware in the operating system, select the **Remediation Engine** check box in the right part of the window.
4. Save your changes.

File Threat Protection

The File Threat Protection component lets you prevent infection of the file system of the computer. By default, the File Threat Protection component permanently resides in the computer's RAM. The component scans files on all drives of the computer, as well as on connected drives. The component provides computer protection with the help of anti-virus databases, the [Kaspersky Security Network cloud service](#), and heuristic analysis.

The component scans the files accessed by the user or application. If a malicious file is detected, Kaspersky Endpoint Security blocks the file operation. The application then disinfects or deletes the malicious file, depending on the settings of the File Threat Protection component.

When attempting to access a file whose contents are stored in the OneDrive cloud, Kaspersky Endpoint Security downloads and scans the file contents.

Enabling and disabling File Threat Protection

By default, the File Threat Protection component is enabled and runs in the mode recommended by Kaspersky experts. You can disable File Threat Protection if necessary.

To enable or disable File Threat Protection:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **File Threat Protection**.
3. Do one of the following:
 - If you want to enable File Threat Protection, select the **File Threat Protection** check box.
 - If you want to disable File Threat Protection, clear the **File Threat Protection** check box.
4. Save your changes.

Automatic pausing of File Threat Protection

You can configure File Threat Protection to automatically pause at a specified time or when working with specific applications.

File Threat Protection should be paused only as a last resort when it conflicts with some applications. In case of any conflicts during the operation of a component, we recommend contacting Kaspersky Technical Support (<https://companyaccount.kaspersky.com>). The support experts will help you set up the File Threat Protection component to run simultaneously with other applications on your computer.

To configure automatic pausing of File Threat Protection:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **File Threat Protection**.
3. In the **Security level** section, click the **Settings** button.
The **File Threat Protection** window opens.
4. In the **File Threat Protection** window, select the **Additional** tab.
5. In the **Pause task** section:
 - If you want to configure automatic pausing of File Threat Protection at a specified time, select the **By schedule** check box and click the **Schedule** button.
The **Pause task** window opens.
 - If you want to configure automatic pausing of File Threat Protection at startup of specified applications, select the **At application startup** check box and click the **Select** button.

The **Applications** window opens.

6. Do one of the following:

- If you are configuring automatic pausing of File Threat Protection at a specified time, in the **Pause task** window, use the **Pause task at** and **Resume task at** fields to specify the time period (in HH:MM format) during which File Threat Protection should be paused. Click **OK**.
- If you are configuring automatic pausing of File Threat Protection at startup of the specified applications, use the **Add**, **Edit**, and **Remove** buttons in the **Applications** window to create a list of applications during whose operation File Threat Protection should be paused. Click **OK**.

7. Save your changes.

Changing the security level

To protect the computer's file system, the File Threat Protection component applies various groups of settings. These groups of settings are called *security levels*. There are three preset security levels: **High**, **Recommended**, and **Low**. The **Recommended** security level settings are considered to be the optimal settings recommended by Kaspersky experts. You can select one of the preset security levels or manually configure security level settings. If you change the security level settings, you can always revert back to the recommended security level settings.

To change a security level:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **File Threat Protection**.
3. In the **Security level** section, do one of the following:
 - If you want to set one of the preset security levels (**High**, **Recommended**, or **Low**), select it with the slider.
 - If you want to configure a custom security level, click the **Settings** button and enter your custom settings in the **File Threat Protection** window that opens.
After you configure a custom security level, the name of the security level in the **Security level** section changes to **Custom**.
 - If you want to change the security level to **Recommended**, click the **By default** button.
4. Save your changes.

Changing the action taken on infected files by the File Threat Protection component

By default, the File Threat Protection component automatically tries to disinfect all infected files that are detected. If disinfection fails, the File Threat Protection component deletes these files.

To change the action taken on infected files by the File Threat Protection component:

1. In the main application window, click the **Settings** button.

2. In the application settings window, select **Essential Threat Protection** → **File Threat Protection**.

3. In the **Action on threat detection** section, select the required option:

- **Disinfect; delete if disinfection fails.**

If this option is selected, the File Threat Protection component automatically attempts to disinfect all infected files that are detected. If disinfection fails, the File Threat Protection component deletes these files.

- **Disinfect; block if disinfection fails.**

If this option is selected, the File Threat Protection component automatically attempts to disinfect all infected files that are detected. If disinfection fails, the File Threat Protection component blocks these files.

- **Block.**

If this option is selected, the File Threat Protection component automatically blocks all infected files without attempting to disinfect them.

4. Save your changes.

Forming the protection scope of the File Threat Protection component

The protection scope refers to the objects that the component scans when enabled. The protection scopes of different components have different properties. The location and type of files to be scanned are properties of the protection scope of the File Threat Protection component. By default, the File Threat Protection component scans only [potentially infectable files](#) that are run from hard drives, removable drives and network drives.

To create the protection scope:

1. In the main application window, click the **Settings** button.

2. In the application settings window, select **Essential Threat Protection** → **File Threat Protection**.

3. In the **Security level** section, click the **Settings** button.

The **File Threat Protection** window opens.

4. In the **File Threat Protection** window, select the **General** tab.

5. In the **File types** section, specify the type of files that you want the File Threat Protection component to scan:

- If you want to scan all files, select **All files**.
- If you want to scan files of formats which are the most vulnerable to infection, select **Files scanned by format**.
- If you want to scan files with extensions that are the most vulnerable to infection, select **Files scanned by extension**.

When selecting the type of files to scan, remember the following information:

- There are some file formats (such as .txt) for which the probability of intrusion of malicious code and its subsequent activation is quite low. At the same time, there are file formats that contain or may contain

executable code (such as .exe, .dll, and .doc). The risk of intrusion and activation of malicious code in such files is quite high.

- An intruder may send a virus or another malicious application to your computer in an executable file that has been renamed with the .txt extension. If you select scanning of files by extension, such a file is skipped by the scan. If scanning of files by format is selected, the File Threat Protection component analyzes the file header regardless of the extension. This analysis may reveal that the file is in EXE format. Such a file is thoroughly scanned for viruses and other malware.

6. In the **Protection scope** list, do one of the following:

- If you want to add a new object to the scan scope, click the **Add** button.
- If you want to change the location of an object, select the object from the scan scope and click the **Edit** button.

The **Select scan scope** window opens.

- If you want to remove an object from the list of objects to be scanned, select one from the list of objects to be scanned and click the **Delete** button.

A window for confirming deletion opens.

7. Do one of the following:

- If you want to add a new object or change the location of an object from the list of objects to be scanned, select the object in the **Select scan scope** window and click the **Add** button.

All objects that are selected in the **Select scan scope** window are displayed in the **Protection scope** list in the **File Threat Protection** window.

Click **OK**.

- If you want to remove an object, click the **Yes** button in the window for confirming removal.

8. To exclude an object from the list of objects to be scanned, clear the check box next to the object in the **Protection scope** list. However, the object remains on the list of objects to be scanned, though it is excluded from scanning by the File Threat Protection component.

9. Save your changes.

Using heuristic analysis in the operation of the File Threat Protection component

The File Threat Protection component uses a scanning technique called Machine learning and signature analysis. During signature analysis, the File Threat Protection component compares the detected object with records in the application anti-virus databases. Based on the recommendations of Kaspersky experts, machine learning and signature analysis is always enabled.

To increase the effectiveness of protection, you can use heuristic analysis. During heuristic analysis, the File Threat Protection component analyzes the activity of objects in the operating system. Heuristic analysis enables detection of malicious objects for which no records are currently available in the antivirus databases of the application.

To configure the use of heuristic analysis in the operation of the File Threat Protection component:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **File Threat Protection**.
3. In the **Security level** section, click the **Settings** button.
The **File Threat Protection** window opens.
4. In the **File Threat Protection** window, select the **Performance** tab.
5. In the **Scan methods** section:
 - If you want the File Threat Protection component to use heuristic analysis, select the **Heuristic analysis** check box and use the slider to set the heuristic analysis level: **Light scan**, **Medium scan**, or **Deep scan**.
 - If you do not want the File Threat Protection component to use heuristic analysis, clear the **Heuristic analysis** check box.
6. Save your changes.

Using scan technologies in the operation of the File Threat Protection component

To configure the use of scan technologies in the operation of the File Threat Protection component:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **File Threat Protection**.
3. In the **Security level** section, click the **Settings** button.
The **File Threat Protection** window opens.
4. In the **File Threat Protection** window, select the **Additional** tab.
5. In the **Scan technologies** section:
 - Select the check boxes next to the names of the technologies that you want to use in the operation of the File Threat Protection component.
 - Clear the check boxes next to the names of the technologies that you do not want to use in the operation of the File Threat Protection component.
6. Save your changes.

Optimizing file scanning

You can optimize the file scanning that is performed by the File Threat Protection component by reducing the scan time and increasing the operating speed of Kaspersky Endpoint Security. This can be achieved by scanning only new files and those files that have been modified since the previous scan. This mode applies both to simple and to compound files.

You can also enable the use of the iChecker and iSwift technologies that optimize the speed of file scanning by excluding files that have not been modified since the most recent scan.

To optimize file scanning:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **File Threat Protection**.
3. Click the **Settings** button.
The **File Threat Protection** window opens.
4. In the **File Threat Protection** window, select the **Performance** tab.
5. In the **Scan optimization** section, select the **Scan only new and changed files** check box.
6. Save your changes.

Scanning compound files

A common technique for concealing viruses and other malware is to embed them in compound files such as archives or email databases. To detect viruses and other malware that are hidden in this way, the compound file must be unpacked, which may slow down scanning. You can limit the set of compound files to be scanned, thus speeding up scanning.

The method used to process an infected compound file (disinfection or deletion) depends on the type of file.

The File Threat Protection component disinfects compound files in the RAR, ARJ, ZIP, CAB, and LHA formats and deletes files in all other formats (except mail databases).

To configure scanning of compound files:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **File Threat Protection**.
3. In the **Security level** section, click the **Settings** button.
The **File Threat Protection** window opens.
4. In the **File Threat Protection** window, select the **Performance** tab.
5. In the **Scan of compound files** section, specify the types of compound files that you want to scan: archives, installation packages, or files in office formats.
6. To scan only new and changed compound files, select the **Scan only new and changed files** check box.
The File Threat Protection component will scan only new and changed compound files of all types.
7. Click the **Additional** button.

The **Compound files** window opens.

8. In the **Background scan** section, do one of the following:

- To block the File Threat Protection component from unpacking compound files in the background, clear the **Unpack compound files in the background** check box.
- To allow the File Threat Protection component to unpack compound files when scanning in the background, select the **Unpack compound files in the background** check box and specify the required value in the **Minimum file size** field.

9. In the **Size limit** section, do one of the following:

- To block the File Threat Protection component from unpacking large compound files, select the **Do not unpack large compound files** check box and specify the required value in the **Maximum file size** field. The File Threat Protection component will not unpack compound files that are larger than the specified size.
- To allow the File Threat Protection component to unpack large compound files, clear the **Do not unpack large compound files** check box.

A file is considered large if its size exceeds the value in the **Maximum file size** field.

The File Threat Protection component scans large-sized files that are extracted from archives, regardless of whether the **Do not unpack large compound files** check box is selected.

10. Save your changes.

Changing the scan mode

Scan mode refers to the condition that triggers file scanning by the File Threat Protection component. By default, Kaspersky Endpoint Security scans files in smart mode. In this file scan mode, the File Threat Protection component decides whether or not to scan files after analyzing operations that are performed with the file by the user, by an application on behalf of the user (under the account that was used to log in or a different user account), or by the operating system. For example, when working with a Microsoft Office Word document, Kaspersky Endpoint Security scans the file when it is first opened and last closed. Intermediate operations that overwrite the file do not cause it to be scanned.

To change the file scan mode:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **File Threat Protection**.
3. In the **Security level** section, click the **Settings** button.

The **File Threat Protection** window opens.

4. In the **File Threat Protection** window, select the **Additional** tab.

5. In the **Scan mode** section, select the required mode:

- **Smart mode.**
- **On access and modification.**

- On access.
- On execution.

6. Save your changes.

Web Threat Protection

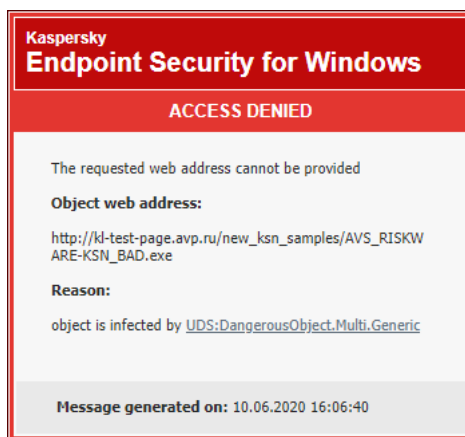
This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Windows for workstations. This component is unavailable if Kaspersky Endpoint Security is installed on a computer that runs on Windows for servers.

The Web Threat Protection component prevents downloads of malicious files from the Internet, and also blocks malicious and phishing websites. The component provides computer protection with the help of anti-virus databases, the [Kaspersky Security Network cloud service](#), and heuristic analysis.

Kaspersky Endpoint Security scans HTTP-, HTTPS- and FTP-traffic. Kaspersky Endpoint Security scans URLs and IP addresses. You can [specify the ports that Kaspersky Endpoint Security will monitor](#), or select all ports.

For HTTPS traffic monitoring, you need to [enable encrypted connections scan](#).

When a user tries to open a malicious or phishing website, Kaspersky Endpoint Security will block access and show a warning (see the figure below).



Website access denied message

Enabling and disabling Web Threat Protection

By default, the Web Threat Protection component is enabled and runs in the mode recommended by Kaspersky experts. You can disable the Web Threat Protection component if necessary.

To enable or disable the Web Threat Protection component:

1. In the main application window, click the **Settings** button.

2. In the application settings window, select **Essential Threat Protection** → **Web Threat Protection**.
3. Do one of the following:
 - If you want to enable the Web Threat Protection component, select the **Web Threat Protection** check box.
 - If you want to disable the Web Threat Protection component, clear the **Web Threat Protection** check box.
4. Save your changes.

Changing the web traffic security level

To protect data that is received and transmitted via the HTTP and FTP protocols, the Web Threat Protection component applies various groups of settings. Such groups of settings are called *web traffic security levels*. There are three pre-installed web traffic security levels: **High, Recommended, and Low**. The **Recommended** web traffic security level is considered the optimal setting, and is recommended by Kaspersky. You can select one of the pre-installed security levels for web traffic that is received or transmitted via the HTTP and FTP protocols, or configure a custom web traffic security level. If you change the web traffic security level settings, you can always revert to the recommended web traffic security level settings.

To change the web traffic security level:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Web Threat Protection**.
3. In the **Security level** section, do one of the following:
 - If you want to install one of the pre-installed web traffic security levels (**High, Recommended, or Low**), use the slider to select one.
 - If you want to configure a custom web traffic security level, click the **Settings** button and specify settings in the **Web Threat Protection** window that opens.

When you have configured a custom web traffic security level, the name of the security level in the **Security level** section changes to **Custom**.
 - If you want to change the web traffic security level to **Recommended**, click the **By default** button.
4. Save your changes.

Changing the action to take on malicious web traffic objects

By default, on detection of an infected object in web traffic, the Web Threat Protection component blocks access to the object and displays a notification about the action.

To change the action to take on malicious web traffic objects:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Web Threat Protection**.

3. In the **Action on threat detection** section, select the action that Kaspersky Endpoint Security performs on malicious web traffic objects:

- **Block download.**

If this option is selected, on detecting an infected object in web traffic, the Web Threat Protection component blocks access to the object, displays a notification about the blocked access attempt, and makes a log entry with information about the infected object.

- **Inform.**

If this option is selected and an infected object is detected in the web traffic, the Web Threat Protection component allows this object to be downloaded to the computer; Kaspersky Endpoint Security logs an event containing information about the infected object and adds information about the infected object to the list of active threats.

4. Save your changes.

Using Web Threat Protection to check links against databases of phishing and malicious web addresses

Scanning links to see if they are included in the list of phishing web addresses allows avoiding *phishing attacks*. A phishing attack can be disguised, for example, as an email message supposedly from your bank with a link to the official website of the bank. By clicking the link, you go to an exact copy of the bank's website and can even see its real web address in the browser, even though you are on a counterfeit site. From this point forward, all of your actions on the site are tracked and can be used to steal your money.

Because links to phishing websites may be received not only in an email message but also from other sources such as ICQ messages, the Web Threat Protection component monitors attempts to access a phishing website at the web traffic scan level and blocks access to such websites. Lists of phishing URLs are included with the Kaspersky Endpoint Security distribution kit.

To configure the Web Threat Protection component to check links against the databases of phishing and malicious web addresses:

1. In the main application window, click the **Settings** button.

2. In the application settings window, select **Essential Threat Protection** → **Web Threat Protection**.

3. Click the **Settings** button.

The **Web Threat Protection** window opens.

4. In the **Web Threat Protection** window, select the **General** tab.

5. Do the following:

- If you want the Web Threat Protection component to check links against the databases of malicious web addresses, in the **Scan methods** section, select the **Check if links are listed in the database of malicious links** check box.

Kaspersky Endpoint Security scans links against malicious web address databases, even if network traffic is transmitted over an encrypted connection and the [Scan encrypted connections check box](#) is cleared.

- If you want the Web Threat Protection component to check links against the databases of phishing web addresses, in the **Anti-Phishing Settings** section, select the **Check if links are listed in the database of phishing links** check box.

You can also check links against the reputation databases of Kaspersky Security Network.

6. Save your changes.

Using heuristic analysis in the operation of the Web Threat Protection component

To increase the effectiveness of protection, you can use heuristic analysis. During heuristic analysis, Kaspersky Endpoint Security analyzes the activity of applications in the operating system. Heuristic analysis can detect threats for which there are currently no records in the Kaspersky Endpoint Security databases.

To configure the use of heuristic analysis:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Web Threat Protection**.
3. In the **Security level** section, click the **Settings** button.
The **Web Threat Protection** window opens.
4. Select the **General** tab.
5. If you want the Web Threat Protection component to use heuristic analysis to scan web traffic for viruses and other malware, in the **Scan methods** section, select the **Heuristic analysis for detecting viruses** check box and use the slider to set the heuristic analysis level: **Light scan**, **Medium scan**, or **Deep scan**.
6. If you want the Web Threat Protection component to use heuristic analysis to scan web pages for phishing links, in the **Anti-Phishing Settings** section, select the **Heuristic analysis for detecting phishing links** check box.
7. Save your changes.

Creating the list of trusted web addresses

You can create a list of URLs whose content you trust. The Web Threat Protection component does not analyze information from trusted web addresses to check them for viruses or other threats. This option may be useful, for example, if the Web Threat Protection component interferes with the downloading of a file from a known website.

A URL may be the address of a specific web page or the address of a website.

To create a list of trusted web addresses:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Web Threat Protection**.
3. Click the **Settings** button.
The **Web Threat Protection** window opens.
4. Select the **Trusted web addresses** tab.
5. Select the **Do not scan web traffic from trusted web addresses** check box.
6. Create a list of URLs / web pages whose content you trust. To create a list:
 - a. Click the **Add** button.
The **Web address / Web address mask** window opens.
 - b. Enter the address of the website / web page or the address mask of the website / web page.
 - c. Click **OK**.
A new record appears in the list of trusted web addresses.
7. Save your changes.

Mail Threat Protection

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Windows for workstations. This component is unavailable if Kaspersky Endpoint Security is installed on a computer that runs on Windows for servers.

The Mail Threat Protection component scans the attachments of incoming and outgoing email messages for viruses and other threats. The component also scans messages for malicious and phishing links. By default, the Mail Threat Protection component permanently resides in the computer's RAM and scans all messages received or sent using the POP3, SMTP, IMAP, or NNTP protocols, or the Microsoft Office Outlook mail client (MAPI). The component provides computer protection with the help of anti-virus databases, the [Kaspersky Security Network cloud service](#), and heuristic analysis.

The Mail Threat Protection component does not scan messages if the mail client is open in a browser.

When a malicious file is detected in an attachment, Kaspersky Endpoint Security renames the message subject: [Message is infected] <message subject> or [Infected object deleted] <message subject>.

This component interacts with mail clients installed on the computer. For the Microsoft Office Outlook mail client, an [extension with additional parameters](#) is provided. The Mail Threat Protection extension is embedded in the Microsoft Office Outlook mail client during installation of Kaspersky Endpoint Security.

Enabling and disabling Mail Threat Protection

By default, the Mail Threat Protection component is enabled and runs in the mode recommended by Kaspersky experts.

To enable or disable the Mail Threat Protection component:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Mail Threat Protection**.
3. Do one of the following:
 - If you want to enable the Mail Threat Protection component, select the **Mail Threat Protection** check box.
 - If you want to disable the Mail Threat Protection component, clear the **Mail Threat Protection** check box.
4. Save your changes.

Changing the mail security level

The Mail Threat Protection component applies various groups of settings to protect mail. The settings groups are called *email security levels*. There are three email security levels: **High**, **Recommended**, and **Low**. The **Recommended** file security level is considered the optimal setting, and is recommended by Kaspersky. You can select one of the pre-installed email security levels or configure a custom email security level. If you have changed the email security level settings, you can always revert to the recommended email security level settings.

To change the email security level:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Mail Threat Protection**.
3. In the **Security level** section, do one of the following:
 - If you want to install one of the pre-installed email security levels (**High**, **Recommended**, or **Low**), use the slider to select one.
 - If you want to configure a custom security level, click the **Settings** button and enter your custom settings in the **Mail Threat Protection** window that opens.
After you configure a custom email security level, the name of the security level in the **Security level** section changes to **Custom**.
 - If you want to change the email security level to **Recommended**, click the **By default** button.
4. Save your changes.

Changing the action to take on infected email messages

By default, the Mail Threat Protection component automatically attempts to disinfect all infected email messages that are detected. If disinfection fails, the Mail Threat Protection component deletes the infected email messages.

To change the action to take on infected email messages:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Mail Threat Protection**.
3. In the **Action on threat detection** section, select the action for Kaspersky Endpoint Security to perform when an infected message is detected:
 - **Disinfect; delete if disinfection fails.**

If this option is selected, the Mail Threat Protection component automatically attempts to disinfect all infected email messages that are detected. If disinfection fails, the Mail Threat Protection component deletes the infected email messages.
 - **Disinfect; block if disinfection fails.**

If this option is selected, the Mail Threat Protection component automatically attempts to disinfect all infected email messages that are detected. If disinfection fails, the Mail Threat Protection component blocks the infected email messages.
 - **Block.**

If this option is selected, the Mail Threat Protection component automatically blocks all infected email messages without attempting to disinfect them.
4. Save your changes.

Forming the protection scope of the Mail Threat Protection component

The protection scope refers to the objects that are scanned by the component when it is active. The protection scopes of different components have different properties. The properties of the protection scope of the Mail Threat Protection component include the settings for integrating the Mail Threat Protection component into mail clients, and the type of email messages and email protocols whose traffic is scanned by the Mail Threat Protection component. By default, Kaspersky Endpoint Security scans both incoming and outgoing email messages and traffic of the POP3, SMTP, NNTP, and IMAP protocols, and is integrated into the Microsoft Office Outlook mail client.

To form the protection scope of the Mail Threat Protection component:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Mail Threat Protection**.
3. Click the **Settings** button.

The **Mail Threat Protection** window opens.
4. Select the **General** tab.
5. In the **Protection scope** section, do one of the following:
 - If you want the Mail Threat Protection component to scan all incoming and outgoing messages on your computer, select the **Incoming and outgoing messages** option.

- If you want the Mail Threat Protection component to scan only incoming messages on your computer, select the **Incoming messages only** option.

If you choose to scan only incoming messages, it is recommended that you perform a one-time scan of all outgoing messages because there is a chance that your computer has email worms that are being spread over email. This helps to avoid problems resulting from unmonitored mass emailing of infected messages from your computer.

6. In the **Connectivity** section, do the following:

- If you want the Mail Threat Protection component to scan messages that are transmitted via the POP3, SMTP, NNTP and IMAP protocols before they arrive on your computer, select the **POP3 / SMTP / NNTP / IMAP traffic** check box.

If you do not want the Mail Threat Protection component to scan messages that are transmitted via the POP3, SMTP, NNTP and IMAP protocols before they arrive on your computer, clear the **POP3 / SMTP / NNTP / IMAP traffic** check box. In this case, messages are scanned by the Mail Threat Protection extension embedded in the Microsoft Office Outlook mail client after they are received on the user computer if the **Additional: Microsoft Office Outlook extension** check box is selected.

If you use a mail client other than Microsoft Office Outlook, messages that are transmitted via the POP3, SMTP, NNTP and IMAP protocols are not scanned by the Mail Threat Protection component when the **POP3 / SMTP / NNTP / IMAP traffic** check box is cleared.

- If you want to allow access to Mail Threat Protection component settings from Microsoft Office Outlook and enable scanning of messages that are transmitted via the POP3, SMTP, NNTP, IMAP, and MAPI protocols after they arrive on the computer using the extension that is embedded into Microsoft Office Outlook, select the **Additional: Microsoft Office Outlook extension** check box.

If you want to block access to Mail Threat Protection component settings from Microsoft Office Outlook and disable scanning of messages that are transmitted via the POP3, SMTP, NNTP, IMAP, and MAPI protocols after they arrive on the computer using the extension that is embedded into Microsoft Office Outlook, clear the **Additional: Microsoft Office Outlook extension** check box.

The Mail Threat Protection extension is embedded in the Microsoft Office Outlook mail client during installation of Kaspersky Endpoint Security.

7. Save your changes.

Scanning compound files attached to email messages

You can enable or disable scanning of message attachments, limit the maximum size of message attachments to be scanned, and limit the maximum message attachment scan duration.

To configure scanning of compound files attached to email messages:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Mail Threat Protection**.
3. Click the **Settings** button.

The **Mail Threat Protection** window opens.

4. Select the **General** tab.

5. Perform the following in the **Scan of compound files** section:

- If you want the Mail Threat Protection component to skip archives that are attached to messages, clear the **Scan attached archives** check box.
- If you want the Mail Threat Protection component to skip Office format files that are attached to messages, clear the **Scan attached files of Office formats** check box.
- If you want the Mail Threat Protection to skip message attachments that are larger than N megabytes in size, select the **Do not scan archives larger than N MB** check box. If you select this check box, specify the maximum archive size in the field that is opposite the name of the check box.
- If you want the Mail Threat Protection component to scan message attachments that take more than N seconds to scan, clear the **Do not scan archives for more than N sec** check box.

6. Save your changes.

Filtering email message attachments

The attachment filtering functionality is not applied to outgoing email messages.

Malicious applications can be distributed in the form of attachments in email messages. You can configure filtering based on the type of message attachments so that files of the specified types are automatically renamed or deleted. By renaming an attachment of a certain type, Kaspersky Endpoint Security can protect your computer against automatic execution of a malicious application.

To configure filtering of attachments:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Mail Threat Protection**.
3. In the **Security level** section, click the **Settings** button.

The **Mail Threat Protection** window opens.

4. In the **Mail Threat Protection** window, select the **Attachment filter** tab.

5. Do one of the following:

- If you do not want the Mail Threat Protection component to filter message attachments, select the **Disable filtering** option.
- If you want the Mail Threat Protection component to rename message attachments of the [specified types](#), select the **Rename attachments of selected types** option.
- If you want the Mail Threat Protection component to delete message attachments of the specified types, select the **Delete attachments of selected types** option.

6. If you selected the **Rename attachments of selected types** option or the **Delete attachments of selected types** option during the previous step, select the check boxes opposite the relevant types of files.

7. Save your changes.

Scanning emails in Microsoft Office Outlook

During installation of Kaspersky Endpoint Security, the Mail Threat Protection extension is embedded into Microsoft Office Outlook (hereinafter also referred to as Outlook). It allows you to open the Mail Threat Protection component settings from within Outlook, and to specify when email messages are to be scanned for viruses and other threats. The Mail Threat Protection extension for Outlook can scan incoming and outgoing messages that are transmitted via the POP3, SMTP, NNTP, IMAP, and MAPI protocols. Kaspersky Endpoint Security also supports working with other email clients (including Microsoft Outlook Express®, Windows Mail, and Mozilla™ Thunderbird™).

The Mail Threat Protection extension supports operations with Outlook 2010, 2013, 2016, and 2019.

When working with the Mozilla Thunderbird mail client, the Mail Threat Protection component does not scan messages that are transmitted via the IMAP protocol for viruses and other threats if filters are used to move messages from the **Inbox** folder.

In Outlook, incoming messages are first scanned by the Mail Threat Protection component (if the **POP3 / SMTP / NNTP / IMAP traffic** check box is selected in the interface of Kaspersky Endpoint Security) and then by the Mail Threat Protection extension for Outlook. If the Mail Threat Protection component detects a malicious object in a message, it notifies you about this event.

The Mail Threat Protection component settings can be configured directly in Outlook if the **Additional: Microsoft Office Outlook extension** check box is selected in the interface of Kaspersky Endpoint Security.

Outgoing messages are first scanned by the Mail Threat Protection extension for Outlook, and are then scanned by the Mail Threat Protection component.

Configuring mail scanning in Outlook

To configure mail scanning in Outlook 2007:

1. Open the main window of Outlook 2007.
2. Select **Service** → **Settings** from the menu bar.
The **Options** window opens.
3. In the **Options** window, select the **Email protection** tab.

To configure mail scanning in Outlook 2010 / 2013 / 2016:

1. Open the main Outlook window.
Select the **File** tab in the upper left corner.

2. Click the **Options** button.

The **Outlook Options** window opens.

3. Select the **Add-Ins** section.

Settings of plug-ins embedded into Outlook are displayed in the right part of the window.

4. Click the **Add-In Options** button.

Configuring mail scan using Kaspersky Security Center

If mail is scanned using the Mail Threat Protection extension for Outlook, it is recommended to use Cached Exchange Mode. For more detailed information about the Exchange caching mode and recommendations on its use, please refer to the Microsoft Knowledge Base: <https://technet.microsoft.com/en-us/library/cc179175.aspx>

To configure the operating mode of the Mail Threat Protection extension for Outlook using Kaspersky Security Center:

1. Open the Kaspersky Security Center Administration Console.

2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.

3. In the workspace, select the **Policies** tab.

4. Select the necessary policy and double-click to open the policy properties.

5. In the policy window, select **Essential Threat Protection** → **Mail Threat Protection**.

6. In the **Security level** section, click the **Settings** button.

The **Mail Threat Protection** window opens.

7. In the **Connectivity** section, click the **Settings** button.

8. In the **Email protection** window:

- Select the **Scan when receiving** check box if you want the Mail Threat Protection extension for Outlook to scan incoming messages as they arrive to the mailbox.
- Select the **Scan when reading** check box if you want the Mail Threat Protection extension for Outlook to scan incoming messages when the user opens them.
- Select the **Scan when sending** check box if you want the Mail Threat Protection extension for Outlook to scan outgoing messages as they are sent.

9. Save your changes.

Network Threat Protection

The Network Threat Protection component scans inbound network traffic for activity that is typical of network attacks. When Kaspersky Endpoint Security detects an attempted network attack on the user's computer, it blocks the network connection with the attacking computer.

Descriptions of currently known types of network attacks and ways to counteract them are provided in Kaspersky Endpoint Security databases. The list of network attacks that the Network Threat Protection component detects is updated during [database and application module updates](#).

Enabling and disabling Network Threat Protection

By default, Network Threat Protection is enabled and running in the optimal mode. You can disable Network Threat Protection if necessary.

To enable or disable Network Threat Protection:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Network Threat Protection**.
3. Do the following:
 - If you want to enable Network Threat Protection, select the **Network Threat Protection** check box.
 - If you want to disable Network Threat Protection, clear the **Network Threat Protection** check box.
4. Save your changes.

Editing the settings used in blocking an attacking computer

To edit the settings for blocking an attacking computer:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Network Threat Protection**.
3. Select the **Add the attacking computer to the list of blocked computers for** check box.

If this check box is selected, on detecting a network attack attempt, the Network Threat Protection component blocks network activity from the attacking computer for the specified amount of time. This automatically protects the computer against possible future network attacks from the same address.

If this check box is cleared, on detecting a network attack attempt, the Network Threat Protection component does not enable automatic protection against possible future network attacks from the same address.
4. Change the amount of time during which an attacking computer is blocked in the field next to the **Add the attacking computer to the list of blocked computers for** check box.
5. Save your changes.

Configuring addresses of exclusions from blocking

To configure addresses of exclusions from blocking:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Network Threat Protection**.
3. Click the **Exclusions** button.
The **Exclusions** window opens.
4. Do one of the following:
 - If you want to add a new IP address, click the **Add** button.
 - If you want to edit a previously added IP address, select it in the list of addresses and click the **Edit** button.The **IP address** window opens.
5. Enter the IP address of the computer from which network attacks must not be blocked.
6. Save your changes.

MAC Spoofing Protection

The Network Threat Protection component tracks vulnerabilities in the Address Resolution Protocol (ARP). This way, the component protects the computer against *attacks such as MAC spoofing*. A MAC spoofing attack consists of changing the MAC address of a network device (network card). As a result, an attacker can redirect data sent to a device to another device and gain access to this data.

By default, Kaspersky Endpoint Security does not monitor MAC spoofing attacks.

To change the mode of protection against MAC spoofing attacks:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Network Threat Protection**.
3. In the **MAC spoofing Protection operating mode** section, select one of the following options:
 - **Do not track MAC Spoofing attacks.**
 - **Notify about all activity characteristic of MAC spoofing attacks.**
 - **Block all activity characteristic of MAC spoofing attacks.**

Encrypted connections scan

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Windows for workstations. This component is unavailable if Kaspersky Endpoint Security is installed on a computer that runs on Windows for servers.

After installation, Kaspersky Endpoint Security adds the Kaspersky certificate to the system storage of trusted certificates. Kaspersky Endpoint Security also includes the use of system storage of trusted certificates in Firefox and Thunderbird to scan the traffic of these applications.

The [Web Control](#), [Mail Threat Protection](#), [Web Threat Protection](#) components can decrypt and scan network traffic transmitted over encrypted connections using the following protocols:

- SSL 3.0.
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Configuring the encrypted connections scan settings

To configure the encrypted connections scan settings:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Network settings**.
3. Select the **Scan encrypted connections** check box if you want Kaspersky Endpoint Security to monitor encrypted network traffic.
4. If necessary, [add scan exclusions: trusted addresses and applications](#).
5. Click the **Advanced settings** button.
6. Configure the settings for scanning encrypted connections (see table below).
7. Save your changes.

Encrypted connections scan settings

Parameter	Description
When visiting a domain with an untrusted certificate	<ul style="list-style-type: none">• Allow. If this option is selected, when visiting a domain with an untrusted certificate, Kaspersky Endpoint Security allows the network connection. <p>When opening a domain with an untrusted certificate in a browser, Kaspersky Endpoint Security displays an HTML page showing a warning and the reason why visiting that domain is not recommended. A user can click the link from the HTML warning page to obtain access to the requested web resource. After following this link, during the next hour Kaspersky Endpoint Security will not display warnings about an untrusted certificate when visiting other resources on this same domain.</p> <ul style="list-style-type: none">• Block connection. If this option is selected, when visiting a domain with an untrusted certificate, Kaspersky Endpoint Security blocks the network connection. <p>When opening a domain with an untrusted certificate in a browser, Kaspersky Endpoint Security displays an HTML page showing the reason why that domain is blocked.</p>
When encrypted connection scan errors occur	<ul style="list-style-type: none">• Block connection. If this item is selected, when an encrypted connection scan error occurs, Kaspersky Endpoint Security blocks the network connection.

	<ul style="list-style-type: none"> • Add domain to exclusions. If this item is selected, when an encrypted connection scan error occurs, Kaspersky Endpoint Security adds the domain that resulted in the error to the list of domains with scan errors and does not monitor encrypted network traffic when this domain is visited. You can view a list of domains with encrypted connections scan errors only in the local interface of the application. To clear the list contents, you need to select Block connection.
Block SSL 2.0 connections	<p>If the check box is selected, Kaspersky Endpoint Security blocks network connections established over the SSL 2.0 protocol.</p> <p>If the check box is cleared, Kaspersky Endpoint Security does not block network connections established over the SSL 2.0 protocol and does not monitor network traffic transmitted over these connections.</p>
Decrypt encrypted connections with websites that use EV certificates	<p>EV certificates (Extended Validation Certificates) confirm the authenticity of websites and enhance the security of the connection. Browsers use a lock icon in their address bar to indicate that a website has an EV certificate. Browsers may also fully or partially color the address bar in green.</p> <p>If the check box is selected, Kaspersky Endpoint Security decrypts and monitors encrypted connections with websites that use an EV certificate.</p> <p>If the check box is cleared, Kaspersky Endpoint Security does not have access to the contents of HTTPS traffic. For this reason, the application monitors HTTPS traffic only based on the website address, for example, <code>https://facebook.com</code>.</p> <p>If you are opening a website with an EV certificate for the first time, the encrypted connection will be decrypted regardless of whether or not the check box is selected.</p>

Excluding encrypted connections from scanning

Most web resources use encrypted connections. Kaspersky experts recommend that you enable [Encrypted connections scan](#). If scanning encrypted connections interferes with work-related activity, you can add a website to exclusions referred to as *trusted addresses*. If a trusted application uses an encrypted connection, you can [disable encrypted connections scan for this application](#). For example, you can disable encrypted connections scan for cloud storage applications that use two-factor authentication with their own certificate.

To exclude a web address from encrypted connection scans:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Network settings**.
3. In the **Encrypted connections scan** section, click the **Trusted addresses** button.
4. Click the **Add** button.
5. Enter a domain name or an IP address if you do not want Kaspersky Endpoint Security to scan encrypted connections established when visiting that domain.
6. Save your changes.

By default, Kaspersky Endpoint Security does not scan encrypted connections when errors occur and adds the website to a special list of *Domains with scan errors*. Kaspersky Endpoint Security compiles a separate list for each user and does not send data to Kaspersky Security Center. You can [enable blocking the connection when a scan error occurs](#). You can view a list of domains with encrypted connections scan errors only in the local interface of the application.

To view the list of domains with scan errors:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Network settings**.
3. In the **Encrypted connections scan** section, click the **Advanced settings** button.
4. In the window that opens, click the **Domains with scan errors** link.

A list of domains with scan errors opens. To reset the list, enable blocking connection when scan errors occur in the policy, apply the policy, then reset the parameter to its initial value and apply the policy again.

Kaspersky specialists make a list of *global exceptions* — trusted websites that Kaspersky Endpoint Security does not check regardless of the application settings.

To view the global exclusions from encrypted traffic scans:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Network settings**.
3. In the **Encrypted connections scan** section, click the **websites** link.

The **Global exclusions from encrypted traffic scan** window opens. The window displays the table compiled by Kaspersky experts with information about the websites and applications for which Kaspersky Endpoint Security does not scan encrypted network connections. The table may be updated when Kaspersky Endpoint Security databases and modules are updated.

Firewall

The Firewall blocks unauthorized connections to the computer while working on the Internet or local network. The Firewall also controls the network activity of applications on the computer. This allows you to protect your corporate LAN from identity theft and other attacks. The component provides computer protection with the help of anti-virus databases, the Kaspersky Security Network cloud service, and predefined *network rules*.

Network rules

You can configure network rules at the following levels:

- *Network packet rules*. Network packet rules impose restrictions on network packets, regardless of the application. Such rules restrict inbound and outbound network traffic through specific ports of the selected data protocol. Kaspersky Endpoint Security has predefined network packet rules with permissions recommended by Kaspersky experts.
- *Application network rules*. Application network rules impose restrictions on the network activity of a specific application. They factor in not only the characteristics of the network packet, but also the specific application to which this network packet is addressed or which issued this network packet.

Controlled access of applications to operating system resources, processes and personal data is provided by the [Host Intrusion Prevention component](#) by using *application rights*.

During the first startup of the application, the Firewall performs the following actions:

1. Checks the security of the application using downloaded anti-virus databases.
2. Checks the security of the application in Kaspersky Security Network.
You are advised to [participate in Kaspersky Security Network](#) to help the Firewall work more effectively.
3. Puts the application in one of the *trust groups*: Trusted, Low Restricted, High Restricted, Untrusted.

A [trust group defines the rights](#) used by Kaspersky Endpoint Security when controlling network activity of applications. Kaspersky Endpoint Security places an application in a trust group depending on the level of danger that this application may pose to the computer.

Kaspersky Endpoint Security places an application in a trust group for the Firewall and Host Intrusion Prevention components. You cannot change the trust group only for the Firewall or Host Intrusion Prevention.

If you refused to participate in KSN or there is no network, Kaspersky Endpoint Security places the application in a trust group depending on the [settings of the Host Intrusion Prevention component](#). After receiving the reputation of the application from KSN, the trust group can be changed automatically.

4. It blocks network activity of the application depending on the trust group. For example, applications in the High Restricted trust group are not allowed to use any network connections.

The next time the application is started, Kaspersky Endpoint Security checks the integrity of the application. If the application is unchanged, the component uses the current network rules for it. If the application has been modified, Kaspersky Endpoint Security analyzes the application as if it were being started for the first time.

Network Rule Priorities

Each rule has a priority. The higher a rule is on the list, the higher its priority. If network activity is added to several rules, the Firewall regulates network activity according to the rule with the highest priority.

Network packet rules have a higher priority than network rules for applications. If both network packet rules and network rules for applications are specified for the same type of network activity, the network activity is handled according to the network packet rules.

Network packet rules have a higher priority than network rules for applications. If both network packet rules and network rules for applications are specified for the same type of network activity, the network activity is handled according to the network packet rules.

Network rules for applications work as follows: a network rule for applications includes access rules based on the network status: *public*, *local*, or *trusted*. For example, applications in the High Restricted trust group are not allowed any network activity in networks of all statuses by default. If a network rule is specified for an individual application (parent application), then the child processes of other applications will run according to the network rule of the parent application. If there is no network rule for the application, the child processes will run according to network access rule of the application's trust group.

For example, you have prohibited any network activity in networks of all statuses for all applications, except browser X. If you start browser Y installation (child process) from browser X (parent application), then browser Y installer will access the network and download the necessary files. After installation, browser Y will be denied any network connections according to the Firewall settings. To prohibit network activity of browser Y installer as a child process, you must add a network rule for the installer of browser Y.

Network connection statuses

The Firewall allows you to control network activity depending on the status of the network connection. Kaspersky Endpoint Security receives the network connection status from the computer's operating system. The status of the network connection in the operating system is set by the user when setting up the connection. You can [change the status of the network connection in the Kaspersky Endpoint Security settings](#). The Firewall will monitor network activity depending on the network status in the Kaspersky Endpoint Security settings, and not in the operating system.

The network connection can have one of the following status types:

- **Public network.** The network is not protected by antivirus applications, firewalls, or filters (such as Wi-Fi in a cafe). When the user operates a computer that is connected to such a network, Firewall blocks access to files and printers of this computer. External users are also unable to access data through shared folders and remote access to the desktop of this computer. Firewall filters the network activity of each application according to the network rules that are set for it.

Firewall assigns *Public network* status to the Internet by default. You cannot change the status of the Internet.

- **Local network.** Network for users with restricted access to files and printers on this computer (such as for a corporate LAN or home network).

Trusted network. Safe network in which the computer is not exposed to attacks or unauthorized data access attempts. Firewall permits any network activity within networks with this status.

Enabling or disabling Firewall

By default, Firewall is enabled and functions in the optimal mode.

To enable or disable Firewall:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Firewall**.
3. Do one of the following:
 - To enable Firewall, select the **Firewall** check box.
 - To disable Firewall, clear the **Firewall** check box.
4. Save your changes.

Changing the network connection status

To change the network connection status:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Firewall**.
3. Click the **Available networks** button.
The **Firewall** window opens.
4. Select the network connection whose status you want to change.
5. In the context menu, select the network connection status:
 - **Public network.**
 - **Local network.**
 - **Trusted network.**
6. Save your changes.

Managing network packet rules

You can perform the following actions while managing network packet rules:

- Create a new network packet rule.
You can create a new network packet rule by creating a set of conditions and actions that is applied to network packets and data streams.
- Enable or disable a network packet rule.
All network packet rules that are created by Firewall by default have *Enabled* status. When a network packet rule is enabled, Firewall applies this rule.
You can disable any network packet rule that is selected in the list of network packet rules. When a network packet rule is disabled, Firewall temporarily does not apply this rule.

A new custom network packet rule is added to the list of network packet rules by default with *Enabled* status.
- Edit the settings of an existing network packet rule.
After you create a new network packet rule, you can always return to editing its settings and modify them as needed.
- Change the Firewall action for a network packet rule.
In the list of network packet rules, you can edit the action that is taken by Firewall on detecting network activity that matches a specific network packet rule.
- Change the priority of a network packet rule.
You can raise or lower the priority of a network packet rule that is selected in the list.
- Remove a network packet rule.

You can remove a network packet rule to stop Firewall from applying this rule on detecting network activity and to stop this rule from showing in the list of network packet rules with *Disabled* status.

Creating and editing a network packet rule

When creating network packet rules, remember that they have priority over network rules for applications.

To create or edit a network packet rule:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Firewall**.
3. Click the **Network packet rules** button.

4. The **Firewall** window opens to the **Network packet rules** tab.

This tab shows a list of default network packet rules that are set by Firewall.

5. Do one of the following:


- To create a new network packet rule, click the **Add** button.
- To edit a network packet rule, select it in the list of network packet rules and click the **Edit** button.

The **Network rule** window opens.

6. In the **Action** drop-down list, select the action to be performed by Firewall on detecting this kind of network activity:

- **Allow.**
- **Block.**
- **By application rules.**

7. In the **Name** field, specify the name of the network service in one of the following ways:

- Click the  icon to the right of the **Name** field and select the name of the network service in the drop-down list.

The drop-down list includes network services that define the most frequently used network connections.

- Manually enter the name of the network service in the **Name** field.

8. Specify the data transfer protocol:

- a. Select the **Protocol** check box.

- b. In the drop-down list, select the type of protocol for which network activity is to be monitored.

Firewall monitors network connections that use the TCP, UDP, ICMP, ICMPv6, IGMP, and GRE protocols. If you select a network service from the **Name** drop-down list, the **Protocol** check box is selected automatically and the drop-down list next to the check box contains the protocol type that corresponds to the selected network service. By default, the **Protocol** check box is cleared.

9. In the **Direction** drop-down list, select the direction of the monitored network activity.

Firewall monitors network connections with the following directions:

- **Inbound (packet).**
- **Inbound.**
- **Inbound / Outbound.**
- **Outbound (packet).**
- **Outbound.**

10. If ICMP or ICMPv6 is selected as the protocol, you can specify the ICMP packet type and code:

- a. Select the **ICMP type** check box and select the ICMP packet type in the drop-down list.
- b. Select the **ICMP code** check box and select the ICMP packet code in the drop-down list.

11. If TCP or UDP is selected as the protocol type, you can specify the comma-delimited port numbers of the local and remote computers between which the connection is to be monitored:

- a. Type the ports of the remote computer in the **Remote ports** field.
- b. Type the ports of the local computer in the **Local ports** field.

12. In the **Network adapters** table, specify the settings of network adapters from which network packets can be sent or which can receive network packets. To do so, use the **Add**, **Edit**, and **Delete** buttons.

13. If you want to restrict control of network packets based on their time to live (TTL), select the **Time to live (TTL)** check box and in the field next to it, specify the range of values of the time to live for inbound and/or outbound network packets.

A network rule will control the transmission of network packets whose time to live does not exceed the specified value.

Otherwise, clear the **Time to live (TTL)** check box.

14. Specify the network addresses of remote computers that can send and/or receive network packets. To do so, select one of the following values in the **Remote addresses** drop-down list:

- **Any address.** The network rule controls network packets sent and/or received by remote computers with any IP address.
- **Subnet addresses.** The network rule controls network packets sent and/or received by remote computers with IP addresses associated with the selected network type: **Trusted networks**, **Local networks**, or **Public networks**.
- **Addresses from the list.** The network rule controls network packets sent and/or received by remote computers with IP addresses that can be specified in the list below using the **Add**, **Edit**, and **Delete** buttons.

15. Specify the network addresses of computers that have Kaspersky Endpoint Security installed and can send and/or receive network packets. To do so, select one of the following values in the **Local addresses** drop-down

list:

- **Any address.** The network rule controls network packets sent and/or received by computers with Kaspersky Endpoint Security installed and with any IP address.
- **Addresses from the list.** The network rule controls network packets sent and/or received by computers with Kaspersky Endpoint Security installed and with IP addresses that can be specified in the list below using the **Add**, **Edit**, and **Delete** buttons.

Sometimes a local address cannot be obtained for applications that work with network packets. If this is the case, the value of the **Local addresses** setting is ignored.

16. If you want the actions of the network rule to be reflected in the [report](#), select the **Log events** check box.

17. In the **Network rule** window, click **OK**.

If you create a new network rule, the rule is displayed on the **Network packet rules** tab of the **Firewall** window. By default, the new network rule is placed at the end of the list of network packet rules.

18. Save your changes.

Enabling or disabling a network packet rule

To enable or disable a network packet rule:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Firewall**.
3. Click the **Network packet rules** button.
The **Firewall** window opens to the **Network packet rules** tab.
4. Select the necessary network packet rule in the list.
5. Do one of the following:
 - To enable the rule, select the check box next to the name of the network packet rule.
 - To disable the rule, clear the check box next to the name of the network packet rule.
6. Save your changes.

Changing the Firewall action for a network packet rule

To change the Firewall action that is applied to a network packet rule:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Firewall**.

3. Click the **Network packet rules** button.

The **Firewall** window opens to the **Network packet rules** tab.

4. In the list, select the network packet rule whose action you want to change.

5. In the **Permission** column, right-click to bring up the context menu and select the action that you want to assign:

- **Allow.**
- **Block.**
- **According to the application rule**
- **Log events.**

6. Save your changes.

Changing the priority of a network packet rule

The priority of a network packet rule is determined by its position in the list of network packet rules. The topmost network packet rule in the list of network packet rules has the highest priority.

Every manually created network packet rule is added to the end of the list of network packet rules and is of the lowest priority.

Firewall executes rules in the order in which they appear in the list of network packet rules, from top to bottom. According to each processed network packet rule that applies to a particular network connection, Firewall either allows or blocks network access to the address and port that are specified in the settings of this network connection.

To change the network packet rule priority:

1. In the main application window, click the **Settings** button.

2. In the application settings window, select **Essential Threat Protection** → **Firewall**.

3. Click the **Network packet rules** button.

The **Firewall** window opens to the **Network packet rules** tab.

4. In the list, select the network packet rule whose priority you want to change.

5. Use the **Move up** and **Move down** buttons to move the network packet rule to the desired spot in the list of network packet rules.

6. Save your changes.

Managing application network rules

By default, Kaspersky Endpoint Security groups all applications that are installed on the computer by the name of the vendor of the software whose file or network activity it monitors. Application groups are in turn categorized into [trust groups](#). All applications and application groups inherit properties from their parent group: application control rules, application network rules, and their execution priority.

Like the [Host Intrusion Prevention](#) component, by default the Firewall component applies the network rules for an application group when filtering the network activity of all applications within the group. The application group network rules define the rights of applications within the group to access different network connections.

By default, Firewall creates a set of network rules for each application group that is detected by Kaspersky Endpoint Security on the computer. You can change the Firewall action that is applied to the application group network rules that are created by default. You cannot edit, remove, disable, or change the priority of application group network rules that are created by default.

You can also create a network rule for an individual application. Such a rule will have a higher priority than the network rule of the group to which the application belongs.

You can perform the following actions while managing network rules of applications:

- Create a new network rule.

You can create a new network rule by which the Firewall must regulate the network activity of the application or applications that belong to the selected group of applications.

- Enable or disable a network rule.

All network rules are added to the list of network rules of applications with *Enabled* status. If a network rule is enabled, Firewall applies this rule.

You can disable a network rule that was manually created. If a network rule is disabled, Firewall temporarily does not apply this rule.

- Change the settings of a network rule.

After you create a new network rule, you can always return to its settings and modify them as needed.

- Change the Firewall action for a network rule.

In the list of network rules, you can edit the action that the Firewall applies for the network rule upon detecting network activity in this application or application group.

- Change the priority of a network rule.

You can raise or lower the priority of a custom network rule.

- Delete a network rule.

You can delete a custom network rule to stop the Firewall from applying this network rule to the selected application or application group upon detecting network activity, and to stop this rule from being displayed in the list of application network rules.

Creating and editing an application network rule

To create or edit a network rule for an application or application group:

1. In the main application window, click the **Settings** button.

2. In the application settings window, select **Essential Threat Protection** → **Firewall**.

3. Click the **Application rules** button.

The **Firewall** window opens to the **Application network rules** tab.

4. In the list of applications, select the application or group of applications for which you want to create or edit a network rule.

5. Right-click to bring up the context menu and select **Application rights** or **Group rights** depending on what you need to do.

This opens the **Application rights** or **Group rights** window.

6. Select the **Network rules** tab in the **Application rights** or **Group rights** window.

7. Do one of the following:


- To create a new network rule, click the **Add** button.
- To edit a network rule, select it in the list of network rules and click the **Edit** button.

The **Network rule** window opens.

8. In the **Action** drop-down list, select the action to be performed by Firewall on detecting this kind of network activity:

- **Allow**.
- **Block**.

9. In the **Name** field, specify the name of the [network service](#) in one of the following ways:

- Click the  icon to the right of the **Name** field and select the name of the network service in the drop-down list.

The drop-down list includes network services that define the most frequently used network connections.

- Manually enter the name of the network service in the **Name** field.

10. Specify the data transfer protocol:

a. Select the **Protocol** check box.

b. In the drop-down list, select the type of protocol on which to monitor network activity.

Firewall monitors network connections that use the TCP, UDP, ICMP, ICMPv6, IGMP, and GRE protocols. If you select a network service from the **Name** drop-down list, the **Protocol** check box is selected automatically and the drop-down list next to the check box contains the protocol type that corresponds to the selected network service. By default, the **Protocol** check box is cleared.

11. In the **Direction** drop-down list, select the direction of the monitored network activity.

Firewall monitors network connections with the following directions:

- **Inbound**.
- **Inbound / Outbound**.
- **Outbound**.

12. If ICMP or ICMPv6 is selected as the protocol, you can specify the ICMP packet type and code:
 - a. Select the **ICMP type** check box and select the ICMP packet type in the drop-down list.
 - b. Select the **ICMP code** check box and select the ICMP packet code in the drop-down list.
 13. If TCP or UDP is selected as the protocol type, you can specify the comma-delimited port numbers of the local and remote computers between which the connection is to be monitored:
 - a. Type the ports of the remote computer in the **Remote ports** field.
 - b. Type the ports of the local computer in the **Local ports** field.
 14. Specify the network addresses of remote computers that can send and/or receive network packets. To do so, select one of the following values in the **Remote addresses** drop-down list:
 - **Any address.** The network rule controls network packets sent and/or received by remote computers with any IP address.
 - **Subnet addresses.** The network rule controls network packets sent and/or received by remote computers with IP addresses associated with the selected network type: **Trusted networks**, **Local networks**, or **Public networks**.
 - **Addresses from the list.** The network rule controls network packets sent and/or received by remote computers with IP addresses that can be specified in the list below using the **Add**, **Edit**, and **Delete** buttons.
 15. Specify the network addresses of computers that have Kaspersky Endpoint Security installed and can send and/or receive network packets. To do so, select one of the following values in the **Local addresses** drop-down list:
 - **Any address.** The network rule controls network packets sent and/or received by computers with Kaspersky Endpoint Security installed and with any IP address.
 - **Addresses from the list.** The network rule controls network packets sent and/or received by computers with Kaspersky Endpoint Security installed and with IP addresses that can be specified in the list below using the **Add**, **Edit**, and **Delete** buttons.
- Sometimes a local address cannot be obtained for applications that work with network packets. If this is the case, the value of the **Local addresses** setting is ignored.
16. If you want the actions of the network rule to be reflected in the [report](#), select the **Log events** check box.
 17. In the **Network rule** window, click **OK**.

If you created a new network rule, the rule is displayed on the **Network rules** tab.
 18. Click **OK** in the **Group rights** window if the rule is intended for a group of applications, or in the **Application rights** window if the rule is intended for an application.
 19. Save your changes.

Enabling and disabling an application network rule

To enable or disable an application network rule:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Firewall**.
3. Click the **Application rules** button.
The **Firewall** window opens to the **Application network rules** tab.
4. In the list, select the application or group of applications for which you want to enable or disable a network rule.
5. Right-click to bring up the context menu and select **Application rights** or **Group rights** depending on what you need to do.
This opens the **Application rights** or **Group rights** window.
6. In the window that opens, select the **Network rules** tab.
7. In the list of network rules for an application group, select the relevant network rule.
8. Do one of the following:
 - If you want to enable the rule, select the check box next to the name of the network rule.
 - If you want to disable the rule, clear the check box next to the name of the network rule.

You cannot disable an application group network rule that is created by Firewall by default.

9. Click **OK** in the **Group rights** window if the rule is intended for a group of applications, or in the **Application rights** window if the rule is intended for an application.
10. Save your changes.

Changing the Firewall action for an application network rule

You can change the Firewall action that is applied to all network rules for an application or application group that were created by default, and change the Firewall action for a single custom network rule for an application or application group.

To change the Firewall action for all network rules for an application or group of applications:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Firewall**.
3. Click the **Application rules** button.
The **Firewall** window opens to the **Application network rules** tab.
4. If you want to change the Firewall action that is applied to all network rules that are created by default, select an application or group of applications in the list. Manually created network rules are left unchanged.
5. In the **Network** column, click to display the context menu and select the action that you want to assign:

- **Inherit.**
- **Allow.**
- **Block.**

6. Save your changes.

To change the Firewall response for one network rule for an application or application group:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Firewall**.
3. Click the **Application rules** button.
The **Firewall** window opens to the **Application network rules** tab.
4. In the list, select the application or group of applications for which you want to change the action for one network rule.
5. Right-click to bring up the context menu and select **Application rights** or **Group rights** depending on what you need to do.
This opens the **Application rights** or **Group rights** window.
6. In the window that opens, select the **Network rules** tab.
7. Select the network rule for which you want to change the Firewall action.
8. In the **Permission** column, right-click to bring up the context menu and select the action that you want to assign:
 - **Allow.**
 - **Block.**
 - **Log events.**
9. Click **OK** in the **Group rights** window if the rule is intended for a group of applications, or in the **Application rights** window if the rule is intended for an application.
10. Save your changes.

Changing the priority of an application network rule

The priority of a network rule is determined by its position in the list of network rules. Firewall executes the rules in the order in which they appear in the list of network rules, from top to bottom. According to each processed network rule that applies to a particular network connection, Firewall either allows or blocks network access to the address and port that are indicated in the settings of this network connection.

Manually created network rules have a higher priority than default network rules.

You cannot change the priority of application group network rules that are created by default.

To change the priority of a network rule:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **Firewall**.
3. Click the **Application rules** button.
The **Firewall** window opens to the **Application network rules** tab.
4. In the list of applications, select the application or group of applications for which you want to change the priority of a network rule.
5. Right-click to bring up the context menu and select **Application rights** or **Group rights** depending on what you need to do.
This opens the **Application rights** or **Group rights** window.
6. In the window that opens, select the **Network rules** tab.
7. Select the network rule whose priority you want to change.
8. Use the **Move up** and **Move down** buttons to move the network rule to the desired spot in the list of network rules.
9. Click **OK** in the **Group rights** window if the rule is intended for a group of applications, or in the **Application rights** window if the rule is intended for an application.
10. Save your changes.

Network Monitor

Network Monitor is a tool designed for viewing information about network activity of a user's computer in real time.

To start Network Monitor:

1. In the main application window, click the **Protection components** section.
2. Click the **Network Monitor** link in the lower part of the window.
The **Network Monitor** window opens. In this window, information about the network activity of the computer is shown on four tabs:
 - The **Network activity** tab shows all currently active network connections with the computer. Both outbound and inbound network connections are displayed.
 - The **Open ports** tab lists all open network ports of the computer.
 - The **Network traffic** tab shows the volume of inbound and outbound network traffic between the user's computer and other computers in the network to which the user is currently connected.

- The **Blocked computers** tab lists the IP addresses of remote computers whose network activity has been blocked by the Network Threat Protection component after detecting network attack attempts from such IP addresses.

BadUSB Attack Prevention

Some viruses modify the firmware of USB devices to trick the operating system into detecting the USB device as a keyboard.

The BadUSB Attack Prevention component prevents infected USB devices emulating a keyboard from connecting to the computer.

When a USB device is connected to the computer and identified by the application as a keyboard, the application prompts the user to enter a numerical code generated by the application from this keyboard, or using On-Screen Keyboard (if it is available). This procedure is known as keyboard authorization. The application allows use of an authorized keyboard and blocks a keyboard that has not been authorized.

The BadUSB Attack Prevention component is not installed by default. If you need the BadUSB Attack Prevention component, you can add the component in the properties of the [installation package](#) before installing the application or [change the available application components](#) after installing the application.

Enabling and disabling BadUSB Attack Prevention

To enable or disable BadUSB Attack Prevention:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **BadUSB Attack Prevention**.
3. Do one of the following:
 - If you want to enable BadUSB Attack Prevention, select the **BadUSB Attack Prevention** check box.
 - If you want to disable BadUSB Attack Prevention, clear the **BadUSB Attack Prevention** check box.
4. Save your changes.

Allowing and prohibiting the use of On-Screen Keyboard for authorization

On-Screen Keyboard should be used only for authorization of USB devices that do not support the input of random characters (e.g. bar code scanners). It is not recommended to use On-Screen Keyboard for authorization of unknown USB devices.

To allow or prohibit the use of On-Screen Keyboard for authorization:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **BadUSB Attack Prevention**.

The component settings are displayed in the right part of the window.

3. Do one of the following:

- Select the **Prohibit use of On-Screen Keyboard for authorization of USB devices** check box if you want to block the use of the On-Screen Keyboard for authorization.
- Clear the **Prohibit use of On-Screen Keyboard for authorization of USB devices** check box if you want to allow the use of the On-Screen Keyboard for authorization.

4. Save your changes.

Keyboard authorization

USB devices identified by the operating system as keyboards and connected to the computer before installation of the BadUSB Attack Prevention component are considered authorized after installation of the component.

The application requires authorization of the connected USB device that has been identified by the operating system as a keyboard only if the prompt for USB keyboard authorization is enabled. The user cannot use an unauthorized keyboard until it is authorized.

If the prompt for USB keyboard authorization is disabled, the user can use all connected keyboards. Immediately after the prompt for USB keyboard authorization is enabled, the application shows a prompt for authorization of each unauthorized keyboard that is connected.

To authorize a keyboard:

1. With USB keyboard authorization enabled, connect the keyboard to a USB port.

The **<Keyboard name> keyboard authorization** window opens with the details of the connected keyboard and a numerical code for its authorization.

2. Enter the randomly generated numerical code in the authorization window from the connected keyboard or On-Screen Keyboard (if available).

3. Click **OK**.

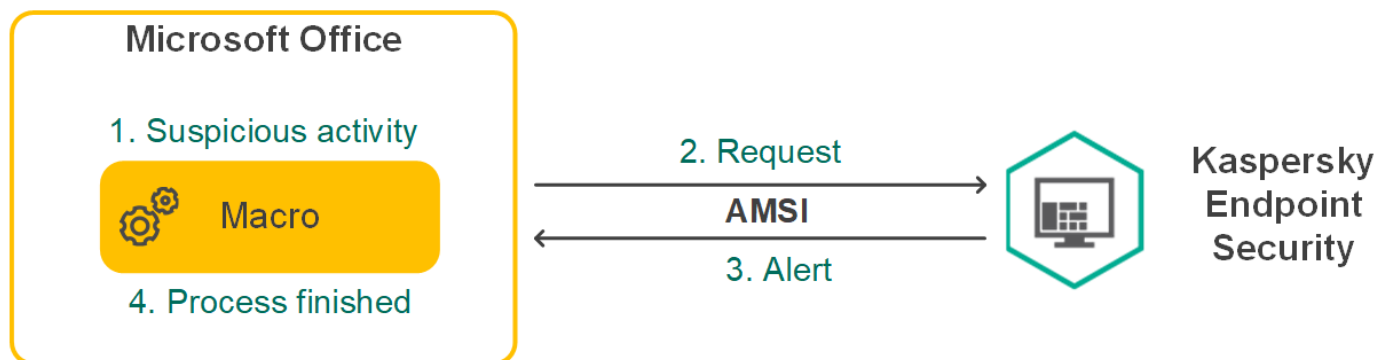
If the code has been entered correctly, the application saves the identification parameters – VID/PID of the keyboard and the number of the port to which it has been connected – in the list of authorized keyboards. Authorization does not need to be repeated when the keyboard is reconnected or after the operating system is restarted.

When the authorized keyboard is connected to a different USB port of the computer, the application shows a prompt for authorization of this keyboard again.

If the numerical code has been entered incorrectly, the application generates a new code. Three attempts are available for entering the numerical code. If the numerical code is entered incorrectly three times in a row or the **<Keyboard name> keyboard authorization** window is closed, the application blocks input from this keyboard. When the keyboard is reconnected or the operating system is restarted, the application prompts the user to perform keyboard authorization again.

AMSI Protection Provider is intended to support Antimalware Scan Interface from Microsoft. The *Antimalware Scan Interface (AMSI)* allows third-party applications with AMSI support to send objects (for example, PowerShell scripts) to Kaspersky Endpoint Security for an additional scan and then receive the results from scanning these objects. Third-party applications may include, for example, Microsoft Office applications (see the figure below). For details on AMSI refer to [Microsoft documentation](#).

The AMSI Protection Provider can only detect a threat and notify a third-party application about the detected threat. Third-party application after receiving a notification of a threat does not allow to perform malicious actions (for example, terminates).



AMSI operation example

AMSI Protection Provider may decline a request from a third-party application, for example, if this application exceeds maximum number of requests within a specified interval. Kaspersky Endpoint Security sends information about a rejected request from a third-party application to the Administration Server. The AMSI Protection Provider component does not reject requests from those third-party applications for which the [Do not block interaction with AMSI Protection Provider](#) check box is selected

The AMSI Protection Provider is available for the following operating systems for workstations and servers:

- Windows 10 Home / Pro / Education / Enterprise;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter.

Enabling and disabling the AMSI Protection Provider

By default, the AMSI Protection Provider is enabled.

To enable or disable the AMSI Protection Provider:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Essential Threat Protection** → **AMSI Protection Provider**.
3. Do one of the following:
 - Select the **AMSI Protection Provider** check box if you want to enable the AMSI Protection Provider.
 - Clear the **AMSI Protection Provider** check box if you want to disable the AMSI Protection Provider.

4. Save your changes.

Scanning compound files with the AMSI Protection Provider

A common technique for concealing viruses and other malware is to embed them in compound files such as archives. To detect viruses and other malware that are hidden in this way, the compound file must be unpacked, which may slow down scanning. You can limit the types of compound files to be scanned, thus speeding up scanning.

To configure scanning of compound files by the AMSI Protection Provider:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **AMSI Protection Provider**.
3. In the **Scan of compound files** section, specify the types of compound files that you want to scan: archives, distribution package, or files in office formats.
4. In the **Size limit** section, do one of the following:
 - To block the AMSI Protection Provider component from unpacking large compound files, select the **Do not unpack large compound files** check box and specify the required value in the **Maximum file size** field. The AMSI Protection Provider component will not unpack compound files that are larger than the specified size.
 - To allow the AMSI Protection Provider component to unpack large compound files, clear the **Do not unpack large compound files** check box.

The AMSI Protection Provider component scans large files that are extracted from archives, regardless of whether the **Do not unpack large compound files** check box is selected.

5. Save your changes.

Computer control

Application Control

Application Control manages the startup of applications on users' computers. This allows you to implement a corporate security policy when using applications. Application Control also reduces the risk of computer infection by restricting access to applications.

Configuring Application Control consists of the following steps:

1. [Creating application categories.](#)

The administrator creates categories of applications that the administrator wants to manage. Categories of applications are intended for all computers in the corporate network, regardless of administration groups. To create a category, you can use the following criteria: KL category (for example, *Browsers*), file hash, application vendor, and other criteria.

2. [Creating Application Control rules.](#)

The administrator creates Application Control rules in the policy for the administration group. The rule includes the categories of applications and the startup status of applications from these categories: blocked or allowed.

3. [Selecting the Application Control mode.](#)

The administrator chooses the mode for working with applications that are not included in any of the rules: black list or white list.

When a user attempts to start a prohibited application, Kaspersky Endpoint Security will block the application from starting and will display a notification (see the figure below).

A *test mode* is provided to check the configuration of Application Control. In this mode, Kaspersky Endpoint Security does the following:

- Allows the startup of applications, including prohibited ones.
- Shows a notification about the startup of a prohibited application and adds information to the report on the user's computer.
- Sends data about the startup of prohibited applications to Kaspersky Security Center.



Application Control notification

Application Control operating modes

The Application Control component operates in two modes:

- **Black List.** In this mode, Application Control allows users to start all applications except for applications that are prohibited in Application Control rules.

This mode of Application Control is enabled by default.

- **White List.** In this mode, Application Control blocks users from starting any applications except for applications that are allowed and not prohibited in Application Control rules.

If the allow rules of Application Control are fully configured, the component blocks the startup of all new applications that have not been verified by the LAN administrator, while allowing the operation of the operating system and of trusted applications that users rely on in their work.

You can read the [recommendations on configuring application control rules in white list mode](#).

Application Control can be configured to operate in these modes both by using the Kaspersky Endpoint Security local interface and by using Kaspersky Security Center.

However, Kaspersky Security Center offers tools that are not available in the Kaspersky Endpoint Security local interface, such as the tools that are needed for the following tasks:

- [Creating application categories](#).

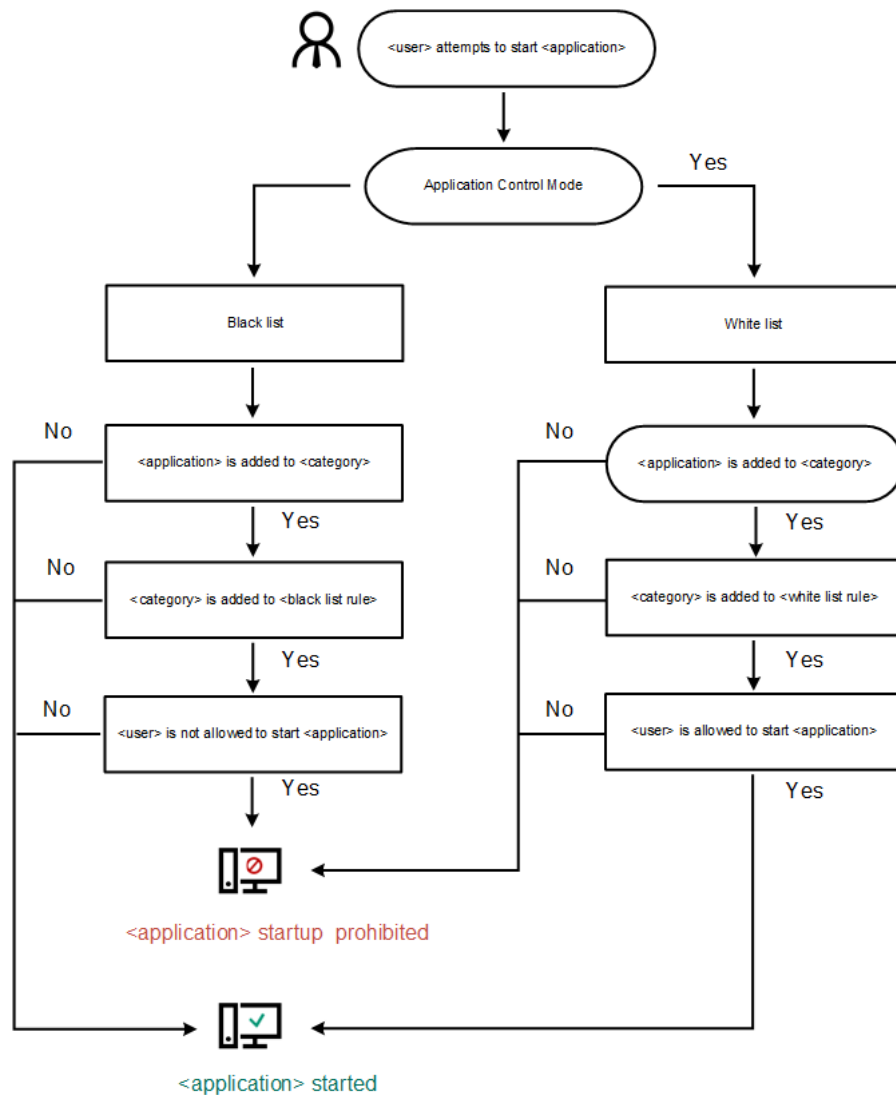
Application Control rules created in the Kaspersky Security Center Administration Console are based on your custom application categories and not on inclusion and exclusion conditions as is the case in the Kaspersky Endpoint Security local interface.

- [Receiving information about applications that are installed on corporate LAN computers](#).

This is why it is recommended to use Kaspersky Security Center to configure the operation of the Application Control component.

Application Control operating algorithm

Kaspersky Endpoint Security uses an algorithm to make a decision about starting an application (see the figure below).



Application Control operating algorithm

Application Control functionality limitations

Operation of the Application Control component is limited in the following cases:

- When the application version is upgraded, importing Application Control component settings is not supported.
- When the application version is upgraded, the import of Application Control settings is supported only if Kaspersky Endpoint Security 10 Service Pack 2 for Windows or later is upgraded to Kaspersky Endpoint Security 11.4.0 for Windows.

When application versions other than Kaspersky Endpoint Security 10 Service Pack 2 for Windows are upgraded, the Application Control settings have to be configured anew in order to restore this component to operational state.

- If there is no connection with KSN servers, Kaspersky Endpoint Security receives information about the reputation of applications and their modules only from local databases.

The list of applications assigned by Kaspersky Endpoint Security to the KL category **Applications trusted according to reputation in KSN** when a connection to KSN servers is available may differ from the list of applications assigned by Kaspersky Endpoint Security to the KL category **Applications trusted according to reputation in KSN** when there is no connection to KSN.

- At the Kaspersky Security Center database, information on 150,000 processed files may be stored. Once this number of records has been achieved, new files will not be processed. To resume inventory operations, you must delete the files that were previously inventoried in the Kaspersky Security Center database from the computer on which Kaspersky Endpoint Security is installed.
- The component does not control the startup of scripts unless the script is sent to the interpreter via the command line.

If the startup of an interpreter is allowed by Application Control rules, the component will not block a script started from this interpreter.

If at least one of the scripts specified in the interpreter command line is blocked from start by Application control rules, the component blocks all the scripts, specified in the interpreter command line.

- The component does not control the startup of scripts from interpreters that are not supported by Kaspersky Endpoint Security.

Kaspersky Endpoint Security supports the following interpreters:

- Java
- PowerShell

The following types of interpreters are supported:

- %ComSpec%;
- %SystemRoot%\system32\regedit.exe;
- %SystemRoot%\regedit.exe;
- %SystemRoot%\system32\regedt32.exe;
- %SystemRoot%\system32\cscript.exe;
- %SystemRoot%\system32\wscript.exe;
- %SystemRoot%\system32\msiexec.exe;
- %SystemRoot%\system32\mshta.exe;
- %SystemRoot%\system32\rundll32.exe;
- %SystemRoot%\system32\wwahost.exe;
- %SystemRoot%\syswow64\cmd.exe;
- %SystemRoot%\syswow64\regedit.exe;

- %SystemRoot%\syswow64\regedt32.exe;
- %SystemRoot%\syswow64\cscript.exe;
- %SystemRoot%\syswow64\wscript.exe;
- %SystemRoot%\syswow64\msiexec.exe;
- %SystemRoot%\syswow64\mshta.exe;
- %SystemRoot%\syswow64\rundll32.exe;
- %SystemRoot%\syswow64\wwahost.exe.

Enabling and disabling Application Control

By default, Application Control is disabled.

To enable or disable Application Control:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Application Control**.
3. Do one of the following:
 - If you want to enable Application Control, select the **Application Control** check box.
 - If you want to disable Application Control, clear the **Application Control** check box.
4. Save your changes.

Managing Application Control rules

Kaspersky Endpoint Security controls the startup of applications by users by means of rules. An Application Control rule specifies the triggering conditions and actions performed by the Application Control component when the rule is triggered (allowing or blocking application startup by users).

Rule-triggering conditions

A condition for triggering the rule has the following correspondence: "condition type - condition criterion - condition value" (see the figure below). Based on the rule-triggering conditions, Kaspersky Endpoint Security applies (or does not apply) a rule to an application.

The screenshot shows the 'Application Control rule' configuration window. It includes fields for 'Rule name' and 'Description'. Below these are two sections for conditions: 'Inclusion conditions' and 'Exclusion conditions'. Each section has a search box and a table with columns for 'Condition criterion' and 'Condition value'. The 'Inclusion conditions' table has buttons for '+ Add', 'Edit', 'Remove', and 'Convert into exclusion'. The 'Exclusion conditions' table has buttons for '+ Add', 'Edit', 'Remove', and 'Convert into inclusion condition'. The 'Subjects and their rights' section contains a table with columns for 'Subject', 'Allow', and 'Deny'. The 'Everyone' subject has 'Allow' unchecked and 'Deny' checked. Below this table are checkboxes for 'Deny for other users' and 'Trusted Updaters'. At the bottom right are 'OK' and 'Cancel' buttons.

Application Control rule. Rule-triggering condition parameters

Rules use inclusion and exclusion conditions:

- *Inclusion conditions.* Kaspersky Endpoint Security applies the rule to the application if the application matches at least one of the inclusion conditions.
- *Exclusion conditions.* Kaspersky Endpoint Security does not apply the rule to the application if the application matches at least one of the exclusion conditions and does not match any of the inclusion conditions.

Rule-triggering conditions are created using criteria. The following criteria are used to create rules in Kaspersky Endpoint Security:

- Path to the folder containing the executable file of the application or path to the executable file of the application.
- Metadata: application executable file name, application executable file version, application name, application version, application vendor.
- Hash of the executable file of the application.
- Certificate: issuer, subject, thumbprint.
- Inclusion of the application in a KL category.
- Location of the application executable file on a removable drive.

The criterion value must be specified for each criterion used in the condition. If the parameters of the application being started match the values of criteria specified in the inclusion condition, the rule is triggered. In this case, Application Control performs the action prescribed in the rule. If application parameters match the values of criteria specified in the exclusion condition, Application Control does not control startup of the application.

Decisions made by the Application Control component when a rule is triggered

When a rule is triggered, Application Control allows users (or user groups) to start applications or blocks startup according to the rule. You can select individual users or groups of users that are allowed or not allowed to start applications that trigger a rule.

If a rule does not specify those users allowed to start applications satisfying the rule, this rule is called a *block* rule.

If a rule that does not specify any users who are not allowed to start applications that match the rule, this rule is called an *allow* rule.

The priority of a block rule is higher than the priority of an allow rule. For example, if an Application Control allow rule has been assigned for a user group while an Application Control block rule has been assigned for one user in this user group, this user will be blocked from starting the application.

Operating status of a rule

Application Control rules can have one of the following operating statuses:

- **On.** This status means that the rule is used when Application Control is in operation.
- **Off.** This status means that the rule is ignored when Application Control is in operation.

Test. This status signifies that Kaspersky Endpoint Security allows the startup of applications to which the rules apply but logs information about the startup of such applications in the report.

Receiving information about the applications that are installed on users' computers

To create optimal Application Control rules, it is recommended to first get a picture of the applications that are used on computers on the corporate LAN. To do this, you can obtain the following information:

- Vendors, versions, and localizations of applications used on the corporate LAN.
- Frequency of application updates.
- Application usage policies adopted in the company (this may be security policies or administrative policies).
- Storage location of application distribution packages.

Information about applications that are used on corporate LAN computers is available in the **Applications registry** folder and in the **Executable files** folder. The **Applications registry** folder and the **Executable files** folder are located in the **Application management** folder in the Kaspersky Security Center Administration Console tree.

The **Applications registry** folder contains the list of applications that were detected by [Network Agent](#) which is installed on the client computer.

The **Executable files** folder contains a list of all executable files that have ever been started on client computers or that were detected during the inventory task of Kaspersky Endpoint Security.

To view general information about the application and its executable files, and the list of computers on which an application is installed, open the properties window of an application that is selected in the **Applications registry** folder or in the **Executable files** folder.

*To open the application properties window in the **Applications registry** folder:*

1. Open the Kaspersky Security Center Administration Console.
2. In the Administration Console tree, select **Additional** → **Application management** → **Applications registry**.
3. Select an application.
4. In the context menu of the application, select **Properties**.

*To open the properties window for an executable file in the **Executable files** folder:*

1. Open the Kaspersky Security Center Administration Console.
2. In the Administration Console tree, select the **Additional** → **Application management** → **Executable files** folder.
3. Select an executable file.
4. In the context menu of the executable file, select **Properties**.

Creating application categories

For more convenience when creating Application Control rules, you can create application categories.

It is recommended to create a "Work applications" category that covers the standard set of applications that are used at the company. If different user groups use different sets of applications in their work, a separate application category can be created for each user group.

To create an application category:

1. Open the Kaspersky Security Center Administration Console.
2. In the Administration Console tree, select the **Additional** → **Application management** → **Application categories** folder.
3. Click the **Create a category** button in the workspace.
The user category creation wizard starts.
4. Follow the instructions of the user category creation wizard.

Step 1. Selecting the category type

At this step, select one of the following types of application categories:

- **Category with content added manually.** If you selected this type of category, at the "Configuring the conditions for including applications in a category" step and the "Configuring the conditions for excluding applications from a category" step, you will be able to define the criteria whereby executable files will be included into the category.
- **Category which includes executable files from selected devices.** If you selected this type of category, at the "Settings" step you will be able to specify a computer whose executable files will be automatically included in the category.
- **Category that includes executable files from a specific folder.** If you selected this type of category, at the "Repository folder" step you will be able to specify a folder from which executable files will be automatically included in the category.

When creating a category with content added automatically, Kaspersky Security Center performs inventory on files with the following formats: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX, and SCR.

Step 2. Entering a user category name

At this step, specify a name for the application category.

Step 3. Configuring the conditions for including applications in a category

This step is available if you selected the **Category with content added manually** category type.

At this step, in the **Add** drop-down list, select the conditions for including applications into the category:

- **From the list of executable files.** Add applications from the list of executable files on the client device to the custom category.
- **From file properties.** Specify detailed data of executable files as a condition for adding applications to the custom category.
- **Metadata from files in folder.** Select a folder on the client device that contains executable files. Kaspersky Security Center will indicate the metadata of these executable files as a condition for adding applications to the custom category.
- **Checksums of files in folder.** Select a folder on the client device that contains executable files. Kaspersky Security Center will indicate the hashes of these executable files as a condition for adding applications to the custom category.
- **Certificates for files from folder.** Select a folder on the client device that contains executable files signed with certificates. Kaspersky Security Center will indicate the certificates of these executable files as a condition for adding applications to the custom category.

It is not recommended to use conditions whose properties do not have the **Certificate thumbprint** parameter specified.

- **MSI installer files metadata.** Select the MSI package. Kaspersky Security Center will indicate the metadata of executable files packed in this MSI package as a condition for adding applications to the custom category.

- **Checksums of files from MSI installer of the application.** Select the MSI package. Kaspersky Security Center will indicate the hashes of executable files packed in this MSI package as a condition for adding applications to the custom category.
- **KL category.** Specify a KL category as a condition for adding applications to the custom category. A *KL category* is a list of applications that have shared theme attributes. The list is maintained by Kaspersky experts. For example, the KL category known as "Office applications" includes applications from the Microsoft Office suite, Adobe Acrobat, and others.

You can select all KL categories to generate an extended list of trusted applications.

- **Path to application.** Select a folder on the client device. Kaspersky Security Center will add executable files from this folder to the custom category.
- **Certificates from certificate repository.** Select certificates that were used to sign executable files as a condition for adding applications to the custom category.

It is not recommended to use conditions whose properties do not have the **Certificate thumbprint** parameter specified.

- **Drive type.** Specify the type of storage device (all hard drives and removable drives, or only removable drives) as a condition for adding applications to the custom category.

Step 4. Configuring the conditions for excluding applications from a category

This step is available if you selected the **Category with content added manually** category type.

Applications specified at this step are excluded from the category even if these applications were specified at the "Configuring the conditions for including applications in a category" step.

At this step, in the **Add** drop-down list, select conditions for excluding applications from the category:

- **From the list of executable files.** Add applications from the list of executable files on the client device to the custom category.
- **From file properties.** Specify detailed data of executable files as a condition for adding applications to the custom category.
- **Metadata from files in folder.** Select a folder on the client device that contains executable files. Kaspersky Security Center will indicate the metadata of these executable files as a condition for adding applications to the custom category.
- **Checksums of files in folder.** Select a folder on the client device that contains executable files. Kaspersky Security Center will indicate the hashes of these executable files as a condition for adding applications to the custom category.
- **Certificates for files from folder.** Select a folder on the client device that contains executable files signed with certificates. Kaspersky Security Center will indicate the certificates of these executable files as a condition for adding applications to the custom category.
- **MSI installer files metadata.** Select the MSI package. Kaspersky Security Center will indicate the metadata of executable files packed in this MSI package as a condition for adding applications to the custom category.

- **Checksums of files from MSI installer of the application.** Select the MSI package. Kaspersky Security Center will indicate the hashes of executable files packed in this MSI package as a condition for adding applications to the custom category.
- **KL category.** Specify a KL category as a condition for adding applications to the custom category. A *KL category* is a list of applications that have shared theme attributes. The list is maintained by Kaspersky experts. For example, the KL category known as "Office applications" includes applications from the Microsoft Office suite, Adobe Acrobat, and others.

You can select all KL categories to generate an extended list of trusted applications.

- **Path to application.** Select a folder on the client device. Kaspersky Security Center will add executable files from this folder to the custom category.
- **Certificates from certificate repository.** Select certificates that were used to sign executable files as a condition for adding applications to the custom category.
- **Drive type.** Specify the type of storage device (all hard drives and removable drives, or only removable drives) as a condition for adding applications to the custom category.

Step 5. Settings

This step is available if you selected the **Category which includes executable files from selected devices** category type.

At this step, click the **Add** button and specify the computers whose executable files will be added to the application category by Kaspersky Security Center. All executable files from the specified computers presented in the [Executable files](#) folder will be added to the application category by Kaspersky Security Center.

At this step, you can also configure the following settings:

- Algorithm for hash function calculation by Kaspersky Security Center. To select an algorithm, you must select at least one of the following check boxes:
 - **Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and any later versions).**
 - **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows).**
- **Synchronize data with the Administration Server repository** check box. Select this check box if you want Kaspersky Security Center to periodically clear the application category and add to it all executable files from the specified computers presented in the **Executable files** folder.

If the **Synchronize data with the Administration Server repository** check box is cleared, Kaspersky Security Center will not make any modifications to an application category after it is created.

- **Scan period (h)** field. In this field, you can specify the period of time (in hours) after which Kaspersky Security Center clears the application category and adds to it all executable files from the specified computers presented in the **Executable files** folder.

The field is available if the **Synchronize data with the Administration Server repository** check box is selected.

Step 6. Repository folder

This step is available if you selected the **Category that includes executable files from a specific folder** category type.

At this step, click the **Browse** button and specify the folder in which Kaspersky Security Center will search for executable files to automatically add applications to the application category.

At this step, you can also configure the following settings:

- **Include dynamic-link libraries (DLL) in this category** check box. Select this check box if you want dynamic-link libraries (DLL files) to be included in the application category.

Including DLL files in the application category may reduce the performance of Kaspersky Security Center.

- **Include script data in this category** check box. Select this check box if you want scripts to be included in the application category.

Including scripts in the application category may reduce the performance of Kaspersky Security Center.

- Algorithm for hash function calculation by Kaspersky Security Center. To select an algorithm, you must select at least one of the following check boxes:

- **Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and any later versions).**
- **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows).**

- **Force folder scan for changes** check box. Select this check box if you want Kaspersky Security Center to periodically search for executable files in the folder used for automatically adding to the application category.

If the **Force folder scan for changes** check box is cleared, Kaspersky Security Center searches for executable files in the folder used for automatically adding to the application category only if changes have been made in the folder, files have been added to it or deleted from it.

- **Scan period (h)** field. In this field, you can specify the time interval (in hours) after which Kaspersky Security Center will search for executable files in the folder used for automatically adding to the application category.

This field is available if the **Force folder scan for changes** check box is selected.

Step 7. Creating a custom category

To exit the Application Setup Wizard, click the **Finish** button.

Adding executable files from the Executable files folder to the application category

In the **Executable files** folder the list of executable files detected on computers is displayed. Kaspersky Endpoint Security generates a list of executable files after executing the Inventory task.

*To add executable files from the **Executable files** folder to the application category:*

1. Open the Kaspersky Security Center Administration Console.
2. In the Administration Console tree, select **Additional** → **Application management** → **Executable files** folder.
3. In the workspace, select the executable files that you want to add to the application category.
4. Right-click to open the context menu for the selected executable files and select **Add to category**.
The **Select application category** window opens.
5. In the **Select application category** window:
 - In the upper part of the window, choose one of the following options:
 - **Create category of applications**. Choose this option if you want to create a new application category and add executable files to it.
 - **Add rules to specified category**. Choose this option if you want to select an existing application category and add executable files to it.
 - In the **Rule type** section, choose one of the following options:
 - **Add to inclusion rules**. Select this option if you want to create a condition that adds executable files to the application category.
 - **Add to exclusion rules**. Select this option if you want to create a condition that excludes executable files from the application category.
 - In the **File info type** section, choose one of the following options:
 - **Certificate data (or SHA-256 for files without a certificate)**.
 - **Certificate data (files without a certificate will be skipped)**.
 - **Only SHA-256 (files without SHA-256 will be skipped)**.
 - **MD5 (discontinued mode, only for Kaspersky Endpoint Security 10 Service Pack 1)**.
6. Click **OK**.

Adding event-related executable files to the application category

To add executable files related to Application Control events to the application category:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Administration Server** node of the Administration Console tree, select the **Events** tab.
3. Choose a selection of events related to operation of the Application Control component ([Viewing events resulting from operation of the Application Control component](#), [Viewing events resulting from test operation of the Application Control component](#)) in the **Selection events** drop-down list.
4. Click the **Run selection** button.

5. Select the events whose associated executable files you want to add to the application category.

6. Right-click to open the context menu for the selected events and select **Add to category**.

The **Select application category** window opens.

7. In the **Select application category** window:

- In the upper part of the window, choose one of the following options:
 - **Create category of applications.** Choose this option if you want to create a new application category and add executable files to it.
 - **Add rules to specified category.** Choose this option if you want to select an existing application category and add executable files to it.
- In the **Rule type** section, choose one of the following options:
 - **Add to inclusion rules.** Select this option if you want to create a condition that adds executable files to the application category.
 - **Add to exclusion rules.** Select this option if you want to create a condition that excludes executable files from the application category.
- In the **File info type** section, choose one of the following options:
 - **Certificate data (or SHA-256 for files without a certificate).**
 - **Certificate data (files without a certificate will be skipped).**
 - **Only SHA-256 (files without SHA-256 will be skipped).**
 - **MD5 (discontinued mode, only for Kaspersky Endpoint Security 10 Service Pack 1).**

8. Click OK.

Adding and modifying an Application Control rule using Kaspersky Security Center

To add or modify an Application Control rule using Kaspersky Security Center:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Security Controls** → **Application Control**.

In the right part of the window, the settings of the Application Control component are displayed.

6. Do one of the following:

- To add a rule, click the **Add** button.
- If you want to edit an existing rule, select it in the list of rules and click the **Edit** button.

The **Application Control rule** window opens.

7. Do one of the following:

- If you want to create a new category:
 - a. Click the **Create a category** button.
The user category creation wizard starts.
 - b. Follow the instructions of the user category creation wizard.
 - c. In the **Category** drop-down list, select the created application category.
- If you want to edit an existing category:
 - a. In the **Category** drop-down list, select the created application category that you want to edit.
 - b. Click the **Properties** button.
The **Properties: <Category name>** window opens.
 - c. Modify the settings of the selected application category.
 - d. Click **OK**.
 - e. In the **Category** drop-down list, select the created application category based on which you want to create a rule.

8. In the **Subjects and their rights** table, click the **Add** button.

The standard Microsoft Windows **Select Users or Groups** window opens.

9. In the **Select Users or Groups** window, specify the list of users and/or user groups for which you want to configure permission to start applications from the selected category.

10. In the **Subjects and their rights** table:

- If you want to allow users and/or groups of users to start applications that belong to the selected category, select the **Allow** check box in the relevant rows.
- If you want to block users and/or groups of users from starting applications that belong to the selected category, select the **Deny** check box in the relevant rows.

11. Select the **Deny for other users** check box if you want all users that do not appear in the **Subject** column and that are not part of the group of users specified in the **Subject** column to be blocked from starting applications that belong to the selected category.

12. If you want Kaspersky Endpoint Security to consider applications included in the selected application category as trusted updaters allowed to create other executable files that will be subsequently allowed to run, select the **Trusted Updaters** check box.

When Kaspersky Endpoint Security settings are migrated, the list of executable files created by trusted updaters is migrated as well.

13. Click **OK**.

14. In the **Application Control** section of the policy properties window, click the **Apply** button.

Changing the status of an Application Control rule via Kaspersky Security Center

To change the status of an Application Control rule:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Security Controls** → **Application Control**.
In the right part of the window, the settings of the Application Control component are displayed.
6. In the **Status** column, left-click to display the context menu and select one of the following:
 - **On**. This status means that the rule is used when Application Control is in operation.
 - **Off**. This status means that the rule is ignored when Application Control is in operation.
 - **Test**. This status means that Kaspersky Endpoint Security always allows the startup of applications to which the rule applies but logs information about the startup of such applications in the report.

You can use the **Test** status to assign the [action equivalent to the Test rules](#) option for a portion of rules when the **Apply rules** option is selected in the **Action** drop-down list.

7. Save your changes.

Testing Application Control rules using Kaspersky Security Center

To ensure that Application Control rules do not block applications required for work, it is recommended to enable testing of Application Control rules and analyze their operation after creating new rules. When testing of Application Control rules is enabled, Kaspersky Endpoint Security will not block applications whose startup is forbidden by Application Control, but will instead send notifications about their startup to the Administration Server.

An analysis of the operation of Application Control rules requires a review of the resultant Application Control events that are reported to Kaspersky Security Center. If test mode results in no blocked startup events for all applications required for the work of the computer user, this means that the correct rules were created. Otherwise, you are advised to update the settings of the rules you have created, create additional rules, or delete the existing rules.

By default, Kaspersky Endpoint Security allows the startup of all applications except for applications prohibited by the rules.

To enable or disable testing of Application Control rules in Kaspersky Security Center:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Security Controls** → **Application Control**.
In the right part of the window, the settings of the Application Control component are displayed.
6. In the **Control mode** drop-down list, select one of the following items:
 - **Black List**, if you want to allow the startup of all applications except the applications prohibited by rules.
 - **White List**, if you want to block the startup of all applications except the applications allowed by rules.
7. Do one of the following:
 - If you want to enable testing of Application Control rules, select the **Test rules** option in the **Action** drop-down list.
 - If you want to enable Application Control to manage the startup of applications on users' computers, select the **Apply rules** option in the **Action** drop-down list.
8. Save your changes.

Viewing events resulting from test operation of the Application Control component

To view Application Control testing events received by Kaspersky Security Center:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Administration Server** node of the Administration Console tree, select the **Events** tab.
3. Click the **Create a selection** button.
The **Properties: <Selection name>** window opens.
4. Open the **Events** section.

5. Click the **Clear all** button.
6. In the **Events** table, select the **Application startup prohibited in test mode** and **Application startup allowed in test mode** check boxes.
7. Click **OK**.
8. In the **Selection events** drop-down list, select the created selection.
9. Click the **Run selection** button.

Viewing a report on blocked applications in test mode

To view the report on blocked applications in test mode:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Administration Server** node of the Administration Console tree, select the **Reports** tab.
3. Click the **New report template** button.
The Report Template Wizard starts.
4. Follow the instructions of the Report Template Wizard. At the **Selecting the report template type** step, select **Other** → **Report on blocked applications in test mode**.
After you have finished with the New Report Template Wizard, the new report template appears in the table on the **Reports** tab.
5. Run the report generation process created at previous steps of the instructions by using one of the following methods:
 - In the context menu of the report, select **Show report**.
 - Click the **Show report** link located in the right part of the Administration Console workspace.
 - Open the report by double-clicking it.

The report generation process starts. The report is displayed in a new window.

Viewing events resulting from operation of the Application Control component

To view events resulting from the operation of the Application Control component received by Kaspersky Security Center:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Administration Server** node of the Administration Console tree, select the **Events** tab.
3. Click the **Create a selection** button.
The **Properties: <Selection name>** window opens.

4. Open the **Events** section.
5. Click the **Clear all** button.
6. In the **Events** table, select the **Application startup prohibited** check box.
7. Click **OK**.
8. In the **Selection events** drop-down list, select the created selection.
9. Click the **Run selection** button.

Viewing a report on blocked applications

To view the report on blocked applications:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Administration Server** node of the Administration Console tree, select the **Reports** tab.
3. Click the **New report template** button.
The Report Template Wizard starts.
4. Follow the instructions of the Report Template Wizard. At the **Selecting the report template type** step, select **Other** → **Report on blocked applications**.
After you have finished with the New Report Template Wizard, the new report template appears in the table on the **Reports** tab.
5. Run the report generation process created at previous steps of the instructions by using one of the following methods:
 - In the context menu of the report, select **Show report**.
 - Click the **Show report** link located in the right part of the Administration Console workspace.
 - Open the report by double-clicking it.

The report generation process starts. The report is displayed in a new window.

Selecting the Application Control mode

To select the Application Control mode:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Application Control**.
3. Select the **Application Control** check box to make the component settings available for editing.
4. In the **Control mode** drop-down list, select one of the following items:

- **Black List**, if you want to allow the startup of all applications except the applications specified in block rules.
- **White List**, if you want to block the startup of all applications except the applications specified in allow rules.

The initially defined rules for white list mode are the **Golden Image** rule, which allows the startup of applications that are included in the "Golden Image" category, and the **Trusted Updaters** rule, which allows the startup of applications that are included in the "Trusted Updaters" KL category. The "Golden Image" KL category includes programs that ensure normal operation of the operating system. The "Trusted Updaters" KL category includes updaters for the most reputable software vendors. You cannot delete these rules. The settings of these rules cannot be edited. By default, the **Golden Image** rule is enabled, and the **Trusted Updaters** rule is disabled. All users are allowed to start applications that match the trigger conditions of these rules.

All rules created during the selected mode are saved after the mode is changed so that the rules can be used again. To revert to using these rules, select the required mode in the **Control mode** drop-down list.

5. In the **Action** drop-down list, select the action to be performed by the component when a user attempts to start an application that is blocked by Application Control rules.
6. Select the **Control DLL and drivers** check box if you want Kaspersky Endpoint Security to monitor the loading of DLL modules when applications are started by users.

Information about the module and the application that loaded the module will be saved to a report.

Kaspersky Endpoint Security monitors only the DLL modules and drivers loaded since the **Control DLL and drivers** check box was selected. Restart the computer after selecting the **Control DLL and drivers** check box if you want Kaspersky Endpoint Security to monitor all DLL modules and drivers, including ones loaded before Kaspersky Endpoint Security is started.

When enabling control over which DLL modules and drivers are loaded, make sure that one of the following [rules is enabled](#) in the **Application Control** section: the default [Golden Image](#) rule or another rule that contains the Trusted certificates KL category and ensures that trusted DLL modules and drivers are loaded before Kaspersky Endpoint Security is started. Application Control rules that were created based on other KL categories (except for the Trusted certificates KL category) are not used for startup control of DLL modules and drivers. Enabling control of the loading of DLL modules and drivers when the **Golden Image** rule is disabled may cause instability in the operating system.

We recommend turning on [password protection](#) for configuring application settings, so that it is possible to turn off the rules blocking critical DLL modules and drivers from start, without modifying Kaspersky Security Center policy settings.

7. Save your changes.

Actions with Application Control rules

Kaspersky Endpoint Security controls the startup of applications by users by means of rules. An Application Control rule specifies the triggering conditions and actions performed by the Application Control component when the rule is triggered (allowing or blocking application startup by users).

Rule-triggering conditions

A condition for triggering the rule has the following correspondence: "condition type - condition criterion - condition value" (see the figure below). Based on the rule-triggering conditions, Kaspersky Endpoint Security applies (or does not apply) a rule to an application.

The screenshot shows the 'Application Control rule' configuration window. It includes fields for 'Rule name' and 'Description'. Below these are sections for 'Inclusion conditions' and 'Exclusion conditions', each featuring a search icon and a table with two columns: 'Condition criterion' and 'Condition value'. Action buttons like '+ Add', 'Edit', 'Remove', and 'Convert into exclusion' are provided for each table. The 'Subjects and their rights' section contains a table with columns for 'Subject', 'Allow', and 'Deny', with 'Everyone' listed as a subject. At the bottom, there are checkboxes for 'Deny for other users' and 'Trusted Updaters', and 'OK' and 'Cancel' buttons.

Application Control rule. Rule-triggering condition parameters

Rules use inclusion and exclusion conditions:

- *Inclusion conditions.* Kaspersky Endpoint Security applies the rule to the application if the application matches at least one of the inclusion conditions.
- *Exclusion conditions.* Kaspersky Endpoint Security does not apply the rule to the application if the application matches at least one of the exclusion conditions and does not match any of the inclusion conditions.

Rule-triggering conditions are created using criteria. The following criteria are used to create rules in Kaspersky Endpoint Security:

- Path to the folder containing the executable file of the application or path to the executable file of the application.
- Metadata: application executable file name, application executable file version, application name, application version, application vendor.
- Hash of the executable file of the application.
- Certificate: issuer, subject, thumbprint.
- Inclusion of the application in a KL category.
- Location of the application executable file on a removable drive.

The criterion value must be specified for each criterion used in the condition. If the parameters of the application being started match the values of criteria specified in the inclusion condition, the rule is triggered. In this case, Application Control performs the action prescribed in the rule. If application parameters match the values of criteria specified in the exclusion condition, Application Control does not control startup of the application.

Decisions made by the Application Control component when a rule is triggered

When a rule is triggered, Application Control allows users (or user groups) to start applications or blocks startup according to the rule. You can select individual users or groups of users that are allowed or not allowed to start applications that trigger a rule.

If a rule does not specify those users allowed to start applications satisfying the rule, this rule is called a *block* rule.

If a rule that does not specify any users who are not allowed to start applications that match the rule, this rule is called an *allow* rule.

The priority of a block rule is higher than the priority of an allow rule. For example, if an Application Control allow rule has been assigned for a user group while an Application Control block rule has been assigned for one user in this user group, this user will be blocked from starting the application.

Operating status of a rule

Application Control rules can have one of the following operating statuses:

- **On.** This status means that the rule is used when Application Control is in operation.
- **Off.** This status means that the rule is ignored when Application Control is in operation.
- **Test.** This status signifies that Kaspersky Endpoint Security allows the startup of applications to which the rules apply but logs information about the startup of such applications in the report.

Adding and editing an Application Control rule

To add or edit an Application Control rule:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Application Control**.
3. Select the **Application Control** check box to make the component settings available for editing.
4. Do one of the following:
 - To add a rule, click the **Add** button.
 - If you want to edit an existing rule, select it in the list of rules and click the **Edit** button.

The **Application Control rule** window opens.

5. Specify or edit the settings of the rule:

- a. In the **Rule name** field, enter or edit the name of the rule.
- b. In the **Inclusion conditions** table, [create](#) or edit the list of inclusion conditions that trigger a rule by clicking the **Add**, **Edit**, **Delete**, and **Convert into exclusion** buttons.
- c. In the **Exclusion conditions** table, create or edit the list of exclusion conditions that trigger a rule by clicking the **Add**, **Edit**, **Delete**, and **Convert into inclusion condition** buttons.
- d. If required, change the type of rule-triggering condition:
 - To change the condition type from an inclusion condition to an exclusion condition, select a condition in the **Inclusion conditions** table and click the **Convert into exclusion** button.
 - To change the condition type from an exclusion condition to an inclusion condition, select a condition in the **Exclusion conditions** table and click the **Convert into inclusion condition** button.
- e. Compile or edit a list of users and/or groups of users who are allowed or not allowed to start applications that meet the rule trigger conditions. To do this, click the **Add** button in the **Subjects and their rights** table. By default, the **Everyone** value is added to the list of users. The rule applies to all users.

If there is no user specified in the table, the rule cannot be saved.

- f. In the **Subjects and their rights** table, select the **Allow** or **Block** check boxes opposite the users and/or groups of users to determine their right to start applications.
The check box that is selected by default depends on the Application Control operating mode.
- g. Select the **Deny for other users** check box if you want all users that do not appear in the **Subject** column and that are not part of the group of users specified in the **Subject** column to be blocked from starting applications that match the rule trigger conditions.

If the **Deny for other users** check box is cleared, Kaspersky Endpoint Security does not control the startup of applications by users that are not specified in the **Subjects and their rights** table and that do not belong to the groups of users specified in the **Subjects and their rights** table.

- h. If you want Kaspersky Endpoint Security to consider applications matching the rule trigger conditions as trusted updaters allowed to create other executable files that will be allowed to run subsequently, select the **Trusted Updaters** check box.

6. When Kaspersky Endpoint Security settings are migrated, the list of executable files created by trusted updaters is migrated as well.

7. Save your changes.

Adding a trigger condition for an Application Control rule

To add a new trigger condition for an Application Control rule:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Application Control**.

In the right part of the window, the settings of the Application Control component are displayed.

3. Select the **Application Control** check box to make the component settings available for editing.
4. Do one of the following:
 - If you want to create a new rule and add a trigger condition to it, click the **Add** button.
 - If you want to add a trigger condition to an existing rule, select the rule in the list of rules and click the **Edit** button.

The **Application Control rule** window opens.

5. In the **Inclusion conditions** or **Exclusion conditions** table, click the **Add** button.

You can use the drop-down list under the **Add** button to add various trigger conditions to the rule (please refer to the instructions below).

To add a rule trigger condition based on the properties of files in the specified folder:

1. In the drop-down list under the **Add** button, select **Conditions from properties of files in the specified folder**.
The standard **Select folder** window of Microsoft Windows opens.
2. In the **Select folder** window, select a folder that contains the executable files of applications whose properties you want to use as the basis for one or several conditions for triggering a rule.
3. Click **OK**.
The **Add condition** window opens.
4. In the **Show criterion** drop-down list, select the criterion based on which you want to create one or several rule trigger conditions: **File hash code**, **Certificate**, **KL category**, **Metadata** or **Selected path**.

Kaspersky Endpoint Security does not support an MD5 file hash and does not control startup of applications based on an MD5 hash. An SHA256 hash is used as a rule trigger condition.

5. If you selected **Metadata** in the **Show criterion** drop-down list, select the check boxes opposite the executable file properties that you want to use in the rule trigger condition: **File name**, **File version**, **Application name**, **Application version**, and **Vendor**.

If none of the specified properties are selected, the rule cannot be saved.

6. If you selected **Certificate** in the **Show criterion** drop-down list, select the check boxes opposite the settings that you want to use in the rule trigger condition: **Issuer**, **Subject**, and **Thumbprint**.

If none of the specified settings are selected, the rule cannot be saved.

It is not recommended to use only the **Issuer** and **Subject** criteria as rule trigger conditions. Use of these criteria is unreliable.

7. Select the check boxes opposite the names of application executable files whose properties you want to include in the rule trigger conditions.
8. Click the **Next** button.

A list of formulated rule trigger conditions appears.

9. In the list of formulated rule trigger conditions, select the check boxes opposite the rule trigger conditions that you want to add to the Application Control rule.
10. Click the **Terminate** button.

To add a rule trigger condition based on the properties of applications that started on the computer:

1. In the drop-down list under the **Add** button, select **Conditions from properties of started applications**.
2. In the **Add condition** window, in the **Show criterion** drop-down list, select the criterion based on which you want to create one or several rule trigger conditions: **File hash code**, **Certificate**, **KL category**, **Metadata** or **Selected path**.

Kaspersky Endpoint Security does not support an MD5 file hash code and does not control startup of applications based on an MD5 hash. An SHA256 hash is used as a rule trigger condition.

3. If you selected **Metadata** in the **Show criterion** drop-down list, select the check boxes opposite the executable file properties that you want to use in the rule trigger condition: **File name**, **File version**, **Application name**, **Application version**, and **Vendor**.

If none of the specified properties are selected, the rule cannot be saved.

4. If you selected **Certificate** in the **Show criterion** drop-down list, select the check boxes opposite the settings that you want to use in the rule trigger condition: **Issuer**, **Subject**, and **Thumbprint**.

If none of the specified settings are selected, the rule cannot be saved.

It is not recommended to use only the **Issuer** and **Subject** criteria as rule trigger conditions. Use of these criteria is unreliable.

5. Select the check boxes opposite the names of application executable files whose properties you want to include in the rule trigger conditions.
6. Click the **Next** button.

A list of formulated rule trigger conditions appears.

7. In the list of formulated rule trigger conditions, select the check boxes opposite the rule trigger conditions that you want to add to the Application Control rule.
8. Click the **Terminate** button.

To add a rule trigger condition based on a KL category:

1. In the drop-down list under the **Add** button, select **Conditions "KL category"**.

A *KL category* is a list of applications that have shared theme attributes. The list is maintained by Kaspersky experts. For example, the KL category of "Office applications" includes applications from the Microsoft Office suite, Adobe® Acrobat®, and others.

2. In the **Conditions "KL category"** window, select the check boxes next to the names of the KL categories based on which you want to create rule triggering conditions.
3. Click **OK**.

To add a custom rule trigger condition:

1. In the drop-down list under the **Add** button, select **Custom condition**.
2. In the **Custom condition** window, click the **Select** button and specify the path to the application executable file.
3. Select the criterion based on which you want to create a rule trigger condition: **File hash code**, **Certificate**, **Metadata** or **Path to file or folder**.

Kaspersky Endpoint Security does not support an MD5 file hash code and does not control startup of applications based on an MD5 hash. An SHA256 hash is used as a rule trigger condition.

If you are using a symbolic link in the **Path to file or folder** field, you are advised to resolve the symbolic link for correct operation of the Application Control rule. To do so, click the **Resolve symbolic link** button.

4. Configure the settings of the selected criterion.
5. Click **OK**.

To add a rule trigger condition based on information about the drive storing the executable file of an application:

1. In the drop-down list under the **Add** button, select **Condition by file drive**.
2. In the **Condition by file drive** window, in the **Drive** drop-down list, select the type of storage device from which the startup of applications will serve as a rule trigger condition.
3. Click **OK**.

Changing the status of an Application Control rule

To change the status of an Application Control rule:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Application Control**.
3. Select the **Application Control** check box to make the component settings available for editing.
4. In the **Status** column, left-click to display the context menu and select one of the following:
 - **On**. This status means that the rule is used when Application Control is in operation.
 - **Off**. This status means that the rule is ignored when Application Control is in operation.
 - **Test**. This status means that Kaspersky Endpoint Security always allows the startup of applications to which this rule applies but logs information about the startup of such applications in the report.

You can use the **Test** status to assign the [action equivalent to the Test rules](#) option for a portion of rules when the **Apply rules** option is selected in the **Action** drop-down list.

5. Save your changes.

Testing Application Control rules

To ensure that Application Control rules do not block applications required for work, it is recommended to enable testing of Application Control rules and analyze their operation after creating new rules.

An analysis of the operation of Application Control rules requires a review of the resultant Application Control events that are reported to Kaspersky Security Center. If test mode results in no blocked startup events for all applications required for the work of the computer user, this means that the correct rules were created. Otherwise, you are advised to update the settings of the rules you have created, create additional rules, or delete the existing rules.

By default, the **Apply rules** action is selected for Application Control rules.

To enable testing of Application Control rules or to select a blocking action for Application Control:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Application Control**.
3. Select the **Application Control** check box to make the component settings available for editing.
4. In the **Control mode** drop-down list, select one of the following items:
 - **Black List**, if you want to allow the startup of all applications except the applications specified in block rules.
 - **White List**, if you want to block the startup of all applications except the applications specified in allow rules.
5. Do one of the following:
 - If you want to enable test mode for Application Control rules, select the **Test rules** option in the **Action** drop-down list.
 - If you want to enable blocking mode for Application Control rules, select the **Apply rules** option in the **Action** drop-down list.

6. Save your changes.

Kaspersky Endpoint Security will not block applications whose startup is forbidden by the Application Control component, but will send notifications about their startup to the Administration Server.

Rules for creating name masks for files or folders

A *mask of a file or folder name* is a representation of the name of a folder or name and extension of a file using common characters.

You can use the following common characters to create a file or folder name mask:

- The * (asterisk) character, which takes the place of any set of characters (including an empty set). For example, the C:*.txt mask will include all paths to files with the txt extension located in folders and subfolders on the (C:) drive.
- The ? (question mark) character, which takes the place of any single character, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\Folder\???.txt will include paths to all files residing in the folder named FoLder that have the TXT extension and a name consisting of three characters.

Editing Application Control message templates

When a user attempts to start an application that is blocked by an Application Control rule, Kaspersky Endpoint Security displays a message stating that the application is blocked from starting. If the user believes that an application was mistakenly blocked from starting, the user can use the link in the message text to send a message to the local corporate network administrator.

Special templates are available for the message that is displayed when an application is blocked from starting and for the message sent to the administrator. You can modify the message templates.

To edit a message template:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Application Control**.
3. Select the **Application Control** check box to make the component settings available for editing.
4. Click the **Templates** button.
The **Message templates** window opens.
5. Do one of the following:
 - If you want to edit the template of the message that is displayed when an application is blocked from starting, select the **Blockage** tab.
 - If you want to modify the template of the message that is sent to the LAN administrator, select the **Message to administrator** tab.
6. Modify the template of the message that is displayed when an application is blocked from starting or the message sent to the administrator. To do this, use the **By default** and **Variable** buttons.
7. Save your changes.

Device Control

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Windows for workstations. This component is unavailable if Kaspersky Endpoint Security is installed on a computer that runs on Windows for servers.

Device Control manages user access to devices that are installed on or connected to the computer (for example, hard drives, cameras, or Wi-Fi modules). This lets you protect the computer from infection when such devices are connected, and prevent loss or leaks of data.

Device access levels

Device Control controls access at the following levels:

- **Device type.** For example, printers, removable drives, and CD/DVD drives.

You can configure device access as follows:

- Allow – ✓.
 - Block – ⓧ.
 - Depends on connection bus (except for Wi-Fi) – 🌐.
 - Block with exceptions (only Wi-Fi and portable devices (MTP)) – 📁.
- **Connection bus.** A *connection bus* is an interface used for connecting devices to the computer (for example, USB or FireWire). Therefore, you can restrict the connection of all devices, for example, over USB.

You can configure device access as follows:

- Allow – ✓.
 - Block – ⓧ.
- **Trusted devices.** *Trusted devices* are devices to which users that are specified in the trusted device settings have full access at all times.

You can add trusted devices based on the following data:

- **Devices by ID.** Each device has a unique identifier (Hardware ID, or HWID). You can view the ID in the device properties by using operating system tools. Example device ID: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Adding devices by ID is convenient if you want to add several specific devices.
- **Devices by model.** Each device has a vendor ID (VID) and a product ID (PID). You can view the IDs in the device properties by using operating system tools. Template for entering the VID and PID: `VID_1234&PID_5678`. Adding devices by model is convenient if you use devices of a certain model in your organization. This way, you can add all devices of this model.
- **Devices by ID mask.** If you are using multiple devices with similar IDs, you can add devices to the trusted list by using masks. The `*` character replaces any set of characters. Kaspersky Endpoint Security does not support the `?` character when entering a mask. For example, `WDC_C*`.
- **Devices by model mask.** If you are using multiple devices with similar VIDs or PIDs (for example, devices from the same manufacturer), you can add devices to the trusted list by using masks. The `*` character replaces any set of characters. Kaspersky Endpoint Security does not support the `?` character when entering a mask. For example, `VID_05AC & PID_*`.

Device Control regulates user access to devices by using [access rules](#). Device Control also lets you save device connection/disconnection events. To save events, you need to configure the registration of events in a policy.

If access to a device depends on the connection bus (the 🌐 status), Kaspersky Endpoint Security does not save device connection/disconnection events. To enable Kaspersky Endpoint Security to save device connection/disconnection events, allow access to the corresponding type of device (the ✓ status) or add the device to the trusted list.

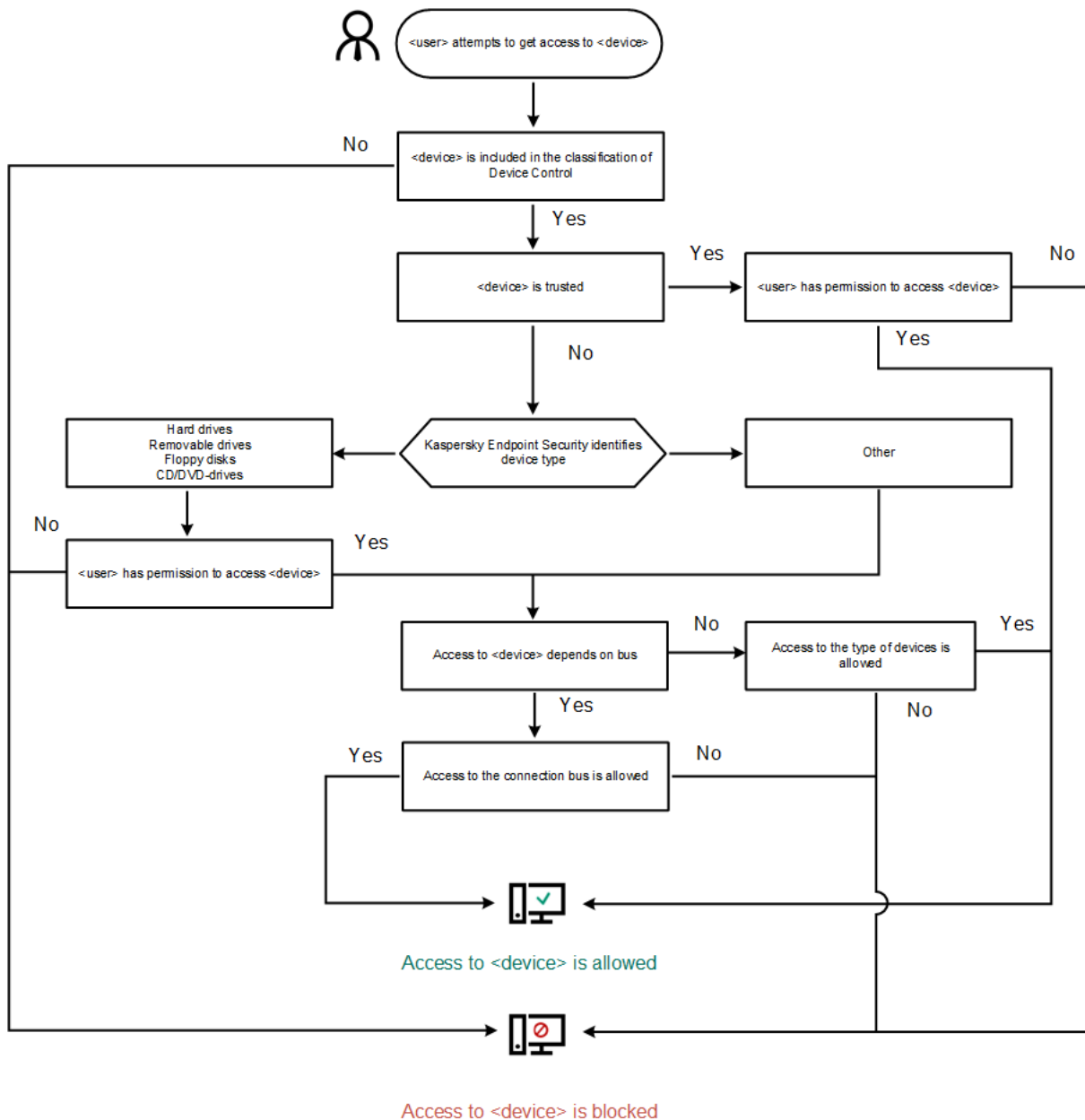
When a device that is blocked by Device Control is connected to the computer, Kaspersky Endpoint Security will block access and show a notification (see the figure below).



Device Control notification

Device Control operating algorithm

Kaspersky Endpoint Security makes a decision on whether to allow access to a device after the user connects the device to the computer (see the figure below).



Device Control operating algorithm

If a device is connected and access is allowed, you can edit the access rule and block access. In this case, the next time someone attempts to access the device (such as to view the folder tree, or perform read or write operations), Kaspersky Endpoint Security blocks access. A device without a file system is blocked only the next time that the device is connected.

If a user of the computer with Kaspersky Endpoint Security installed must request access to a device that the user believes was blocked by mistake, send the user the [request access instructions](#).

Enabling and disabling Device Control

By default, Device Control is enabled.

To enable or disable Device Control:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Device Control**.

3. Do one of the following:

- If you want to enable Device Control, select the **Device Control** check box.
- If you want to disable Device Control, clear the **Device Control** check box.

4. Save your changes.

About access rules

Access rules comprise a group of settings that determine which users can access devices that are installed or connected to the computer. You cannot add a device that is outside of Device Control classification. Access to such devices is allowed for all users.

Device Access Rules



The group of settings for an access rule differs depending on the type of device (see the table below).


Access rule settings

Devices	Access (✓ / ✗ / 🚫)	Schedule for access to a device	Assignment of users and/or a group of users	Read/write permission
Hard drives	✓	✓	✓	✓
Removable drives	✓	✓	✓	✓
Printers	✓	–	–	–
Floppy disks	✓	✓	✓	✓
CD/DVD drives	✓	✓	✓	✓
Modems	✓	–	–	–
Tape devices	✓	–	–	–
Multifunctional devices	✓	–	–	–
Smart card readers	✓	–	–	–
Windows CE USB ActiveSync devices	✓	–	–	–
External network adapters	✓	–	–	–
Portable devices (MTP)	✓	✓	✓	✓
Bluetooth	✓	–	–	–
Cameras and scanners	✓	–	–	–




Mobile devices running Android or iOS are categorized as portable devices (MTP). When a mobile device is connected to the computer, the operating system determines the device type. If Android Debug Bridge (ADB), iTunes or their equivalent applications are installed on the computer, the operating system identifies mobile devices as ADB or iTunes devices. In all other cases, the operating system may identify the mobile device type as a portable device (MTP) for file transfer, a PTP device (camera) for image transfer, or another device. The device type depends on the model of the mobile device.

Please note the following special considerations regarding access to ADB- or iTunes devices:



- You cannot configure a device access schedule. If access to devices is restricted by rules (they have the  status), ADB- and iTunes devices are always accessible.
- You cannot configure device access for individual users, or configure access permissions (read/write). If access to devices is restricted by rules (they have the  status), ADB- and iTunes devices are accessible to all users with all permissions.
- You cannot configure access to trusted ADB- or iTunes devices for individual users. If the device is trusted, ADB- and iTunes devices are accessible to all users.
- If you installed the ADB or iTunes applications after connecting a device to the computer, the unique ID of the device may be reset. This means that Kaspersky Endpoint Security will identify this device as a new device. If a device is trusted, add the device to the trusted list again.

By default, access rules grant all users full access to the devices at all times, if access to the connection buses for the corresponding types of devices is allowed (the  status).

Access rules for Wi-Fi networks

A Wi-Fi network access rule determines whether the use of Wi-Fi networks is allowed (the  status) or forbidden (the  status). You can add a *trusted Wi-Fi network* (the  status) to a rule. Use of a trusted Wi-Fi network is allowed without limitations. By default, a Wi-Fi network access rule allows access to any Wi-Fi network.

Connection bus access rules

Connection bus access rules determine whether the connection of devices is allowed (the  status) or forbidden (the  status). Rules that allow access to buses are created by default for all connection buses that are present in the classification of the Device Control component.

Editing a device access rule

Depending on the type of device, you can modify various access settings, such as the list of users receiving access to the device, the access schedule, and allowed / blocked access.

To edit a device access rule:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Device Control**.
3. In the right part of the window, select the **Types of devices** tab.

The **Types of devices** tab contains access rules for all devices that are included in the classification of the Device Control component.

4. Select the access rule that you want to edit.

5. Click the **Edit** button. This button is only available for device types which have a file system.

The **Configuring device access rule** window opens.

By default, a device access rule grants all users full access to the specified type of devices at any time. In the **Users and / or groups of users** list, this access rule contains the **All** group. In the **Rights of the selected group of users by access schedules** table, this access rule contains the **Default schedule** for access to devices, with the rights to perform all types of operations with devices.

6. Click the **Select** button.

The **Select users and/or groups** window opens.

7. Do the following:

- To add users or user groups to the table in the **Select users and/or groups** window:
 - a. In the **Select users and/or groups** window click the **Add** button.
The standard **Select users or groups** window in Microsoft Windows opens.
 - b. In the **Select users or groups** window in Microsoft Windows, specify users and / or groups of users for which Kaspersky Endpoint Security recognizes the selected devices as trusted.
 - c. In the **Select users or groups** window click the **OK** button.
The names of users and / or groups of users that are specified in the **Select users or groups** window of Microsoft Windows are displayed in the **Select users and/or groups** window.
- To delete users or user groups from the table in the **Select users and/or groups** window, select one or more rows in the table and click **Delete**.
To select multiple rows, select them while holding down the **CTRL** key.

8. In the **Select users and/or groups** window click the **OK** button.

9. In the **Rights of the selected group of users by access schedules** table, configure the schedule for access to devices for the selected user and / or group of users. To do this, select the check boxes next to the names of the access schedules for devices that you want to use in the device access rule that is to be edited.

10. To edit the list of access schedules to devices, use the **Create**, **Edit**, **Copy**, and **Remove** buttons in the **Rights of the selected group of users by access schedules** table.

11. For each schedule for access to devices used in the rule being edited, specify the operations that are allowed when working with devices. To do so, in the **Rights of the selected group of users by access schedules** table, select the check boxes in the columns containing the names of the relevant operations.

12. Click **OK**.

After you have edited the default settings of a device access rule, the setting for access to the type of device in the **Access** column in the table on the **Types of devices** tab is changed to the *Restrict by rules* value.

13. Save your changes.

Adding or excluding records to or from the event log

Event logging is available only for operations with files on removable drives.

To enable or disable event logging:

1. In the main application window, click the **Settings** button.

2. In the application settings window, select **Security Controls** → **Device Control**.

3. In the right part of the window, select the **Types of devices** tab.

The **Types of devices** tab contains access rules for all devices that are included in the classification of the Device Control component.

4. Select **Removable drives** in the table of devices.

The **Logging** button becomes available in the upper part of the table.

5. Click the **Logging** button.

This opens the **Logging Settings** window.

6. Do one of the following:

- If you want to enable logging of file deletion and write operations on removable drives, select the **Enable logging** check box.

Kaspersky Endpoint Security will save an event to the log file and send a message to the Kaspersky Security Center Administration Server whenever the user performs write or delete operations with files on removable drives.

- Otherwise, clear the **Enable logging** check box.

7. Specify which operations must be logged. To do so, perform one of the following:

- If you want Kaspersky Endpoint Security to log all events, select the **All formats** check box.
- If you want Kaspersky Endpoint Security to log only information about files of a specific format, in the **Filter on file formats** section, select the check boxes opposite the relevant file formats.

8. Click the **Select** button.

The **Select users and/or groups** window opens.

When the users specified in the **Users** section write to files located on removable drives or delete files from removable drives, Kaspersky Endpoint Security will save information about such operations to the event log and send a message to the Kaspersky Security Center Administration Server.

9. Do the following:

- To add users or user groups to the table in the **Select users and/or groups** window:

1. In the **Select users and/or groups** window click the **Add** button.

The standard **Select users or groups** window in Microsoft Windows opens.

2. In the **Select users or groups** window in Microsoft Windows, specify users and / or groups of users for which Kaspersky Endpoint Security recognizes the selected devices as trusted.

3. In the **Select users or groups** window click the **OK** button.

The names of users and / or groups of users that are specified in the **Select users or groups** window of Microsoft Windows are displayed in the **Select users and/or groups** window.

- To delete users or user groups from the table in the **Select users and/or groups** window, select one or more rows in the table and click **Delete**.

To select multiple rows, select them while holding down the **CTRL** key.

10. Save your changes.

You can view events associated with files on removable drives in the Kaspersky Security Center Administration Console in the workspace of the **Administration Server** node on the **Events** tab. For events to be displayed in the local Kaspersky Endpoint Security event log, you must select the **File operation performed** check box in the [notification settings](#) for the Device Control component.

Adding a Wi-Fi network to the trusted list

You can allow users connect to Wi-Fi networks that you consider to be secure, such as a corporate Wi-Fi network. To do so, you must add the network to the list of trusted Wi-Fi networks. Device Control will block access to all Wi-Fi networks except those specified in the trusted list.

To add a Wi-Fi network to the trusted list:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Device Control**.
3. In the right part of the window, select the **Types of devices** tab.

The **Types of devices** tab contains access rules for all devices that are included in the classification of the Device Control component.

4. In the **Access** column opposite the **Wi-Fi** device, right-click to open the context menu.
5. Select the **Block with exceptions** option.
6. In the list of devices, select **Wi-Fi** and click the **Edit** button.

This opens the **Trusted Wi-Fi networks** window.

7. Click the **Add** button.

This opens the **Trusted Wi-Fi network** window.

8. In the **Trusted Wi-Fi network** window:

- In the **Network name** field, specify the name of the Wi-Fi network that you want to add to the trusted list.
- In the **Authentication type** drop-down list, select the type of authentication used when connecting to the trusted Wi-Fi network.
- In the **Encryption type** drop-down list, select the type of encryption used for securing traffic of the trusted Wi-Fi network.
- In the **Comment** field, you can specify any information about the added Wi-Fi network.

A Wi-Fi network is considered trusted if its settings match all settings specified in the rule.

9. Save your changes.

Editing a connection bus access rule

To edit a connection bus access rule:

1. In the main application window, click the **Settings** button.

2. In the application settings window, select **Security Controls** → **Device Control**.

3. Select the **Connection buses** tab.

The **Connection buses** tab displays the access rules for all connection buses that are classified in the Device Control component.

4. Select the bus connection rule that you want to edit.

5. Change the value of the access parameter:

- To allow access to a connection bus, click the **Access** column to open the context menu and select **Allow**.
- To block access to a connection bus, click the **Access** column to open the context menu and select **Block**.

6. Save your changes.

Actions with trusted devices

Trusted devices are devices to which users that are specified in the trusted device settings have full access at all times.

To work with trusted devices, you can grant access to an individual user, to a group of users, or to all users of the organization.

For example, if your organization does not allow the use of removable drives but administrators use removable drives in their work, you can allow removable drives only for a group of administrators. To do so, add removable drives to the trusted list and configure user access permissions.

Kaspersky Endpoint Security allows you to add a device to the trusted list in the following ways:

- If Kaspersky Security Center is not deployed in your organization, you can connect the device to the computer and [add it to the trusted list in the application settings](#). To distribute the list of trusted devices to all computers in your organization, you can enable merging the lists of trusted devices in a policy or use the [export / import procedure](#).
- If Kaspersky Security Center is deployed in your organization, you can detect all connected devices remotely and [create a list of trusted devices in the policy](#). The list of trusted devices will be available on all computers to which the policy is applied.

Adding a device to the Trusted list from the application interface

By default, when a device is added to the list of trusted devices, access to the device is granted to all users (the Everyone group of users).

To add a device to the Trusted list from the application interface:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Device Control**.
3. In the right part of the window, select the **Trusted devices** tab.
4. Click the **Select** button.
The **Select trusted devices** window opens.
5. Select the check box next to the name of a device that you want to add to the list of trusted devices.
The list in the **Devices** column depends on the value that is selected in the **Display connected devices** drop-down list.
6. Click the **Select** button.
The **Select users and/or groups** window opens.
7. Do the following:
 - To add users or user groups to the table in the **Select users and/or groups** window:
 - a. In the **Select users and/or groups** window click the **Add** button.
The standard **Select users or groups** window in Microsoft Windows opens.
 - b. In the **Select users or groups** window in Microsoft Windows, specify users and / or groups of users for which Kaspersky Endpoint Security recognizes the selected devices as trusted.
 - c. In the **Select users or groups** window click the **OK** button.
The names of users and / or groups of users that are specified in the **Select users or groups** window of Microsoft Windows are displayed in the **Select users and/or groups** window.
 - To delete users or user groups from the table in the **Select users and/or groups** window, select one or more rows in the table and click **Delete**.
To select multiple rows, select them while holding down the **CTRL** key.
8. In the **Select users and/or groups** window click the **OK** button.
9. Click **OK**.
10. In the **Select trusted devices** window, click **OK**.
In the table, on the **Trusted devices** tab of the **Device Control** component settings window, a row appears with the parameters of the newly added trusted device.
11. Repeat steps 4-7 for each device that you want to add to the list of trusted devices for the specified users and / or user groups.

12. Save your changes.

Adding a device to the Trusted list from Kaspersky Security Center

Kaspersky Security Center receives information about devices if Kaspersky Endpoint Security is installed on the computers and [Device Control is enabled](#). It is not possible to add a device to the trusted list unless information about that device is available in Kaspersky Security Center.

You can add a device to the trusted list according to the following data:

- **Devices by ID.** Each device has a unique identifier (Hardware ID, or HWID). You can view the ID in the device properties by using operating system tools. Example device ID: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Adding devices by ID is convenient if you want to add several specific devices.
- **Devices by model.** Each device has a vendor ID (VID) and a product ID (PID). You can view the IDs in the device properties by using operating system tools. Template for entering the VID and PID: `VID_1234&PID_5678`. Adding devices by model is convenient if you use devices of a certain model in your organization. This way, you can add all devices of this model.
- **Devices by ID mask.** If you are using multiple devices with similar IDs, you can add devices to the trusted list by using masks. The `*` character replaces any set of characters. Kaspersky Endpoint Security does not support the `?` character when entering a mask. For example, `WDC_C*`.
- **Devices by model mask.** If you are using multiple devices with similar VIDs or PIDs (for example, devices from the same manufacturer), you can add devices to the trusted list by using masks. The `*` character replaces any set of characters. Kaspersky Endpoint Security does not support the `?` character when entering a mask. For example, `VID_05AC & PID_*`.

To add devices to the list of trusted devices:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Security Controls** → **Device Control**.
6. In the right part of the window, select the **Trusted devices** tab.
7. Select the **Merge values when inheriting** check box if you want to create a consolidated list of trusted devices for all computers in the company.
The lists of trusted devices in the parent and child policies will be merged. The lists will be merged provided that merging values when inheriting is enabled. Trusted devices from the parent policy are displayed in child policies in a read-only view. Changing or deleting trusted devices of the parent policy is not possible.
8. Click the **Add** button and select a method for adding a device to the trusted list.
9. To filter devices, select a device type from the **Device type** drop-down list (for example, **Removable Drives**).

10. In the **Name / Model** field, enter the device ID, model (VID and PID) or mask, depending on the selected addition method.

Adding devices by model mask (VID and PID) works as follows: if you enter a model mask that does not match any model, Kaspersky Endpoint Security checks if the device ID (HWID) matches the mask. Kaspersky Endpoint Security checks only the part of the device ID that determines the manufacturer and the type of the device (SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000). If the model mask matches this part of the device ID, the devices that match the mask will be added to the list of trusted devices on the computer. At the same time, the list of devices in Kaspersky Security Center remains empty when you click the **Refresh** button. To display the list of devices correctly, you can add devices by device ID mask.

11. To filter devices, in the **Computer** field, enter the computer name or a mask for the name of the computer to which the device is connected.

The ***** character replaces any set of characters. The **?** character replaces any single character.

12. Click the **Refresh** button.

The table displays a list of devices that satisfy the defined filtering criteria.

13. Select the check boxes next to the names of devices that you want to add to the trusted list.

14. In the **Comment** field, enter a description of the reason for adding devices to the trusted list.

15. Click the **Select** button to the right of the **Allow to users and / or groups of users** field.

16. Select a user or a group in Active Directory and confirm your selection.

By default, access to trusted devices is allowed for the Everyone group.

17. Save your changes.

When a device is connected, Kaspersky Endpoint Security checks the list of trusted devices for an authorized user. If the device is trusted, Kaspersky Endpoint Security allows access to the device with all permissions, even if access to the device type or connection bus is denied. If the device is untrusted and access is denied, you can [request access to the locked device](#).

Exporting and importing the list of trusted devices

To distribute the list of trusted devices to all computers in your organization, you can use the export/import procedure.

For example, if you need to distribute a list of trusted removable drives, you need to do the following:

1. Sequentially connect removable drives to your computer.
2. In the Kaspersky Endpoint Security settings, [add the removable drives to the trusted list](#). If required, configure user access permissions. For example, allow only administrators to access removable drives.
3. Export the list of trusted devices in the Kaspersky Endpoint Security settings (see the instructions below).
4. Distribute the trusted device list file to other computers in your organization. For example, place the file in a shared folder.

5. Import the list of trusted devices in the Kaspersky Endpoint Security settings on other computers in the organization (see the instructions below).

To import or export the list of trusted devices:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Device Control**.
3. In the right part of the window, select the **Trusted devices** tab.
4. To export the list of trusted devices:
 - a. Click the **Export** button.
 - b. In the window that opens, specify the name of the XML file to which you want to export the list of trusted devices, and select the folder in which you want to save this file.

Kaspersky Endpoint Security exports the entire list of trusted devices to the XML file.
5. To import the list of trusted devices:
 - a. Click the **Import** button.
 - b. In the window that opens, select the XML file from which you want to import the list of trusted devices.

If the computer already has a list of trusted devices, Kaspersky Endpoint Security will prompt you to delete the existing list or add new entries to it from the XML file.
6. Save your changes.

When a device is connected, Kaspersky Endpoint Security checks the list of trusted devices for an authorized user. If the device is trusted, Kaspersky Endpoint Security allows access to the device with all permissions, even if access to the device type or connection bus is denied.

Obtaining access to a blocked device

When configuring Device Control, you can accidentally block access to a device that is necessary for work.

If Kaspersky Security Center is not deployed in your organization, you can provide access to a device in the settings of Kaspersky Endpoint Security. For example, you can [add the device to the trusted list](#) or temporarily [disable Device Control](#).

If Kaspersky Security Center is deployed in your organization and a policy has been applied to computers, you can provide access to a device in the Administration Console.

Online mode for granting access

You can grant access to a blocked device in online mode only if Kaspersky Security Center is deployed in the organization and a policy has been applied to the computer. The computer must have the capability to establish a connection with the Administration Server.

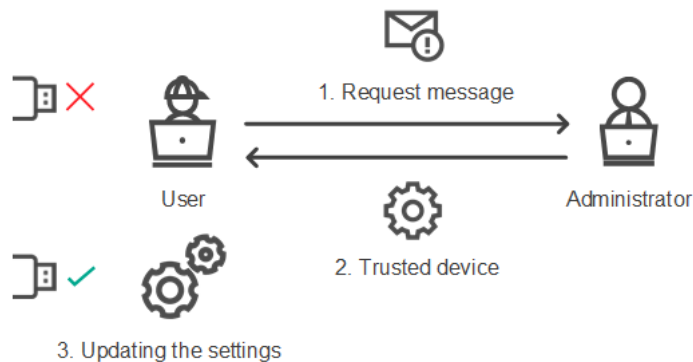
Granting access in online mode consists of the following steps:

1. The user sends the administrator a message containing an access request.

2. The administrator adds the device to the trusted list.

You can add a trusted device in a policy for the administration group or in the local application settings for an individual computer.

3. The administrator updates the settings of Kaspersky Endpoint Security on the user's computer.



Schematic for granting access to a device in online mode

Offline mode for granting access

You can grant access to a blocked device in offline mode only if Kaspersky Security Center is deployed in the organization and a policy has been applied to the computer. In the policy settings, in the **Device Control** section, the **Allow requests for temporary access** check box must be selected.

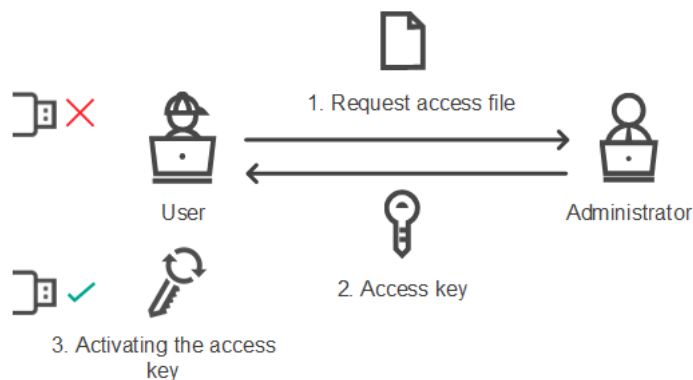
If you need to grant temporary access to a blocked device but you cannot [add the device to the trusted list](#), you can grant access to the device in offline mode. This way, you can grant access to a blocked device even if the computer does not have network access or if the computer is outside of the corporate network.

Granting access in offline mode consists of the following steps:

1. The user creates a request access file and sends it to the administrator.

2. The administrator creates an access key from the request access file and sends it to the user.

3. The user activates the access key.



Schematic for granting access to a device in offline mode

Online mode for granting access

You can grant access to a blocked device in online mode only if Kaspersky Security Center is deployed in the organization and a policy has been applied to the computer. The computer must have the capability to establish a connection with the Administration Server.

A user requests access to a blocked device as follows:

1. Connect the device to the computer.

Kaspersky Endpoint Security will show a notification stating that access to the device is blocked (see the figure below).

2. Click the **Request access** link.

The **Administrator's message** window opens. This message contains information about the blocked device.

3. Click the **Send** button.

The administrator will receive a message containing a request to provide access, for example, by email. For more details about processing the requests of users, please refer to [Kaspersky Security Center Help](#). After [adding the device to the trusted list](#) and updating Kaspersky Endpoint Security settings on the computer, the user will receive access to the device.



Device Control notification

Offline mode for granting access

You can grant access to a blocked device in offline mode only if Kaspersky Security Center is deployed in the organization and a policy has been applied to the computer. In the policy settings, in the **Device Control** section, the **Allow requests for temporary access** check box must be selected.

A user requests access to a blocked device as follows:

1. Connect the device to the computer.

Kaspersky Endpoint Security will show a notification stating that access to the device is blocked.

2. Click the **Request temporary access** link.

The **Request access to device** window opens with a list of connected devices.

3. In the list of connected devices, select the device to which you want to gain access.
4. Click the **Generate request access file** button.
5. In the **Access duration** field, specify the period of time for which you want to have access to the device.
6. Save the file to computer memory.

As a result, a request access file with the *.akey extension will be downloaded to computer memory. Use any available method to send the device request access file to the corporate LAN administrator.

The administrator creates an access key for a blocked device as follows:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder of the Administration Console tree, open the folder with the name of the administration group to which the relevant client computer belongs.
3. In the workspace, select the **Devices** tab.
4. In the list of client computers, select the computer whose user needs to be granted temporary access to a locked device.
5. In the context menu of the computer, select **Grant access in offline mode**.
6. In the opened window, select the **Device Control** tab.
7. Click the **Browse** button and download the request access file received from the user.
You will see information about the blocked device to which the user has requested access.
8. If necessary, change the value of the **Access duration** setting.
By default, the **Access duration** setting takes the value that was indicated by the user when creating the access request file.
9. Specify the value of the **Activate by** setting.
This setting defines the time period during which the user can activate access to the blocked device by using the provided access key.
10. Save the access key file to computer memory.

As a result, the blocked device access key will be downloaded to computer memory. An access key file has the *.acode extension. Use any available method to send the blocked device access key to the user.

The user activates the access key as follows:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Device Control**.
3. In the right part of the window, click the **Request access** button.
4. In the **Request access to device** window, click the **Activate access key** button.

5. In the opened window, select the file with the device access key received from the corporate LAN administrator. Click the **Open** button.

This opens a window containing information about access provision.

6. Click **OK**.

As a result, the user receives access to the device for the time period set by the administrator. The user receives the full set of rights for accessing the device (read and write). When the key expires, access to the device will be blocked. If the user requires permanent access to the device, [add the device to the trusted list](#).

Editing templates of Device Control messages

When the user attempts to access a blocked device, Kaspersky Endpoint Security displays a message stating that access to the device is blocked or that an operation with the device contents is forbidden. If the user believes that access to the device was mistakenly blocked or that an operation with device contents was forbidden by mistake, the user can send a message to the local corporate network administrator by clicking the link in the displayed message about the blocked action.

Templates are available for messages about blocked access to devices or forbidden operations with device contents, and for the message sent to the administrator. You can modify the message templates.

To edit the templates for Device Control messages:

1. In the main application window, click the **Settings** button.

2. In the application settings window, select **Security Controls** → **Device Control**.

3. In the right part of the window, click the **Templates** button.

The **Message templates** window opens.

4. Do one of the following:

- To modify the template of the message about blocked access to a device or a forbidden operation with device contents, select the **Blockage** tab.
- To modify the template of the message that is sent to the LAN administrator, select the **Message to administrator** tab.

5. Edit the message template. You can also use the following buttons: **Variable**, **By default**, and **Link** (this button is available only on the **Blockage** tab).

6. Save your changes.

Best practices for implementing white list mode

When planning implementation of white list mode, it is recommended to perform the following actions:

1. Form the following types of groups:

- User groups. Groups of users for whom you need to allow use of various sets of applications.

- Administration groups. One or several groups of computers to which Kaspersky Security Center will apply white list mode. Creating several groups of computers is necessary if different white list mode settings are used for those groups.
2. Create a list of applications that must be allowed to start.
- Prior to creating a list, you are advised to do the following:
- a. Run the inventory task.
Information about the creation, reconfiguration, and startup of an inventory task is available in the Task management section.
 - b. View the [list of executable files](#).

Configuring white list mode

When configuring white list mode, it is recommended to perform the following actions:

1. Create [application categories](#) containing the applications that must be allowed to start.

You can select one of the following methods for creating application categories:

- **Category with content added manually.** You can manually add to this category by using the following conditions:
 - File metadata. Kaspersky Security Center adds all executable files accompanied by the specified metadata to the application category.
 - File hash code. Kaspersky Security Center adds all executable files with the specified hash to the application category.

Use of this condition excludes the capability to automatically install updates because different versions of files will have a different hash.

- File certificate. Kaspersky Security Center adds all executable files signed with the specified certificate to the application category.
- KL category. Kaspersky Security Center adds all applications that are in the specified KL category to the application category.
- Path to application. Kaspersky Security Center adds all executable files from this folder to the application category.

Use of the Application folder condition may be unsafe because any application from the specified folder will be allowed to start. It is recommended to apply rules that use the application categories with the Application folder condition only to those users for whom the automatic installation of updates must be allowed.

- **Category that includes executable files from a specific folder.** You can specify a folder from which executable files will be automatically assigned to the created application category.

- **Category which includes executable files from selected devices.** You can specify a computer for which all executable files will be automatically assigned to the created application category.

When using this method of creating application categories, Kaspersky Security Center receives information about applications on the computer from the [Executable files folder](#).

2. [Select white list mode](#) for the Application Control component.
3. [Create Application Control rules](#) using the created application categories.

The initially defined rules for white list mode are the **Golden Image** rule, which allows the startup of applications that are included in the "Golden Image" category, and the **Trusted Updaters** rule, which allows the startup of applications that are included in the "Trusted Updaters" KL category. The "Golden Image" KL category includes programs that ensure normal operation of the operating system. The "Trusted Updaters" KL category includes updaters for the most reputable software vendors. You cannot delete these rules. The settings of these rules cannot be edited. By default, the **Golden Image** rule is enabled, and the **Trusted Updaters** rule is disabled. All users are allowed to start applications that match the trigger conditions of these rules.

4. Determine the applications for which automatic installation of updates must be allowed.

You can allow automatic installation of updates in one of the following ways:

- Specify an extended list of allowed applications by allowing the startup of all applications that belong to any KL category.
- Specify an extended list of allowed applications by allowing the startup of all applications that are signed with certificates.
To allow the startup of all applications signed with certificates, you can create a category with a certificate-based condition that uses only the **Subject** parameter with the value *.
- For the Application control rule, select the **Trusted Updaters** parameter. If this check box is selected, Kaspersky Endpoint Security considers the applications included in the rule as Trusted Updaters. Kaspersky Endpoint Security allows the startup of applications that have been installed or updated by applications included in the rule, provided that no blocking rules are applied to those applications.

When Kaspersky Endpoint Security settings are migrated, the list of executable files created by trusted updaters is migrated as well.

- Create a folder and place within it the executable files of applications for which you want to allow automatic installation of updates. Then create an application category with the "Application folder" condition and specify the path to that folder. Then create an allow rule and select this category.

Use of the Application folder condition may be unsafe because any application from the specified folder will be allowed to start. It is recommended to apply rules that use the application categories with the Application folder condition only to those users for whom the automatic installation of updates must be allowed.

Testing white list mode

To ensure that Application Control rules do not block applications required for work, it is recommended to enable testing of Application Control rules and analyze their operation after creating new rules. When testing is enabled, Kaspersky Endpoint Security will not block applications whose startup is forbidden by Application Control rules, but will instead send notifications about their startup to the Administration Server.

When testing white list mode, it is recommended to perform the following actions:

1. Determine the testing period (ranging from several days to two months).
2. Enable [testing of Application Control rules](#).
3. Examine the [events resulting from testing the operation of Application Control](#) and [reports on blocked applications in test mode](#) to analyze the testing results.
4. Based on the analysis results, make changes to the white list mode settings.
In particular, based on the test results, you can add [executable files related to events to an application category](#).

Supporting white list mode

After [selecting a blocking action for Application Control](#), it is recommended to continue supporting white list mode by performing the following actions:

- [Examine the events resulting from the operation of Application Control](#) and [reports on blocked runs](#) to analyze the effectiveness of Application Control.
- Analyze users' requests to access applications.
- Analyze unfamiliar executable files by checking their reputation [in Kaspersky Security Network](#) or on the [Kaspersky Whitelist](#) ^{external link} portal.
- Prior to installing updates for the operating system or for software, install those updates on a test group of computers to check how they will be processed by Application Control rules.
- Add the necessary applications to categories used in Application Control rules.

Anti-Bridging

Anti-Bridging inhibits the creation of network bridges by preventing the simultaneous establishment of multiple network connections for a computer. This lets you protect a corporate network from attacks over unprotected, unauthorized networks.

Anti-Bridging regulates the establishment of network connections by using *connection rules*.

Connection rules are created for the following predefined types of devices:

- Network adapters
- Wi-Fi adapters
- Modems

If a connection rule is enabled, Kaspersky Endpoint Security:

- Blocks the active connection when establishing a new connection, if the device type specified in the rule is used for both connections.
- Blocks connections that are established using the types of devices for which lower-priority rules are used.

Enabling and disabling Anti-Bridging

Anti-Bridging is disabled by default.

To enable or disable Anti-Bridging:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Device Control**.
3. Click the **Anti-Bridging** button.
The **Anti-Bridging** window opens.
4. Do one of the following:
 - Select the **Enable Anti-Bridging** check box to enable protection against network bridges.
After Anti-Bridging is enabled, Kaspersky Endpoint Security blocks already established connections according to the connection rules.
 - Clear the **Enable Anti-Bridging** check box to disable protection against network bridges.
5. Save your changes.

Changing the status of a connection rule

To change the status of a connection rule:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Device Control**.
3. Click the **Anti-Bridging** button.
The **Anti-Bridging** window opens.
4. Select the rule whose status you want to edit.
5. In the **Control** column, left-click to open the context menu and do one of the following:
 - If you want to enable use of the rule, select **On**.
 - If you want to disable use of the rule, select **Off**.
6. Save your changes.

Change the priority of a connection rule

To change the priority of a connection rule:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Device Control**.
3. Click the **Anti-Bridging** button.
The **Anti-Bridging** window opens.
4. Select the rule whose priority you want to change.
5. Do one of the following:
 - Click the **Move up** button to move the rule up a level in the table of rules.
 - Click the **Move down** button to move the rule down a level in the table of rules.

The higher a rule is positioned in the table of rules, the higher its priority. Anti-Bridging blocks all connections except one connection established using the type of device for which the highest-priority rule is used.

6. Save your changes.

Web Control

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Windows for workstations. This component is unavailable if Kaspersky Endpoint Security is installed on a computer that runs on Windows for servers.

Web Control manages users' access to web resources. This helps reduce traffic and inappropriate use of work time. When a user tries to open a website that is restricted by Web Control, Kaspersky Endpoint Security will block access or show a warning (see the figure below).

Kaspersky Endpoint Security monitors only HTTP- and HTTPS traffic.

For HTTPS traffic monitoring, you need to [enable encrypted connections scan](#).

Methods for managing access to websites

Web Control lets you configure access to websites by using the following methods:

- **Website category**. Websites are categorized according to the Kaspersky Security Network cloud service, heuristic analysis, and the database of known websites (included in application databases). You can restrict users' access, for example, to the "Social networks" category or to [other categories](#).

- **Data type.** You can restrict users' access to data on a website, and hide graphic images, for example. Kaspersky Endpoint Security determines the data type based on the file format and not based on its extension.

Kaspersky Endpoint Security does not scan files within archives. For example, if image files were placed in an archive, Kaspersky Endpoint Security identifies the "Archives" data type and not "Graphic files".

- **Individual address.** You can enter a web address or [use masks](#).

You can simultaneously use multiple methods for regulating access to websites. For example, you can restrict access to the "Office files" data type just for the "Web-based email" website category.

Website access rules

Web Control manages users' access to websites by using *access rules*. You can configure the following advanced settings for a website access rule:

- Users to which the rule applies.

For example, you can restrict Internet access through a browser for all users of the company except the IT department.

- Rule schedule.

For example, you can restrict Internet access through a browser during working hours only.

Access rule priorities

Each rule has a priority. The higher a rule is on the list, the higher its priority. If a website has been added to multiple rules, Web Control regulates access to the website based on the rule with the highest priority. For example, Kaspersky Endpoint Security may identify a corporate portal as a social network. To restrict access to social networks and provide access to the corporate web portal, create two rules: one block rule for the "Social networks" website category and one allow rule for the corporate web portal. The access rule for the corporate web portal must have a higher priority than the access rule for social networks.

The image shows two screenshots of Kaspersky Endpoint Security for Windows messages. The left screenshot is titled "ACCESS DENIED" and the right one is titled "WARNING". Both messages provide details about a blocked web page and offer instructions on how to access it.

ACCESS DENIED Message:

The requested web page cannot be provided.
 Address: <http://kaspersky.ru/>.
 The web page has been blocked by the TestRule f1afc1b0-685f-4693-9e3e-1fd03ac14702 rule.
 Reason: the web resource belongs to the Undetermined content category(-ies) and the Undetermined data type category(-ies).
 This web resource is prohibited at the company. If you consider the blocking to be mistaken or if you need to access this web resource, contact the administrator of the local corporate network ([Request access](#)).

Message generated on: 10.06.2020 14:24:50

WARNING Message:

The requested web page may be insecure or prohibited by the company policy.
 Address: <http://kaspersky.ru/>.
 The web page has been blocked by the TestRule d4f38cdf-3ff9-47a0-a22e-b87ae4da2b02 rule.
 Reason: the web resource belongs to the Undetermined content category(-ies) and the Undetermined data type category(-ies).
 Click the link <http://kaspersky.ru/> to open the requested web page.
 Click the link http://kaspersky.ru/* to obtain access to the entire content of the website on which the requested web page is located.
 Click the link http://*.kaspersky.ru/* to obtain access to all existing domains of lower or equal level with the one that is marked with \[*\].
 Access to above-listed web resources will be granted during the current session of Kaspersky Endpoint Security. In case of a mistaken warning, contact the administrator of the local corporate network ([Request access](#)).

Message generated on: 10.06.2020 14:22:56

Enabling and disabling Web Control

By default, Web Control is enabled.

To enable or disable Web Control:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Web Control**.
3. Do one of the following:
 - If you want to enable Web Control, select the **Web Control** check box.
 - If you want to disable Web Control, clear the **Web Control** check box.

If Web Control is disabled, Kaspersky Endpoint Security does not control access to web resources.

4. Save your changes.

Actions with web resource access rules

It is not recommended to create more than 1000 rules of access to web resources, as this can cause the system to become unstable.

A web resource access rule is a set of filters and actions that Kaspersky Endpoint Security performs when the user visits web resources that are described in the rule during the time span that is indicated in the rule schedule. Filters allow you to precisely specify a pool of web resources to which access is controlled by the Web Control component.

The following filters are available:

- **Filter by content.** Web Control categorizes [web resources by content](#) and data type. You can control user access to web resources with content and data falling into the types defined by these categories. When the users visit web resources that belong to the selected content category and / or data type category, Kaspersky Endpoint Security performs the action that is specified in the rule.
- **Filter by web resource addresses.** You can control user access to all web resource addresses or to individual web resource addresses and / or groups of web resource addresses.

If filtering by content and filtering by web resource addresses are specified, and the specified web resource addresses and / or groups of web resource addresses belong to the selected content categories or data type categories, Kaspersky Endpoint Security does not control access to all web resources in the selected content categories and / or data type categories. Instead, the application controls access only to the specified web resource addresses and / or groups of web resource addresses.

- **Filter by names of users and user groups.** You can specify the names of users and / or groups of users for which access to web resources is controlled according to the rule.
- **Rule schedule.** You can specify the rule schedule. The rule schedule determines the time span during which Kaspersky Endpoint Security monitors access to web resources covered by the rule.

After Kaspersky Endpoint Security is installed, the list of rules of the Web Control component is not blank. Two rules are preset:

- The Scripts and Stylesheets rule, which grants all users access at all times to web resources whose addresses contain the names of files with the css, js, or vbs extensions. For example: <http://www.example.com/style.css>, <http://www.example.com/style.css?mode=normal>.
- "Default rule". This rule is applied to any web resources that are not covered by other rules, and allows or blocks access to these web resources for all users.

Adding and editing a web resource access rule

To add or edit a web resource access rule:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Web Control**.
3. Do one of the following:
 - To add a rule, click the **Add** button.
 - If you want to edit a rule, select the rule in the table and click the **Edit** button.

The **Rule of access to web resources** window opens.

4. Specify or edit the settings of the rule. To do so:
 - a. In the **Name** field, enter or edit the name of the rule.
 - b. From the **Filter content** drop-down list, select the required option:
 - **Any content.**
 - **By content categories.**
 - **By types of data.**
 - **By content categories and types of data.**
 - c. If an option other than **Any content** is selected, sections open for selecting categories of content and/or data types. Select the check boxes next to the names of the required categories of content and/or data types.

Selecting the check box next to the name of a content category and/or data type means that Kaspersky Endpoint Security applies the rule to control access to web resources that belong to the selected categories of content and/or data types.
 - d. From the **Apply to addresses** drop-down list, select the required option:
 - **To all addresses.**
 - **To individual addresses.**

- e. If the **To individual addresses** option is selected, a section opens where you create a list of web resources. You can add or edit the addresses and / or groups of addresses of web resources by using the **Add**, **Edit**, and **Delete** buttons.

If Encrypted Connections Scan is disabled, for the HTTPS protocol you can only filter by the server name.

- f. From the **Apply to addresses** drop-down list, select the required option:

- **To all users.**
- **To individual users or groups.**

- g. If you selected the **To individual users or groups** item, the section is displayed, where you can create the list of users or user groups, whose access to the web resources described by the rule, is controlled by this rule. You can add or delete users and user groups by using the **Add** and **Delete** buttons.

By clicking the **Add** button the **Select Users or Groups** dialog opens, standard for Microsoft Windows.

- h. From the **Action** drop-down list, select the required option:

- **Allow.** If this value is selected, Kaspersky Endpoint Security allows access to web resources that match the parameters of the rule.
- **Block.** If this value is selected, Kaspersky Endpoint Security blocks access to web resources that match the parameters of the rule.
- **Warn.** If this value is selected, Kaspersky Endpoint Security displays a warning that a web resource is unwanted when the user attempts to access web resources that match the rule. By using links from the warning message, the user can obtain access to the requested web resource.

- i. In the **Rule schedule** drop-down list, select the name of the necessary schedule or generate a new schedule based on the selected rule schedule. To do so:

1. Opposite the **Rule schedule** drop-down list, click the **Settings** button.

The **Rule schedule** window opens.

2. To add to the rule schedule a time interval during which the rule does not apply, in the table that shows the rule schedule, click the table cells that correspond to the time and day of the week that you want to select.

The color of the cells turns gray.

3. To substitute a time interval during which the rule applies with a time interval during which the rule does not apply, click the gray cells in the table that correspond to the time and day of the week that you want to select.

The color of the cells turns green.

4. Click the **Save as** button.

The **Rule schedule name** window opens.

5. Type a rule schedule name or leave the default name that is suggested.

6. Click **OK**.

5. Save your changes.

Assigning priorities to web resource access rules

You can assign priorities to each rule from the list of rules, by arranging the rules in a certain order.

To assign a priority to a web resource access rule:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Web Control**.
3. In the right part of the window, select the rule for which you want to change the priority.
4. Use the **Move up** and **Move down** buttons to move the rule to the required rank in the list of rules.
5. Repeat steps 3-4 for the rules whose priority you want to change.
6. Save your changes.

Testing web resource access rules

To check the consistency of Web Control rules, you can test them. For this purpose, the Web Control component includes a Rules Diagnostics function.

To test the web resource access rules:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Web Control**.
3. In the right part of the window, click the **Diagnostics** button.
The **Rules diagnostics** window opens.
4. Fill in the fields in the **Conditions** section:
 - a. If you want to test the rules that Kaspersky Endpoint Security uses to control access to a specific web resource, select the **Specify address** check box. Enter the address of the web resource in the field below.
 - b. If you want to test the rules that Kaspersky Endpoint Security uses to control access to web resources for specified users and / or groups of users, specify a list of users and / or groups of users.
 - c. If you want to test the rules that Kaspersky Endpoint Security uses to control access to web resources of specified content categories and / or data type categories, from the **Filter content** drop-down list, select the required option (**By content categories**, **By types of data**, or **By content categories and types of data**).
 - d. If you want to test the rules with account of the time and day of the week when an attempt is made to access the web resources that are specified in the rule diagnostics conditions, select the **Include time of access attempt** check box. Then specify the day of the week and the time.
5. Click the **Test** button.

Test completion is followed by a message with information about the action that is taken by Kaspersky Endpoint Security, according to the first rule that is triggered on the attempt to access the specified web resource (allow, block, or warn). The first rule to be triggered is the one with a rank on the list of Web Control rules which is higher than that of other rules meeting the diagnostics conditions. The message is displayed on the right of the **Test** button. The following table lists the remaining triggered rules, specifying the action taken by Kaspersky Endpoint Security. The rules are listed in the order of declining priority.

Enabling and disabling a web resource access rule

To enable or disable a web resource access rule:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Web Control**.
3. In the right part of the window, select the rule that you want to enable or disable.
4. In the **Status** column, do the following:
 - If you want to enable the use of the rule, select the *On* value.
 - If you want to disable the use of the rule, select the *Off* value.
5. Save your changes.

Migrating web resource access rules from previous versions of the application

When Kaspersky Endpoint Security 10 Service Pack 2 for Windows or an earlier version of the application is upgraded to Kaspersky Endpoint Security 11.4.0 for Windows, the web resource access rules based on web resource content categories are migrated as follows:

- Web resource access rules that are based on one or several web resource content categories from the "Chats and forums", "Web-based email", and "Social networks" lists migrate to the "Internet communication" web resource content category.
- Web resource access rules based on one or several web resource content categories from the "E-stores" and "Payment systems" lists migrate to the "Online stores, banks, payment systems" web resource content category.
- Web resource access rules based on the "Gambling" web resource content category migrate to the "Gambling, lotteries, sweepstakes" content category.
- Web resource access rules based on the "Browser games" web resource content category migrate to the "Computer games" content category.
- Web resource access rules based on web resource content categories that are not enumerated in the list above are migrated without changes.

Exporting and importing the list of web resource addresses

If you have created a list of web resource addresses in a web resource access rule, you can export it to a .txt file. You can subsequently import the list from this file to avoid creating a new list of web resource addresses manually when configuring an access rule. The option of exporting and importing the list of web resource addresses may be useful if, for example, you create access rules with similar parameters.

To export a list of web resource addresses to a file:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Web Control**.
3. Select the rule whose list of web resource addresses you want to export to a file.
4. Click the **Edit** button.

The **Rule of access to web resources** window opens.

5. If you do not want to export the entire list of web resource addresses, but rather just a part of it, select the required web resource addresses.

6. To the right of the field with the list of web resource addresses, click the  button.

The action confirmation window opens.

7. Do one of the following:

- If you want to export only the selected items of the web resource address list, in the action confirmation window, click the **Yes** button.
- If you want to export all items of the list of web resource addresses, in the action confirmation window, click the **No** button.

The standard **Save as** window of Microsoft Office opens.

8. In the **Save as** Microsoft Windows window, select the file to which you want to export the list of web resource addresses. Click the **Save** button.

To import the list of web resource addresses from a file into a rule:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Web Control**.
3. Do one of the following:

- If you want to create a new web resource access rule, click the **Add** button.
- Select the web resource access rule that you want to edit. Then click the **Edit** button.

The **Rule of access to web resources** window opens.

4. Do one of the following:

- If you are creating a new web resource access rule, select **To individual addresses** from the **Apply to addresses** drop-down list.
- If you are editing a web resource access rule, go to step 5 of these instructions.

5. To the right of the field with the list of web resource addresses, click the  button.

If you are creating a new rule, the standard Microsoft Windows **Open file** window opens.

If you are editing a rule, a window requesting your confirmation opens.

6. Do one of the following:

- If you are editing a new web resource access rule, go to step 7 of these instructions.
- If you are editing a web resource access rule, do one of the following actions in the action confirmation window:
 - If you want to add imported items of the list of web resource addresses to the existing ones, click the **Yes** button.
 - If you want to delete the existing items of the list of web resource addresses and to add the imported ones, click the **No** button.

The **Open file** window in Microsoft Windows opens.

7. In the **Open file** window in Microsoft Windows, select a file with a list of web resource addresses to import.

8. Click the **Open** button.




9. In the **Rule of access to web resources** window, click **OK**.

Monitoring user Internet activity

Kaspersky Endpoint Security lets you log data on user visits to all websites, including allowed websites. This enables you to obtain the complete history of browser views. Kaspersky Endpoint Security sends user activity events to Kaspersky Security Center, to [the local log of Kaspersky Endpoint Security](#), and to the Windows Event log. To receive events in Kaspersky Security Center, you need to configure the settings of events in a policy in the Administration Console or Web Console. You can also configure the transmission of Web Control events by email and the display of on-screen notifications on the user's computer.

For HTTPS traffic monitoring, you need to [enable encrypted connections scan](#).

Kaspersky Endpoint Security creates the following user Internet activity events:

- Block the website (*Critical events* status .
- Visit to a non-recommended website (*Warnings* status .
- Visit to an allowed website (*Informational messages* status .

To configure logging of Web Control events on the user's computer:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Interface**.
3. In the **Notifications** section, click the **Settings** button.

4. In the opened window, select the **Web Control** section.

This opens the table of Web Control events and notification methods.

5. Configure the notification method for each event: **Save in local report** or **Save in Windows Event Log**.

To log allowed website visit events, you need to also configure Web Control (see the instructions below).

In the events table, you can also enable an on-screen notification and an email notification. To send notifications by email, you need to configure the SMTP server settings. For more details about sending notifications by email, please refer to [Kaspersky Security Center Help](#).

6. Save your changes.

As a result, Kaspersky Endpoint Security begins logging user Internet activity events.

Web Control sends user activity events to Kaspersky Security Center as follows:

- If you are using Kaspersky Security Center, Web Control sends events for all the objects that make up the web page. For this reason, multiple events may be created when one web page is blocked. For example, when blocking the web page `http://www.example.com`, Kaspersky Endpoint Security may relay events for the following objects: `http://www.example.com`, `http://www.example.com/icon.ico`, `http://www.example.com/file.js`, etc.
- If you are using the Kaspersky Security Center Cloud Console, Web Control groups events and sends only the protocol and domain of the website. For instance, if a user visits non-recommended web pages `http://www.example.com/main`, `http://www.example.com/contact`, and `http://www.example.com/gallery`, Kaspersky Endpoint Security will send only one event with the `http://www.example.com` object.

To enable logging of events for visiting allowed websites:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Web Control**.
3. Click the **Advanced settings** button.
4. In the opened window, select the **Log the opening of allowed pages** check box.
5. Save your changes.

As a result, you will be able to view the full browser history.

Editing masks for web resource addresses

Using a *web resource address mask* (also referred to as "address mask") may be useful if you need to enter numerous similar web resource addresses when creating a web resource access rule. If crafted well, one address mask can replace a large number of web resource addresses.

When creating an address mask, follow these rules:

1. The ***** character replaces any sequence that contains zero or more characters.

For example, if you enter the `*abc*` address mask, the access rule is applied to all web resources that contain the sequence `abc`. Example: `http://www.example.com/page_0-9abcdef.html`.

To include the ***** character in the address mask, enter the ***** character twice.

2. The `www.` character sequence at the start of the address mask is interpreted as a `*` sequence.
Example: the address mask `www.example.com` is interpreted as `*.example.com`.
3. If an address mask does not start with the `*` character, the content of the address mask is equivalent to the same content with the `*` prefix.
4. A sequence of `*` characters at the beginning of an address mask is interpreted as `*` or an empty string.
Example: the address mask `http://www.*.example.com` covers the address `http://www2.example.com`.
5. If an address mask ends with a character other than `/` or `*`, the content of the address mask is equivalent to the same content with the `/*` postfix.
Example: the address mask `http://www.example.com` covers such addresses as `http://www.example.com/abc`, where a, b, and c are any characters.
6. If an address mask ends with the `/` character, the content of the address mask is equivalent to the same content with the `/*` postfix.
7. The character sequence `/*` at the end of an address mask is interpreted as `/*` or an empty string.
8. Web resource addresses are verified against an address mask, taking into account the protocol (http or https):
 - If the address mask contains no network protocol, this address mask covers addresses with any network protocol.
Example: the address mask `example.com` covers the addresses `http://example.com` and `https://example.com`.
 - If the address mask contains a network protocol, this address mask only covers addresses with the same network protocol as that of the address mask.
Example: the address mask `http://*.example.com` covers the address `http://www.example.com` but does not cover `https://www.example.com`.
9. An address mask that is in double quotes is treated without considering any additional replacements, except the `*` character if it has been initially included in the address mask. Rules 5 and 7 do not apply to address masks enclosed in double quotation marks (see examples 14 – 18 in the table below).
10. The user name and password, connection port, and character case are not taken into account during comparison with the address mask of a web resource.

Examples of how to use rules for creating address masks

No.	Address mask	Address of web resource to verify	Is the address covered by the address mask	Comment
1	<code>*.example.com</code>	<code>http://www.123example.com</code>	No	See rule 1.
2	<code>*.example.com</code>	<code>http://www.123.example.com</code>	Yes	See rule 1.
3	<code>*example.com</code>	<code>http://www.123example.com</code>	Yes	See rule 1.
4	<code>*example.com</code>	<code>http://www.123.example.com</code>	Yes	See rule 1.
5	<code>http://www.*.example.com</code>	<code>http://www.123example.com</code>	No	See rule 1.

6	www.example.com	http://www.example.com	Yes	See rules 2, 1.
7	www.example.com	https://www.example.com	Yes	See rules 2, 1.
8	http://www.*.example.com	http://123.example.com	Yes	See rules 2, 4, 1.
9	www.example.com	http://www.example.com/abc	Yes	See rules 2, 5, 1.
10	example.com	http://www.example.com	Yes	See rules 3, 1.
11	http://example.com/	http://example.com/abc	Yes	See rule 6.
12	http://example.com/*	http://example.com	Yes	See rule 7.
13	http://example.com	https://example.com	No	See rule 8.
14	"example.com"	http://www.example.com	No	See rule 9.
15	"http://www.example.com"	http://www.example.com/abc	No	See rule 9.
16	"*.example.com"	http://www.example.com	Yes	See rules 1, 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Yes	See rules 1, 9.
18	"www.example.com"	http://www.example.com; https://www.example.com	Yes	See rules 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	No	An address mask contains more information than the address of a web resource.

Editing templates of Web Control messages

Depending on the type of action that is specified in the properties of Web Control rules, Kaspersky Endpoint Security displays a message of one of the following types when users attempt to access Internet resources (the application substitutes an HTML page with a message for the HTTP server response):

- **Warning message.** This message warns the user that visiting the web resource is not recommended and/or violates the corporate security policy. Kaspersky Endpoint Security displays a warning message if the **Warn** option is selected from the **Action** drop-down list in the settings of the rule that describes this web resource. If the user believes that the warning is mistaken, the user may click the link from the warning to send a pre-generated message to the local corporate network administrator.
- **Message informing of blocking of a web resource.** Kaspersky Endpoint Security displays a message informing that a web resource is blocked if the **Block** option is selected from the **Action** drop-down list in the settings of the rule that describes this web resource. If the user believes that the web resource is blocked by mistake, the user may click the link in the web resource block notification message to send a pre-generated message to the local corporate network administrator.

Special templates are provided for the warning message, the message informing that a web resource is blocked, and the message sent to the LAN administrator. You can modify their content.

To change the template for Web Control messages:

1. In the main application window, click the **Settings** button.

2. In the application settings window, select **Security Controls** → **Web Control**.
3. In the right part of the window, click the **Templates** button.
The **Message templates** window opens.
4. Do one of the following:
 - If you want to edit the template of the message that warns the user against visiting a web resource, select the **Warning** tab.
 - If you want to edit the template of the message that informs the user that access to a web resource is blocked, select the **Blockage** tab.
 - To edit the template of the message sent to the administrator, select the **Message to administrator** tab.
5. Edit the message template. You can also use the **Variable** drop-down list, as well as the **By default** and **Link** (this button is not available on the **Message to administrator** tab) buttons.
6. Save your changes.

Adaptive Anomaly Control

The Adaptive Anomaly Control component is available only for Kaspersky Endpoint Security for Business Advanced and Kaspersky Total Security for Business (learn more about Kaspersky Endpoint Security products for business at the [Kaspersky website](#) ²).

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Windows for workstations. This component is unavailable if Kaspersky Endpoint Security is installed on a computer that runs on Windows for servers.

The Adaptive Anomaly Control component monitors and blocks actions that are not typical of the computers in a company's network. Adaptive Anomaly Control uses a set of rules to track uncharacteristic behavior (for example, the *Start of Microsoft PowerShell from office application* rule). Rules are created by Kaspersky specialists based on typical scenarios of malicious activity. You can configure how Adaptive Anomaly Control handles each rule and, for example, allow the execution of PowerShell scripts that automate certain workflow tasks. Kaspersky Endpoint Security updates the set of rules along with the application databases. Updates to the sets of rules must be [confirmed manually](#).

Adaptive Anomaly Control settings

Configuring Adaptive anomaly control consists of the following steps:

1. Training Adaptive Anomaly Control.

After you enable Adaptive Anomaly Control, its rules work in *training mode*. During the training, Adaptive Anomaly Control monitors rule triggering and sends triggering events to Kaspersky Security Center. Each rule has its own duration of the training mode. The duration of the training mode is set by Kaspersky experts. Normally, the training mode is active for two weeks.

If a rule is not triggered at all during the training, Adaptive Anomaly Control will consider the actions associated with this rule as non-typical. Kaspersky Endpoint Security will block all actions associated with that rule.

If a rule was triggered during training, Kaspersky Endpoint Security logs events in the [rule triggering report](#) and the **Triggering of rules in Smart Training mode** repository.

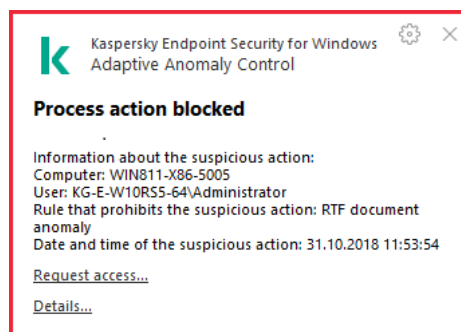
2. Analyzing the rule triggering report.

The administrator analyzes the [rule triggering report](#) or the contents of the **Triggering of rules in Smart Training mode** repository. Then the administrator can select the behavior of Adaptive Anomaly Control when the rule is triggered: either block or allow. The administrator can also continue to monitor how the rule works and extend the duration of the training mode. If the administrator does not take any action, the application will also continue to work in training mode. The training mode term is restarted.

Adaptive Anomaly Control is configured in real time. Adaptive Anomaly Control is configured via the following channels:

- Adaptive Anomaly Control automatically starts to block the actions associated with the rules that were never triggered in training mode.
- Kaspersky Endpoint Security adds new rules or removes obsolete ones.
- The administrator configures the operation of the Adaptive Anomaly Control after reviewing the rule triggering report and the contents of the **Triggering of rules in Smart Training mode** repository. It is recommended to check the rule triggering report and the contents of the **Triggering of rules in Smart Training mode repository**.

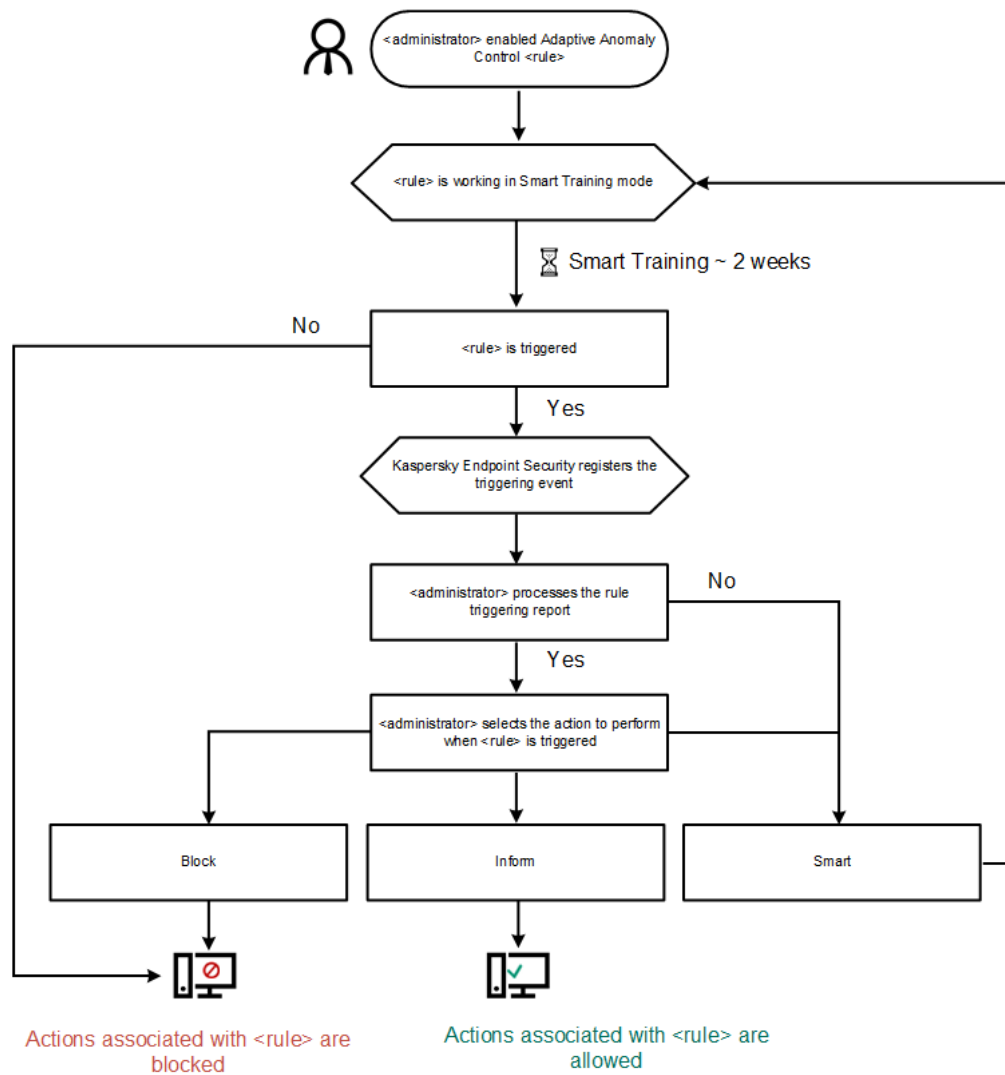
When a malicious application attempts to perform an action, Kaspersky Endpoint Security will block the action and display a notification (see figure below).



Adaptive Anomaly Control notification

Adaptive Anomaly Control operating algorithm

Kaspersky Endpoint Security decides whether to allow or block an action that is associated with a rule based on the following algorithm (see the figure below).



Adaptive Anomaly Control operating algorithm

Enabling and disabling Adaptive Anomaly Control

Adaptive Anomaly Control is enabled by default.

To enable or disable Adaptive Anomaly Control:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Adaptive Anomaly Control**.
3. Do one of the following:
 - Select the **Adaptive Anomaly Control** check box if you want to enable Adaptive Anomaly Control.
 - Clear the **Adaptive Anomaly Control** check box if you want to disable Adaptive Anomaly Control.
4. Save your changes.

Enabling and disabling an Adaptive Anomaly Control rule

To enable or disable an Adaptive Anomaly Control rule:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Adaptive Anomaly Control**.
3. In the table in the right part of the window, select a rule.
4. In the **Status** column, right-click to display the context menu and select one of the following:
 - **On**. This status means that the rule is used when the Adaptive Anomaly Control component is running.
 - **Off**. This status means that the rule is not used when the Adaptive Anomaly Control component is running.
5. Save your changes.

Modifying the action taken when an Adaptive Anomaly Control rule is triggered

To edit the action that is taken when an Adaptive Anomaly Control rule is triggered:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Adaptive Anomaly Control**.
3. In the table in the right part of the window, select a rule.
4. In the **Action** column, right-click to display the context menu and select one of the following:
 - **Smart**. If this option is selected, the Adaptive Anomaly Control rule works in Smart training mode for a period of time defined by Kaspersky experts. In this mode, when an Adaptive Anomaly Control rule is triggered, Kaspersky Endpoint Security allows the activity covered by the rule and logs an entry in the **Triggering of rules in Smart Training mode** storage of the Kaspersky Security Center Administration Server. When the time period set for working in Smart Training mode ends, Kaspersky Endpoint Security blocks the activity covered by an Adaptive Anomaly Control rule and logs an entry containing information about the activity.
 - **Block**. If this action is selected, when an Adaptive Anomaly Control rule is triggered Kaspersky Endpoint Security blocks the activity covered by the rule and logs an entry containing information about the activity.
 - **Inform**. If this action is selected, when an Adaptive Anomaly Control rule is triggered Kaspersky Endpoint Security allows the activity covered by the rule and logs an entry containing information about the activity.
5. Save your changes.

Creating and editing an exclusion for an Adaptive Anomaly Control rule

You cannot create more than 1,000 exclusions for Adaptive Anomaly Control rules. It is not recommended to create more than 200 exclusions. To reduce the number of exclusions used, it is recommended to use masks in the settings of exclusions.

An exclusion for an Adaptive Anomaly Control rule includes a description of the source and target objects. The *source object* is the object performing the actions. The *target object* is the object on which the actions are being performed. For example, you have opened a file named `file.xlsx`. As a result, a library file with the DLL extension is loaded into the computer memory. This library is used by a browser (executable file named `browser.exe`). In this example, `file.xlsx` is the source object, Excel is the source process, `browser.exe` is the target object, and Browser is the target process.

To create or edit an exclusion for an Adaptive Anomaly Control rule:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Adaptive Anomaly Control**.
3. In the table in the right part of the window, select a rule.
4. Click the **Edit** button.

The **Adaptive Anomaly Control rule** window opens.

5. Do one of the following:

- If you want to add an exclusion, click the **Add** button.
- If you want to edit an existing exclusion, select the row in the **Exclusions** table and click the **Edit** button.

The **Exclusion from rule** window opens.

6. In the **Description** field, enter a description of the exclusion.
7. Click the **Browse** button next to the **User** field to specify the users to whom the exclusion is applied.
8. Define the settings of the source object or source process started by the object:

The standard **Select users or groups** window in Microsoft Windows opens.

- **Source process.** Path or mask of the path to the file or folder containing files (for example, `C:\Dir\File.exe` or `Dir*.exe`).
- **Source process hash.** File hash code.
- **Source object.** Path or mask of the path to the file or folder containing files (for example, `C:\Dir\File.exe` or `Dir*.exe`). For example, file path `document.docm`, which uses a script or macro to start the target processes.

You can also specify other objects to exclude, such as a web address, macro, command in the command line, registry path, or others. Specify the object according to the following template: `object://<object>`, where `<object>` refers to the name of the object, for example, `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. You can also use masks, for example, `object://*C:\Windows\temp*`.

- **Source object hash.** File hash code.

The Adaptive Anomaly Control rule is not applied to actions performed by the object, or to processes started by the object.

9. Specify the settings of the target object or target processes started on the object.

- **Target process.** Path or mask of the path to the file or folder containing files (for example, `C:\Dir\File.exe` or `Dir*.exe`).
- **Target process hash.** File hash code.
- **Target object.** The command to start the target process. Specify the command using the following pattern `object://<command>`, for example, `object://cmdline:powershell -Command "$result = 'C:\windows\temp\result_local_users_pwdage txt' "`. You can also use masks, for example, `object://*C:\windows\temp*`.
- **Target object hash.** File hash code.

The Adaptive Anomaly Control rule is not applied to actions taken on the object, or to processes started on the object.

10. Save your changes.

Deleting an Adaptive Anomaly Control rule exclusion

To delete an exclusion for an Adaptive Anomaly Control rule:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Adaptive Anomaly Control**.
3. In the table in the right part of the window, select a rule.
4. Click the **Edit** button.
The **Adaptive Anomaly Control rule** window opens.
5. In the **Exclusions from rule** table, select the relevant row.
6. Click the **Delete** button.
7. Save your changes.

Importing exclusions for Adaptive Anomaly Control rules

To import exclusions for Adaptive Anomaly Control rules:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Adaptive Anomaly Control**.
3. Click the **Import** button.

The **Please select a configuration file** window opens.

4. In the **Please select a configuration file** window, specify the XML file from which you want to import the list of exclusions.
5. Click the **Open** button.
6. Confirm import of exclusions by clicking **Yes**.
7. Save your changes.

Exporting exclusions for Adaptive Anomaly Control rules

To export exclusions for selected rules:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Adaptive Anomaly Control**.
3. In the table in the right part of the window, select one or multiple rules whose exclusions you want to export.
4. Click the **Export** button.
The **Please select a configuration file** window opens.
5. In the **Please select a configuration file** window:
 - a. Specify the name of the XML file to which you want to export the exclusions.
 - b. Select the folder in which you want to save this file.
 - c. Click the **Save** button.
6. In the dialog box that opens, perform one of the following actions:
 - Click **Yes** if you want to export exclusions only for the selected rules.
 - Click **No** if you want to export exclusions for all rules.
7. Save your changes.

Applying updates for Adaptive Anomaly Control rules

New Adaptive Anomaly Control rules may be added to the table of rules and existing Adaptive Anomaly Control rules may be deleted from the table of rules when anti-virus databases are updated. Kaspersky Endpoint Security distinguishes Adaptive Anomaly Control rules that are to be deleted or added to the table, if an update for these rules has not been applied.

Until the update is applied, Kaspersky Endpoint Security displays the Adaptive Anomaly Control rules set to be deleted by the update in the table of rules and assigns the *Disabled* status to them. It is not possible to change the settings of these rules.

To apply updates for Adaptive Anomaly Control rules:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Adaptive Anomaly Control**.
3. Click the **Approve updates** button.
The **Approve updates** button is available if an update for Adaptive Anomaly Control rules is available.
4. Save your changes.

Editing Adaptive Anomaly Control message templates

When a user tries to do an action, blocked by Adaptive Anomaly Control rules, Kaspersky Endpoint Security displays a message that potentially harmful actions are blocked. If the user believes that an action was mistakenly blocked, the user can use the link in the message text to send a message to the local corporate network administrator.

Special templates are available for the message about blocking potentially harmful actions and for the message to be sent to the administrator. You can modify the message templates.

To edit a message template:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **Security Controls** → **Adaptive Anomaly Control**.
3. Select the **Adaptive Anomaly Control** check box to make the component settings available for editing.
4. Click the **Templates** button.
The **Message templates** window opens.
5. Do one of the following:
 - If you want to edit the template of the message that is displayed when a potentially harmful action is blocked, select the **Blockage** tab.
 - If you want to modify the template of the message that is sent to the LAN administrator, select the **Message to administrator** tab.
6. Modify the template of the message that is displayed when an application is blocked from starting or the message sent to the administrator.
7. Save your changes.

Viewing Adaptive Anomaly Control reports

To view Adaptive Anomaly Control reports:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the **Security Controls** section, select the **Adaptive Anomaly Control** subsection.

The settings of the Adaptive Anomaly Control component are displayed in the right part of the window.

6. Do one of the following:
 - If you want to view a report on the settings of Adaptive Anomaly Control rules, click the **Rule status report** button.
 - If you want to view a report on the triggering of Adaptive Anomaly Control rules, click the **Rule triggering report** button.
7. The report generation process starts.

The report is displayed in a new window.

Network ports monitoring

During the operation of Kaspersky Endpoint Security, the [Web Control](#), [Mail Threat Protection](#) and [Web Threat Protection](#) components monitor data streams that are transmitted via specific protocols and that pass through specific open TCP and UDP ports on user computer. For example, the Mail Threat Protection component analyzes information transmitted via SMTP, while the Web Threat Protection component analyzes information transmitted via HTTP and FTP.

Kaspersky Endpoint Security divides TCP and UDP ports of the user's computer into several groups, depending on the likelihood of their being compromised. Some network ports are reserved for vulnerable services. You are advised to monitor these ports more thoroughly because they have a greater likelihood of being targeted by a network attack. If you use non-standard services that rely on non-standard network ports, these network ports may also be targeted by an attacking computer. You can specify a list of network ports and a list of applications that request network access. These ports and applications then receive special attention from the Mail Threat Protection and Web Threat Protection components during network traffic monitoring.

Enabling monitoring of all network ports

To enable monitoring of all network ports:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Network settings**.
3. In the **Monitored ports** section, select the **Monitor all network ports** option.
4. Save your changes.

Enabling port monitoring for applications from the list generated by Kaspersky experts

To create a list of monitored network ports:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Network settings**.
3. In the **Monitored ports** section, select **Monitor selected network ports only**.
4. Click the **Settings** button.
The **Network ports** window opens.
5. Select the **Monitor all ports for the applications from the list recommended by Kaspersky** check box.
If this check box is selected, Kaspersky Endpoint Security monitors all ports for the following applications:
 - Adobe Reader.
 - AIM for Windows.
 - Apple Application Support.
 - Chrome.
 - Digsby.
 - Edge.
 - Firefox.
 - Google Talk.
 - ICQ.
 - Internet Explorer.
 - Java.
 - Mail.ru Agent.
 - Miranda IM.
 - mIRC.

- Opera.
- Pidgin.
- QIP Infium.
- QIP.
- QNext.
- QNextClient.
- Rockmelt.
- Safari.
- Simple Instant Messenger.
- Trillian.
- Windows Live Messenger.
- Windows Messenger.
- X-Chat.
- Yahoo! Messenger.
- Yandex Browser.

Creating a list of monitored network ports

To create a list of monitored network ports:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Network settings**.
3. In the **Monitored ports** section, select **Monitor selected network ports only**.
4. Click the **Settings** button.

The **Network ports** window opens. The **Network ports** window displays a list of network ports that are normally used for transmission of email and network traffic. This list of network ports is included in the Kaspersky Endpoint Security package.

5. In the list of network ports, perform the following:
 - Select the check boxes opposite those network ports that you want to include in the list of monitored network ports.

By default, the check boxes are selected opposite all network ports that are listed in the **Network ports** window.

- Clear the check boxes opposite those network ports that you want to exclude from the list of monitored network ports.

6. If a network port is not shown in the list of network ports, add it by doing the following:

- a. Under the list of network ports, click the **Add** link to open the **Network port** window.
- b. Enter the network port number in the **Port** field.
- c. Enter the name of the network port in the **Description** field.
- d. Click **OK**.

The **Network port** window closes. The newly added network port is shown at the end of the list of network ports.

7. Save your changes.

When the FTP protocol runs in passive mode, the connection can be established via a random network port that is not added to the list of monitored network ports. To protect such connections, select the **Monitor all network ports** check box in the **Monitored ports** section or [configure the monitoring of all ports for applications](#) that establish the FTP connection.

Creating a list of applications for which all network ports are monitored

You can create a list of applications for which Kaspersky Endpoint Security monitors all network ports.

We recommend including applications that receive or transmit data via the FTP protocol in the list of applications for which Kaspersky Endpoint Security monitors all network ports.

To create a list of applications for which all network ports are monitored:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Network settings**.
3. In the **Monitored ports** section, select **Monitor selected network ports only**.
4. Click the **Settings** button.
The **Network ports** window opens.
5. Select the **Monitor all ports for specified applications** check box.
6. In the list of applications under the **Monitor all ports for specified applications** check box, do the following:
 - Select the check boxes next to the names of applications for which you want to monitor all network ports. By default, the check boxes are selected next to all applications that are listed in the **Network ports** window.
 - Clear the check boxes next to the names of applications for which you do not want to monitor all network ports.

7. If an application is not included in the list of applications, add it as follows:

- a. Click the **Add** link under the list of applications and open the context menu.
- b. In the context menu, select the way in which to add the application to the list of applications:
 - To select an application from the list of applications that are installed on the computer, select the **Applications** command. The **Select application** window opens, letting you specify the name of the application.
 - To specify the location of the application's executable file, select the **Browse** command. The standard **Open** window in Microsoft Windows opens, letting you specify the name of the application executable file.

The **Application** window opens after you select the application.

- c. In the **Name** field, enter a name for the selected application.
- d. Click **OK**.

The **Application** window closes. The application that you have added appears at the end of the list of applications.

8. Save your changes.

Wipe Data

Kaspersky Endpoint Security lets you use a task to remotely delete data from users' computers.

Kaspersky Endpoint Security deletes data as follows:

- In silent mode;
- On hard drives and removable drives;
- For all user accounts on the computer.

Kaspersky Endpoint Security performs the *Wipe data* task no matter which licensing type is being used, even after the license has expired.

Data Wipe modes

This task enables you to delete data in the following modes:

- Immediate data deletion.
In this mode, you can, for example, delete outdated data to free up disk space.
- Postponed data deletion.
This mode is intended, for example, to protect data on a laptop in case it is lost or stolen. You can configure automatic data deletion if the laptop goes outside the boundaries of the corporate network and has not been synchronized with Kaspersky Security Center in a long time.

It is not possible to set a schedule for deleting data in task properties. You can only delete data immediately after starting the task manually, or configure delayed data deletion if there is no connection with Kaspersky Security Center.

Limitations

Data Wipe has the following limitations:

- Only a Kaspersky Security Center administrator can manage the *Wipe data* task. You cannot configure or start a task in the local interface of Kaspersky Endpoint Security.
- For the NTFS file system, Kaspersky Endpoint Security deletes only the names of the main data streams. Alternate data stream names cannot be deleted.
- When you delete a symbolic link file, Kaspersky Endpoint Security also deletes the files whose paths are specified in the symbolic link.

Creating a Wipe data task

To delete data on users' computers:

1. In the main window of Web Console, select **Devices** → **Tasks**.

The list of tasks opens.

2. Click the **Add** button.

The Task Wizard starts.

3. Configure the task settings:

a. In the **Application** drop-down list, select **Kaspersky Endpoint Security for Windows (11.4.0)**.

b. In the **Task type** drop-down list, select **Wipe data**.

c. In the **Task name** field, enter a brief description, for example, **Wipe data (Anti-Theft)**.

d. In the **Select devices to which the task will be assigned** section, select the task scope.

4. Select devices according to the selected task scope option. Click the **Next** button.

If new computers are added to an administration group within the task scope, the immediate data deletion task is run on the new computers only if the task is completed within 5 minutes of the addition of the new computers.

5. Finish the wizard by clicking the **Finish** button.

A new task will be displayed in the list of tasks.

6. Click the **Wipe data** task of Kaspersky Endpoint Security.

The task properties window opens.

7. Select the **Application settings** tab.

8. Select the data deletion method:

- **Delete by means of the operating system.** Kaspersky Endpoint Security uses the operating system resources to delete files without sending them to the recycle bin.
- **Delete completely, no recovery possible.** Kaspersky Endpoint Security overwrites files with random data. It is practically impossible to restore data after it is deleted.

9. If you want to postpone data deletion, select the **Automatically delete data if there is no connection to Kaspersky Security Center for more than N days** check box. Define the number of days.

The postponed data deletion task will be performed each time that a connection with Kaspersky Security Center is absent for the defined period of time.

When configuring postponed data deletion, bear in mind that employees may turn off their computer before going on vacation. In this case, the absent connection term may be exceeded and data will be deleted. Also consider the work schedule of offline users. For more details about working with offline computers and out-of-office users, refer to [Kaspersky Security Center Help](#).

If the check box is cleared, the task will be performed immediately after synchronization with Kaspersky Security Center.

10. Create a list of objects to delete:

- **Folders.** Kaspersky Endpoint Security deletes all files in the folder, and its subfolders. Kaspersky Endpoint Security does not support masks and environment variables for entering a folder path.
- **Files by extension.** Kaspersky Endpoint Security searches for files with the specified extensions on all computer drives, including removable drives. Use the ";" or "," characters to specify multiple extensions.
- **Predefined folders.** Kaspersky Endpoint Security will delete files from the following areas:
 - **Documents.** Files in the standard *Documents* folder of the operating system, and its subfolders.
 - **Cookies.** Files in which the browser saves data from the websites visited by the user (such as user authorization data).
 - **Desktop.** Files in the standard *Desktop* folder of the operating system, and its subfolders.
 - **Temporary Internet Explorer files.** Temporary files related to the operation of Internet Explorer, such as copies of web pages, images, and media files.
 - **Temporary files.** Temporary files related to the operation of applications installed on the computer. For example, Microsoft Office applications create temporary files containing backup copies of documents.
 - **Outlook files.** Files related to the operation of the Outlook mail client: data files (PST), offline data files (OST), offline address book files (OAB), and personal address book files (PAB).
 - **User profile.** Set of files and folders that store operating system settings for the local user account.

You can create a list of objects to delete on each tab. Kaspersky Endpoint Security will create a consolidated list and delete files from this list when a task is complete.

You cannot delete files that are required for operation of Kaspersky Endpoint Security.

11. Click the **Save** button.
12. Select the check box next to the task.
13. Click the **Run** button.

As a result, data on users' computers will be deleted according to the selected mode: immediate or when a connection is absent. If Kaspersky Endpoint Security cannot delete a file, such as when a user is currently using a file, the application does not attempt to delete it again. To complete data deletion, run the task again.

Password protection

Multiple users with different levels of computer literacy can share a computer. If users have unrestricted access to Kaspersky Endpoint Security and its settings, the overall level of computer protection may be reduced. Password protection lets you restrict users' access to Kaspersky Endpoint Security according to the permissions granted to them (for example, permission to exit the application).

If the user that started the Windows session (*session user*) has the permission to perform the action, Kaspersky Endpoint Security does not request the user name and password or a temporary password. The user receives access to Kaspersky Endpoint Security in accordance with the granted permissions.

If a session user does not have the permission to perform an action, the user can obtain access to the application in the following ways:

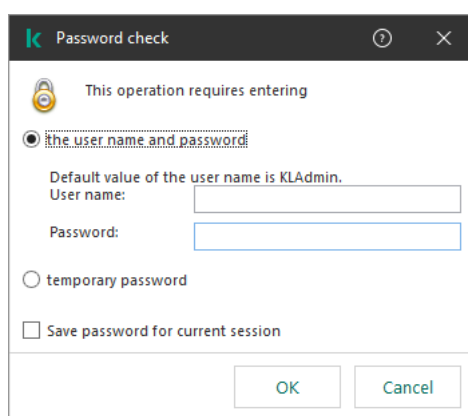
- Enter a user name and password.

This method is suitable for day-to-day operations. To perform a password-protected action, you must enter the domain account credentials of the user with the required permission. In this case, the computer must be in that domain. If the computer is not in the domain, you can use the KLAdmin account.

- Enter a temporary password.

This method is suitable for granting temporary permissions to perform blocked actions (for example, exiting the application) to users outside the corporate network. When a temporary password expires or a session ends, Kaspersky Endpoint Security reverts its settings to their previous state.

When a user attempts to perform a password-protected action, Kaspersky Endpoint Security prompts the user for the user name and password or temporary password (see the figure below).



Kaspersky Endpoint Security access password prompt

User name and password

To access Kaspersky Endpoint Security, you must enter your domain account credentials. Password protection supports the following accounts:

- **KLAdmin.** An Administrator account with unrestricted access to Kaspersky Endpoint Security. The KLAdmin account has the right to perform any action that is password-protected. The permissions for the KLAdmin account cannot be revoked. When you enable password protection, Kaspersky Endpoint Security prompts you to set a password for the KLAdmin account.
- **The Everyone group.** A built-in Windows group that includes all users within the corporate network. Users in the Everyone group can access the application according to the permissions that are granted to them.

- **Individual users or groups.** User accounts for which you can configure individual permissions. For example, if an action is blocked for the Everyone group, you can allow this action for an individual user or a group.
- **Session user.** Account of the user who started the Windows session. You can switch to another session user when prompted for a password (the **Save password for current session** check box). In this case, Kaspersky Endpoint Security regards the user whose account credentials were entered as the session user instead of the user who started the Windows session.

Temporary password

A temporary password can be used to grant temporary access to Kaspersky Endpoint Security for an individual computer outside of the corporate network. The Administrator generates a temporary password for an individual computer in the computer properties in Kaspersky Security Center. The Administrator selects the actions that will be protected with the temporary password, and specifies the temporary password's validity period.

Password protection operating algorithm

Kaspersky Endpoint Security decides whether to allow or block a password-protected action based on the following algorithm (see the figure below).



Password protection operating algorithm

Enabling Password protection

Password protection lets you restrict users' access to Kaspersky Endpoint Security according to the permissions granted to them (for example, permission to exit the application).

To enable password protection:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Interface**.
3. In the **Password protection** section, click the **Settings** button.
The **Password protection** window opens.
4. In the window that opens, select the **Enable password protection** check box.
5. Specify the password for the KLAdmin account:

a. In the **Permissions** table, double-click to open the list of permissions for the KLAdmin account.

The KLAdmin account has the right to perform any action that is password-protected.

b. In the window that opens, click the **Password** button.

c. Specify the password for the KLAdmin account and confirm it.

d. Click **OK**.

If a computer is running under a policy, the Administrator can reset the password for the KLAdmin account in the policy properties. If the computer is not connected to Kaspersky Security Center and you have forgotten the password for the KLAdmin account, it is not possible to recover the password.

6. Set permissions for all users within the corporate network:

a. In the **Permissions** table, double-click to open the list of permissions for the Everyone group.

The Everyone group is a built-in Windows group that includes all users within the corporate network.

b. Select the check boxes next to the actions that users will be allowed to perform without entering the password.

If a check box is cleared, the users are blocked from performing the action. For example, if the check box next to the **Exit the application** permission is cleared, you can exit the application only if you are logged in as KLAdmin, or as an [individual user who has the required permission](#), or if you enter a [temporary password](#).

Password protection permissions have some important [aspects to consider](#). Make sure that all conditions for accessing Kaspersky Endpoint Security are fulfilled.

c. Click the **OK** button.

7. Save your changes.

When password protection is enabled, the application will restrict users' access to Kaspersky Endpoint Security according to the permissions granted to the Everyone group. You can perform the actions that are blocked for the Everyone group only if you use the KLAdmin account, [another account that is granted the required permissions](#), or if you enter a [temporary password](#).

You can disable Password protection only if you are logged in as KLABAdmin. It is not possible to disable password protection if you are using any other user account or a temporary password.

During the password check, you can select the **Save password for current session** check box. In this case, Kaspersky Endpoint Security will not prompt for a password when a user attempts to perform another password-protected action for the duration of the session.

Granting permissions to individual users or groups

You can grant access to Kaspersky Endpoint Security to individual users or groups. For example, if exiting the application is blocked for the Everyone group, you can grant the **Exit the application** permission to an individual user. As a result, you can exit the application only if you are logged in as that user or as KLABAdmin.

You can use account credentials to access the application only if the computer is in the domain. If the computer is not in the domain, you can use the KLABAdmin account or a [temporary password](#).

To grant permissions to individual users or groups:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Interface**.
3. In the **Password protection** section, click the **Settings** button.
The **Password protection** window opens.
4. In the **Permissions** table, click the **Add** button.
The **Permissions of a user/group** window opens.
5. Click the **Select** button to the right of the **User / Group** field.
The standard Select Users or Groups dialog opens.
6. Select a user or a group in Active Directory and confirm your selection.
7. In the **Permissions** table, select the check boxes next to the actions that the selected user or group will be allowed to perform without being prompted for a password.
If a check box is cleared, the users are blocked from performing the action. For example, if the check box next to the **Exit the application** permission is cleared, you can exit the application only if you are logged in as KLABAdmin, or as an [individual user who has the required permission](#), or if you enter a [temporary password](#).

Password protection permissions have some important [aspects to consider](#). Make sure that all conditions for accessing Kaspersky Endpoint Security are fulfilled.

8. Save your changes.

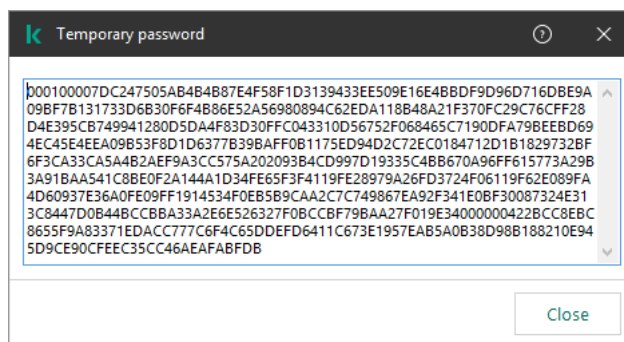
As a result, if access to the application is restricted for the Everyone group, users will be granted permissions to access Kaspersky Endpoint Security according to the users' individual permissions.

Using a temporary password to grant permissions

A temporary password can be used to grant temporary access to Kaspersky Endpoint Security for an individual computer outside of the corporate network. This is necessary to allow the user to perform a blocked action without obtaining the KLAdmin account credentials. To use a temporary password, the computer must be added to Kaspersky Security Center.

To allow a user to perform a blocked action using a temporary password:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Devices** tab.
4. Double-click to open the computer properties window.
5. In the computer properties window, select the **Applications** section.
6. In the list of Kaspersky applications that are installed on the computer, select **Kaspersky Endpoint Security for Windows** and double-click to open the application properties.
7. In the application settings window, select **General Settings** → **Interface**.
8. In the **Password protection** section, click the **Settings** button.
The **Password protection** window opens.
9. In the **Temporary password** section, click the **Settings** button.
The **Create temporary password** window opens.
10. In the **Expiration date** field, specify the expiration date when the temporary password will expire.
11. In the **Temporary password scope** table, select the check boxes next to the actions that will be available to the user after entering the temporary password.
12. Click the **Create** button.
A window containing the temporary password opens (see the figure below).
13. Copy the password and provide it to the user.




Temporary password

Special aspects of Password protection permissions

Password protection permissions have some important aspects and limitations to consider.


Configure application settings

If a user's computer is running under a policy, make sure that all the required settings in the policy are available for editing (the  attributes are open).


Exit the application

There are no special considerations or limitations.

Disable protection components

- It is not possible to grant the permission to disable protection components for the Everyone group. To allow users other than KLAdmin to disable protection components, [add a user or group](#) that has the **Disable protection components** permission in the Password Protection settings.
- If a user's computer is running under a policy, make sure that all the required settings in the policy are available for editing (the  attributes are open).
- To disable protection components in the application settings, a user must have the **Configure application settings** permission.
- To disable protection components from the context menu (by using the **Pause protection and control** menu item), a user must have the **Disable control components** permission in addition to the **Disable protection components** permission.

Disable control components

- It is not possible to grant the permission to disable control components for the Everyone group. To allow users other than KLAdmin to disable control components, [add a user or group](#) that has the **Disable control components** permission in the Password Protection settings.
- If a user's computer is running under a policy, make sure that all the required settings in the policy are available for editing (the  attributes are open).
- To disable control components in the application settings, a user must have the **Configure application settings** permission.
- To disable control components from the context menu (by using the **Pause protection and control** menu item), a user must have the **Disable protection components** permission in addition to the **Disable control components** permission.

Disable Kaspersky Security Center policy

You cannot grant the "Everyone" group the permission to disable the Kaspersky Security Center policy. To allow users other than KLAdmin to disable the policy, [add a user or a group](#) that has the **Disable Kaspersky Security Center policy** permission in the Password Protection settings.

Remove key

There are no special considerations or limitations.

Remove / modify / restore the application

If you have allowed removing, modifying, and restoring the application for the "All" group, Kaspersky Endpoint Security does not request a password when the user attempts to carry out these operations. Therefore, any user including users from outside the domain, can install, modify, or restore the application.

Restore access to data on encrypted drives

You can restore access to data on encrypted drives only if you are logged in as KLAdmin. Permission to perform this action cannot be granted to any other user.

Viewing reports

There are no special considerations or limitations.

Restore from Backup

There are no special considerations or limitations.

Trusted zone

A *trusted zone* is a system administrator-configured list of objects and applications that Kaspersky Endpoint Security does not monitor when active. In other words, it is a set of scan exclusions.

The administrator forms the trusted zone independently, taking into account the features of the objects that are handled and the applications that are installed on the computer. It may be necessary to include objects and applications in the trusted zone when Kaspersky Endpoint Security blocks access to a certain object or application, if you are sure that the object or application is harmless.

You can exclude objects from scans by using the following methods:

- specify the path to the file or folder;
- enter the object hash;
- Use masks:
 - The * (asterisk) character, which takes the place of any set of characters, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:**.txt will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.
 - Two consecutive * characters take the place of any set of characters (including an empty set) in the file or folder name, including the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\Folder***.txt will include all paths to files with the TXT extension located in the folder named Folder and its subfolders. The mask must include at least one nesting level. The mask C:***.txt is not a valid mask.
 - The ? (question mark) character, which takes the place of any single character, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\Folder\???.txt will include paths to all files residing in the folder named Folder that have the TXT extension and a name consisting of three characters.
- Enter the name of the object according to the classification of the [Kaspersky IT Encyclopedia](#) (for example, Email-Worm, Rootkit or RemoteAdmin).

Scan exclusions

A *scan exclusion* is a set of conditions that must be fulfilled so that Kaspersky Endpoint Security will not scan a particular object for viruses and other threats.

Scan exclusions make it possible to safely use legitimate software that can be exploited by criminals to damage the computer or user data. Although they do not have any malicious functions, such applications can be exploited by intruders. For details on legitimate software that could be used by criminals to harm the computer or personal data of a user, please visit the website of the [Kaspersky IT Encyclopedia](#).

Such applications may be blocked by Kaspersky Endpoint Security. To prevent them from being blocked, you can configure scan exclusions for the applications in use. To do so, add the name or name mask that is listed in the Kaspersky IT Encyclopedia to the trusted zone. For example, you often use the Radmin application for remote administration of computers. Kaspersky Endpoint Security regards this activity as suspicious and may block it. To prevent the application from being blocked, create a scan exclusion with the name or name mask that is listed in the Kaspersky IT Encyclopedia.

If an application that collects information and sends it to be processed is installed on your computer, Kaspersky Endpoint Security may classify this application as malware. To avoid this, you can exclude the application from scanning by configuring Kaspersky Endpoint Security as described in this document.

Scan exclusions can be used by the following application components and tasks that are configured by the system administrator:

- Behavior Detection.
- Exploit Prevention.
- Host Intrusion Prevention.
- File Threat Protection.
- Web Threat Protection.
- Mail Threat Protection.
- Scan tasks.

List of trusted applications

The *list of trusted applications* is a list of applications whose file and network activity (including malicious activity) and access to the system registry are not monitored by Kaspersky Endpoint Security. By default, Kaspersky Endpoint Security scans objects that are opened, executed, or saved by any application process and controls the activity of all applications and network traffic that is generated by them. Kaspersky Endpoint Security excludes applications in the [list of trusted applications](#) from scanning.

For example, if you consider objects that are used by the standard Microsoft Windows Notepad application to be safe without scanning, meaning that you trust this application, you can add Microsoft Windows Notepad to the list of trusted applications. Scanning then skips objects that are used by this application.

In addition, certain actions that are classified by Kaspersky Endpoint Security as suspicious may be safe within the context of the functionality of a number of applications. For example, the interception of text that is typed from the keyboard is a routine process for automatic keyboard layout switchers (such as Punto Switcher). To take account of the specifics of such applications and exclude their activity from monitoring, we recommend that you add such applications to the trusted applications list.

Excluding trusted applications from scanning allows avoiding compatibility conflicts between Kaspersky Endpoint Security and other programs (for example, the problem of double-scanning of the network traffic of a third-party computer by Kaspersky Endpoint Security and by another anti-virus application), and also increases the computer's performance, which is critical when using server applications.

At the same time, the executable file and process of the trusted application are still scanned for viruses and other malware. An application can be fully excluded from Kaspersky Endpoint Security scanning by means of scan exclusions.

Creating a scan exclusion

Kaspersky Endpoint Security does not scan an object if the drive or folder containing this object is included in the scan scope at the start of one of the scan tasks. However, the scan exclusion is not applied when a custom scan task is started for this particular object.

To create a scan exclusion:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Exclusions**.
3. In the **Scan exclusions and trusted applications** section, click the **Settings** button.
4. In the window that opens, select the **Merge values when inheriting** check box if you want to create a consolidated list of scan exclusions for all computers in the company.

The lists of scan exclusions in the parent and child policies will be merged. The lists will be merged provided that merging values when inheriting is enabled. Scan exclusions from the parent policy are displayed in child policies in a read-only view. Changing or deleting scan exclusions of the parent policy is not possible.

5. Click the **Add** button.

The **Scan exclusion** window opens. In this window, you can create a scan exclusion using one or both of the criteria from the **Properties** section.

6. To exclude a file or folder from scanning:
 - a. In the **Properties** section, select the **File or folder** check box.
 - b. Click the **select file or folder** link in the **Scan exclusion description** section to open the **Name of file or folder** window.
 - c. Enter the file or folder name or the mask of the file or folder name, or select the file or folder in the folder tree by clicking **Browse**.

Use masks:

- The * (asterisk) character, which takes the place of any set of characters, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:**.txt` will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.
- Two consecutive * characters take the place of any set of characters (including an empty set) in the file or folder name, including the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder***.txt` will include all paths to files with the TXT extension located in the folder named Folder and its subfolders. The mask must include at least one nesting level. The mask `C:***.txt` is not a valid mask.
- The ? (question mark) character, which takes the place of any single character, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\???.txt` will include paths to all files residing in the folder named Folder that have the TXT extension and a name consisting of three characters.

In a file or folder name mask, you can use the asterisk character (*) to take the place of any set of characters in the file name.

For example, you can use masks for adding the following paths:

- Paths to files located in any folder:

- The mask *.exe will include all paths to files that have the exe extension.
- The mask example* will include all paths to files named EXAMPLE.
- Paths to files located in a specified folder:
 - The C:\dir*. * mask will include all paths to files located in the C:\dir\ folder, but not in the subfolders of C:\dir\.
 - The mask C:\dir* will include all paths to files located in the C:\dir\ folder, but not in the subfolders of C:\dir\.
 - The mask C:\dir\ will include all paths to files located in the C:\dir\ folder, but not in the subfolders of C:\dir\.
 - The mask C:\dir*.exe will include all paths to files with the EXE extension located in the C:\dir\ folder, but not in the subfolders of C:\dir\.
 - The mask C:\dir\test will include all paths to files named "test" located in the C:\dir\ folder, but not in the subfolders of C:\dir\.
 - The mask C:\dir*\test will include all paths to files named "test" located in the C:\dir\ folder and in the subfolders of C:\dir\.
- Paths to files located in all folders with a specified name:
 - The mask dir*. * will include all paths to files in folders named "dir", but not in the subfolders of those folders.
 - The mask dir* will include all paths to files in folders named "dir", but not in the subfolders of those folders.
 - The mask dir\ will include all paths to files in folders named "dir", but not in the subfolders of those folders.
 - The mask dir*.exe will include all paths to files with the EXE extension in folders named "dir", but not in the subfolders of those folders.
 - The mask dir\test will include all paths to files named "test" in folders named "dir", but not in the subfolders of those folders.

d. In the **Name of file or folder** window, click **OK**.

A link to the added file or folder appears in the **Scan exclusion description** section of the **Scan exclusion** window.

7. To exclude objects with a specific name from scanning:

- a. In the **Properties** section, select the **Object name** check box.
- b. Click the **enter object name** link in the **Scan exclusion description** section to open the **Object name** window.
- c. Enter the object name or name mask according to the classification of the Kaspersky IT Encyclopedia:
- d. Click **OK** in the **Object name** window.

A link to the added object name appears in the **Scan exclusion description** section of the **Scan exclusion** window.

8. If necessary, in the **Comment** field, enter a brief comment on the scan exclusion that you are creating.

9. Specify the Kaspersky Endpoint Security components that should use the scan exclusion:

- a. Click the **any** link in the **Scan exclusion description** section to activate the **select components** link.
- b. Click the **select components** link to open the **Protection components** window.
- c. Select the check boxes opposite the components to which the scan exclusion must be applied.
- d. In the **Protection components** window, click **OK**.

If the components are specified in the settings of the scan exclusion, this exclusion is applied only during scanning by these components of Kaspersky Endpoint Security.

If the components are not specified in the settings of the scan exclusion, this exclusion is applied during scanning by all components of Kaspersky Endpoint Security.

10. In the **Scan exclusion** window, click **OK**.

The scan exclusion you have added appears in the table on the **Scan exclusions** tab of the **Trusted zone** window. The configured settings of this scan exclusion appear in the **Scan exclusion description** section.

11. Save your changes.

Modifying a scan exclusion

To modify a scan exclusion:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Exclusions**.
3. In the **Scan exclusions and trusted applications** section, click the **Settings** button.

The **Trusted zone** window opens on the **Scan exclusions** tab.

4. Select the scan exclusion that you want to modify in the list.

5. Change the scan exclusion settings using one of the following methods:

- Click the **Edit** button.
The **Scan exclusions** window opens.
- Open the window for editing the necessary setting by clicking the link in the **Scan exclusion description** field.

6. If you clicked the **Edit** button during the previous step, click **OK** in the **Scan exclusion** window.

The modified settings of this scan exclusion appear in the **Scan exclusion description** section.

7. Save your changes.

Deleting a scan exclusion

To delete a scan exclusion:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Exclusions**.
3. In the **Scan exclusions and trusted applications** section, click the **Settings** button.
The **Trusted zone** window opens on the **Scan exclusions** tab.
4. Select the scan exclusion that you need in the list of scan exclusions.
5. Click the **Delete** button.
The deleted scan exclusion disappears from the list.
6. Save your changes.

Enabling and disabling a scan exclusion

To enable or disable a scan exclusion:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Exclusions**.
3. In the **Scan exclusions and trusted applications** section, click the **Settings** button.
The **Trusted zone** window opens on the **Scan exclusions** tab.
4. Select the exclusion that you need in the list of scan exclusions.
5. Do one of the following:
 - To enable a scan exclusion, select the check box next to the name of this scan exclusion.
 - To disable a scan exclusion, clear the check box next to the name of this scan exclusion.
6. Save your changes.

Editing the list of trusted applications

To edit the list of trusted applications:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Exclusions**.

3. In the **Scan exclusions and trusted applications** section, click the **Settings** button.

The **Trusted zone** window opens.

4. In the **Trusted zone** window, select the **Trusted applications** tab.

5. In the window that opens, select the **Merge values when inheriting** check box if you want to create a consolidated list of trusted applications for all computers in the company.

The lists of trusted applications in the parent and child policies will be merged. The lists will be merged provided that merging values when inheriting is enabled. Trusted applications from the parent policy are displayed in child policies in a read-only view. Changing or deleting trusted applications of the parent policy is not possible.

6. To add an application to the trusted applications list:

a. Click the **Add** button.

b. In the context menu that opens, do one of the following:

- If you want to find the application in the list of applications installed on the computer, select the **Applications** item in the menu.

The **Select application** window opens.

- If you want to specify the path to the executable file of the relevant application, select **Browse**.

The standard **Open file** window in Microsoft Windows opens.

c. Select the application in one of the following ways:

- If you selected **Applications** during the previous step, select the application in the list of applications installed on the computer and click **OK** in the **Select application** window.
- If you selected **Browse** during the previous step, specify the path to the executable file of the relevant application and click the **Open** button in the standard **Open** window of Microsoft Windows.

These actions cause the **Scan exclusions for application** window to open.

d. Select the check boxes opposite the relevant trusted zone rules for the selected application:

- **Do not scan opened files.**
- **Do not monitor application activity.**
- **Do not inherit restrictions of the parent process (application).**
- **Do not monitor child application activity.**
- **Do not block interaction with the application interface.**
- **Do not block interaction with AMSI Protection Provider.**
- **Do not scan network traffic.**

e. In the **Scan exclusions for application** window, click **OK**.

The trusted application that you have added appears in the trusted applications list.

7. To edit the settings of a trusted application:

- a. Select a trusted application in the trusted applications list.
- b. Click the **Edit** button.
- c. The **Scan exclusions for application** window opens.
- d. Select or clear the check boxes opposite the relevant trusted zone rules for the selected application:

If no trusted zone rules are selected in the **Scan exclusions for application** window, the [trusted application is included in the scan](#). In this case, the trusted application is not removed from the list of trusted applications, but its check box is cleared.

- e. In the **Scan exclusions for application** window, click **OK**.
8. To remove a trusted application from the trusted applications list:
- a. Select a trusted application in the trusted applications list.
 - b. Click the **Delete** button.
9. Save your changes.

Enabling and disabling trusted zone rules for an application in the list of trusted applications

To enable or disable the action of trusted zone rules applied to an application from the list of trusted applications:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Exclusions**.
3. In the **Scan exclusions and trusted applications** section, click the **Settings** button.
The **Trusted zone** window opens.
4. In the **Trusted zone** window, select the **Trusted applications** tab.
5. In the list of trusted applications, select the necessary trusted application.
6. Do one of the following:
 - To exclude a trusted application from Kaspersky Endpoint Security scanning, select the check box next to its name.
 - To include a trusted application in Kaspersky Endpoint Security scanning, clear the check box next to its name.
7. Save your changes.

Using trusted system certificate storage

Use of system certificate storage lets you exclude applications signed by a trusted digital signature from virus scans. Kaspersky Endpoint Security automatically assigns such applications to the *Trusted* group.

To begin using trusted system certificate storage:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Exclusions**.
3. In the **Scan exclusions and trusted applications** section, click the **Settings** button.
The **Trusted zone** window opens.
4. In the **Trusted zone** window, select the **Trusted system certificate store** tab.
5. Select the **Use trusted system certificate store** check box.
6. In the **Trusted system certificate store** drop-down list, select which system store must be considered as trusted by Kaspersky Endpoint Security .
7. Save your changes.

Managing Backup

Backup stores reserve copies of files that were deleted or modified during disinfection. A *backup copy* is a file copy created before the file was disinfected or deleted. Backup copies of files are stored in a special format and do not pose a threat.

Backup copies of files are stored in the folder C:\ProgramData\Kaspersky Lab\KES\QB.

Users in the Administrators group are granted full permission to access this folder. Limited access rights to this folder are granted to the user whose account was used to install Kaspersky Endpoint Security.

Kaspersky Endpoint Security does not provide the capability to configure user access permissions to backup copies of files.

Sometimes it is not possible to maintain the integrity of files during disinfection. If you partially or completely lose access to important information in a disinfected file after disinfection, you can attempt to restore the file from its backup copy to its original folder.

If Kaspersky Endpoint Security is running under the management of Kaspersky Security Center, backup copies of files may be transmitted to the Kaspersky Security Center Administration Server. For more details about managing backup copies of files in Kaspersky Security Center, please refer to the Kaspersky Security Center Help system.

Configuring the maximum storage period for files in Backup

The default maximum storage period for copies of files in Backup is 30 days. After expiration of the maximum storage term, Kaspersky Endpoint Security deletes the oldest files from Backup. You can cancel the time-based restriction or change the maximum file storage term.

To configure the maximum storage period for files in Backup:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Reports and Storage**.
3. Do one of the following:
 - If you want to limit the storage period for copies of files in Backup, in the **Backup** section in the right part of the window, select the **Store objects no longer than** check box. In the field on the right of the **Store objects no longer than** check box, specify the maximum storage period for copies of files in Backup. The default maximum storage period for copies of files in Backup is 30 days.
 - If you want to cancel the storage period limit for copies of files in Backup, in the **Backup** section in the right part of the window, clear the **Store objects no longer than** check box.
4. Save your changes.

Configuring the maximum size of Backup

By default, the maximum size of Backup is 100 MB. After the maximum size is reached, Kaspersky Endpoint Security automatically deletes the oldest files from Backup so that the maximum size is not exceeded. You can cancel the Backup size limit or change the maximum size.

To configure the maximum size of Backup:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Reports and Storage**.
3. Do one of the following:
 - If you want to limit the total size of Backup, select the **Maximum storage size** check box in the right part of the window in the **Backup** section and specify the maximum size of Backup in the field to the right of the **Maximum storage size** check box.
By default, the maximum storage size for data comprising the backup copies of files is 100 MB.
 - If you want to cancel the limitation of the Backup size, clear the **Maximum storage size** check box in the right part of the window in the **Backup** section.

The size of Backup is unlimited by default.

4. Save your changes.

Restoring files from Backup

If malicious code is detected in a file, Kaspersky Endpoint Security blocks the file, assigns the *Infected* status to it, places a copy of it in Backup, and attempts to disinfect it. If file disinfection succeeds, the status of the backup copy of the file changes to *Disinfected*. The file becomes available in its original folder. If a file cannot be disinfected, Kaspersky Endpoint Security deletes it from its original folder. You can restore the file from its backup copy to its original folder.

Files with the *Will be disinfected on computer restart* status cannot be restored. Restart the computer, and the file status will change to *Disinfected* or *Deleted*. You can also restore the file from its backup copy to its original folder.

Upon detecting malicious code in a file that is part of the Windows Store application, Kaspersky Endpoint Security immediately deletes the file without moving a copy of the file to Backup. You can restore the integrity of the Windows Store application by using the appropriate tools of the Microsoft Windows 8 operating system (see the *Microsoft Windows 8 help files* for details on restoring a Windows Store application).

The set of backup copies of files is presented as a table. For a backup copy of a file, the path to the original folder of the file is displayed. The path to the original folder of the file may contain personal data.

You can copy information about selected Backup files to the clipboard. To select multiple Backup files, right-click to open the context menu of any file and choose **Select all**. To deselect files that you do not want to scan, click them while holding down the **CTRL** key.

If several files with identical names and different content located in the same folder are moved to Backup, only the file that was last placed in Backup can be restored.

To restore files from Backup:

1. In the main application window, click the **Backup** button.

The **Backup** window opens.

2. If you want to restore all files from Backup, in the **Backup** window select **Restore all** from the context menu of any file.

Kaspersky Endpoint Security restores all files from their backup copies to their original folders.

3. To restore one or more files from Backup:

a. In the table in the **Backup** window, select one or multiple Backup files.

To select multiple Backup files, right-click to open the context menu of any file and choose **Select all**. To deselect files that you do not want to scan, click them while holding down the **CTRL** key.

b. Restore files in one of the following ways:

- Click the **Restore** button.
- Right-click to open the context menu and select **Restore**.

Kaspersky Endpoint Security restores files from the selected backup copies to their original folders.

Deleting backup copies of files from Backup

Kaspersky Endpoint Security automatically deletes backup copies of files with any status from Backup after the storage term configured in application settings has elapsed. You can also manually delete any copy of a file from Backup.

To delete backup copies of files from Backup:

1. In the main application window, click the **Backup** button.

2. The **Backup** window opens.

3. If you want to delete all files from Backup, perform one of the following actions:

- In the context menu of any file, select **Delete all**.
- Click the **Clear storage** button.

Kaspersky Endpoint Security deletes all backup copies of files from Backup.

4. If you want to delete one or more files from Backup:

a. In the table in the **Backup** window, select one or multiple Backup files.

To select multiple Backup files, right-click to open the context menu of any file and choose **Select all**. To deselect files that you do not want to scan, click them while holding down the **CTRL** key.

b. Click the **Delete** button.

Kaspersky Endpoint Security deletes the selected backup copies of files from Backup.

Notification service

All sorts of events occur during the operation of Kaspersky Endpoint Security. Notifications of these events can be either be purely informational or contain critical information. For example, notifications may inform of a successful database and application modules update or log component errors that need remedying.

Kaspersky Endpoint Security supports the logging of information about events in the operation of the Microsoft Windows application log and / or the Kaspersky Endpoint Security event log.

Kaspersky Endpoint Security delivers notifications in the following ways:

- using pop-up notifications in the Microsoft Windows taskbar notification area;
- by email.

You can configure the delivery of event notifications. The method of notification delivery is configured for each type of event.

You can perform the following actions for configuring the notification service:

- configure the settings of event logs where Kaspersky Endpoint Security records events;
- configure how on-screen notifications are displayed;
- configure the delivery of email notifications.

When using the table of events to configure the notification service, you can perform the following actions:

- Filter notification service events by column values or by custom filter conditions.
- Use the search function for notification service events.
- Sort notification service events.
- Change the order and set of columns that are displayed in the list of notification service events.

Configuring event log settings

To configure event log settings:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Interface**.
3. In the **Notifications** section, click the **Settings** button.

This opens the **Notifications** window.

Kaspersky Endpoint Security components and tasks are shown in the left part of the window. The right part of the window lists the events generated for the selected component or task.

Events may contain the following user data:

- Paths to files scanned by Kaspersky Endpoint Security.

- Paths to registry keys modified during the operation of Kaspersky Endpoint Security.
 - Microsoft Windows user name.
 - Addresses of web pages opened by the user.
4. In the left part of the window, select the component or task for which you want to configure the event log settings.
 5. Select check boxes opposite the relevant events in the **Save in local report** and **Save in Windows Event Log** columns.

Events whose check boxes are selected in the **Save in local report** column are displayed in **Applications and Services Logs** in the **Kaspersky Event Log** section. Events whose check boxes are selected in the **Save in Windows Event Log** column are displayed in **Windows logs** in the **Application** section. To open the event logs, select **Start** → **Control Panel** → **Administration** → **Event Viewer**.
 6. Save your changes.

Configuring the display and delivery of notifications

To configure the display and delivery of notifications:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Interface**.
3. In the **Notifications** section, click the **Settings** button.

This opens the **Notifications** window.

Kaspersky Endpoint Security components and tasks are shown in the left part of the window. The right part of the window lists events generated for the selected component or the selected task.

Events may contain the following user data:

 - Paths to files scanned by Kaspersky Endpoint Security.
 - Paths to registry keys modified during the operation of Kaspersky Endpoint Security.
 - Microsoft Windows user name.
 - Addresses of web pages opened by the user.
4. In the left part of the window, select the component or task for which you want to configure the delivery of notifications.
5. In the **Notify on screen** column, select the check boxes next to the required events.

Information about the selected events is displayed on the screen as pop-up messages in the Microsoft Windows taskbar notification area.
6. In the **Notify by email** column, select the check boxes next to the required events.

Information about the selected events is delivered by email if the mail notification delivery settings are configured.
7. Click the **Email notification settings** button.



This opens the **Email notification settings** window.

8. Select the **Send event notifications** check box to enable the delivery of information about Kaspersky Endpoint Security events selected in the **Notify by email** column.
9. Specify the email notification delivery settings.
10. Save your changes.

Configuring the display of warnings about the application status in the notification area

To configure the display of application status warnings in the notification area:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Interface**.
3. In the **Warnings** section, select the check boxes opposite those categories of events about which you want to see notifications in the notification area of Microsoft Windows.
4. Save your changes.

When events associated with the selected categories occur, the [application icon](#) in the notification area will change to  or  depending on the severity of the warning.


Managing reports

Information about the operation of each Kaspersky Endpoint Security component, data encryption events, the performance of each scan task, the update task and integrity check task, and the overall operation of the application is recorded in reports.

Reports are stored in the folder C:\ProgramData\Kaspersky Lab\KES\Report.

Reports may contain the following user data:

- Paths to files scanned by Kaspersky Endpoint Security.
- Paths to registry keys modified during the operation of Kaspersky Endpoint Security.
- Microsoft Windows user name.
- Addresses of web pages opened by the user.


The data in the report is presented in tabular form. Each table row contains information on a separate event. Event attributes are located in the table columns. Certain columns are compound ones which contain nested columns with additional attributes. To view additional attributes, click the  button next to the name of the column. Events that are logged during the operation of various components or during the performance of various tasks have different sets of attributes.


The following reports are available:

- **System Audit** report. Contains information about events occurring during the interaction between the user and the application and in the course of application operation in general, which are unrelated to any particular Kaspersky Endpoint Security components or tasks.
- Reports on the operation of Kaspersky Endpoint Security components.
- Kaspersky Endpoint Security task reports.
- **Data encryption** report. Contains information about events occurring during data encryption and decryption.

Reports use the following event importance levels:


 **Informational messages.** Reference events that normally do not contain important information.

 **Warnings.** Events that need attention because they reflect important situations in the operation of Kaspersky Endpoint Security.

 **Critical events.** Events of critical importance that indicate problems in the operation of Kaspersky Endpoint Security or vulnerabilities in the protection of the user's computer.

For convenient processing of reports, you can modify the presentation of data on the screen in the following ways:

- Filter the event list by various criteria.
- Use the search function to find a specific event.
- View the selected event in a separate section.

- Sort the list of events by each report column.
- Display and hide events grouped by the event filter using the  button.
- Change the order and arrangement of columns that are shown in the report.

You can save a generated report to a text file, if necessary. You can also [delete report information](#) on Kaspersky Endpoint Security components and tasks that are combined into groups.

If Kaspersky Endpoint Security is running under the management of Kaspersky Security Center, information about events may be relayed to the Kaspersky Security Center Administration Server (for more details, please refer to the [Kaspersky Security Center Help Guide](#)).

Viewing reports

If a user can view reports, the user can also view all events reflected in the reports.

To view reports:

1. In the main application window, click the **Reports** button.

The **Reports** window opens.

2. In the left part of the **Reports** window, in the list of components and tasks, select a component or task.

The right part of the window displays a report containing a list of events resulting from the operation of the selected component or selected task of Kaspersky Endpoint Security. You can sort events in the report based on the values in cells of one of the columns. By default, report events are sorted in ascending order of the values in cells of the **Event date** column.

3. To view detailed information about an event, select the event in the report.

A section with the event summary is displayed in the lower part of the window.

Configuring the maximum report storage term

The default maximum storage term for reports on events that are logged by Kaspersky Endpoint Security is 30 days. After that period of time, Kaspersky Endpoint Security automatically deletes the oldest entries from the report file. You can cancel the time-based restriction or change the maximum report storage duration.

To modify the report maximum storage term:

1. In the main application window, click the **Settings** button.

2. In the application settings window, select **General Settings** → **Reports and Storage**.

3. In the right part of the window, in the **Reports** section, perform one of the following actions:

- To limit the report storage term, select the **Store reports no longer than** check box. In the field next to the **Store reports no longer than** check box, specify the maximum report storage term.

The default maximum storage term for reports is 30 days.

- To cancel the limit on the report storage term, clear the **Store reports no longer than** button.

The limit on the report storage term is enabled by default.

4. Save your changes.

Configuring the maximum size of the report file

You can specify the maximum size of the file that contains the report. By default, the maximum report file size is 1024 MB. To avoid exceeding the maximum report file size, Kaspersky Endpoint Security automatically deletes the oldest entries from the report file when the maximum report file size is reached. You can cancel the restriction on the size of the report file or set a different value.

To configure the maximum report file size:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Reports and Storage**.
3. In the right part of the window, in the **Reports** section, perform one of the following actions:
 - To limit the report file size, select the **Maximum file size** check box. In the field on the right of the **Maximum file size** check box, specify the maximum report file size.
By default, the report file size is limited to 1024 MB.
 - To remove the restriction on the report file size, clear the **Maximum file size** check box.

The report file size limit is enabled by default.

4. Save your changes.

Saving a report to file

The user is personally responsible for ensuring the security of information from a report saved to file, and particularly for controlling and restricting access to this information.

You can save the report that you generate to a file in text format (TXT) or a CSV file.

Kaspersky Endpoint Security logs events in the report in the same way as they are displayed on the screen: in other words, with the same set and sequence of event attributes.

To save a report to file:

1. In the main application window, click the **Reports** button.
The **Reports** window opens.
2. In the left part of the **Reports** window, in the list of components and tasks, select a component or task.

A report is displayed in the right part of the window, which contains a list of events in the operation of the selected Kaspersky Endpoint Security component or task.

3. If necessary, you can modify data presentation in the report by:

- Filtering events
- Running an event search
- Rearranging columns
- Sorting events

4. Click the **Save report** button in the upper right part of the window.

A context menu opens.

5. In the context menu, select the encoding for saving the report file: **Save as ANSI** or **Save as Unicode**.

6. In the **Save as** window, specify the destination folder for the report file.

7. In the **File name** field, type the report file name.

8. In the **File type** field, select the necessary report file format: TXT or CSV.

9. Save your changes.

Clearing reports

To remove information from reports:

1. In the main application window, click the **Settings** button.

2. In the application settings window, select **General Settings** → **Reports and Storage**.

3. In the right part of the window, in the **Reports** section, click the **Delete reports** button.

The **Delete reports** window opens.

4. Select check boxes opposite the reports from which you want to delete information:

- **All reports.**
- **Protection components report.** Contains information about the operation of the following Kaspersky Endpoint Security components:
 - Behavior Detection.
 - Exploit Prevention.
 - Host Intrusion Prevention.
 - File Threat Protection.
 - Web Threat Protection.

- Mail Threat Protection.
- Network Threat Protection.
- BadUSB Attack Prevention.
- AMSI Protection Provider.
- **Control components report.** Contains information about the operation of the following Kaspersky Endpoint Security components:
 - Application Control.
 - Device Control.
 - Web Control.
 - Adaptive Anomaly Control.
- **Data encryption report.** Contains information about completed data encryption tasks.
- **Scan tasks report.** Contains information about the following completed scan tasks:
 - Full Scan.
 - Critical Areas Scan.
 - Custom Scan.

Information about completed Integrity check task is deleted only if the **All reports** check box is selected.

- **Update task report.** Contains information about completed update tasks:
- **Firewall report.** Contains information about Firewall operation.
- **Endpoint Sensor component report.** Contains information about Endpoint Sensor component operation.

5. Click **OK**.

Kaspersky Endpoint Security Self-Defense

Kaspersky Endpoint Security protects the computer from malicious applications, including malware that attempts to block the operation of Kaspersky Endpoint Security or even delete it from the computer.

Kaspersky Endpoint Security ensures the stability of the computer security system by using the following technologies:

- Self-Defense mechanism. Prevents alteration or deletion of application files on the hard drive, memory processes, and entries in the system registry.
- AM-PPL (Antimalware Protected Process Light). Protects Kaspersky Endpoint Security processes against malicious actions. For more details about AM-PPL technology, please visit the [Microsoft website](#).

AM-PPL technology is available for Windows 10 version 1703 (RS2) or later, and Windows Server 2019 operating systems.

- External management defense mechanism. Lets you block all attempts to manage application services from a remote computer.

On computers that run on 64-bit operating systems, only Kaspersky Endpoint Security Self-Defense is available for preventing the alteration and deletion of application files on the hard drive and system registry entries.

Enabling and disabling Self-Defense

The Self-Defense mechanism of Kaspersky Endpoint Security is enabled by default.

To enable or disable Self-Defense:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Application Settings**.
3. Do one of the following:
 - To enable the Self-Defense mechanism, select the **Enable Self-Defense** check box.
 - To disable the Self-Defense mechanism, clear the **Enable Self-Defense** check box.
4. Save your changes.

Enabling and disabling AM-PPL support

Kaspersky Endpoint Security supports Antimalware Protected Process Light technology (hereinafter referred to as "AM-PPL") from Microsoft. AM-PPL protects Kaspersky Endpoint Security processes against malicious actions (for example, terminating the application). AM-PPL allows only trusted processes to run. Kaspersky Endpoint Security processes are signed in accordance with Windows security requirements, and therefore they are trusted. For more details about AM-PPL technology, please visit the [Microsoft website](#). AM-PPL technology is enabled by default.

Kaspersky Endpoint Security also has built-in mechanisms for protecting application processes. AM-PPL support lets you delegate process security functions to the operating system. You can thereby increase the speed of the application and reduce the consumption of computer resources.

The AM-PPL service is available for Windows 10 version 1703 (RS2) or later, and Windows Server 2019 operating systems.

To enable or disable AM-PPL technology:

1. [Turn off the application's Self-Defense mechanism.](#)

The Self-Defense mechanism prevents modification and deletion of application processes in the computer memory, including changing the AM-PPL status.

2. Run the command line interpreter (cmd.exe) as an administrator.

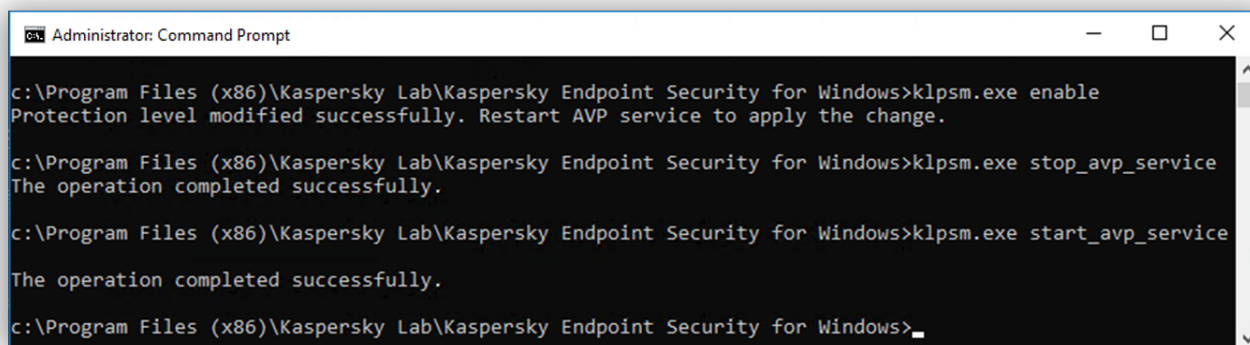
3. Go to the folder where the Kaspersky Endpoint Security executable file is located.

4. Type the following in the command line:

- `klpsm.exe enable` – enable support for AM-PPL technology (see the figure below).
- `klpsm.exe disable` – disable support for AM-PPL technology.

5. Restart Kaspersky Endpoint Security.

6. [Resume the application's Self-Defense mechanism.](#)



```
Administrator: Command Prompt
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe enable
Protection level modified successfully. Restart AVP service to apply the change.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe stop_avp_service
The operation completed successfully.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe start_avp_service
The operation completed successfully.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>_
```

Enabling support for AM-PPL technology

Enabling and disabling external management defense

The external management defense mechanism is enabled by default.

To enable or disable the external management defense mechanism:

1. In the main application window, click the **Settings** button.

2. In the application settings window, select **General Settings** → **Application Settings**.

3. Do one of the following:

- If you want to enable external management defense, select the **Disable external management of system services** check box.
- If you want to disable external management defense, clear the **Disable external management of system services** check box.

To stop the application from the command line, the **Disable external management of system services** check box must be cleared.

4. Save your changes.

Supporting remote administration applications

You may occasionally need to use a remote administration application while external management defense is enabled.

To enable the operation of remote administration applications:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Exclusions**.
3. In the **Scan exclusions and trusted applications** section, click the **Settings** button.
The **Trusted zone** window opens.
4. In the **Trusted zone** window, select the **Trusted applications** tab.
5. Click the **Add** button.
6. In the context menu that opens, do one of the following:
 - To find the remote administration application in the list of applications that are installed on the computer, select the **Applications** item.
The **Select application** window opens.
 - To specify the path to the executable file of the remote administration application, select **Browse**.
The standard **Open file** window in Microsoft Windows opens.
7. Select the application in one of the following ways:
 - If you selected **Applications** during the previous step, select the application in the list of applications installed on the computer and click **OK** in the **Select application** window.
 - If you selected **Browse** during the previous step, specify the path to the executable file of the relevant application and click the **Open** button in the standard **Open** window of Microsoft Windows.

These actions cause the **Scan exclusions for application** window to open.

8. Select the **Do not monitor application activity** check box.

9. Save your changes.

Kaspersky Endpoint Security performance and compatibility with other applications

Performance of Kaspersky Endpoint Security

The performance of Kaspersky Endpoint Security refers to the number of types of objects that can harm the computer that are detectable, as well as energy consumption and use of computer resources.

Selecting types of detectable objects

Kaspersky Endpoint Security lets you fine-tune the protection of your computer and select the [types of objects](#) that the application detects during operation. Kaspersky Endpoint Security always scans the operating system for viruses, worms, and Trojans. You cannot disable scanning of these types of objects. Such malware can cause significant harm to the computer. For greater security on your computer, you can expand the range of detectable object types by enabling monitoring of legal software that can be used by criminals to damage your computer or personal data.

Using energy-saving mode

Energy consumption by applications is a key consideration for portable computers. Kaspersky Endpoint Security scheduled tasks usually use up considerable resources. When the computer is running on battery power, you can use energy-saving mode to consume power more sparingly.

In energy-saving mode, the following scheduled tasks are postponed automatically:

- Update task
- Full Scan task
- Critical Areas Scan task
- Custom Scan task
- Integrity Check task

Whether or not energy saving mode is enabled, Kaspersky Endpoint Security pauses encryption tasks when a portable computer switches to battery power. The application resumes encryption tasks when the portable computer switches from battery power to mains power.

Conceding computer resources to other applications

Use of computer resources by Kaspersky Endpoint Security may impact the performance of other applications. To resolve the problem of simultaneous operation during increased load on the CPU and hard drive subsystems, Kaspersky Endpoint Security can pause scheduled tasks and concede resources to other applications.

However, a number of applications start immediately when CPU resources become available, proceeding to work in background mode. To prevent scanning from depending on the performance of other applications, it is better to not concede operating system resources to them.

You can start such tasks manually, if necessary.

Using advanced disinfection technology

Today's malicious applications can penetrate the lowest levels of an operating system, which makes them virtually impossible to eliminate. After detecting malicious activity in the operating system, Kaspersky Endpoint Security performs an extensive disinfection procedure that uses special advanced disinfection technology. *Advanced disinfection technology* is aimed at purging the operating system of malicious applications that have already started their processes in RAM and that prevent Kaspersky Endpoint Security from removing them by using other methods. The threat is neutralized as a result. While Advanced Disinfection is in progress, you are advised to refrain from starting new processes or editing the operating system registry. The advanced disinfection technology uses considerable operating system resources, which may slow down other applications.

After the Advanced Disinfection process has been completed on a computer running Microsoft Windows for workstations, Kaspersky Endpoint Security requests the user's permission to reboot the computer. After system reboot, Kaspersky Endpoint Security deletes malware files and starts a "lite" full scan of the computer.

A reboot prompt is impossible on a computer running Microsoft Windows for servers due to the specifics of Kaspersky Endpoint Security. An unplanned reboot of a file server can lead to problems involving temporary unavailability of file server data or loss of unsaved data. It is recommended to reboot a file server strictly according to schedule. This is why Advanced Disinfection technology is [disabled](#) by default for file servers.

If active infection is detected on a file server, an event is relayed to Kaspersky Security Center with information that Active Disinfection is required. To disinfect an active infection of a server, enable Active Disinfection technology for servers and start a *Virus scan* group task at a time convenient for server users.

Selecting types of detectable objects

To select types of detectable objects:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Exclusions**.
3. In the **Objects for detection** section, click the **Settings** button.

The **Objects for detection** window opens.

4. Select check boxes opposite the types of objects that you want Kaspersky Endpoint Security to detect:

- **Malicious tools**
- **Adware**
- **Auto-dialers**
- **Other**
- **Packed files that may cause harm**
- **Multi-packed files**

5. Click **OK**.

The **Objects for detection** window closes. In the **Objects for detection** section, the selected types of objects are listed under **Detection of objects of the following types is enabled**.

6. Save your changes.

Enabling or disabling Advanced Disinfection technology

To enable or disable Advanced Disinfection technology for workstations:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Application Settings**.
3. In the right part of the window, do one of the following:
 - Select the **Enable Advanced Disinfection technology** to enable advanced disinfection technology.
 - Clear the **Enable Advanced Disinfection technology** to disable advanced disinfection technology.
4. Save your changes.

When the Advanced Disinfection task is started through Kaspersky Security Center, the majority of operating system functions are unavailable to the user. The workstation is restarted after the task has been completed.

To enable Advanced Disinfection technology for servers, perform one of the following actions:

- Enable Advanced Disinfection technology in the properties of the active Kaspersky Security Center policy. To do so:
 - a. Open the **Application Settings** section in the policy properties window.
 - b. Select the **Enable Advanced Disinfection technology** check box.
 - c. To save the changes, click **OK** in the policy properties window.
- In the properties of the Virus scan group task of Kaspersky Security Center, select the **Run Advanced Disinfection immediately** check box.

To disable Advanced Disinfection technology for servers, perform one of the following:

- Enable Advanced Disinfection technology in the properties of the Kaspersky Security Center policy. To do so:
 - a. Open the **Application Settings** section in the policy properties window.
 - b. Clear the **Enable Advanced Disinfection technology** check box.
 - c. To save the changes, click **OK** in the policy properties window.
- In the properties of the Virus scan group task of Kaspersky Security Center, clear the **Run Advanced Disinfection immediately** check box.

Enabling or disabling energy-saving mode

To enable or disable energy conservation mode:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Application Settings**.
3. In the **Performance** section:
 - To enable energy conservation mode, select the **Postpone scheduled tasks while running on battery power** check box.
When energy conservation mode is enabled and the computer is running on battery power, the following tasks are not run even if scheduled:
 - Update task
 - Full Scan task
 - Critical Areas Scan task
 - Custom Scan task
 - Integrity Check task
 - If you want to disable energy conservation mode, clear the **Postpone scheduled tasks while running on battery power** check box. In this case, Kaspersky Endpoint Security carries out scheduled tasks regardless of the computer's source of power.
4. Save your changes.

Enabling or disabling conceding of resources to other applications

To enable or disable conceding of resources to other applications:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Application Settings**.
3. In the **Performance** section:
 - If you want to enable the mode in which resources are conceded to other applications, select the **Concede resources to other applications** check box.
When configured to concede resources to other applications, Kaspersky Endpoint Security postpones scheduled tasks that slow down other applications:
 - Update task
 - Full Scan task
 - Critical Areas Scan task
 - Custom Scan task
 - Integrity Check task

- If you want to disable the mode in which resources are conceded to other applications, clear the **Concede resources to other applications** check box. In this case Kaspersky Endpoint Security carries out scheduled tasks regardless of the operation of other applications.

By default, the application is configured to concede resources to other applications.

4. Save your changes.

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent supports interaction between the application and other Kaspersky solutions for detecting advanced threats (e.g. Kaspersky Sandbox). Kaspersky solutions are compatible with specific versions of Kaspersky Endpoint Agent. For more information about the supported solutions, refer to [Kaspersky Endpoint Agent help](#).

Kaspersky Endpoint Agent is included in the [Kaspersky Endpoint Security distribution kit](#). You can install Kaspersky Endpoint Agent during installation of Kaspersky Endpoint Security. To do so, you must select the Endpoint Agent component during installation of the application (for example, in the [installation package](#)). After installing the application with Endpoint Agent, Kaspersky Endpoint Security and Kaspersky Endpoint Agent will be added to the list of installed applications. After uninstalling Kaspersky Endpoint Security, Kaspersky Endpoint Agent will also be uninstalled automatically.

Creating and using a configuration file

A configuration file with Kaspersky Endpoint Security settings lets you accomplish the following tasks:

- Perform local installation of Kaspersky Endpoint Security via the command line with predefined settings.
To do so, you must save the configuration file in the same folder where the distribution kit is located.
- Perform remote installation of Kaspersky Endpoint Security via Kaspersky Security Center with predefined settings.
- Migrate Kaspersky Endpoint Security settings from one computer to another.

To create a configuration file:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Manage Settings**.
3. In the **Manage settings** section, click the **Save** button.
This opens the standard **Please select a configuration file** window of Microsoft Windows.
4. Specify the path in which you want to save the configuration file, and enter its name.

To use the configuration file for local or remote installation of Kaspersky Endpoint Security, you must name it `install.cfg`.

5. Click the **Save** button.

To import Kaspersky Endpoint Security settings from a configuration file:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Manage Settings**.
3. In the **Manage settings** section, click the **Load** button.
This opens the standard **Please select a configuration file** window of Microsoft Windows.
4. Specify the path to the configuration file.
5. Click the **Open** button.

All values of Kaspersky Endpoint Security settings will be set according to the selected configuration file.

Messaging between users and the administrator

The [Application Control](#), [Device Control](#), [Web Control](#) and [Adaptive Anomaly Control](#) components enable LAN users whose computers have Kaspersky Endpoint Security installed to send messages to the administrator.

A user may need to send a message to the local corporate network administrator in the following cases:

- Device Control blocked access to the device.

The message template for a request to access a blocked device is available in the Kaspersky Endpoint Security interface in the [Device Control](#) section.

- Application Control blocked the startup of an application.

The message template for a request to allow the startup of a blocked application is available in the Kaspersky Endpoint Security interface in the [Application Control](#) section.

- Web Control blocked access to a web resource.

The message template for a request to access a blocked web resource is available in the Kaspersky Endpoint Security interface in the [Web Control](#) section.

The method used to send messages and the utilized template depends on whether or not there is an active Kaspersky Security Center policy running on the computer that has Kaspersky Endpoint Security installed, and whether or not there is a connection with the Kaspersky Security Center Administration Server. The following scenarios are possible:

- If a Kaspersky Security Center policy is not running on the computer that has Kaspersky Endpoint Security installed, a user's message is sent to the local area network administrator by email.

The message fields are populated with the values of fields from the template defined in the local interface of Kaspersky Endpoint Security.

- If a Kaspersky Security Center policy is running on the computer that has Kaspersky Endpoint Security installed, the standard message is sent to the Kaspersky Security Center Administration Server.

In this case, user messages are available for viewing in the Kaspersky Security Center event storage (see instruction below). The message fields are populated with the values of fields from the template defined in the Kaspersky Security Center policy.

- If a Kaspersky Security Center out-of-office policy is running on the computer with Kaspersky Endpoint Security installed, the method used to send messages depends on whether or not there is a connection with Kaspersky Security Center.

- If a connection with Kaspersky Security Center is established, Kaspersky Endpoint Security sends the standard message to the Kaspersky Security Center Administration Server.

- If a connection with Kaspersky Security Center is absent, a user's message is sent to the local area network administrator by email.

In both cases, the message fields are populated with the values of fields from the template defined in the Kaspersky Security Center policy.

To view a user message in the Kaspersky Security Center event storage:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Administration Server** node of the Administration Console tree, select the **Events** tab.

The Kaspersky Security Center workspace displays all events occurring during the operation of Kaspersky Endpoint Security, including messages to the administrator that are received from LAN users.

3. To configure the event filter, in the **Selection events** drop-down list, select **User requests**.
4. Select the message sent to the administrator.
5. Click the **Open event properties window** button in the right part of the Administration Console workspace.

Data Encryption

Kaspersky Endpoint Security lets you encrypt files and folders that are stored on local and removable drives, or entire removable drives and hard drives. Data encryption minimizes the risk of information leaks that may occur when a portable computer, removable drive or hard drive is lost or stolen, or when data is accessed by unauthorized users or applications. Kaspersky Endpoint Security uses the Advanced Encryption Standard (AES) encryption algorithm.

If the license has expired, the application does not encrypt new data, and old encrypted data remains encrypted and available for use. In this event, encrypting new data requires the application be activated with a new license that permits the use of encryption.

If your license has expired, or the End User License Agreement has been violated, the license key, Kaspersky Endpoint Security, or encryption components has been removed, the encrypted status of previously encrypted files is not guaranteed. This is because some applications, such as Microsoft Office Word, create a temporary copy of files during editing. When the original file is saved, the temporary copy replaces the original file. As a result, on a computer that has no or inaccessible encryption functionality, the file remains unencrypted.

Kaspersky Endpoint Security offers the following aspects of data protection:

- **File Level Encryption on local computer drives.** You can [compile lists of files](#) by extension or group of extensions and lists of folders stored on local computer drives, and create [rules for encrypting files that are created by specific applications](#). After a policy is applied, Kaspersky Endpoint Security encrypts and decrypts the following files:

- files individually added to lists for encryption and decryption;
- files stored in folders added to lists for encryption and decryption;
- files created by separate applications.

- **Encryption of removable drives.** You can specify a default encryption rule, according to which the application applies the same action to all removable drives, or specify encryption rules for individual removable drives.

The default encryption rule has a lower priority than encryption rules created for individual removable drives. Encryption rules created for removable drives of the specified device model have a lower priority than encryption rules created for removable drives with the specified device ID.

To select an encryption rule for files on a removable drive, Kaspersky Endpoint Security checks whether or not the device model and ID are known. The application then performs one of the following operations:

- If only the device model is known, the application uses the encryption rule (if any) created for removable drives of the specific device model.
- If only the device ID is known, the application uses the encryption rule (if any) created for removable drives with the specific device ID.
- If the device model and ID are known, the application applies the encryption rule (if any) created for removable drives with the specific device ID. If no such rule exists, but there is an encryption rule created for removable drives with the specific device model, the application applies this rule. If no encryption rule is specified for the specific device ID nor for the specific device model, the application applies the default encryption rule.
- If neither the device model nor device ID is known, the application uses the default encryption rule.

The application lets you prepare a removable drive for using encrypted data stored on it in portable mode. After enabling portable mode, you can access encrypted files on removable drives connected to a computer without encryption functionality.

- **Managing rules of application access to encrypted files.** For any application, you can create an encrypted file access rule that blocks access to encrypted files or allows access to encrypted files only as ciphertext, which is a sequence of characters obtained when encryption is applied.
- **Creating encrypted packages.** You can create encrypted archives and protect access to such archives with a password. The contents of encrypted archives can be accessed only by entering the passwords with which you protected access to those archives. Such archives can be securely transmitted over networks or on removable drives.
- **Full Disk Encryption.** You can select an encryption technology: Kaspersky Disk Encryption or BitLocker Drive Encryption (hereinafter also referred to as simply "BitLocker").

BitLocker is a technology that is part of the Windows operating system. If a computer is equipped with a Trusted Platform Module (TPM), BitLocker uses it to store recovery keys that provide access to an encrypted hard drive. When the computer starts, BitLocker requests the hard drive recovery keys from the Trusted Platform Module and unlocks the drive. You can configure the use of a password and/or PIN code for accessing recovery keys.

You can specify the default full disk encryption rule and create a list of hard drives to be excluded from encryption. Kaspersky Endpoint Security performs full disk encryption by sector after the Kaspersky Security Center policy is applied. The application encrypts all logical partitions of hard drives simultaneously.

After the system hard drives have been encrypted, at the next computer startup the user must complete authentication using the [Authentication Agent](#) before the hard drives can be accessed and the operating system is loaded. This requires entering the password of the token or smart card connected to the computer, or the user name and password of the Authentication Agent account created by the local area network administrator using *Authentication Agent account management* task. These accounts are based on Microsoft Windows accounts under which users log into the operating system. You can also [use Single Sign-On \(SSO\) technology](#), which lets you automatically log in to the operating system using the user name and password of the Authentication Agent account.

If you back up a computer and then encrypt the computer data, after which you restore the backup copy of the computer and encrypt the computer data again, Kaspersky Endpoint Security creates duplicates of Authentication Agent accounts. To remove the duplicate accounts, you must use the `klmover` utility with the `dupfix` key. The `klmover` utility is included in the Kaspersky Security Center build. You can read more about its operation in the Kaspersky Security Center Help.

Access to encrypted hard drives is possible only from computers on which Kaspersky Endpoint Security with full disk encryption functionality is installed. This precaution minimizes the risk of data leaks from an encrypted hard drive when an attempt to access it is made outside of the local area network of the company.

To encrypt hard drives and removable drives, you can use the **Encrypt used disk space only** function. It is recommended you only use this function for new devices that have not been previously used. If you are applying encryption to a device that is already in use, it is recommended you encrypt the entire device. This ensures that all data is protected – even deleted data that might still contain retrievable information.

Before beginning encryption, Kaspersky Endpoint Security obtains the map of file system sectors. The first wave of encryption includes sectors that are occupied by files at the moment when encryption is started. The second wave of encryption includes sectors that were written to after encryption began. After encryption is complete, all sectors containing data are encrypted.

After encryption is complete and a user deletes a file, the sectors that stored the deleted file become available for storing new information at the file system level but remain encrypted. Thus, as files are written to a new device and the device is regularly encrypted with the **Encrypt used disk space only** function enabled, all sectors will be encrypted after some time.

The data needed to decrypt files is provided by the Kaspersky Security Center Administration Server that controlled the computer at the time of encryption. If the computer with encrypted objects was managed by a different Administration Server for some reason, you can obtain access to the encrypted data in one of the following ways:

- Administration Servers in the same hierarchy:
 - You do not need to take any additional actions. The user will retain access to the encrypted objects. Encryption keys are distributed to all Administration Servers.
- Separated Administration Servers:
 - Request access to encrypted objects from the LAN administrator.
 - Restore data on encrypted devices using the Restore Utility.
 - Restore the configuration of the Kaspersky Security Center Administration Server that controlled the computer at the time of encryption from a backup copy and use this configuration on the Administration Server that now controls the computer with encrypted objects.

If there is no access to encrypted data, follow the special instructions for working with encrypted data ([Restoring access to encrypted files](#), [Working with encrypted devices when there is no access to them](#)).

Encryption functionality limitations

Data Encryption has the following limitations:

- The application creates service files during encryption. Around 0.5% of non-fragmented free space on the hard drive is required to store them. If there is not enough non-fragmented free space on the hard drive, encryption will not start until enough space is freed up.
- Data Encryption is available only when using Kaspersky Endpoint Security with the Kaspersky Security Center administration system. Data Encryption when using Kaspersky Endpoint Security in offline mode is not possible because Kaspersky Endpoint Security stores encryption keys in Kaspersky Security Center.
- Data encryption management is available in the Kaspersky Security Center Administration Console and the Kaspersky Security Center 12 Web Console. It is not possible to manage data encryption in the Kaspersky Security Center Cloud Console.
- If Kaspersky Endpoint Security is installed on a computer running [Microsoft Windows for Servers](#), only full disk encryption using BitLocker Drive Encryption technology is available. If Kaspersky Endpoint Security is installed on a computer running Windows for Workstations, data encryption functionality is fully available.

Full disk encryption using Kaspersky Disk Encryption technology is unavailable for hard drives that do not meet the hardware and software requirements.

Compatibility between the full disk encryption functionality of Kaspersky Endpoint Security and Kaspersky Anti-Virus for UEFI is not supported. Kaspersky Anti-Virus for UEFI starts before the operating system loads. When using full disk encryption, the application will detect the absence of an installed operating system on the computer. As a result, the operation of Kaspersky Anti-Virus for UEFI will end with an error. File Level Encryption (FLE) does not affect the operation of Kaspersky Anti-Virus for UEFI.

Kaspersky Endpoint Security does not support the following configurations:

- The boot loader is located on one drive while the operating system is on a different drive.
- The system contains embedded software of the UEFI 32 standard.
- Intel® Rapid Start Technology and drives that have a hibernation partition even when Intel® Rapid Start Technology is disabled.
- Drives in MBR format with more than four extended partitions.
- Swap file located on a non-system drive.
- Multiboot system with several simultaneously installed operating systems.
- Dynamic partitions (only primary partitions are supported).
- Drives with less than 0.5% free unfragmented disk space.
- Drives with a sector size different from 512 bytes or 4096 bytes that emulate 512 bytes.
- Hybrid drives.

Changing the length of the encryption key (AES56 / AES256)

Kaspersky Endpoint Security uses the Advanced Encryption Standard (AES) encryption algorithm. Kaspersky Endpoint Security supports the AES encryption algorithm with an effective key length of 256 or 56 bits. The data encryption algorithm depends on the AES encryption library that is included in the distribution package: *Strong encryption (AES256)* or *Lite encryption (AES56)*. The AES encryption library is installed together with the application.

Changing the length of the encryption key is available only for Kaspersky Endpoint Security 11.2.0 or later.

Changing the encryption key length consists of the following steps:

1. Decrypt objects that Kaspersky Endpoint Security encrypted before you begin changing the encryption key length:
 - a. [Decrypt hard drives.](#)
 - b. [Decrypt files on local drives.](#)
 - c. [Decrypt removable drives.](#)

After the encryption key length is changed, objects that were previously encrypted become unavailable.

2. [Remove Kaspersky Endpoint Security.](#)
3. [Install Kaspersky Endpoint Security](#) from the Kaspersky Endpoint Security distribution package containing a different encryption library.

You can also change the encryption key length by upgrading the application. The key length can be changed through an application upgrade only if the following conditions are met:

- Kaspersky Endpoint Security version 10 Service Pack 2 or later is installed on the computer.
- Data encryption components (File Level Encryption, Full Disk Encryption) are not installed on the computer.
By default, data encryption components are not included in Kaspersky Endpoint Security. The BitLocker Management component does not affect the change in the length of the encryption key.

To change the encryption key length, run the `kes_win.msi` or `setup_kes.exe` file from the distribution package containing the necessary encryption library. You can also remotely upgrade the application by using the installation package.

It is impossible to change the length of the encryption key using the distribution package of the same version of the application that is installed on your computer without first uninstalling the application.

Kaspersky Disk Encryption

Kaspersky Disk Encryption is available only for computers running a Windows operating system for workstations. For computers running a Windows operating system for servers, use BitLocker Drive Encryption technology.

Kaspersky Endpoint Security supports full disk encryption in FAT32, NTFS and exFat file systems.

For optimal computer performance after encryption, it is required that the processor supports AES-NI instruction set (Intel Advanced Encryption Standard New Instructions). If the processor does not support AES-NI, computer performance might decrease.

Before starting full disk encryption, the application runs a series of checks to determine if the device can be encrypted, which includes checking the system hard drive for compatibility with Authentication Agent or with BitLocker encryption components. To check for compatibility, the computer must be restarted. After the computer has been rebooted, the application performs all the necessary checks automatically. If the compatibility check is successful, full disk encryption starts after the operating system has loaded and the application has started. If the system hard drive is found to be incompatible with Authentication Agent or with BitLocker encryption components, the computer must be restarted by pressing the Reset hardware button. Kaspersky Endpoint Security logs information about the incompatibility. Based on this information, the application does not start full disk encryption at operating system startup. Information about this event is logged in Kaspersky Security Center reports.

If the hardware configuration of the computer has changed, the incompatibility information logged by the application during the previous check should be deleted in order to check the system hard drive for compatibility with Authentication Agent and BitLocker encryption components. To do so, prior to full disk encryption, type `avp pbatestreset` in the command line. If the operating system fails to load after the system hard drive has been checked for compatibility with Authentication Agent, [you must remove the objects and data remaining after test operation of Authentication Agent](#) by using the Restore Utility and then start Kaspersky Endpoint Security and execute the `avp pbatestreset` command again.

After full disk encryption has started, Kaspersky Endpoint Security encrypts all data that is written to hard drives.

If the user shuts down or restarts the computer during full disk encryption, Authentication Agent is loaded before the next startup of the operating system. Kaspersky Endpoint Security resumes full disk encryption after successful authentication in Authentication Agent and operating system startup.

If the operating system switches to hibernation mode during full disk encryption, Authentication Agent is loaded when the operating system switches back from hibernation mode. Kaspersky Endpoint Security resumes full disk encryption after successful authentication in Authentication Agent and operating system startup.

If the operating system goes into sleep mode during full disk encryption, Kaspersky Endpoint Security resumes full disk encryption when the operating system comes out of sleep mode without loading Authentication Agent.

User authentication in the Authentication Agent can be performed in two ways:

- Enter the name and password of the Authentication Agent account created by the LAN administrator using Kaspersky Security Center tools.
- Enter the password of a token or smart card connected to the computer.

Use of a token or smart card is available only if the computer hard drives were encrypted using the AES256 encryption algorithm. If the computer hard drives were encrypted using the AES56 encryption algorithm, addition of the electronic certificate file to the command will be denied.

The authentication agent supports keyboard layouts for the following languages:

- English (UK)
- English (USA)
- Arabic (Algeria, Morocco, Tunis; AZERTY layout)
- Spanish (Latin America)
- Italian
- German (Germany and Austria)
- German (Switzerland)
- Portuguese (Brazil, ABNT2 layout)
- Russian (for 105-key IBM / Windows keyboards with the QWERTY layout)
- Turkish (QWERTY layout)
- French (France)
- French (Switzerland)
- French (Belgium, AZERTY layout)
- Japanese (for 106-key keyboards with the QWERTY layout)

A keyboard layout becomes available in the Authentication Agent if this layout has been added in the language and regional standards settings of the operating system and has become available on the welcome screen of Microsoft Windows.

If the Authentication Agent account name contains symbols that cannot be entered using keyboard layouts available in the Authentication Agent, encrypted hard drives can be accessed only after they are restored using the Restore Utility or after [the Authentication Agent account name and password are restored](#).

Full disk encryption using Kaspersky Disk Encryption technology

Prior to starting full disk encryption, you are advised to make sure that the computer is not infected. To do so, start the Full Scan or Critical Areas Scan task. Performing full disk encryption on a computer that is infected by a rootkit may cause the computer to become inoperable.

To perform full disk encryption using Kaspersky Disk Encryption technology:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Data Encryption** → **Full Disk Encryption**.
6. In the **Encryption technology** drop-down list, select **Kaspersky Disk Encryption**.

Kaspersky Disk Encryption technology cannot be used if the computer has hard drives that were encrypted by BitLocker.

7. In the **Encryption mode** drop-down list, select **Encrypt all hard drives**.

If the computer has several operating systems installed, after encrypting all hard drives you will be able to load only the operating system that has the application installed.

If you need to exclude some of the hard drives from encryption, [create a list of such hard drives](#).

8. Select one of the following encryption methods:
 - If you want to apply encryption only to those hard drive sectors that are occupied by files, select the **Encrypt used disk space only** check box.

If you are applying encryption on a drive that is already in use, it is recommended to encrypt the entire drive. This ensures that all data is protected – even deleted data that might still contain retrievable information. The **Encrypt used disk space only** function is recommended for new drives that have not been previously used.

- If you want to apply encryption to the entire hard drive, clear the **Encrypt used disk space only** check box.

If a device was previously encrypted using the **Encrypt used disk space only** function, after applying a policy in **Encrypt all hard drives** mode, sectors that are not occupied by files will still not be encrypted.

9. If a hardware incompatibility problem occurs during computer encryption, you can select the **Use Legacy USB Support** check box.

Legacy USB Support is a BIOS/UEFI function that allows you to use USB devices (such as a security token) during the computer's boot phase before starting the operating system (BIOS mode). Legacy USB Support does not affect support for USB devices after the operating system is started.

When the Legacy USB Support function is enabled, the Authentication Agent in BIOS mode does not support working with tokens via USB. It is recommended to use this option only when there is a hardware compatibility issue and only for those computers on which the problem occurred.

10. Save your changes.

If system hard drives are encrypted, the Authentication Agent loads before startup of the operating system. Use the Authentication Agent to complete authentication for obtaining access to encrypted system hard drives and load the operating system. After successful completion of the authentication procedure, the operating system loads. The authentication process is repeated every time the operating system restarts.

Creating a list of hard drives excluded from encryption

You can create a list of exclusions from encryption only for Kaspersky Disk Encryption technology.

To form a list of hard drives excluded from encryption:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Data Encryption** → **Full Disk Encryption**.
6. In the **Encryption technology** drop-down list, select the **Kaspersky Disk Encryption** option.

Entries corresponding to hard drives excluded from encryption appear in the **Do not encrypt the following hard drives** table. This table is empty if you have not previously formed a list of hard drives excluded from encryption.

7. To add hard drives to the list of hard drives excluded from encryption:

a. Click the **Add** button.

The **Add devices from Kaspersky Security Center list** window opens.

b. In the **Add devices from Kaspersky Security Center list** window, specify the values of the following parameters: **Name**, **Computer**, **Disk type**, and **Kaspersky Disk Encryption**.

c. Click the **Refresh** button.

d. In the **Name** column, select the check boxes in the table rows corresponding to those hard drives that you want to add to the list of hard drives excluded from encryption.

e. Click **OK**.

The selected hard drives appear in the **Do not encrypt the following hard drives** table.

8. If you want to remove hard drives from the table of exclusions, select one or several rows in the **Do not encrypt the following hard drives** table and click the **Delete** button.

To select multiple rows in the table, select them while holding down the **CTRL** key.

9. Save your changes.

Enabling Single Sign-On (SSO) technology

Single Sign-On (SSO) technology allows you to automatically log into the operating system using the credentials of the Authentication Agent.

When using Single Sign-on technology, the Authentication Agent ignores the password strength requirements specified in Kaspersky Security Center. You can set the password strength requirements in the operating system settings.

Single Sign-On technology is incompatible with third-party providers of account credentials.

[How to enable the use of Single Sign-On technology in the Administration Console \(MMC\)](#) 

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Data Encryption** → **Common Encryption Settings**.
6. In the **Password settings** section, click the **Settings** button.
7. In the window that opens, on the **Authentication Agent** tab, select the **Use Single Sign-On (SSO) technology** check box.
8. Save your changes.

As a result, the user needs to complete the authentication procedure only once with the Agent. The authentication procedure is not required for loading the operating system. The operating system loads automatically.

[How to enable use of Single Sign-On in the Web Console [?]](#)

1. In the main window of Web Console, select the **Devices** → **Policies and policy profiles** tab.
2. Click the name of the Kaspersky Endpoint Security policy for computers on which you want to enable use of Single Sign-On.
The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Data Encryption** → **Full Disk Encryption**.
5. Select the **Kaspersky Disk Encryption** technology and follow the link to configure the settings.
The encryption settings open.
6. In the **Password settings** section, select the **Use Single Sign-On (SSO) technology** check box.
7. Click **OK**.

As a result, the user needs to complete the authentication procedure only once with the Agent. The authentication procedure is not required for loading the operating system. The operating system loads automatically.

For Single Sign-On to work, the Windows account password and the password for the Authentication Agent account must match. If the passwords do not match, the user needs to perform the authentication procedure twice: in the interface of the Authentication Agent and before loading the operating system. After that, Kaspersky Endpoint Security replaces the password of the Authentication Agent account with the password of the Windows account.

Managing Authentication Agent accounts

Authentication Agent is needed for working with drives that are protected using Kaspersky Disk Encryption (FDE) technology. Before the operating system is loaded, the user needs to complete authentication with the Agent. The *Manage Authentication Agent accounts* task is designed for configuring user authentication settings. You can use local tasks for individual computers as well as group tasks for computers from separate administration groups or a selection of computers.

You cannot configure a schedule for starting the *Manage Authentication Agent accounts* task. It is also impossible to forcibly stop a task.

[How to create the Manage Authentication Agent accounts task in the Administration Console \(MMC\)](#) 

1. In the Administration Console, go to the folder **Administration Server** → **Tasks**.

The list of tasks opens.

2. Click the **New task** button.

The Task Wizard starts. Follow the instructions of the Wizard.

Step 1. Selecting task type

Select **Kaspersky Endpoint Security for Windows (11.4.0)** → **Manage Authentication Agent accounts**.

Step 2. Selecting an Authentication Agent account management command

Generate a list of Authentication Agent account management commands. Management commands allow you to add, modify, and delete Authentication Agent accounts (see instructions below). Only users who have an Authentication Agent account can complete the authentication procedure, load the operating system, and gain access to the encrypted drive.

Step 3. Selecting the devices to which the task will be assigned

Select the computers on which the task will be performed. The following options are available:

- Assign the task to an administration group. In this case, the task is assigned to computers included in a previously created administration group.
- Select computers detected by the Administration Server in the network: *unassigned devices*. The specific devices can include devices in administration groups as well as unassigned devices.
- Specify device addresses manually, or import addresses from a list. You can specify NetBIOS names, IP addresses, and IP subnets of devices to which you want to assign the task.

Step 4. Defining the task name

Enter a name for the task, for example, `Administrator Accounts`.

Step 5. Completing task creation

Exit the Wizard. If necessary, select the **Run task after Wizard finishes** check box. You can monitor the progress of the task in the task properties.

As a result, after the task is completed at the next computer startup, the new user can complete the authentication procedure, load the operating system, and gain access to the encrypted drive.

[How to create the Manage Authentication Agent accounts task in the Web Console](#) 

1. In the main window of Web Console, select **Devices** → **Tasks**.

The list of tasks opens.

2. Click the **Add** button.

The Task Wizard starts. Follow the instructions of the Wizard.

Step 1. Configuring general task settings

Configure the general task settings:

1. In the **Application** drop-down list, select **Kaspersky Endpoint Security for Windows (11.4.0)**.

2. In the **Task type** drop-down list, select **Manage Authentication Agent accounts**.

3. In the **Task name** field, enter a brief description, such as **Administrator accounts**.

4. In the **Select devices to which the task will be assigned** section, select the task scope.

Step 2. Managing Authentication Agent accounts

Generate a list of Authentication Agent account management commands. Management commands allow you to add, modify, and delete Authentication Agent accounts (see instructions below). Only users who have an Authentication Agent account can complete the authentication procedure, load the operating system, and gain access to the encrypted drive.

Step 3. Completing task creation

Finish the wizard by clicking the **Finish** button. A new task will be displayed in the list of tasks.

To run a task, select the check box opposite the task and click the **Start** button.

As a result, after the task is completed at the next computer startup, the new user can complete the authentication procedure, load the operating system, and gain access to the encrypted drive.

To add an Authentication Agent account, you need to add a special command to the *Manage Authentication Agent accounts* task. It is convenient to use a group task, for example, to add an administrator account to all computers.

Kaspersky Endpoint Security allows you to automatically create Authentication Agent accounts before encrypting a drive. You can enable automatic creation of Authentication Agent accounts in the [Full Disk Encryption policy settings](#). You can also [use Single Sign-On \(SSO\) technology](#).

[How to add an Authentication Agent account through the Administration Console \(MMC\)](#) 

1. Open the properties of the *Manage Authentication Agent accounts* task.
2. In the task properties, select the **Options** section.
3. Click **Add** → **Account adding command**.
4. In the window that opens, in the **Windows account** field, specify the name of the Microsoft Windows account that will be used to create the Authentication Agent account.
5. If you manually entered the Windows account name, click the **Allow** button to define the account security identifier (SID).
If you choose not to determine the security identifier (SID) by clicking the **Allow** button, it will be determined when the task is performed on the computer.

Defining a Windows account security identifier is necessary to verify that the Windows account name was entered correctly. If the Windows account does not exist on the computer or in the trusted domain, the *Manage Authentication Agent accounts* task will end with an error.

6. Select the **Replace existing account** check box if you want the existing account previously created for the Authentication Agent to be replaced with the account being created.

This step is available when you are adding an Authentication Agent account creation command in the properties of a group task for managing Authentication Agent accounts. This step is not available if you add a command for creating Authentication Agent account in the properties of the **Full Disk Encryption, account management** local task.

7. In the **User name** field, type the name of the Authentication Agent account that must be entered during authentication for access to encrypted hard drives.
8. Select the **Allow password-based authentication** check box if you want the application to prompt the user to enter the Authentication Agent account password during authentication for accessing encrypted hard drives. Set a password for the Authentication Agent account. If necessary, you can request a new password from the user after the first authentication.
9. Select the **Allow certificate-based authentication** check box if you want the application to prompt the user to connect a token or smart card to the computer during authentication for accessing encrypted hard drives. Select a certificate file for authentication with a smart card or token.
10. If required, in the **Command description** field, enter the Authentication Agent account details that you need for managing the command.
11. Do one of the following:
 - Select the **Allow authentication** option if you want the application to allow the user working under the account specified in the command to access the authentication dialog in Authentication Agent.
 - Select the **Block authentication** option if you want the application to block the user working under the account specified in the command from accessing the authentication dialog in Authentication Agent.
12. Save your changes.

[How to add an Authentication Agent account through the Web Console](#)

1. In the main window of Web Console, select **Devices** → **Tasks**.

The list of tasks opens.

2. Click the **Manage Authentication Agent accounts** task of Kaspersky Endpoint Security.

The task properties window opens.

3. Select the **Application settings** tab.

4. In the list of Authentication Agent accounts, click the **Add** button.

This starts the Authentication Agent Account Management Wizard.

5. Select the **Add account** command type.

6. Select a user account. You can select an account from the list of domain accounts or manually enter the account name. Click the **Next** button.

Kaspersky Endpoint Security determines the account security identifier (SID). This is necessary to verify the account. If you entered the user name incorrectly, Kaspersky Endpoint Security will end the task with an error.

7. Configure the Authentication Agent account settings.

- **Create a new Authentication Agent account to replace the existing account.** Kaspersky Endpoint Security scans existing accounts on the computer. If the user security identifier on the computer and in the task match, Kaspersky Endpoint Security will change the account settings in accordance with the task.
- **User name.** The default user name of the Authentication Agent account corresponds to the domain name of the user.
- **Allow password-based authentication.** Set a password for the Authentication Agent account. If necessary, you can request a new password from the user after the first authentication. This way, each user will have their own unique password. You can also set password strength requirements for the Authentication Agent account in the policy.
- **Allow certificate-based authentication.** Select a certificate file for authentication with a smart card or token. This way, the user will need to enter the password for the smart card or token.
- **Account access to encrypted data.** Configure user access to the encrypted drive. You can, for example, temporarily disable user authentication instead of deleting the Authentication Agent account.
- **Comment.** Enter an account description, if necessary.

8. Save your changes.

9. Select the check box next to the task and click the **Start** button.

As a result, after the task is completed at the next computer startup, the new user can complete the authentication procedure, load the operating system, and gain access to the encrypted drive.

To change the password and other data of the Authentication Agent account, you need to add a special command to the *Manage Authentication Agent accounts* task. It is convenient to use a group task, for example, to replace the administrator token certificate on all computers.

[How to change the Authentication Agent account through the Administration Console \(MMC\) !\[\]\(8af806fb1314382d09bc5ec5b767526c_img.jpg\)](#)

1. Open the properties of the *Manage Authentication Agent accounts* task.
2. In the task properties, select the **Options** section.
3. Click **Add** → **Account editing command**.
4. In the window that opens, in the **Windows account** field, specify the name of the Microsoft Windows user account that you want to change.
5. If you manually entered the Windows account name, click the **Allow** button to define the account security identifier (SID).
If you choose not to determine the security identifier (SID) by clicking the **Allow** button, it will be determined when the task is performed on the computer.

Defining a Windows account security identifier is necessary to verify that the Windows account name was entered correctly. If the Windows account does not exist on the computer or in the trusted domain, the *Manage Authentication Agent accounts* task will end with an error.

6. Select the **Change user name** check box and enter a new name for the Authentication Agent account if you want Kaspersky Endpoint Security to change the user name for all Authentication Agent accounts created using the Microsoft Windows account with the name indicated in the **Windows account** field to the name typed in the field below.
7. Select the **Modify password-based authentication settings** check box to make password-based authentication settings editable.
8. Select the **Allow password-based authentication** check box if you want the application to prompt the user to enter the Authentication Agent account password during authentication for accessing encrypted hard drives. Set a password for the Authentication Agent account.
9. Select the **Edit the rule of password change upon authentication in Authentication Agent** check box if you want Kaspersky Endpoint Security to change the value of the password change setting for all Authentication Agent accounts created using the Microsoft Windows account with the name indicated in the **Windows account** field to the setting value specified below.
10. Specify the value of the password change setting upon authentication in Authentication Agent.
11. Select the **Modify certificate-based authentication settings** check box to make settings of authentication based on the electronic certificate of a token or smart card editable.
12. Select the **Allow certificate-based authentication** check box if you want the application to prompt the user to enter the password to the token or smart card connected to the computer during the authentication process in order to access encrypted hard drives. Select a certificate file for authentication with a smart card or token.
13. Select the **Edit command description** check box and edit the command description if you want Kaspersky Endpoint Security to change the command description for all Authentication Agent accounts created using the Microsoft Windows account with the name indicated in the **Windows account** field.
14. Select the **Edit the rule of access to authentication in Authentication Agent** check box if you want Kaspersky Endpoint Security to change the rule for user access to the authentication dialog in Authentication Agent to the value specified below for all Authentication Agent accounts created using the Microsoft Windows account with the name indicated in the **Windows account** field.

15. Specify the rule for accessing the authentication dialog in Authentication Agent.

16. Save your changes.

[How to change the Authentication Agent account through the Web Console](#) 

1. In the main window of Web Console, select **Devices** → **Tasks**.

The list of tasks opens.

2. Click the **Manage Authentication Agent accounts** task of Kaspersky Endpoint Security.

The task properties window opens.

3. Select the **Application settings** tab.

4. In the list of Authentication Agent accounts, click the **Add** button.

This starts the Authentication Agent Account Management Wizard.

5. Select the **Edit account** command type.

6. Select a user account. You can select an account from the list of domain accounts or manually enter the account name. Click the **Next** button.

Kaspersky Endpoint Security determines the account security identifier (SID). This is necessary to verify the account. If you entered the user name incorrectly, Kaspersky Endpoint Security will end the task with an error.

7. Select the check boxes next to the settings that you want to edit.

8. Configure the Authentication Agent account settings.

- **Create a new Authentication Agent account to replace the existing account.** Kaspersky Endpoint Security scans existing accounts on the computer. If the user security identifier on the computer and in the task match, Kaspersky Endpoint Security will change the account settings in accordance with the task.
- **User name.** The default user name of the Authentication Agent account corresponds to the domain name of the user.
- **Allow password-based authentication.** Set a password for the Authentication Agent account. If necessary, you can request a new password from the user after the first authentication. This way, each user will have their own unique password. You can also set password strength requirements for the Authentication Agent account in the policy.
- **Allow certificate-based authentication.** Select a certificate file for authentication with a smart card or token. This way, the user will need to enter the password for the smart card or token.
- **Account access to encrypted data.** Configure user access to the encrypted drive. You can, for example, temporarily disable user authentication instead of deleting the Authentication Agent account.
- **Comment.** Enter an account description, if necessary.

9. Save your changes.

10. Select the check box next to the task and click the **Start** button.

To delete an Authentication Agent account, you need to add a special command to the *Manage Authentication Agent accounts* task. It is convenient to use a group task, for example, to delete the account of a dismissed employee.

[How to delete an Authentication Agent account through the Administration Console \(MMC\)](#) 

1. Open the properties of the *Manage Authentication Agent accounts* task.
2. In the task properties, select the **Options** section.
3. Click **Add** → **Account deletion command**.
4. In the window that opens, in the **Windows account** field, specify the name of the Windows user account that was used to create the Authentication Agent account that you want to delete.
5. If you manually entered the Windows account name, click the **Allow** button to define the account security identifier (SID).
If you choose not to determine the security identifier (SID) by clicking the **Allow** button, it will be determined when the task is performed on the computer.

Defining a Windows account security identifier is necessary to verify that the Windows account name was entered correctly. If the Windows account does not exist on the computer or in the trusted domain, the *Manage Authentication Agent accounts* task will end with an error.

6. Save your changes.

[How to delete an Authentication Agent account through the Web Console](#)

1. In the main window of Web Console, select **Devices** → **Tasks**.
The list of tasks opens.
2. Click the **Manage Authentication Agent accounts** task of Kaspersky Endpoint Security.
The task properties window opens.
3. Select the **Application settings** tab.
4. In the list of Authentication Agent accounts, click the **Add** button.
This starts the Authentication Agent Account Management Wizard.
5. Select the **Remove account** command type.
6. Select a user account. You can select an account from the list of domain accounts or manually enter the account name.
7. Save your changes.
8. Select the check box next to the task and click the **Start** button.

As a result, after the task is completed at the next computer startup, the user will not be able to complete the authentication procedure and load the operating system. Kaspersky Endpoint Security will deny access to encrypted data.

To view the list of users who can complete authentication with the Agent and load the operating system, you need to go to the properties of the managed computer.

[How to view the list of Authentication Agent accounts through the Administration Console \(MMC\) [?]](#)

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Devices** tab.
4. Double-click to open the computer properties window.
5. In the computer properties window, select the **Tasks** section.
The list of local tasks opens.
6. Select the **Manage Authentication Agent accounts** task.
7. In the task properties, select the **Options** section.

As a result, you will be able to access a list of Authentication Agent accounts on this computer. Only users from the list can complete authentication with the Agent and load the operating system.

[How to view a list of Authentication Agent accounts through the Web Console [?]](#)

1. In the main window of Web Console, select **Devices** → **Managed devices**.
2. Click the name of the computer on which you want to view the list of Authentication Agent accounts.
This opens the computer properties.
3. In the computer properties window, select the **Tasks** section.
The list of local tasks opens.
4. Select the **Manage Authentication Agent accounts** task.
5. In the task properties, select the **Application Settings** tab.

As a result, you will be able to access a list of Authentication Agent accounts on this computer. Only users from the list can complete authentication with the Agent and load the operating system.

Using a token and smart card with Authentication Agent

A token or smart card can be used for authentication when accessing encrypted hard drives. To do so, you must add the electronic certificate file of a token or smart card to the *Manage Authentication Agent accounts* task.

Use of a token or smart card is available only if the computer hard drives were encrypted using the AES256 encryption algorithm. If the computer hard drives were encrypted using the AES56 encryption algorithm, addition of the electronic certificate file to the command will be denied.

Kaspersky Endpoint Security supports the following tokens, smart card readers, and smart cards:

- SafeNet eToken PRO 64K (4.2b) (USB).
- SafeNet eToken PRO 72K Java (USB).
- SafeNet eToken PRO 72K Java (Smart Card).
- SafeNet eToken 4100 72K Java (Smart Card).
- SafeNet eToken 5100 (USB).
- SafeNet eToken 5105 (USB).
- SafeNet eToken 7300 (USB).
- EMC RSA SecurID 800 (USB).
- Rutoken EDS (USB).
- Rutoken EDS (Flash).
- Aladdin-RD JaCarta PKI (USB).
- Aladdin-RD JaCarta PKI (Smart Card).
- Athena IDProtect Laser (USB).
- Gemalto IDBridge CT40 (Reader).
- Gemalto IDPrime .NET 511.

To add the file of a token or smart card electronic certificate to the command for creating an Authentication Agent account, you must first save the file using third-party software for managing certificates.

The token or smart-card certificate must have the following properties:

- The certificate must be compliant with the X.509 standard, and the certificate file must have DER encoding.
- The certificate contains an RSA key with a length of at least 1024 bits.

If the electronic certificate of the token or smart card does not meet these requirements, you cannot load the certificate file into the command for creating an Authentication Agent account.

The `KeyUsage` parameter of the certificate must have the value `keyEncipherment` or `dataEncipherment`. The `KeyUsage` parameter determines the purpose of the certificate. If the parameter has a different value, Kaspersky Security Center will download the certificate file but will display a warning.

If a user has lost a token or smart card, the administrator must add the file of a token or smart card electronic certificate to the command for creating an Authentication Agent account. Then the user must complete the procedure for [receiving access to encrypted devices or restoring data on encrypted devices](#).

Hard drive decryption

You can decrypt hard drives even if there is no active license permitting data encryption.

To decrypt hard drives:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Data Encryption** → **Full Disk Encryption**.
6. In the **Encryption technology** drop-down list, select the technology with which the hard drives were encrypted.
7. Do one of the following:
 - In the **Encryption mode** drop-down list, select the **Decrypt all hard drives** option if you want to decrypt all encrypted hard drives.
 - Add the encrypted hard drives that you want to decrypt to the **Do not encrypt the following hard drives** table.

This option is available only for Kaspersky Disk Encryption technology.

8. Save your changes.

If the user shuts down or restarts the computer during decryption of hard drives that were encrypted using Kaspersky Disk Encryption technology, the Authentication Agent loads before the next startup of the operating system. Kaspersky Endpoint Security resumes hard drive decryption after successful authentication in the authentication agent and operating system startup.

If the operating system switches to hibernation mode during decryption of hard drives that were encrypted using Kaspersky Disk Encryption technology, Authentication Agent loads when the operating system comes out of hibernation mode. Kaspersky Endpoint Security resumes hard drive decryption after successful authentication in the authentication agent and operating system startup. After hard drive decryption, hibernation mode is unavailable until the first reboot of the operating system.

If the operating system goes into sleep mode during hard drive decryption, Kaspersky Endpoint Security resumes hard drive decryption when the operating system comes out of sleep mode without loading the Authentication Agent.

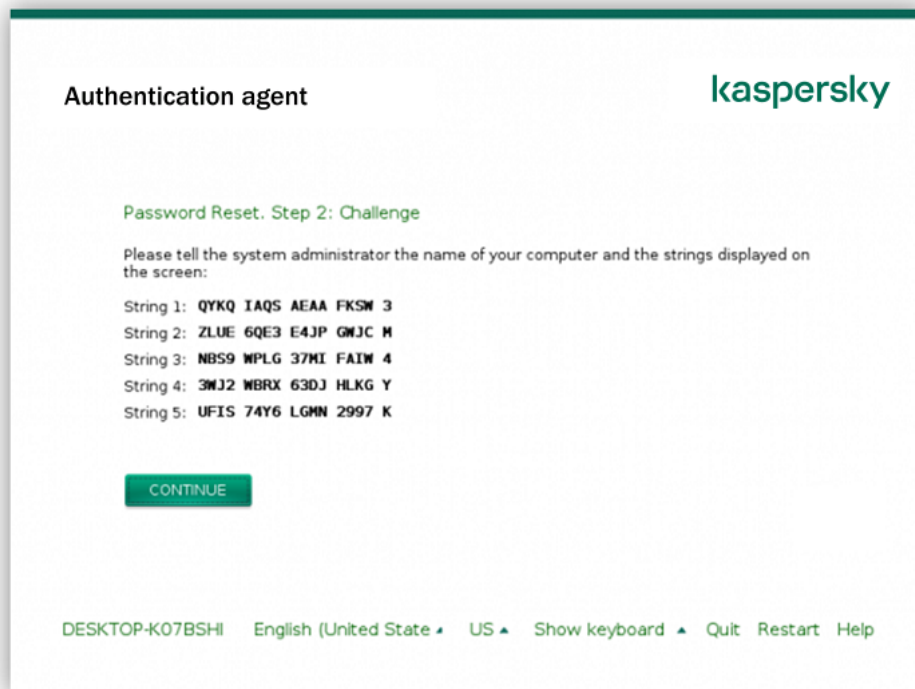
Restoring access to a drive protected by Kaspersky Disk Encryption technology

If a user has forgotten the password for accessing a hard drive protected by Kaspersky Disk Encryption technology, you need to start the recovery procedure (Request-Response).

Restoring access to the system hard drive

Restoring access to a system hard drive protected by Kaspersky Disk Encryption technology consists of the following steps:

1. The user reports the request blocks to the administrator (see the figure below).
2. The administrator enters the request blocks into Kaspersky Security Center, receives the response blocks and reports the response blocks to the user.
3. The user enters the response blocks in the Authentication Agent interface and obtains access to the hard drive.



Restoring access to a system hard drive protected by Kaspersky Disk Encryption technology

To start the recovery procedure, the user needs to click the **Forgot your password** button in the Authentication Agent interface.

[How to obtain response blocks for a system hard drive protected by Kaspersky Disk Encryption technology in the Administration Console \(MMC\)](#)

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Devices** tab.
4. On the **Devices** tab, select the computer of the user requesting access to encrypted data and right-click to open the context menu.
5. In the context menu, select **Grant access in offline mode**.
6. In the window that opens, select the **Authentication Agent** tab.
7. In the **Encryption algorithm in use** section, select an encryption algorithm: **AES56** or **AES256**.

The data encryption algorithm depends on the AES encryption library that is included in the distribution package: *Strong encryption (AES256)* or *Lite encryption (AES56)*. The AES encryption library is installed together with the application.
8. In the **Account** drop-down list, select the name of the Authentication Agent account of the user who requested recovery of access to the drive.
9. In the **Hard drive** drop-down list, select the encrypted hard drive for which you need to recover access.
10. In the **User request** section enter the blocks of request dictated by the user.

As a result, the contents of the blocks of the response to the user's request for recovery of the user name and password of an Authentication Agent account will be displayed in the **Access key** field. Convey the contents of the response blocks to the user.

[How to obtain response blocks for a system hard drive protected by Kaspersky Disk Encryption technology in the Web Console](#)

1. In the main window of Web Console, select **Devices** → **Managed devices**.
2. Select the check box next to the name of the computer whose drive you want to restore access to.
3. Click the **Share this device offline** button.
4. In the window that opens, select the **Authentication Agent** section.
5. In the **Account** drop-down list, select the name of the Authentication Agent account created for the user who is requesting recovery of the Authentication Agent account name and password.
6. Enter the request blocks conveyed by the user.

The contents of the blocks of the response to the user's request for recovery of the user name and password of the Authentication Agent account will be displayed at the bottom of the window. Convey the contents of the response blocks to the user.

After completing the recovery procedure, the Authentication Agent will prompt the user to change the password.

Restoring access to a non-system hard drive

Restoring access to a non-system hard drive protected by Kaspersky Disk Encryption technology consists of the following steps:

1. The user sends a request access file to the administrator.
2. The administrator adds the request access file to Kaspersky Security Center, creates an access key file and sends the file to the user.
3. The user adds the access key file to Kaspersky Endpoint Security and obtains access to the hard drive.

To start the recovery procedure, the user needs to attempt to access a hard drive. As a result, Kaspersky Endpoint Security will create a request access file (a file with the KESDC extension), which the user needs to send to the administrator, for example, by email.

[How to obtain an access key file for an encrypted non-system hard drive in the Administration Console \(MMC\)](#)

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Devices** tab.
4. On the **Devices** tab, select the computer of the user requesting access to encrypted data and right-click to open the context menu.
5. In the context menu, select **Grant access in offline mode**.
6. In the window that opens, select the **Data Encryption** tab.
7. On the **Data Encryption** tab, click the **Browse** button.
8. In the window for selecting a request access file, specify the path to the file received from the user.

You will see information about the user's request. Kaspersky Security Center generates a key file. Email the generated encrypted data access key file to the user. Or save the access file and use any available method to transfer the file.

[How to obtain an encrypted non-system hard drive access key file in the Web Console](#)

1. In the main window of Web Console, select **Devices** → **Managed devices**.
 2. Select the check box next to the name of the computer whose data you want to restore access to.
 3. Click the **Share this device offline** button.
 4. Select the **Data Encryption** section.
 5. Click the **Select file** button and select the request access file that you received from the user (a file with the KESDC extension).
The Web Console will display information about the request. This will include the name of the computer on which the user is requesting access to the file.
 6. Click the **Save key** button and select a folder to save the encrypted data access key file (a file with the KESDR extension).
- As a result, you will be able to obtain the encrypted data access key, which you will need to transfer to the user.

Updating the operating system

There are a number of special considerations for updating the operating system of a computer that is protected by Full Disk Encryption (FDE). Update the operating system as follows: first update the OS on one computer, then update the OS on a small portion of the computers, then update the OS on all computers of the network.

If you are using Kaspersky Disk Encryption technology, Authentication Agent is loaded before the operating system is started. Using Authentication Agent, the user can sign in to the system and receive access to encrypted drives. Then the operating system begins loading.

If you start an update of the operating system on a computer that is protected using Kaspersky Disk Encryption technology, the OS Update Wizard will remove Authentication Agent. As a result, the computer can be locked because the OS loader will not be able to access the encrypted drive.

For details about updating the operating system safely, refer to the [Technical Support Knowledge Base](#).

Automatic updating of the operating system is available under the following conditions:

1. The operating system is updated through WSUS (Windows Server Update Services).
2. Windows 10 version 1607 (RS1) or later is installed on the computer.
3. Kaspersky Endpoint Security version 11.2.0 or later is installed on the computer.

If all the conditions are met, you can update the operating system in the usual way.

If you are using BitLocker Drive Encryption technology, you do not need to decrypt the hard drives to update Windows 10. For more details on BitLocker, please visit the [Microsoft website](#).

Eliminating errors of encryption functionality update

Full Disk Encryption is updated when a previous version of the application is upgraded to Kaspersky Endpoint Security 11.4.0 for Windows.

When starting update of the Full Disk Encryption functionality the following errors may occur:

- Unable to initialize update.
- Device is incompatible with Authentication Agent.

To eliminate errors that occurred when you start update process of the Full Disk Encryption functionality in the new application version:

1. [Decrypt hard drives](#).
2. [Encrypt hard drives](#) once again.

During update of the Full Disk Encryption functionality the following errors may occur:

- Unable to complete the update.
- Full Disk Encryption upgrade rollback completed with an error.

To eliminate errors that occurred during update process of the Full Disk Encryption functionality,

[restore access to encrypted devices using Restore Utility](#).

Selecting the Authentication Agent tracing level

The application logs service information about the operation of the Authentication Agent and information about the user's operations with the Authentication Agent in the trace file.

To select the Authentication Agent tracing level:

1. As soon as a computer with encrypted hard drives starts, press the **F3** button to call up a window for configuring Authentication Agent settings.
2. Select the tracing level in the Authentication Agent settings window:
 - **Disable debug logging (default)**. If this option is selected, the application does not log information about Authentication Agent events in the trace file.
 - **Enable debug logging**. If this option is selected, the application logs information about the operation of the Authentication Agent and the user operations performed with the Authentication Agent in the trace file.
 - **Enable verbose logging**. If this option is selected, the application logs detailed information about the operation of the Authentication Agent and the user operations performed with the Authentication Agent in the trace file.

The level of detail of entries under this option is higher compared to the level of the **Enable debug logging** option. A high level of detail of entries can slow down the startup of the Authentication Agent and the operating system.

- **Enable debug logging and select serial port.** If this option is selected, the application logs information about the operation of the Authentication Agent and the user operations performed with the Authentication Agent in the trace file, and relays it via the COM port.

If a computer with encrypted hard drives is connected to another computer via the COM port, Authentication Agent events can be examined from this other computer.

- **Enable verbose debug logging and select serial port.** If this option is selected, the application logs detailed information about the operation of the Authentication Agent and the user operations performed with the Authentication Agent in the trace file, and relays it via the COM port.

The level of detail of entries under this option is higher compared to the level of the **Enable debug logging and select serial port** option. A high level of detail of entries can slow down the startup of the Authentication Agent and the operating system.

Data is recorded in the Authentication Agent trace file if there are encrypted hard drives on the computer or during full disk encryption.

The Authentication Agent trace file is not sent to Kaspersky, unlike other trace files of the application. If necessary, you can manually send the Authentication Agent trace file to Kaspersky for analysis.

Editing Authentication Agent help texts

Before editing help messages of the Authentication Agent, please review the list of supported characters in a preboot environment (see below).

To edit Authentication Agent help messages:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Data Encryption** → **Common Encryption Settings**.
6. In the **Templates** section, click the **Help** button.
This opens the **Authentication Agent help messages** window.
7. Do the following:

- Select the **Authentication** tab to edit the help text shown in the Authentication Agent window when account credentials are being entered.

- Select the **Change password** tab to edit the help text shown in the Authentication Agent window when the password for the Authentication Agent account is being changed.
- Select the **Recover password** tab to edit the help text shown in the Authentication Agent window when the password for the Authentication Agent account is being recovered.

8. Edit help messages.

If you want to restore the original text, click the **By default** button.

You can enter help text containing 16 lines or less. The maximum length of a line is 64 characters.

9. Save your changes.

Limited support for characters in Authentication Agent help messages

In a preboot environment, the following Unicode characters are supported:

- Basic Latin alphabet (0000 - 007F)
- Additional Latin-1 characters (0080 - 00FF)
- Extended Latin-A (0100 - 017F)
- Extended Latin-B (0180 - 024F)
- Uncombined extended ID characters (02B0 - 02FF)
- Combined diacritical marks (0300 - 036F)
- Greek and Coptic alphabets (0370 - 03FF)
- Cyrillic (0400 - 04FF)
- Hebrew (0590 - 05FF)
- Arabic script (0600 - 06FF)
- Additional extended Latin (1E00 - 1EFF)
- Punctuation marks (2000 - 206F)
- Currency symbols (20A0 - 20CF)
- Letter-like symbols (2100 - 214F)
- Geometric figures (25A0 - 25FF)
- Presentation forms of Arabic script-B (FE70 - FEFF)

Characters that are not specified in this list are not supported in a preboot environment. It is not recommended to use such characters in Authentication Agent help messages.

Removing leftover objects and data after testing the operation of Authentication Agent

During application uninstallation, if Kaspersky Endpoint Security detects objects and data that remained on the system hard drive after test operation of Authentication Agent, application uninstallation is interrupted and becomes impossible until such objects and data are removed.

Objects and data may remain on the system hard drive after test operation of Authentication Agent only in exceptional cases. For example, this can happen if the computer has not been restarted after a Kaspersky Security Center policy with encryption settings was applied, or if the application fails to start after test operation of Authentication Agent.

You can remove objects and data that remained on the system hard drive after test operation of Authentication Agent in the following ways:

- Using the Kaspersky Security Center policy.
- [using Restore Utility](#).

To use a Kaspersky Security Center policy to remove objects and data that remained after test operation of Authentication Agent:

1. Apply to the computer a Kaspersky Security Center policy with settings configured to [decrypt](#) all computer hard drives.
2. Start Kaspersky Endpoint Security.

To remove information about application incompatibility with Authentication Agent,

type the `avp pbatestreset` command in the command line.

BitLocker Management

BitLocker is an encryption technology built into Windows operating systems. Kaspersky Endpoint Security allows you to control and manage BitLocker using Kaspersky Security Center. BitLocker encrypts logical volumes. BitLocker cannot be used for encryption of removable drives. For more details on BitLocker, refer to [Microsoft documentation](#).

BitLocker provides secure storage of access keys using a trusted platform module. A *Trusted Platform Module (TPM)* is a microchip developed to provide basic functions related to security (for example, to store encryption keys). A Trusted Platform Module is usually installed on the computer motherboard and interacts with all other system components via the hardware bus. Using TPM is the safest way to store BitLocker access keys, since TPM provides pre-startup system integrity verification. You can still encrypt drives on a computer without a TPM. In this case, the access key will be encrypted with a password. BitLocker uses the following authentication methods:

- TPM and password.
- TPM and PIN.
- Password.

After encrypting a drive, BitLocker creates a master key. Kaspersky Endpoint Security sends the master key to Kaspersky Security Center so that you can [restore access to the disk](#), for example, if a user has forgotten the password. If a user encrypts a disk using BitLocker, Kaspersky Endpoint Security will send [information about disk encryption to Kaspersky Security Center](#). However, Kaspersky Endpoint Security will not send the master key to Kaspersky Security Center, so it will be impossible to restore access to the disk using Kaspersky Security Center. For BitLocker to work correctly with Kaspersky Security Center, decrypt the drive and re-encrypt the drive using a policy. You can decrypt a drive locally or using a policy.

After encrypting the system hard drive, the user needs to go through BitLocker authentication to boot the operating system. After the authentication procedure, BitLocker will allow for users to log in. BitLocker does not support single sign-on technology (SSO).

If you are using Windows group policies, turn off BitLocker management in the policy settings. Windows policy settings may conflict with Kaspersky Endpoint Security policy settings. When encrypting a drive, errors may occur.

Starting BitLocker Drive Encryption

Prior to starting full disk encryption, you are advised to make sure that the computer is not infected. To do so, start the Full Scan or Critical Areas Scan task. Performing full disk encryption on a computer that is infected by a rootkit may cause the computer to become inoperable.

To use BitLocker Drive Encryption on computers running Windows operating systems for servers, installing the BitLocker Drive Encryption component may be required. Install the component using the operating system tools (*Add Roles and Components Wizard*). For more information about installing BitLocker Drive Encryption, refer to the [Microsoft documentation](#).

[How to run BitLocker Drive Encryption through the Administration Console \(MMC\)](#)

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Data Encryption** → **Full Disk Encryption**.
6. In the **Encryption technology** drop-down list, select **BitLocker Drive Encryption**.
7. In the **Encryption mode** drop-down list, select **Encrypt all hard drives**.

If the computer has several operating systems installed, after encryption you will be able to load only the operating system in which the encryption was performed.

8. Configure advanced BitLocker Drive Encryption options (see table below).
9. Save your changes.

[How to run BitLocker Drive Encryption through the Web Console](#)

1. In the main window of Web Console, select the **Devices** → **Policies and policy profiles** tab.
2. Click the name of Kaspersky Endpoint Security policy for the computers for which you want to start BitLocker Drive Encryption.
The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Data Encryption** → **Full Disk Encryption**.
5. In the **Manage encryption** section, select **BitLocker Drive Encryption**.
6. Click the **BitLocker Drive Encryption** link.
This opens the Bitlocker Drive Encryption settings window.
7. In the **Encryption mode** drop-down list, select **Encrypt all hard drives**.

If the computer has several operating systems installed, after encryption you will be able to load only the operating system in which the encryption was performed.

8. Configure advanced BitLocker Drive Encryption options (see table below).
9. Click **OK**.

After applying the policy on the client computer with Kaspersky Endpoint Security installed, the following queries will be made:

- If a TPM module is available, a PIN code prompt window appears.
- If a TPM module is not available, you will see a password prompt window for preboot authentication.
- If the Federal Information Processing standard compatibility mode is enabled for computer operating system, then in Windows 8 and earlier versions of operating system, a request for connecting a storage device is displayed to save the recovery key file. You can save multiple recovery key files on a single storage device.

After setting a password or a PIN, BitLocker will ask you to restart your computer to complete the encryption. Next, the user needs to go through the BitLocker authentication procedure. After the authentication procedure, the user must log on to the system. After the operating system has loaded, BitLocker will complete the encryption.

If there is no access to encryption keys, the user may [request the local network administrator to provide a recovery key](#) (if the recovery key was not saved earlier on the storage device or was lost).

BitLocker Drive Encryption component settings

Parameter	Description
<p>Enable use of BitLocker authentication requiring preboot keyboard input on slates</p>	<p>This check box enables / disables the use of authentication requiring data input in a preboot environment, even if the platform does not have the capability for preboot input (for example, with touchscreen keyboards on tablets).</p> <div data-bbox="421 987 1493 1144" style="border: 1px solid gray; padding: 5px;"> <p>The touchscreen of tablet computers is not available in the preboot environment. To complete BitLocker authentication on tablet computers, the user must connect a USB keyboard, for example.</p> </div> <p>If the check box is selected, use of authentication requiring preboot input is allowed. It is recommended to use this setting only for devices that have alternative data input tools in a preboot environment, such as a USB keyboard in addition to touchscreen keyboards.</p> <p>If the check box is cleared, BitLocker Drive Encryption is not possible on tablets.</p>
<p>Use hardware encryption</p>	<p>If the check box is selected, the application applies hardware encryption. This lets you increase the speed of encryption and use less computer resources.</p>
<p>Encrypt used disk space only</p>	<p>This check box enables / disables the option that limits the encryption area to only occupied hard drive sectors. This limit lets you reduce encryption time.</p> <div data-bbox="421 1615 1493 1771" style="border: 1px solid gray; padding: 5px;"> <p>After encryption started, enabling / disabling the Encrypt used disk space only function will not change this setting until the hard drives are decrypted. You must select or clear the check box before starting encryption.</p> </div> <p>If the check box is selected, only portions of the hard drive that are occupied by files are encrypted. Kaspersky Endpoint Security automatically encrypts new data as it is added.</p> <p>If the check box is cleared, the entire hard drive is encrypted, including residual fragments of previously deleted and modified files.</p>

This option is recommended for new hard drives whose data has not been modified or deleted. If you are applying encryption on a hard drive that is already in use, it is recommended to encrypt the entire hard drive. This ensures protection of all data, even deleted data that is potentially recoverable.

This check box is cleared by default.

Authentication settings

Use Trusted Platform Module (TPM)

If this option is selected, BitLocker uses a Trusted Platform Module (TPM).

A *Trusted Platform Module (TPM)* is a microchip developed to provide basic functions related to security (for example, to store encryption keys). A Trusted Platform Module is usually installed on the computer motherboard and interacts with all other system components via the hardware bus.

For computers running Windows 7 or Windows Server 2008 R2, only encryption using a TPM module is available. If a TPM module is not installed, BitLocker encryption is not possible. Use of a password on these computers is not supported.

A device equipped with a Trusted Platform Module can create encryption keys that can be decrypted only with the device. A Trusted Platform Module encrypts encryption keys with its own root storage key. The root storage key is stored within the Trusted Platform Module. This provides an additional level of protection against attempts to hack encryption keys.

This action is selected by default.

You can configure the settings for accessing the encryption key:

- **Use PIN.** If this check box is selected, a user can use of a PIN code to obtain access to an encryption key that is stored in a Trusted Platform Module (TPM). If this check box is cleared, users are prohibited from using PIN codes. To access the encryption key, a user must enter the password.
- **Use password if Trusted Platform Module (TPM) is unavailable** If the check box is selected, the user can use a password to obtain access to encryption keys when a Trusted Platform Module (TPM) is not available. If the check box is cleared and the TPM is not available, full disk encryption will not start.

Use password

If this option is selected, Kaspersky Endpoint Security prompts the user for a password when the user attempts to access an encrypted drive.

This option can be selected when a Trusted Platform Module (TPM) is not being used.

Decrypting a hard drive protected by BitLocker

Users can decrypt a disk using the operating system (the *Turn Off BitLocker* function). After that, Kaspersky Endpoint Security will prompt the user to encrypt the disk again. Kaspersky Endpoint Security will be prompting to encrypt the disk unless you enable disk decryption in the policy.

[How to decrypt a hard drive protected by BitLocker through the Administration Console \(MMC\)](#) 

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Data Encryption** → **Full Disk Encryption**.
6. In the **Encryption technology** drop-down list, select **BitLocker Drive Encryption**.
7. In the **Encryption mode** drop-down list, select **Decrypt all hard drives**.
8. Save your changes.

[How to decrypt a hard drive protected by BitLocker through the Web Console](#)

1. In the main window of Web Console, select the **Devices** → **Policies and policy profiles** tab.
2. Click the name of Kaspersky Endpoint Security policy for the computers for which you want to decrypt hard drives.
The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Data Encryption** → **Full Disk Encryption**.
5. Select the **BitLocker Drive Encryption** technology and follow the link to configure the settings.
The encryption settings open.
6. In the **Encryption mode** drop-down list, select **Decrypt all hard drives**.
7. Click **OK**.

Restoring access to a drive protected by BitLocker

If a user has forgotten the password for accessing a hard drive encrypted by BitLocker, you need to start the recovery procedure (Request-Response).

If the computer's operating system has Federal Information Processing standard (FIPS) compatibility mode enabled, then in Windows 8 and older the recovery key file is saved to the removable drive before encryption. To restore access to the drive, insert the removable drive and follow the on-screen instructions.

Restoring access to a hard drive encrypted by BitLocker consists of the following steps:

1. The user tells the administrator the recovery key ID (see the figure below).
2. The administrator verifies the ID of the recovery key in the computer properties in Kaspersky Security Center. The ID that the user provided must match the ID that is displayed in the computer properties.
3. If the recovery key IDs match, the administrator provides the user with the recovery key or sends a recovery key file.

A recovery key file is used for computers running the following operating systems:

- Windows 7
- Windows 8
- Windows Server 2008
- Windows Server 2011
- Windows Server 2012

For all other operating systems, a recovery key is used.

4. The user enters the recovery key and gains access to the hard drive.



Restoring access to a hard drive encrypted by BitLocker

Restoring access to a system drive

To start the recovery procedure, the user needs to press the **Esc** key at the pre-boot authentication stage.

[How to view the recovery key for a system drive encrypted by BitLocker in the Administration Console \(MMC\)](#) 

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Devices** tab.
4. On the **Devices** tab, select the computer of the user requesting access to encrypted data and right-click to open the context menu.
5. In the context menu, select **Grant access in offline mode**.
6. In the window that opens, select the **Access to a BitLocker-protected system drive** tab.
7. Prompt the user for the recovery key ID indicated in the BitLocker password input window, and compare it with the ID in the **Recovery key ID** field.

If the IDs do not match, this key is not valid for restoring access to the specified system drive. Make sure that the name of the selected computer matches the name of the user's computer.

As a result, you will have access to the recovery key or file of the recovery key, which will need to be transferred to the user.

[How to view the recovery key for a BitLocker-encrypted system drive in the Web Console](#) ?

1. In the main window of Web Console, select **Devices** → **Managed devices**.
2. Select the check box next to the name of the computer whose drive you want to restore access to.
3. Click the **Share this device offline** button.
4. In the window that opens, select the **BitLocker** section.
5. Verify the recovery key ID. The ID provided by the user must match the ID that is displayed in the computer settings.

If the IDs do not match, this key is not valid for restoring access to the specified system drive. Make sure that the name of the selected computer matches the name of the user's computer.

6. Click the **Receive key** button.

As a result, you will have access to the recovery key or file of the recovery key, which will need to be transferred to the user.

After the operating system is loaded, the user needs to change the password. To do so, the user needs to open the Control Panel of the operating system and go to the BitLocker settings. In the BitLocker settings, the user needs to clear the old password and set a new one. If the user has not changed the password, you can use the old recovery key the next time the operating system loads.

Restoring access to a non-system drive

To start the recovery procedure, the user needs to click the **Forgot your password** link in the window providing access to the drive. After gaining access to the encrypted drive, the user can enable automatic unlocking of the drive during Windows authentication in the BitLocker settings.

[How to view the recovery key for a non-system drive encrypted by BitLocker in the Administration Console \(MMC\)](#)

1. Open the Kaspersky Security Center Administration Console.
2. In the Administration Console tree, select the **Additional** → **Data encryption and protection** → **Encrypted devices** folder.
3. In the workspace, select the encrypted device for which you want to create an access key file, and in the device context menu select **Get access to the device in Kaspersky Endpoint Security for Windows (11.4.0)**.
4. Prompt the user for the recovery key ID indicated in the BitLocker password input window, and compare it with the ID in the **Recovery key ID** field.

If the IDs do not match, this key is not valid for restoring access to the specified drive. Make sure that the name of the selected computer matches the name of the user's computer.

5. Send the user the key that is indicated in the **Recovery key** field.

[How to view the recovery key for a non-system drive encrypted by BitLocker in the Web Console](#)

1. In the main window of the Web Console, select **Operations** → **Data encryption and protection** → **Encrypted devices**.

2. Select the check box next to the name of the computer whose drive you want to restore access to.

3. Click the **Share this device offline** button.

This starts the Wizard for granting access to a device.

4. Follow the instructions of the Wizard for granting access to a device:

a. Select the **Kaspersky Endpoint Security for Windows** plug-in.

b. Verify the recovery key ID. The ID provided by the user must match the ID that is displayed in the computer settings.

If the IDs do not match, this key is not valid for restoring access to the specified system drive. Make sure that the name of the selected computer matches the name of the user's computer.

c. Click the **Receive key** button.

As a result, you will have access to the recovery key or file of the recovery key, which will need to be transferred to the user.

File Level Encryption on local computer drives

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Windows for workstations. This component is unavailable if Kaspersky Endpoint Security is installed on a computer that runs on Windows for servers.

File encryption has the following special features:

- Kaspersky Endpoint Security encrypts / decrypts files in predefined folders only for local user profiles of the operating system. Kaspersky Endpoint Security does not encrypt or decrypt files in predefined folders of roaming user profiles, mandatory user profiles, temporary user profiles, or redirected folders.
- Kaspersky Endpoint Security does not encrypt files whose modification could harm the operating system and installed applications. For example, the following files and folders with all nested folders are on the list of encryption exclusions:
 - %WINDIR%;
 - %PROGRAMFILES% and %PROGRAMFILES(X86)%;
 - Windows registry files.

The list of encryption exclusions cannot be viewed or edited. While files and folders on the list of encryption exclusions can be added to the encryption list, they will not be encrypted during file encryption.

Encrypting files on local computer drives

Kaspersky Endpoint Security does not encrypt files whose contents are located in OneDrive cloud storage, and blocks the encrypted files from copying to OneDrive cloud storage, if these files are not added to [decryption rule](#).

To encrypt files on local drives:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Data Encryption** → **File Level Encryption**.
6. In the right part of the window, select the **Encryption** tab.
7. In the **Encryption mode** drop-down list, select the **According to rules** item.
8. On the **Encryption** tab, click the **Add** button, and in the drop-down list select one of the following items:
 - a. Select the **Predefined folders** item to add files from folders of local user profiles suggested by Kaspersky experts to an encryption rule.
 - **Documents**. Files in the standard *Documents* folder of the operating system, and its subfolders.
 - **Favorites**. Files in the standard *Favorites* folder of the operating system, and its subfolders.
 - **Desktop**. Files in the standard *Desktop* folder of the operating system, and its subfolders.
 - **Temporary files**. Temporary files related to the operation of applications installed on the computer. For example, Microsoft Office applications create temporary files containing backup copies of documents.
 - **Outlook files**. Files related to the operation of the Outlook mail client: data files (PST), offline data files (OST), offline address book files (OAB), and personal address book files (PAB).
 - b. Select the **Custom folder** item to add a manually entered folder path to an encryption rule.

When adding a folder path, adhere to the following rules:

- Use an environment variable (for example, %FOLDER%\UserFolder\). You can use an environment variable only once and only at the beginning of the path.
- Do not use relative paths. You can use the set `\..\ (e.g. C:\Users\..\UserFolder\). The set \..\ denotes the transition to the parent folder.`
- Do not use the `*` and `?` characters.
- Do not use UNC paths.

- Use ; or , as a separator character.

- c. Select the **Files by extension** item to add individual file extensions to an encryption rule. Kaspersky Endpoint Security encrypts files with the specified extensions on all local drives of the computer.
- d. Select the **Files by groups of extensions** item to add groups of file extensions to an encryption rule (for example, *Microsoft Office Documents*). Kaspersky Endpoint Security encrypts files that have the extensions listed in the groups of extensions on all local drives of the computer.

9. Save your changes.

As soon as the policy is applied, Kaspersky Endpoint Security encrypts the files that are included in the encryption rule and not included in the [decryption rule](#).

File encryption has the following special features:

- If the same file is added to both an encryption rule and a decryption rule, then Kaspersky Endpoint Security performs the following actions:
 - If the file is not encrypted, Kaspersky Endpoint Security does not encrypt this file.
 - If the file is encrypted, Kaspersky Endpoint Security decrypts this file.
- Kaspersky Endpoint Security continues to encrypt new files if these files meet the criteria of the encryption rule. For example, when you change the properties of an unencrypted file (path or extension), the file then meets the criteria of the encryption rule. Kaspersky Endpoint Security encrypts this file.
- When the user creates a new file whose properties meet the encryption rule criteria, Kaspersky Endpoint Security encrypts the file as soon as it is opened.
- Kaspersky Endpoint Security postpones the encryption of open files until they are closed.
- If you move an encrypted file to another folder on the local drive, the file remains encrypted regardless of whether or not this folder is included in the encryption rule.
- If you decrypt a file and copy it to another local folder that is not included in the decryption rule, a copy of the file may be encrypted. To prevent the copied file from being encrypted, create a decryption rule for the target folder.

Forming encrypted file access rules for applications

To form encrypted file access rules for applications:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Data Encryption** → **File Level Encryption**.

6. In the **Encryption mode** drop-down list, select the **According to rules** item.

Access rules are applied only when in the **According to rules** mode. After applying access rules in **According to rules** mode, if you switch to **Leave unchanged** mode, Kaspersky Endpoint Security will ignore all access rules. All applications will have access to all encrypted files.

7. In the right part of the window, select the **Rules for applications** tab.

8. If you want to select applications exclusively from the Kaspersky Security Center list, click the **Add** button and in the drop-down list select the **Applications from Kaspersky Security Center list** item.

- a. Specify the filters to narrow down the list of applications in the table. To do so, specify the values of the **Application**, **Vendor**, and **Period added** parameters, and all check boxes from the **Group** section.
- b. Click the **Refresh** button.
- c. The table lists applications that match the applied filters.
- d. In the **Applications** column, select check boxes opposite the applications for which you want to form encrypted file access rules.
- e. In the **Rule for applications** drop-down list, select the rule that will determine the access of applications to encrypted files.
- f. In the **Actions for applications that were selected earlier** drop-down list, select the action to be taken by Kaspersky Endpoint Security on encrypted file access rules that were previously formed for such applications.
- g. Click **OK**.

The details of an encrypted file access rule for applications appear in the table on the **Rules for applications** tab.

9. If you want to manually select applications, click the **Add** button and in the drop-down list select the **Custom applications** item.

- a. In the entry field, type the name or list of names of executable application files, including their extensions.
You can also add the names of executable files of applications from the Kaspersky Security Center list by clicking the **Add from Kaspersky Security Center list** button.
- b. If required, in the **Description** field, enter a description of the list of applications.
- c. In the **Rule for applications** drop-down list, select the rule that will determine the access of applications to encrypted files.
- d. Click **OK**.

The details of an encrypted file access rule for applications appear in the table on the **Rules for applications** tab.

10. Save your changes.

Encrypting files that are created or modified by specific applications

You can create a rule by which Kaspersky Endpoint Security will encrypt all files created or modified by the applications specified in the rule.

Files that were created or modified by the specified applications before the encryption rule was applied will not be encrypted.

To configure encryption of files that are created or modified by specific applications:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Data Encryption** → **File Level Encryption**.
6. In the **Encryption mode** drop-down list, select the **According to rules** item.

Encryption rules are applied only in **According to rules** mode. After applying encryption rules in **According to rules** mode, if you switch to **Leave unchanged**, mode, Kaspersky Endpoint Security will ignore all encryption rules. Files that were previously encrypted will remain encrypted.

7. In the right part of the window, select the **Rules for applications** tab.
8. If you want to select applications exclusively from the Kaspersky Security Center list, click the **Add** button and in the drop-down list select the **Applications from Kaspersky Security Center list** item.

The **Add applications from Kaspersky Security Center list** window opens.

Do the following:

- a. Specify the filters to narrow down the list of applications in the table. To do so, specify the values of the **Application**, **Vendor**, and **Period added** parameters, and all check boxes from the **Group** section.
- b. Click the **Refresh** button.
The table lists applications that match the applied filters.
- c. In the **Applications** column, select the check boxes next to the applications whose created files you want to encrypt.
- d. In the **Rule for applications** drop-down list, select **Encrypt all created files**.
- e. In the **Actions for applications that were selected earlier** drop-down list, select the action to be taken by Kaspersky Endpoint Security on file encryption rules that were previously formed for such applications.
- f. Click **OK**.

Information about the encryption rule for files created or modified by the selected applications appears in the table on the **Rules for applications** tab.

9. If you want to manually select applications, click the **Add** button and in the drop-down list select the **Custom applications** item.

The **Add / edit names of the executable files of applications** window opens.

Do the following:

- a. In the entry field, type the name or list of names of executable application files, including their extensions.
You can also add the names of executable files of applications from the Kaspersky Security Center list by clicking the **Add from Kaspersky Security Center list** button.
- b. If required, in the **Description** field, enter a description of the list of applications.
- c. In the **Rule for applications** drop-down list, select **Encrypt all created files**.
- d. Click **OK**.

Information about the encryption rule for files created or modified by the selected applications appears in the table on the **Rules for applications** tab.

10. Save your changes.

Generating a decryption rule

To generate a decryption rule:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Data Encryption** → **File Level Encryption**.
6. In the right part of the window, select the **Decryption** tab.
7. In the **Encryption mode** drop-down list, select the **According to rules** item.
8. On the **Decryption** tab, click the **Add** button, and in the drop-down list select one of the following items:
 - a. Select the **Predefined folders** item to add files from folders of local user profiles suggested by Kaspersky experts to a decryption rule.
 - b. Select the **Custom folder** item to add a manually entered folder path to a decryption rule.
 - c. Select the **Files by extension** item to add individual file extensions to a decryption rule. Kaspersky Endpoint Security does not encrypt files with the specified extensions on all local drives of the computer.

- d. Select the **Files by groups of extensions** item to add groups of file extensions to a decryption rule (for example, *Microsoft Office Documents*). Kaspersky Endpoint Security does not encrypt files that have the extensions listed in the groups of extensions on all local drives of the computer.

9. Save your changes.

If the same file has been added to the encryption rule and the decryption rule, Kaspersky Endpoint Security does not encrypt this file if it is not encrypted, and decrypts the file if it is encrypted.

Decrypting files on local computer drives

To decrypt files on local drives:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Data Encryption** → **File Level Encryption**.
6. In the right part of the window, select the **Encryption** tab.
7. Remove files and folders that you want to decrypt from the encryption list. To do so, select files and select the **Delete rule and decrypt files** item in the context menu of the **Remove** button.

You can delete several items from the encryption list at once. To do so, while holding down the **CTRL** key, select the files you need by left-clicking them and select the **Delete rule and decrypt files** item in the context menu of the **Remove** button.

Files and folders removed from the encryption list are automatically added to the decryption list.

8. [Form a file decryption list](#).

9. Save your changes.

As soon as the policy is applied, Kaspersky Endpoint Security decrypts encrypted files that are added to the decryption list.

Kaspersky Endpoint Security decrypts encrypted files if their parameters (file path / file name / file extension) change to match the parameters of objects added to the decryption list.

Kaspersky Endpoint Security postpones the decryption of open files until they are closed.

Creating encrypted packages

To protect your data when sending files to users outside the corporate network, you can use encrypted packages. Encrypted packages can be convenient for transferring large files on removable drives, as email clients have file size restrictions.

Before creating encrypted packages, Kaspersky Endpoint Security will prompt the user for a password. To reliably protect the data, you can enable password strength check and specify password strength requirements. This will prevent users from using short and simple passwords, for example, 1234.

[How to enable password strength check when creating encrypted archives in the Administration Console \(MMC\)](#)

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Data Encryption** → **Common Encryption Settings**.
6. In the **Password settings** section, click the **Settings** button.
7. In the window that opens, select the **Encrypted packages** tab.
8. Configure password complexity settings when creating encrypted packages.

[How to enable password strength check when creating encrypted archives in the Web Console](#)

1. In the main window of Web Console, select the **Devices** → **Policies and policy profiles** tab.
2. Click the name of the Kaspersky Endpoint Security policy for the computers on which you want to enable password strength check.
The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Data Encryption** → **File Level Encryption**.
5. In the **Encrypted package password settings** section, configure the criteria for the password strength required to create encrypted packages.

You can create encrypted packages on computers with Kaspersky Endpoint Security installed with File Level Encryption available.

When adding a file to the encrypted package whose contents reside in OneDrive cloud storage, Kaspersky Endpoint Security downloads the contents of the file and performs encryption.

To create an encrypted package:


1. In any file manager, select the files or folders that you want to add to the encrypted package. Right-click to open their context menu.
2. In the context menu, select **New encrypted package** (see figure below).

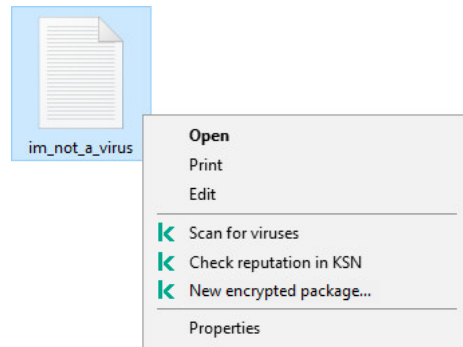
3. In the window that opens, select a location on a removable drive to save the encrypted package → specify the package name and click the **Save** button.

4. In the window that opens, specify the password and confirm it.

The password must meet the complexity criteria specified in the policy.

5. Click the **Create** button.

The encrypted package creation process starts. Kaspersky Endpoint Security does not perform file compression when it creates an encrypted package. When the process finishes, a self-extracting password-protected encrypted package (an executable file with .exe extension – ) is created in the selected destination folder.



Creating an encrypted package

To access files in an encrypted package, double-click it to start the Unpacking Wizard, then enter the password. If you forgot or lost your password, it is not possible to recover it and access the files in the encrypted package. You can recreate the encrypted package.

Restoring access to encrypted files

When files are encrypted, Kaspersky Endpoint Security receives an encryption key required for directly accessing the encrypted files. Using this encryption key, a user working under any Windows user account that was active during file encryption can directly access the encrypted files. Users working under Windows accounts that were inactive during file encryption must connect to Kaspersky Security Center in order to access the encrypted files.

Encrypted files may be inaccessible under the following circumstances:

- The user's computer stores encryption keys, but there is no connection with Kaspersky Security Center for managing them. In this case, the user must request access to encrypted files from the LAN administrator.

If access to Kaspersky Security Center does not exist, you must:

- request an access key for access to encrypted files on computer hard drives;
- to access encrypted files that are stored on removable drives, request separate access keys for encrypted files on each removable drive.
- Encryption components are deleted from the user's computer. In this event, the user may open encrypted files on local and removable disks but the contents of those files will appear encrypted.

The user may work with encrypted files under the following circumstances:

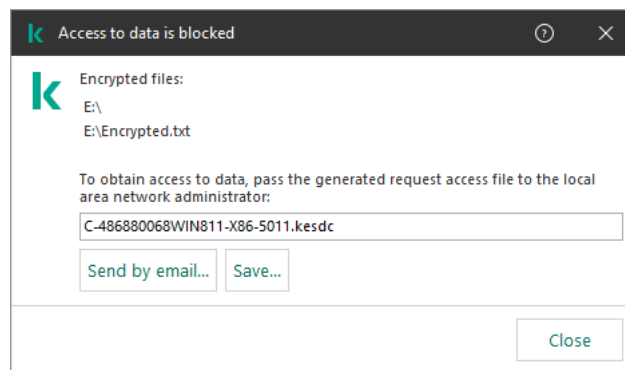
- Files are placed inside [encrypted packages](#) created on a computer with Kaspersky Endpoint Security installed.

- Files are stored on removable drives on which [portable mode](#) has been allowed.

To gain access to encrypted files, the user needs to start the recovery procedure (Request-Response).

Recovering access to encrypted files consists of the following steps:

1. The user sends a request access file to the administrator (see the figure below).
2. The administrator adds the request access file to Kaspersky Security Center, creates an access key file and sends the file to the user.
3. The user adds the access key file to Kaspersky Endpoint Security and gains access to the files.



Restoring access to encrypted files

To start the recovery procedure, the user needs to attempt to access a file. As a result, Kaspersky Endpoint Security will create a request access file (a file with the KESDC extension), which the user needs to send to the administrator, for example, by email.

Kaspersky Endpoint Security generates a request access file for access to all encrypted files stored on the computer's drive (local drive or removable drive).

[How to obtain an encrypted data access key file in the Administration Console \(MMC\)](#) ²

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Devices** tab.
4. On the **Devices** tab, select the computer of the user requesting access to encrypted data and right-click to open the context menu.
5. In the context menu, select **Grant access in offline mode**.
6. In the window that opens, select the **Data Encryption** tab.
7. On the **Data Encryption** tab, click the **Browse** button.
8. In the window for selecting a request access file, specify the path to the file received from the user.

You will see information about the user's request. Kaspersky Security Center generates a key file. Email the generated encrypted data access key file to the user. Or save the access file and use any available method to transfer the file.

[How to obtain an encrypted data access key file in the Web Console [?]](#)

1. In the main window of Web Console, select **Devices** → **Managed devices**.
2. Select the check box next to the name of the computer whose data you want to restore access to.
3. Click the **Share this device offline** button.
4. Select the **Data Encryption** section.
5. Click the **Select file** button and select the request access file that you received from the user (a file with the KESDC extension).

The Web Console will display information about the request. This will include the name of the computer on which the user is requesting access to the file.

6. Click the **Save key** button and select a folder to save the encrypted data access key file (a file with the KESDR extension).

As a result, you will be able to obtain the encrypted data access key, which you will need to transfer to the user.

After receiving the encrypted data access key file, the user needs to run the file by double-clicking it. As a result, Kaspersky Endpoint Security will grant access to all encrypted files stored on the drive. To access encrypted files that are stored on other drives, you must obtain a separate access key file for each drive.

Restoring access to encrypted data after operating system failure

You can restore access to data after operating system failure only for file level encryption (FLE). You cannot restore access to data if full disk encryption (FDE) is used.

To restore access to encrypted data after operating system failure:

1. Reinstall the operating system without formatting the hard drive.
2. [Install Kaspersky Endpoint Security](#).
3. Establish a connection between the computer and the Kaspersky Security Center Administration Server that controlled the computer when the data was encrypted.

Access to encrypted data will be granted under the same conditions that applied before operating system failure.

Editing templates of encrypted file access messages

To edit templates of encrypted file access messages:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Data Encryption** → **Common Encryption Settings**.
6. In the **Templates** section, click the **Templates** button.
The **Templates** window opens.
7. Do the following:
 - If you want to edit the user message template, select the **User's message** tab. The **Access to data is blocked** window opens when the user attempts to access an encrypted file while there is no key available on the computer for access to encrypted files. Clicking the **Send by email** button in the **Access to data is blocked** window automatically creates a user message. This message is sent to the corporate LAN administrator along with the file requesting access to encrypted files.
 - If you want to edit the administrator message template, select the **Administrator's message** tab. This message is created automatically when you click the **Send by email** button in the **Request access to encrypted files** window and is sent to the user after the user is granted access to encrypted files.
8. Edit the message templates.
You can use the **By default** button and the **Variable** drop-down list.
9. Save your changes.

Encryption of removable drives

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Windows for workstations. This component is unavailable if Kaspersky Endpoint Security is installed on a computer that runs on Windows for servers.

Kaspersky Endpoint Security supports encryption of files in FAT32 and NTFS file systems. If a removable drive with an unsupported file system is connected to the computer, the encryption task for this removable drive ends with an error and Kaspersky Endpoint Security assigns the read-only status to the removable drive.

To protect data on removable drives, you can use the following types of encryption:

- Full Disk Encryption (FDE).

Encryption of the entire removable drive, including the file system.

It is not possible to access encrypted data outside the corporate network. It is also impossible to access encrypted data inside the corporate network if the computer is not connected to Kaspersky Security Center (e.g. on a guest computer).

- File Level Encryption (FLE).

Encryption of only files on a removable drive. The file system remains unchanged.

Encryption of files on removable drives provides the capability to access data outside the corporate network using a special mode called [*portable mode*](#).

During encryption, Kaspersky Endpoint Security creates a master key. Kaspersky Endpoint Security saves the master key in the following repositories:

- Kaspersky Security Center.

- User's computer.

The master key is encrypted with the user's secret key.

- Removable drive.

The master key is encrypted with the public key of Kaspersky Security Center.

After encryption is complete, the data on the removable drive can be accessed within the corporate network as if was on an ordinary unencrypted removable drive.

Accessing encrypted data

When a removable drive with encrypted data is connected, Kaspersky Endpoint Security performs the following actions:

1. Checks for a master key in the local storage on the user's computer.

If the master key is found, the user gains access to the data on the removable drive.

If the master key is not found, Kaspersky Endpoint Security performs the following actions:

- a. Sends a request to Kaspersky Security Center.

After receiving the request, Kaspersky Security Center sends a response that contains the master key.

- b. Kaspersky Endpoint Security saves the master key in the local storage on the user's computer for subsequent operations with the encrypted removable drive.

2. Decrypts the data.

Special features of removable drive encryption

Encryption of removable drives has the following special features:

- The policy with preset settings for removable drive encryption is formed for a specific group of managed computers. Therefore, the result of applying the Kaspersky Security Center policy configured for encryption / decryption of removable drives depends on the computer to which the removable drive is connected.
- Kaspersky Endpoint Security does not encrypt / decrypt read-only files that are stored on removable drives.
- The following device types are supported as removable drives:
 - Data media connected via the USB bus
 - hard drives connected via USB and FireWire buses
 - SSD drives connected via USB and FireWire buses

Starting encryption of removable drives

You can use a policy to decrypt a removable drive. A policy with defined settings for removable drive encryption is generated for a specific administration group. Therefore, the result of data decryption on removable drives depends on the computer to which the removable drive is connected.

Kaspersky Endpoint Security supports encryption in FAT32 and NTFS file systems. If a removable drive with an unsupported file system is connected to the computer, removable drive encryption ends with an error and Kaspersky Endpoint Security assigns read-only access for the removable drive.

To encrypt removable drives:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.

5. In the policy window, select **Data Encryption** → **Encryption of removable drives**.
6. In the **Encryption mode** drop-down list, select the default action that you want Kaspersky Endpoint Security to perform on removable drives:
 - **Encrypt entire removable drive (FDE)**. Kaspersky Endpoint Security encrypts the contents of a removable drive sector by sector. As a result, the application encrypts not only the files stored on the removable drive but also its file systems, including the file names and folder structures on the removable drive.
 - **Encrypt all files (FLE)**. Kaspersky Endpoint Security encrypts all files that are stored on removable drives. The application does not encrypt the file systems of removable drives, including the names of files and folder structures.
 - **Encrypt new files only (FLE)**. Kaspersky Endpoint Security encrypts only those files that have been added to removable drives or that were stored on removable drives and have been modified after the Kaspersky Security Center policy was last applied.

Kaspersky Endpoint Security does not encrypt a removable drive that is already encrypted.

7. If you want to [use portable mode](#) for encryption of removable drives, select the **Portable mode** check box.

Portable mode is a mode of file encryption (FLE) on removable drives that provides the ability to access data outside of a corporate network. Portable mode also lets you work with encrypted data on computers that do not have Kaspersky Endpoint Security installed.
8. If you want to encrypt a new removable drive, it is recommended to select the **Encrypt used disk space only** check box. If the check box is cleared, Kaspersky Endpoint Security will encrypt all files, including the residual fragments of deleted or modified files.
9. If you want to configure encryption for individual removable drives, [define encryption rules](#).
10. If you want to use full disk encryption of removable drives in offline mode, select the **Allow removable drive encryption in offline mode** check box.

Offline encryption mode refers to encryption of removable drives (FDE) when there is no connection to Kaspersky Security Center. During encryption, Kaspersky Endpoint Security saves the master key only on the user's computer. Kaspersky Endpoint Security will send the master key to Kaspersky Security Center during the next synchronization.

If the computer on which the master key is saved is corrupted and data is not sent to Kaspersky Security Center, it is not possible to obtain access to the removable drive.

If the **Allow removable drive encryption in offline mode** check box is cleared and there is no connection to Kaspersky Security Center, removable drive encryption is not possible.

11. Save your changes.

After the policy is applied, when the user connects a removable drive or if a removable drive is already connected, Kaspersky Endpoint Security prompts the user for confirmation to perform the encryption operation (see the figure below).

The application lets you perform the following actions:

- If the user confirms the encryption request, Kaspersky Endpoint Security encrypts the data.

- If the user declines the encryption request, Kaspersky Endpoint Security leaves the data unchanged and assigns read-only access for this removable drive.
- If the user does not respond to the encryption request, Kaspersky Endpoint Security leaves the data unchanged and assigns read-only access for this removable drive. The application prompts for confirmation again when subsequently applying a policy or the next time this removable drive is connected.

If the user initiates safe removal of a removable drive during data encryption, Kaspersky Endpoint Security interrupts the data encryption process and allows removal of the removable drive before the encryption process has finished. Data encryption will be continued the next time the removable drive is connected to this computer.

If encryption of a removable drive failed, view the **Data encryption** report in the Kaspersky Endpoint Security interface. Access to files may be blocked by another application. In this case, try unplugging the removable drive from the computer and connecting it again.



Removable drive encryption request

Adding an encryption rule for removable drives

To add an encryption rule for removable drives:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Data Encryption** → **Encryption of removable drives**.
6. Click the **Add** button, and in the drop-down list select one of the following items:
 - If you want to add encryption rules for removable drives that are in the list of trusted devices of the Device Control component, select **From list of trusted devices of this policy**.

- If you want to add encryption rules for removable drives that are in the Kaspersky Security Center list, select **From Kaspersky Security Center list of devices**.

7. In the **Encryption mode for selected devices** drop-down list, select the action to be performed by Kaspersky Endpoint Security on files stored on the selected removable drives.

8. Select the **Portable mode** check box if you want Kaspersky Endpoint Security to prepare removable drives before encryption, making it possible to use encrypted files stored on them in portable mode.

Portable mode lets you use encrypted files stored on removable drives that are connected to computers [without encryption functionality](#).

9. Select the **Encrypt used disk space only** check box if you want Kaspersky Endpoint Security to encrypt only those disk sectors that are occupied by files.

If you are applying encryption on a drive that is already in use, it is recommended to encrypt the entire drive. This ensures that all data is protected - even deleted data that might still contain retrievable information. The **Encrypt used disk space only** function is recommended for new drives that have not been previously used.

If a device was previously encrypted using the **Encrypt used disk space only** function, after applying a policy in **Encrypt entire removable drive** mode, sectors that are not occupied by files will still not be encrypted.

10. In the **Actions for devices that were selected earlier** drop-down list, select the action to be performed by Kaspersky Endpoint Security according to encryption rules that had been previously defined for removable drives:

- If you want the previously created encryption rule for the removable drive to remain unchanged, select **Skip**.
- If you want the previously created encryption rule for the removable drive to be replaced by the new rule, select **Update**.

11. Save your changes.

The added encryption rules for removable drives will be applied to removable drives connected to any computers in the organization.

Editing an encryption rule for removable drives

To edit an encryption rule for a removable drive:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Data Encryption** → **Encryption of removable drives**.
6. In the list of removable drives for which encryption rules have been configured, select an entry corresponding to the removable drive you need.

7. Click the **Set a rule** button to edit the encryption rule for the selected removable drive.

The context menu of the **Set a rule** button opens.

8. In the context menu of the **Set a rule** button, select the action to be performed by Kaspersky Endpoint Security on files stored on the selected removable drive.

9. Save your changes.

The modified removable drive encryption rules are applied to removable drives that are connected to any computers controlled by the modified policy of Kaspersky Security Center.

Portable mode for accessing encrypted files on removable drives

Portable mode is a mode of file encryption (FLE) on removable drives that provides the ability to access data outside of a corporate network. Portable mode also lets you work with encrypted data on computers that do not have Kaspersky Endpoint Security installed.

Portable mode is convenient to use in the following cases:

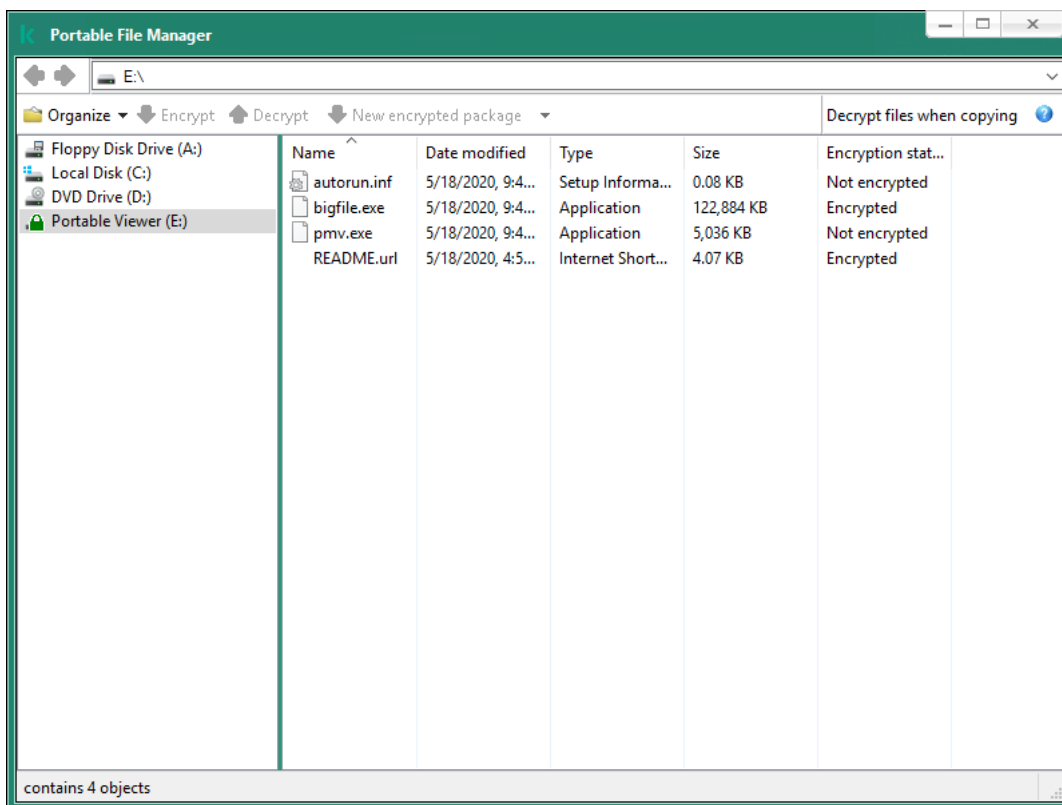
- There is no connection between the computer and the Kaspersky Security Center Administration Server.
- The infrastructure has changed with the change of the Kaspersky Security Center Administration Server.
- Kaspersky Endpoint Security is not installed on the computer.

Portable File Manager

To work in portable mode, Kaspersky Endpoint Security installs a special encryption module named *Portable File Manager* on a removable drive. The Portable File Manager provides an interface for working with encrypted data if Kaspersky Endpoint Security is not installed on the computer (see the figure below). If Kaspersky Endpoint Security is installed on your computer, you can work with encrypted removable drives using your usual file manager (for example, Explorer).

The Portable File Manager stores a key to encrypt files on a removable drive. The key is encrypted with the user password. The user sets a password before encrypting files on a removable drive.

The Portable File Manager starts automatically when a removable drive is connected to a computer on which Kaspersky Endpoint Security is not installed. If automatic startup of applications is disabled on the computer, manually start the Portable File Manager. To do so, run the file named `pmv.exe` that is stored on the removable drive.



Portable File Manager

Support for portable mode for working with encrypted files

[How to enable portable mode support for working with encrypted files on removable drives in the Administration Console \(MMC\)](#) 

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Data Encryption** → **Encryption of removable drives**.
6. In the **Encryption mode for selected devices** drop-down list, select **Encrypt all files** or **Encrypt new files only**.

Portable mode is available only with File Level Encryption (FLE). It is not possible to enable portable mode support for Full Disk Encryption (FDE).

7. Select the **Portable mode** check box.
8. If necessary, [add encryption rules for individual removable drives](#).
9. Save your changes.
10. After applying the policy, connect the removable drive to the computer.
11. Confirm the removable drive encryption operation.
This opens a window in which you can create a password for Portable File Manager.
12. Specify a password that meets the strength requirements and confirm it.
13. Click **OK**.

Kaspersky Endpoint Security will encrypt files on the removable drive. The Portable File Manager used for working with encrypted files will also be added to the removable drive. If there are already encrypted files on the removable drive, Kaspersky Endpoint Security will encrypt them again using its own key. This allows the user to access all files on the removable drive in portable mode.

[How to enable portable mode support for working with encrypted files on removable drives in the Web Console](#) 

1. In the main window of Web Console, select the **Devices** → **Policies and policy profiles** tab.
2. Click the name of the Kaspersky Endpoint Security policy for computers on which you want to enable support for portable mode.
The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Data Encryption** → **Encryption of Removable Drives**.
5. In the **Manage encryption** section, select **Encrypt all files** or **Encrypt new files only**.

Portable mode is available only with File Level Encryption (FLE). It is not possible to enable portable mode support for Full Disk Encryption (FDE).

6. Select the **Portable mode** check box.
7. If necessary, [add encryption rules for individual removable drives](#).
8. Save your changes.
9. After applying the policy, connect the removable drive to the computer.
10. Confirm the removable drive encryption operation.
This opens a window in which you can create a password for Portable File Manager.
11. Specify a password that meets the strength requirements and confirm it.
12. Click **OK**.

Kaspersky Endpoint Security will encrypt files on the removable drive. The Portable File Manager used for working with encrypted files will also be added to the removable drive. If there are already encrypted files on the removable drive, Kaspersky Endpoint Security will encrypt them again using its own key. This allows the user to access all files on the removable drive in portable mode.

Accessing encrypted files on a removable drive

After encrypting files on a removable drive with portable mode support, the following file access methods are available:

- If Kaspersky Endpoint Security is not installed on the computer, the Portable File Manager will prompt you to enter a password. You will need to enter the password each time you restart the computer or reconnect the removable drive.
- If the computer is located outside the corporate network and Kaspersky Endpoint Security is installed on the computer, the application will prompt you to enter the password or send the administrator a request to access the files. After gaining access to files on a removable drive, Kaspersky Endpoint Security will save the secret key in the computer's key storage. This will allow access to files in the future without entering a password or asking the administrator.

- If the computer is located inside the corporate network and Kaspersky Endpoint Security is installed on the computer, you will get access to the device without entering a password. Kaspersky Endpoint Security will receive the secret key from the Kaspersky Security Center Administration Server to which the computer is connected.

Recovering the password for working in portable mode

If you have forgotten the password for working in portable mode, you need to connect the removable drive to a computer with Kaspersky Endpoint Security installed inside the corporate network. You will get access to the files because the secret key is stored in the computer's key storage or on the Administration Server. Decrypt and re-encrypt files with a new password.

Features of portable mode when connecting a removable drive to a computer from another network

If the computer is located outside the corporate network and Kaspersky Endpoint Security is installed on the computer, you can access the files in the following ways:

- **Password-based access**

After entering the password, you will be able to view, modify, and save files on the removable drive (*transparent access*). Kaspersky Endpoint Security can set a read-only access right for a removable drive if the following parameters are configured in the policy settings for encryption of removable drives:

- Portable mode support is disabled.
- The **Encrypt all files** or **Encrypt new files only** mode is selected.

In all other cases, you will get full access to the removable drive (read/write permission). You will be able to add and delete files.

You can change the removable drive access permissions even while the removable drive is connected to the computer. If the removable drive access permissions are changed, Kaspersky Endpoint Security will block access to the files and prompt you for the password again.

After entering the password, you cannot apply encryption policy settings for the removable drive. In this case, it is impossible to decrypt or re-encrypt files on the removable drive.

- **Ask the administrator for access to files**

If you have forgotten the password for working in portable mode, ask the administrator for access to files. To access the files, the user needs to send the administrator a request access file (a file with the KESDC extension). The user can send the request access file by email, for example. The administrator will send an encrypted data access file (a file with the KESDR extension).

After you complete the Request-Response password recovery procedure, you will receive transparent access to files on the removable drive, and full access to the removable drive (read/write permission).

You can apply a removable drive encryption policy, and decrypt files, for example. After recovering the password or when the policy is updated, Kaspersky Endpoint Security will prompt you to confirm the changes.

[How to obtain an encrypted data access file in the Administration Console \(MMC\)](#) 

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Devices** tab.
4. On the **Devices** tab, select the computer of the user requesting access to encrypted data and right-click to open the context menu.
5. In the context menu, select **Grant access in offline mode**.
6. In the window that opens, select the **Data Encryption** tab.
7. On the **Data Encryption** tab, click the **Browse** button.
8. In the window for selecting a request access file, specify the path to the file received from the user.

You will see information about the user's request. Kaspersky Security Center generates a key file. Email the generated encrypted data access key file to the user. Or save the access file and use any available method to transfer the file.

[How to obtain an encrypted data access file in the Web Console](#)

1. In the main window of Web Console, select **Devices** → **Managed devices**.
2. Select the check box next to the name of the computer whose data you want to restore access to.
3. Click the **Share this device offline** button.
4. Select the **Data Encryption** section.
5. Click the **Select file** button and select the request access file that you received from the user (a file with the KESDC extension).
The Web Console will display information about the request. This will include the name of the computer on which the user is requesting access to the file.
6. Click the **Save key** button and select a folder to save the encrypted data access key file (a file with the KESDR extension).

As a result, you will be able to obtain the encrypted data access key, which you will need to transfer to the user.

Decryption of removable drives

You can use a policy to decrypt a removable drive. A policy with defined settings for removable drive encryption is generated for a specific administration group. Therefore, the result of data decryption on removable drives depends on the computer to which the removable drive is connected.

To decrypt removable drives:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. Select the necessary policy and double-click to open the policy properties.
5. In the policy window, select **Data Encryption** → **Encryption of removable drives**.
6. If you want to decrypt all encrypted files that are stored on removable drives, in the **Encryption mode** drop-down list select **Decrypt entire removable drive**.
7. To decrypt data that is stored on individual removable drives, edit the encryption rules for removable drives whose data you want to decrypt. To do so:
 - a. In the list of removable drives for which encryption rules have been configured, select an entry corresponding to the removable drive you need.
 - b. Click the **Set a rule** button to edit the encryption rule for the selected removable drive.
The context menu of the **Set a rule** button opens.
 - c. Select the **Decrypt all files** item in the context menu of the **Set a rule** button.
8. Save your changes.

As a result, if a user connects a removable drive or if it is already connected, Kaspersky Endpoint Security decrypts the removable drive. The application warns the user that the decryption process may take some time. If the user initiates safe removal of a removable drive during data decryption, Kaspersky Endpoint Security interrupts the data decryption process and allows removal of the removable drive before the decryption operation has finished. Data decryption will be continued the next time the removable drive is connected to the computer.

If decryption of a removable drive failed, view the **Data encryption** report in the Kaspersky Endpoint Security interface. Access to files may be blocked by another application. In this case, try unplugging the removable drive from the computer and connecting it again.

Viewing data encryption details

While encryption or decryption is in progress, Kaspersky Endpoint Security relays information about the status of encryption parameters applied to client computers to Kaspersky Security Center.

The following encryption status values are possible:

- *Encryption policy not defined.* A Kaspersky Security Center encryption policy has not been defined for the computer.
- *Applying policy.* Data encryption and / or decryption is in progress on the computer.

- *Error.* An error occurred during data encryption and / or decryption on the computer.
- *Reboot required.* The operating system has to be rebooted in order to start or finish data encryption or decryption on the computer.
- *Compliant with policy.* Data encryption on the computer has been completed using the encryption settings specified in the Kaspersky Security Center policy applied to the computer.
- *Cancelled by user.* The user has declined to confirm the file encryption operation on the removable drive.

Viewing the encryption status

To view the encryption status of computer data:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Devices** tab.
The **Devices** tab in the workspace shows the properties of computers in the selected administration group.
4. On the **Devices** tab in the workspace, slide the scroll bar all the way to the right.
5. If the **Encryption status** column is not displayed:
 - a. Right-click to open the context menu for the table header.
 - b. In the context menu, in the **View** drop-down list, select **Add/Remove columns**.
The **Add/Remove columns** window opens.
 - c. In the **Add/Remove columns** window, select the **Encryption status** check box.
 - d. Click **OK**.

The **Encryption status** column shows the encryption status of data on computers in the selected administration group. This status is formed based on information about file encryption on local drives of the computer, and about full disk encryption.

Viewing encryption statistics on Kaspersky Security Center dashboards

To view the encryption status on Kaspersky Security Center dashboards:

1. Open the Kaspersky Security Center Administration Console.
2. In the console tree, select the **Administration Server – <Computer name>** node.
3. In the workspace to the right of the Administration Console tree, select the **Statistics** tab.
4. Create a new page with details panes containing data encryption statistics. To do so:

a. On the **Statistics** tab, click the **Customize view** button.

The **Properties: Statistics** window opens.

b. In the **Properties: Statistics** window, click **Add**.

The **Properties: New page** window opens.

c. In the **General** section of the **Properties: New page** window, type the page name.

d. In the **Details panes** section, click the **Add** button.

The **New details pane** window opens.

e. In the **New details panel** window in the **Protection status** group, select the **Encryption of devices** item.

f. Click **OK**.

The **Properties: Encryption Control** window opens.

g. If necessary, edit the details pane settings. To do so, use the **View** and **Devices** sections of the **Properties: Encryption of devices** window.

h. Click **OK**.

i. Repeat steps d – h of the instructions, selecting the **Encryption of removable drives** item in the **Protection status** section of the **New details pane** window.

The details panes added appear in the **Details panes** list in the **Properties: New page** window.

j. In the **Properties: New page** window, click **OK**.

The name of the page with details panes created at the previous steps appears in the **Pages** list of the **Properties: Statistics** window.

k. In the **Properties: Statistics** window, click **Close**.

5. On the **Statistics** tab, open the page that was created during the previous steps of the instructions.

The details panes appear, showing the encryption status of computers and removable drives.

Viewing file encryption errors on local computer drives

To view the file encryption errors on local computer drives:

1. Open the Kaspersky Security Center Administration Console.

2. In the **Managed devices** folder of the Administration Console tree, open the folder with the name of the administration group that includes the client computer whose list of file encryption errors you want to view.

3. In the workspace, select the **Devices** tab.

4. On the **Devices** tab, select the name of the computer in the list and right-click it to open the context menu.

5. In the context menu of the computer, select the **Properties** item. In the **Properties: <computer name>** window, select the **Protection** section.

6. In the **Protection** section of the **Properties: <computer name>** window, click the **View list of data encryption errors** link to open the **Data encryption errors** window.

This window shows the details of file encryption errors on local computer drives. When an error is corrected, Kaspersky Security Center removes the error details from the **Data encryption errors** window.

Viewing the data encryption report

To view the data encryption report:

1. Open the Kaspersky Security Center Administration Console.
2. In the **Administration Server** node of the Administration Console tree, select the **Reports** tab.
3. Click the **New report template** button.
The Report Template Wizard starts.
4. Follow the instructions of the Report Template Wizard. In the **Select report template type** window in the **Other** section, select one of the following items:
 - **Managed device encryption status report.**
 - **Mass storage device encryption status report.**
 - **File encryption errors report.**
 - **Report on blocked access to encrypted files.**

After you have finished with the New Report Template Wizard, the new report template appears in the table on the **Reports** tab.

5. Select the report template that was created at the previous steps of the instructions.
6. In the context menu of the template, select **Show report**.

The report generation process starts. The report is displayed in a new window.

Working with encrypted devices when there is no access to them

Obtaining access to encrypted devices

A user may be required to request access to encrypted devices in the following cases:

- The hard drive was encrypted on a different computer.
- The encryption key for a device is not on the computer (for example, upon the first attempt to access the encrypted removable drive on the computer), and the computer is not connected to Kaspersky Security Center.

After the user has applied the access key to the encrypted device, Kaspersky Endpoint Security saves the encryption key on the user's computer and allows access to this device upon subsequent access attempts even if there is no connection to Kaspersky Security Center.

Access to encrypted devices can be obtained as follows:

1. The user uses the Kaspersky Endpoint Security application interface to create a request access file with the kesdc extension and sends it to the corporate LAN administrator.
2. The administrator uses the Kaspersky Security Center Administration Console to create an access key file with the kesdr extension and sends it to the user.
3. The user applies the access key.

Restoring data on encrypted devices

A user can use the [Encrypted Device Restore Utility](#) (hereinafter referred to as the Restore Utility) to work with encrypted devices. This may be required in the following cases:

- The procedure for using an access key to obtain access was unsuccessful.
- Encryption components have not been installed on the computer with the encrypted device.

The data needed to restore access to encrypted devices using the Restore Utility resides in the memory of the user's computer in unencrypted form for some time. To reduce the risk of unauthorized access to such data, you are advised to restore access to encrypted devices on trusted computers.

Data on encrypted devices can be restored as follows:

1. The user uses the Restore Utility to create a request access file with the fdertc extension and sends it to the corporate LAN administrator.
2. The administrator uses the Kaspersky Security Center Administration Console to create an access key file with the fdertr extension and sends it to the user.
3. The user applies the access key.

To restore data on encrypted system hard drives, the user can also specify the Authentication Agent account credentials in the Restore Utility. If the metadata of the Authentication Agent account has been corrupted, the user must complete the restoration procedure using a request access file.

Before restoring data on encrypted devices, it is recommended to cancel the Kaspersky Security Center policy or disable encryption in the Kaspersky Security Center policy settings on the computer where the procedure will be performed. This prevents the device from being encrypted again.

Recovering data by using the FDERT Restore Utility

If the hard drive fails, the file system may be corrupt. If this is the case, data protected by Kaspersky Disk Encryption technology will be unavailable. You can decrypt the data and copy the data to a new drive.

Data recovery on a drive protected by Kaspersky Disk Encryption technology consists of the following steps:

1. Create a stand-alone Restore Utility (see the figure below).
2. Connect a drive to a computer that does not have Kaspersky Endpoint Security encryption components installed.

3. Run the Restore Utility and diagnose the hard drive.
4. Access data on the drive. To do so, enter the credentials of the Authentication Agent or start the recovery procedure (Request-Response).



FDERT Restore Utility

Creating a standalone restore utility

To create the executable file of Restore Utility:

1. In the main application window, click the **Support** button.
2. In the window that opens, click the **Restore encrypted device** button.
Encrypted device Restore Utility starts.
3. Click the **Create Stand-alone Restore Utility** button in the window of Restore Utility.
4. Save the stand-alone Restore Utility to computer memory.

As a result, the executable file of the Restore Utility (fdert.exe) will be saved in the specified folder. Copy the Restore Utility to a computer that does not have Kaspersky Endpoint Security encryption components. This prevents the drive from being encrypted again.

The data needed to restore access to encrypted devices using the Restore Utility resides in the memory of the user's computer in unencrypted form for some time. To reduce the risk of unauthorized access to such data, you are advised to restore access to encrypted devices on trusted computers.

Recovering data on a hard drive

To restore access to an encrypted device using the Restore Utility:

1. Run the file named fdert.exe, which is the executable file of the Restore Utility. This file is created by Kaspersky Endpoint Security.

2. In the Restore Utility window, from the **Select device** drop-down list select an encrypted device to which you want to restore access.
3. Click the **Scan** button to allow the utility to define which of the actions should be taken on the device: whether it should be unlocked or decrypted.

If the computer has access to Kaspersky Endpoint Security encryption functionality, the Restore Utility prompts you to unlock the device. While unlocking the device does not decrypt it, the device becomes directly accessible as a result of being unlocked. If the computer does not have access to Kaspersky Endpoint Security encryption functionality, the Restore Utility prompts you to decrypt the device.

4. If you want to import diagnostic information, click the **Save diagnostics** button.

The utility will save an archive with files containing diagnostic information.

5. Click the **Fix MBR** button if diagnostics of the encrypted system hard drive has returned a message about problems involving the master boot record (MBR) of the device.

Fixing the master boot record of the device can speed up the process of obtaining information that is needed for unlocking or decrypting the device.

6. Click the **Unlock** or **Decrypt** button depending on the results of diagnostics.

7. If you want to restore data using an Authentication Agent account, select the **Use Authentication Agent account settings** option and enter the credentials of the Authentication Agent.

This method is possible only when restoring data on a system hard drive. If the system hard drive was corrupted and Authentication Agent account data has been lost, you must obtain an access key from the corporate LAN administrator to restore data on an encrypted device.

8. If you want to start the recovery procedure, do the following:

- a. Select the **Specify device access key manually** option.
- b. Click the **Receive access key** button and save the request access file to computer memory (a file with the FDERTC extension).
- c. Send the request access file to the corporate LAN administrator.

Do not close the **Receive device access key** window until you have received the access key. When this window is opened again, you will not be able to apply the access key that was previously created by the administrator.

- d. Receive and save the access file (a file with the FDERTR extension) created and sent to you by the corporate LAN administrator (see the instructions below).
- e. Download the access file in the **Receive device access key** window.

9. If you are decrypting a device, you must configure additional decryption settings:

- Specify area to decrypt:
 - If you want to decrypt the entire device, select the **Decrypt entire device** option.
 - If you want to decrypt a portion of the data on a device, select the **Decrypt individual device areas** option and specify the decryption area boundaries.
- Select the location for writing the decrypted data:

- If you want the data on the original device to be rewritten with the decrypted data, clear the **Decrypt to a disk image file** check box.
- If you want to save decrypted data separately from the original encrypted data, select the **Decrypt to a disk image file** check box and use the **Browse** button to specify the path where to save the VHD file.

10. Click **OK**.

The device unlocking / decryption process starts.

[How to create an encrypted data access file in the Administration Console \(MMC\)](#)

1. Open the Kaspersky Security Center Administration Console.
2. In the Administration Console tree, select the **Additional** → **Data encryption and protection** → **Encrypted devices** folder.
3. In the workspace, select the encrypted device for which you want to create an access key file, and in the device context menu select **Get access to the device in Kaspersky Endpoint Security for Windows (11.4.0)**.

If you are not sure for which computer the request access file was generated, in the Administration Console tree select the **Additional** → **Data encryption and protection** folder and in the workspace click the **Get device encryption key in Kaspersky Endpoint Security for Windows (11.4.0)** link.

4. In the window that opens, select the encryption algorithm to use: **AES256** or **AES56**.

The data encryption algorithm depends on the AES encryption library that is included in the distribution package: *Strong encryption (AES256)* or *Lite encryption (AES56)*. The AES encryption library is installed together with the application.

5. Click the **Browse** button. In the window that opens, specify the path to the request access file (with the **FDERTC** extension) received from the user.
6. Click the **Open** button.

You will see information about the user's request. Kaspersky Security Center generates a key file. Email the generated encrypted data access key file to the user. Or save the access file and use any available method to transfer the file.

[How to create an encrypted data access file in the Web Console](#)

1. In the main window of the Web Console, select **Operations** → **Data encryption and protection** → **Encrypted devices**.

2. Select the check box next to the name of the computer on which you want to recover data.

3. Click the **Share this device offline** button.

This starts the Wizard for granting access to a device.

4. Follow the instructions of the Wizard for granting access to a device:

a. Select the **Kaspersky Endpoint Security for Windows** plug-in.

b. Select the encryption algorithm to use: **AES256** or **AES56**.

The data encryption algorithm depends on the AES encryption library that is included in the distribution package: *Strong encryption (AES256)* or *Lite encryption (AES56)*. The AES encryption library is installed together with the application.

c. Click the **Select file** button and select the request access file received from the user (a file with the FDERTC extension).

d. Click the **Save key** button and select a folder to save the key file for accessing encrypted data (a file with the FDERTR extension).

As a result, you will be able to obtain the encrypted data access key, which you will need to transfer to the user.

Creating an operating system rescue disk

The operating system rescue disk can be useful when an encrypted hard drive cannot be accessed for some reason and the operating system cannot load.

You can load an image of the Windows operating system using the rescue disk and restore access to the encrypted hard drive using Restore Utility included in the operating system image.

To create an operating system rescue disk:

1. [Create an executable file for the Encrypted Device Restore Utility](#).

2. Create a custom image of the Windows pre-boot environment. While creating the custom image of the Windows pre-boot environment, add the executable file of Restore Utility to the image.

3. Save the custom image of the Windows pre-installation environment to bootable media such as a CD or removable drive.

Refer to Microsoft help files for instructions on creating a custom image of the Windows pre-boot environment (for example, in the [Microsoft TechNet resource](#)).

Managing the application from the command line

You can manage Kaspersky Endpoint Security from the command line. You can view the list of commands for managing the application by executing the `HELP` command. To read about the syntax of a specific command, enter `HELP <command>`.

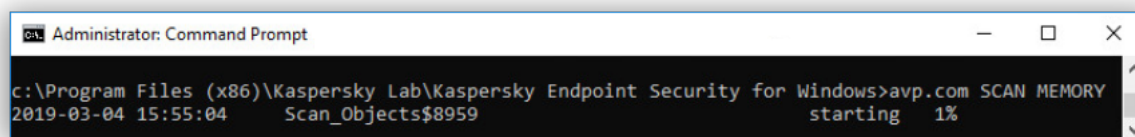
AVP commands

To manage Kaspersky Endpoint Security from the command line:

1. Run the command line interpreter (cmd.exe) as an administrator.
2. Go to the folder where the Kaspersky Endpoint Security executable file is located.
3. To execute a command, enter:

```
avp.com <command> [options]
```

As a result, Kaspersky Endpoint Security will execute the command (see figure below.)



Managing the application from the command line

SCAN. Virus Scan

Run the virus scan task.



Command syntax

```
SCAN [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>]  
[/R[A]:<report file>] [<scan technologies>] [/C:<file with virus scan settings>]
```

Scan scope	
<files to scan>	<p>A space-separated list of files and folders. Long paths must be enclosed in quotation marks. Short paths (MS-DOS format) do not need to be enclosed in quotation marks. For example:</p> <ul style="list-style-type: none">• "C:\Program Files (x86)\Example Folder" – long path.• C:\PROGRA~2\EXAMPL~1 – short path.

/ALL	Run the <i>Full Scan</i> task. Kaspersky Endpoint Security scans the following objects: <ul style="list-style-type: none"> • Kernel memory. • Objects that are loaded at startup of the operating system. • Boot sectors • Operating system backup. • All hard and removable drives
/MEMORY	Scan the kernel memory.
/STARTUP	Scan the objects that are loaded at startup of the operating system.
/MAIL	Scan Outlook mailbox.
/REMDRIVES	Scan removable drives.
/FIXDRIVES	Scan hard drives.
/NETDRIVES	Scan network drives.
/QUARANTINE	Scan the files in the Kaspersky Endpoint Security Backup.
/@:<file list.lst>	Scan the files and folders from a list. Each file in the list must be on a new row. Long paths must be enclosed in quotation marks. Short paths (MS-DOS format) do not need to be enclosed in quotation marks. For example: <ul style="list-style-type: none"> • "C:\Program Files (x86)\Example Folder" – long path. • C:\PROGRA~2\EXAMPL~1 – short path.

Action on threat detection	
/i0	Inform. If this option is selected, Kaspersky Endpoint Security adds the information about infected files to the list of active threats on detection of these files.
/i1	Disinfect; inform if disinfection fails. If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected files that are detected. If disinfection is not possible, Kaspersky Endpoint Security adds the information about the infected files that are detected to the list of active threats.
/i2	Disinfect; delete if disinfection fails. If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected files that are detected. If disinfection fails, Kaspersky Endpoint Security deletes the files. This action is selected by default.
/i3	Disinfect the infected files that are detected. If disinfection fails, delete the infected files. Also delete compound files (for example, archives) if the infected file cannot be disinfecting or deleted.
/i4	Delete infected files. Also delete compound files (for example, archives) if the infected file cannot be deleted.
/i8	Prompt the user for action as soon as a threat is detected.
/i9	Prompt the user for action after the scan is completed.

File types	
/fe	Files scanned by extension. If this setting is enabled, Kaspersky Endpoint Security scans infectable files only  . The file format is then determined based on the file's extension.
/fi	Files scanned by format. If this setting is enabled, Kaspersky Endpoint Security scans infectable files only  . Before scanning a file for malicious code, the internal header of the file is analyzed to determine the format of the file (for example, .txt, .doc, or .exe). During scanning, the extension of the file is also taken into account.
/fa	All files. If this setting is enabled, Kaspersky Endpoint Security checks all files without exception (all formats and extensions). This is the default setting.

Scan exclusions	
-e:a	RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives are excluded from the scan scope.
-e:b	Mail databases, incoming and outgoing e-mails are excluded from the scan scope.
-E:<file mask>	Files that match the file mask are excluded from the scan scope. For example: <ul style="list-style-type: none"> The mask *.exe will include all paths to files that have the exe extension. The mask example* will include all paths to files named EXAMPLE.
-e:<seconds>	Files that take longer to scan than the specified time limit (in seconds) are excluded from the scan scope.
-es:<megabytes>	Files that are larger than the specified size limit (in megabytes) are excluded from the scan scope.

Saving events to a report file mode	
/R:<report file>	Save only critical events to the report file.
/RA:<report file>	Save all events to a report file.

Scan technologies	
/iChecker=on off	This technology allows increasing scan speed by excluding certain files from scanning. Files are excluded from scanning by using a special algorithm that takes into account the release date of Kaspersky Endpoint Security databases, the date that the file was last scanned on, and any modifications to the scanning settings.
/iSwift=on off	This technology allows increasing scan speed by excluding certain files from scanning. Files are excluded from scanning by using a special algorithm that takes into account the release date of Kaspersky Endpoint Security databases, the date that the file was last scanned on, and any modifications to the scanning settings. The iSwift technology is an advancement of the iChecker technology for the NTFS file system.

Advanced settings	
/C:<file	File with Virus scan task settings. The file must be created manually and saved in TXT format.

with virus scan settings>

The file can have the following contents: [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>].

Example:

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Updating databases and application software modules

Run the *Update* task.

Command syntax

```
UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<file with update settings >]
```

Update task settings	
local	<p>Start of the <i>Update</i> task that was created automatically after the application had been installed. You can change the settings of the <i>Update</i> task in the local application interface or in the console of Kaspersky Security Center. If this setting is not configured, Kaspersky Endpoint Security starts the <i>Update</i> task with default settings or with the settings specified in the command. You can configure Update task settings as follows:</p> <ul style="list-style-type: none">• UPDATE starts the <i>Update</i> task with the default settings: the update source is Kaspersky update servers, the account is System, and other default settings.• UPDATE local starts the <i>Update</i> task that was created automatically after installation (predefined task).• UPDATE <update settings> starts the <i>Update</i> task with manually defined settings (see below).

Update source	
"<update source>"	<p>Address of a HTTP or FTP server, or of a shared folder with the update package. You can specify only one update source. If the update source is not specified, Kaspersky Endpoint Security uses the default source – Kaspersky update servers.</p>

Saving events to a report file mode	
/R:<report file>	Save only critical events to the report file.
/RA:<report file>	Save all events to a report file.

Advanced settings	
-------------------	--

/C:<file with update settings>	File with the <i>Update</i> task settings. The file must be created manually and saved in TXT format. The file can have the following contents: ["<update source>"] [/R[A]:<report file>].
--------------------------------	--

```
Example:
avp.com UPDATE local

avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. Last update rollback

Roll back the last anti-virus database update. This lets you roll back the databases and application modules to their previous version when necessary, for example, when the new database version contains an invalid signature that causes Kaspersky Endpoint Security to block a safe application.

Command syntax

```
ROLLBACK [/R[A]:<report file>]
```

Saving events to a report file mode	
/R:<report file>	Save only critical events to the report file.
/RA:<report file>	Save all events to a report file.

```
Example:
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Tracing

Enable / disable tracing. [Trace files](#) are stored on the computer as long as the application is in use, and are deleted permanently when the application is removed. By default, tracing is disabled.

Command syntax

```
TRACES on|off [<tracing level>] [<advanced settings>]
```

Tracing level	
<tracing level>	Level of detail of traces. Available values: <ul style="list-style-type: none"> <li data-bbox="335 1915 949 1960">• 100 (critical). Only messages about fatal errors. <li data-bbox="335 1993 1085 2038">• 200 (high). Messages about all errors, including fatal errors. <li data-bbox="335 2072 1141 2116">• 300 (diagnostic). Messages about all errors, as well as warnings.

- 400 (important). All error messages, warnings, and additional information.
- 500 (normal). Messages about all errors and warnings, as well as detailed information about the operation of the application in normal mode (default).
- 600 (low). All messages.

Advanced settings	
all	Run a command with the <code>dbg</code> , <code>file</code> and <code>mem</code> parameters.
dbg	Use the <code>OutputDebugString</code> function and save the trace file. The <code>OutputDebugString</code> function sends a character string to the application debugger to display on screen. For details, visit the MSDN website .
file	Save one trace file (no size limit).
rot	Save traces to a limited number of files of limited size and overwrite the older files when the maximum size is reached.
mem	Save traces to dump files.

Examples:

- `avp.com TRACES on 500`
- `avp.com TRACES on 500 dbg`
- `avp.com TRACES off`
- `avp.com TRACES on 500 dbg mem`
- `avp.com TRACES off file`

START. Start the profile

Start the profile (for example, to update databases or to enable a protection component).

Command syntax

```
START <profile> [/R[A]:<report file>]
```

Profile	
<profile>	Profile name. A <i>Profile</i> is a Kaspersky Endpoint Security component, task or feature. You can view the list of available profiles by executing the <code>HELP START</code> command.

Saving events to a report file mode	
<code>/R:<report file></code>	Save only critical events to the report file.

```
/RA:<report file>
```

```
Save all events to a report file.
```

Example:

```
avp.com START Scan_Objects
```

STOP. Stopping a profile

Stop the running profile (for example, stop scanning, stop removable drives scan, or disable a protection component).

To execute this command, [Password protection must be enabled](#). The user must have the **Disable protection components** and **Disable control components** permissions.

Command syntax

```
STOP <profile> /login=<user name> /password=<password>
```

Profile	
<profile>	Profile name. A <i>Profile</i> is a Kaspersky Endpoint Security component, task or feature. You can view the list of available profiles by executing the HELP STOP command.

Authentication	
/login=<user name> /password=<password>	Information about the user account that is granted the required Password protection permissions.

STATUS. Profile status

Show status information for [application profiles](#) (for example, `running` or `completed`). You can view the list of available profiles by executing the HELP STATUS command.

Kaspersky Endpoint Security also displays information about the status of service profiles. Information about the status of service profiles may be required when you are contacting Kaspersky Technical Support.

Command syntax

```
STATUS [<profile>]
```

STATISTICS. Profile operation statistics

View statistical information about an [application profile](#) (for example, scan duration or the number of threats detected.) You can view the list of available profiles by executing the HELP STATISTICS command.

Command syntax

```
STATISTICS <profile>
```

RESTORE. Restoring files

You can restore a file from Backup to its original folder. If a file with the same name already exists at the specified path, the suffix "-copy" is appended to the file name. The file that is being restored is copied keeping its original name.

To execute this command, [Password protection must be enabled](#). The user must have the **Restore from Backup** permission.

Backup stores reserve copies of files that were deleted or modified during disinfection. A *backup copy* is a file copy created before the file was disinfected or deleted. Backup copies of files are stored in a special format and do not pose a threat.

Backup copies of files are stored in the folder C:\ProgramData\Kaspersky Lab\KES\QB.

Users in the Administrators group are granted full permission to access this folder. Limited access rights to this folder are granted to the user whose account was used to install Kaspersky Endpoint Security.

Kaspersky Endpoint Security does not provide the capability to configure user access permissions to backup copies of files.

Command syntax

```
RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Advanced settings	
/REPLACE	Overwrite an existing file.
<file name>	The name of the file to be restored.

Authentication	
/login=<user name> /password=<password>	Information about the user account that is granted the required Password protection permissions.

Example:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

EXPORT. Exporting application settings

Export Kaspersky Endpoint Security settings to a file. The file will be located in the C:\Windows\SysWOW64 folder.

Command syntax

```
EXPORT <profile> <file name>
```

Profile	
<profile>	Profile name. A <i>Profile</i> is a Kaspersky Endpoint Security component, task or feature. You can view the list of available profiles by executing the <code>HELP EXPORT</code> command.

File to export	
<file name>	The name of the file to which the application settings will be exported. You can export Kaspersky Endpoint Security settings to a DAT or CFG configuration file, to a TXT text file, or to an XML document.

Examples:

- `avp.com EXPORT ids ids_config.dat`
- `avp.com EXPORT fm fm_config.txt`

IMPORT. Importing application settings

Imports settings for Kaspersky Endpoint Security from a file that was created with the `EXPORT` command.

To execute this command, [Password protection must be enabled](#). The user must have the **Configure application settings** permission.

Command syntax

```
IMPORT <file name> /login=<username> /password=<password>
```

File to import	
<file name>	The name of the file from which the application settings will be imported. You can import Kaspersky Endpoint Security settings from a DAT or CFG configuration file, a TXT text file, or an XML document.

Authentication	
<code>/login=<user name></code> <code>/password=<password></code>	Information about the user account that is granted the required Password protection permissions.

Example:

```
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1
```

ADDKEY. Applying a key file

Apply the key file to activate Kaspersky Endpoint Security. If the application is already activated, the key will be added as a reserve one.

Command syntax

```
ADDKEY <file name> /login=<user name> /password=<password>
```

Key file	
<file name>	Key file name.

Authentication	
/login=<user name> /password=<password>	User account credentials. These credentials need to be entered only if Password protection is enabled.

Example:

```
avp.com ADDKEY file.key
```

LICENSE. Licensing

Perform actions with Kaspersky Endpoint Security license keys.

To execute this command and remove a license key, [Password protection must be enabled](#). The user must have the **Remove key** permission.

Command syntax

```
LICENSE <operation> [/login=<user name> /password=<password>]
```

Operation	
/ADD <file name>	Apply the key file to activate Kaspersky Endpoint Security. If the application is already activated, the key will be added as a reserve one.
/ADD <activation code>	Activate Kaspersky Endpoint Security using an activation code. If the application is already activated, the key will be added as a reserve one.
/REFRESH <file name>	Renew your license with a key file. A reserve key is added as a result. It becomes active upon license expiration. It is not possible to add an active key by executing this command.
/REFRESH <activation code>	Renew your license with an activation code. A reserve key is added as a result. It becomes active upon license expiration. It is not possible to add an active key by executing this command.
/DEL /login=<user	Remove a license key. Reserve key will also be removed.

```
name> /password=  
<password>
```

Authentication

```
/login=<user name>  
/password=<password>
```

Information about the user account that is granted the required [Password protection](#) permissions.

Example:

- avp.com LICENSE /ADD file.key
- avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
- avp.com LICENSE /DEL /login=KLAdmin /password=!Password1

RENEW. Purchasing a license

Open the Kaspersky website to purchase or renew your license.

PBATESTRESET. Reset the disk check results before encrypting the disk

Reset the compatibility check results for Full Disk Encryption(FDE), including both the Kaspersky Disk Encryption and BitLocker Drive Encryption technologies.

Before running Full Disk Encryption, the application performs a number of checks to verify that the computer can be encrypted. If the computer does not support Full Disk Encryption, Kaspersky Endpoint Security logs information about the incompatibility. The next time you try to encrypt, the application does not perform this check and warns you that encryption is not possible. If the hardware configuration of the computer has changed, the compatibility check results previously logged by the application must be reset to re-check the system hard drive for compatibility with Kaspersky Disk Encryption or BitLocker drive encryption technologies.

EXIT. Exit the application

Exits Kaspersky Endpoint Security. The application will be unloaded from the computer's RAM.

To execute this command, [Password protection must be enabled](#). The user must have the **Exit the application** permission.

Command syntax

```
EXIT /login=<user name> /password=<password>
```

EXITPOLICY. Disabling policy

Disables a Kaspersky Security Center policy on the computer. All Kaspersky Endpoint Security settings are available for configuration, including settings that have a closed lock in the policy (🔒).

To execute this command, [Password protection must be enabled](#). The user must have the **Disable Kaspersky Security Center policy** permission.

Command syntax

```
EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY. Enabling policy

Enables a Kaspersky Security Center policy on the computer. The application settings will be configured according to the policy.

DISABLE. Disabling protection

Disables File Threat Protection on a computer with an expired Kaspersky Endpoint Security license. It is not possible to run this command on a computer that has the application that is not activated, or has a valid license.

SPYWARE. Spyware detection

Enable / disable spyware detection. By default, spyware detection is enabled.

Command syntax

```
SPYWARE on|off
```

KESCLI commands

KESCLI commands let you receive information about the state of computer protection using the OPSWAT component, and let you perform standard tasks such as virus scans and database updates.

You can view the list of KESCLI commands by using the `--help` command or by using the abbreviated command `-h`.

To manage Kaspersky Endpoint Security from the command line:

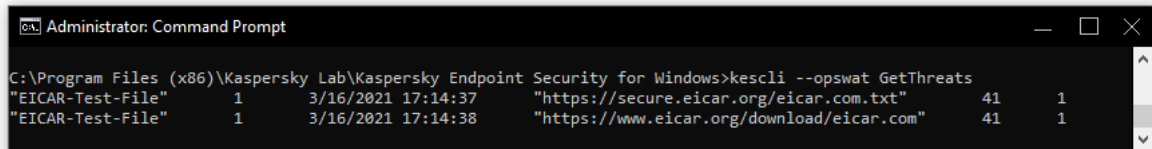
1. Run the command line interpreter (cmd.exe) as an administrator.

2. Go to the folder where the Kaspersky Endpoint Security executable file is located.

3. To execute a command, enter:

```
kescli <command> [options]
```

As a result, Kaspersky Endpoint Security will execute the command (see figure below.)



Managing the application from the command line

Scan. Virus Scan

Run the virus scan task.

Command syntax

```
--opswat Scan <scan scope> <action on threat detection>
```

You can check the status of *Full Scan* task completion by using the [GetScanState command](#) and view the date and time when the scan was last completed by using the [GetLastScanTime command](#).

Scan scope	
<files to scan>	; -separated list of files and folders. E.g., C:\Program Files (x86)\Example Folder.

Action on threat detection	
0	Inform. If this option is selected, Kaspersky Endpoint Security adds the information about infected files to the list of active threats on detection of these files.
1	Disinfect; delete if disinfection fails. If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected files that are detected. If disinfection fails, Kaspersky Endpoint Security deletes the files. This action is selected by default.

Example:

```
kescli --opswat Scan C:\Documents and Settings\All Users\My Documents;C:\Program Files 1
```

GetScanState. Scan completion status

Receive information about the status of *Full Scan* task completion:

- 1 – the scan is in progress.
- 0 – the scan is not running.

Command syntax

```
--opswat GetScanState
```

Example:

```
kescli --opswat GetScanState
```

GetLastScanTime. Determining the scan completion time

Receive information about the date and time of the last *Full Scan* task completion.

Command syntax

```
--opswat GetLastScanTime
```

Example:

```
kescli --opswat GetLastScanTime
```

GetThreats. Obtaining data on detected threats

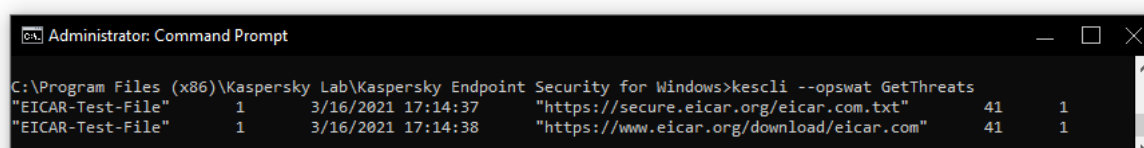
Receive a list of detected threats (*Threats report*). This report contains information about threats and virus activity during the last 30 days prior to creating the report.

Command syntax

```
--opswat GetThreats
```

When this command is executed, Kaspersky Endpoint Security will send a response in the following format:

```
<name of detected object> <type of object> <detection date and time> <path to file> <action on threat detection> <threat danger level>
```



```
Administrator: Command Prompt
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>kescli --opswat GetThreats
"EICAR-Test-File" 1 3/16/2021 17:14:37 "https://secure.eicar.org/eicar.com.txt" 41 1
"EICAR-Test-File" 1 3/16/2021 17:14:38 "https://www.eicar.org/download/eicar.com" 41 1
```

Object type	
0	Not known (Unknown).
1	Viruses (Virware).
2	Trojan programs (Trojware).
3	Malicious programs (Malware).
4	Advertisement programs (Adware).
5	Auto-dialer programs (Pornware).
6	Applications that could be used by a cybercriminal to harm the user's computer or data (Riskware).
7	Packed objects whose packing method may be used to protect malicious code (Packed).
20	Unknown objects (Xfiles).
21	Known applications (Software).
22	Concealed files (Hidden).
23	Application requiring attention (Pupware).
24	Anomalous behavior (Anomaly).
30	Not determined (Undetect).
40	Ad banners (Banner).
50	Network attack (Attack).
51	Registry access (Registry).
52	Suspicious activity (Suspicion).
60	Vulnerabilities (Vulnerability).
70	Phishing.
80	Unwanted email attachment (Attachment).
90	Malware detected by Kaspersky Security Network (Urgent).
100	Unknown link (Suspicious URL).
110	Other malware (Behavioral).

Action on threat detection	
0	Not known (unknown).
1	Threat was remediated (ok).
2	Object was infected and has not been disinfected (infected).
5	Object is in an archive and has not been disinfected (archive).
9	Object has been disinfected (disinfected).
10	Object has not been disinfected (not disinfected).

11	Object was deleted (deleted).
13	A backup copy of the object was created (backupped).
15	Object was moved to Backup (quarantined).
23	Object was deleted on computer restart (delete on reboot).
25	Object was disinfected on computer restart (disinfect on reboot).
29	Object was moved to Backup by a user (added by user).
30	Object was added to exclusions (added to exclude).
31	Object was moved to Backup on computer restart (quarantine on reboot).
36	False positive (false alarm).
38	Process was terminated (terminated).
40	Object was not detected (not found).
41	Cannot resolve the threat (untreatable).
42	Object was restored (rolled back).
43	Object was created as a result of threat activity (produced by threat).
44	Object was restored on computer restart (roll back on reboot).
0xffffffff	Object was not processed (discarded).

Threat danger level	
0	Unknown
1	High
2	Medium scan
4	Low
8	Info (less than <i>Low</i>)

UpdateDefinitions. Updating databases and application software modules

Run the *Update* task. Kaspersky Endpoint Security uses the default source: Kaspersky update servers.

Command syntax

```
--opswat UpdateDefinitions
```

You can view the date and time of the last completed *Update* task by using the [GetDefinitionsetState command](#).

Example:

```
kescli --opswat UpdateDefinitions
```

GetDefinitionState. Determining the update completion time

Receive information about the date and time of the last *Update* task completion.

Command syntax

```
--opswat GetDefinitionState
```

Example:

```
kescli --opswat GetDefinitionState
```

EnableRTP. Enabling protection

Enable Kaspersky Endpoint Security protection components on the computer: File Threat Protection, Web Threat Protection, Mail Threat Protection, Network Threat Protection, Host Intrusion Prevention.

Command syntax

```
--opswat EnableRTP
```

You can check the operating status of File Threat Protection by using the [GetRealTimeProtectionState command](#).

Example:

```
kescli --opswat EnableRTP
```

GetRealTimeProtectionState. File Threat Protection status

Receive information about the operating status of the File Threat Protection component:

- 1 – the component is enabled.
- 0 – the component is disabled.

Command syntax

```
--opswat GetRealTimeProtectionState
```

Example:

```
kescli --opswat GetRealTimeProtectionState
```

Version. Identifying the application version

Identify the version of Kaspersky Endpoint Security for Windows.

Command syntax

```
--Version
```

You can also use the abbreviated command `-v`.

Example:
`kescli -v`

Error codes

Errors may occur when working with the application through the command line. When errors occur, Kaspersky Endpoint Security shows an error message, for example, `Error: Cannot start task 'EntAppControl1'`. Kaspersky Endpoint Security can also show additional information in the form of a code, for example, `error=8947906D` (see the table below).

Error codes

Error code	Description
09479001	License key for Kaspersky Endpoint Security is already in use on this computer.
0947901D	License expired. Database update is not available.
89479002	Key not found.
89479003	Digital signature missing or corrupted.
89479004	Data corrupted.
89479005	Key file corrupted.
89479006	License expired or license key expired.
89479007	Key file not specified.
89479008	Cannot apply key file.
89479009	Failed to save data.
8947900A	Failed to read data.
8947900B	I/O error.
8947900C	Databases not found.
8947900E	Licensing library not loaded.
8947900F	Databases corrupted or updated manually.
89479010	Databases are corrupted.
89479011	Cannot use invalid key file to add a reserve key.
89479012	System error.
89479013	Black list of keys corrupted.
89479014	Digital signature of file does not match the digital signature of Kaspersky.

89479015	Cannot use a key for non-commercial license as a key for commercial license.
89479016	The beta license is required to use the beta version of the application.
89479017	Key file not compatible with this application.
89479018	Key blocked by Kaspersky.
89479019	Application has already been used under a trial license. Cannot add trial key again.
8947901A	Key file corrupted.
8947901B	Digital signature missing, corrupted, or does not match the digital signature of Kaspersky.
8947901C	Cannot add a key if the corresponding non-commercial license has expired.
8947901E	The date the key file was created or used is invalid. Check the system date.
8947901F	Cannot add a key for trial license: another key for trial license is already active.
89479020	Black list of keys corrupted or missing.
89479021	Update description missing or corrupted.
89479022	Error in license key service data.
89479023	Cannot use invalid key file to add a reserve key.
89479025	Error sending request to activation server. Possible reasons: Internet connection error or temporary problems on the activation server. Try to activate the application with the activation code later. If this error persists, contact your Internet provider.
89479026	Error in response from activation server.
89479027	Cannot obtain response status.
89479028	Error occurred when saving temporary file.
89479029	Activation code has been entered incorrectly or system date is incorrect. Check the system date on the computer.
8947902A	Key file not compatible with this application, or license expired. You cannot activate Kaspersky Endpoint Security by using a key file for a different application.
8947902B	Failed to receive key file. Incorrect activation code was entered.
8947902C	Activation server has returned error 400.
8947902D	Activation server has returned error 401.
8947902E	Activation server has returned error 403.
8947902F	Activation server has returned error 404.
89479030	Activation server has returned error 405.
89479031	Activation server has returned error 406.
89479032	Authentication on proxy server required. Check the network settings.
89479033	Request timeout expired.
89479034	Activation server has returned error 409.
89479035	Activation server has returned error 410.
89479036	Activation server has returned error 411.
89479037	Activation server has returned error 412.

89479038	Activation server has returned error 413.
89479039	Activation server has returned error 414.
8947903A	Activation server has returned error 415.
8947903C	Internal server error.
8947903D	Functionality not supported.
8947903E	Invalid response from gateway. Check the network settings.
8947903F	Service unavailable (HTTP Error 503).
89479040	Gateway response timeout has expired. Check the network settings.
89479041	The protocol is not supported by the server.
89479043	Unknown HTTP error.
89479044	Invalid resource ID.
89479046	Invalid URL.
89479047	Invalid destination folder.
89479048	Memory allocation error.
89479049	Error converting parameters to ANSI string (URL, folder, agent).
8947904A	Error creating worker thread.
8947904B	Worker thread already running.
8947904C	Worker thread not running.
8947904D	Key file not found on activation server.
8947904E	Key is blocked.
8947904F	Internal error of activation server.
89479050	Not enough data in activation request.
89479053	License key expired.
89479054	Incorrect system date is set on the computer.
89479055	Trial license has expired.
89479056	License expired.
89479057	The limit of application activations has been exceeded for the specified code.
89479058	Activation procedure ended with a system error.
89479059	Cannot use a key for non-commercial license as a key for commercial license.
8947905C	Activation code is required.
89479062	Cannot connect to activation server.
89479064	Activation server is unavailable. Please check your Internet connection settings and retry activation.
89479065	Application database release date exceeds the license expiration date.
89479066	Cannot replace the active key with an expired key.
89479067	Cannot add a reserve key if it expires before the current license.

89479068	Updated subscription key missing.
8947906A	Incorrect activation code (checksum does not match).
8947906B	Key already active.
8947906C	License types that correspond to active and reserve keys do not match.
8947906D	Component not supported by license.
8947906E	Unable to add subscription key as a reserve key.
89479213	Transport layer general error.
89479214	Failed to connect to activation server.
89479215	Invalid URL format.
89479216	Failed to convert proxy server address.
89479217	Failed to convert server address. Check the Internet connection settings.
89479218	Failed to connect to activation server or proxy server.
89479219	Remote access denied.
8947921A	Response timeout has expired.
8947921B	Error sending HTTP request.
8947921C	SSL connection error.
8947921D	Operation interrupted by callback.
8947921E	Too many forward attempts.
8947921F	Recipient check failed.
89479220	Empty response from activation server.
89479221	Error sending data.
89479222	Error receiving data.
89479223	Local SSL certificate error.
89479224	SSL encryption error.
89479225	Server SSL certificate error.
89479226	Invalid contents of network packet.
89479227	User access denied.
89479228	Invalid SSL certificate file.
89479229	Failed to establish SSL connection.
8947922A	Failed to send or receive network packet. Please try again later.
8947922B	Invalid file with revoked certificates.
8947922C	SSL certificate request error.
89479401	Unknown server error.
89479402	Internal server error.
89479403	No license key available for the activation code entered.
89479404	Active key blocked.

89479405	Required parameters of application activation request are missing.
89479406	Incorrect user name or password.
89479407	Incorrect activation code sent to server.
89479408	Activation code is invalid for Kaspersky Endpoint Security. The activation code is for an unknown application.
89479409	Request is missing an activation code.
8947940B	License expired (according to data from the activation server).
8947940C	Number of activations with this code has been exceeded.
8947940D	Invalid format of request ID.
8947940E	Activation code is invalid for Kaspersky Endpoint Security. Activation code is intended for a different Kaspersky application.
8947940F	Cannot update license key.
89479410	Activation code is invalid for this region.
89479411	Activation code is invalid for the Kaspersky Endpoint Security language version.
89479412	Additional access to the activation server is required.
89479413	Activation server has returned error 643.
89479414	Activation server has returned error 644.
89479415	Activation server has returned error 645.
89479416	Activation server has returned error 646.
89479417	Activation code format not supported by activation server.
89479418	Invalid activation code format.
89479419	Incorrect system time is set on the computer.
8947941A	Activation code is invalid for the Kaspersky Endpoint Security version.
8947941B	Subscription expired.
8947941C	Number of activations exceeded for this license key.
8947941D	Invalid digital signature of license key.
8947941E	Additional data is needed.
8947941F	User data verification failed.
89479420	Subscription inactive.
89479421	Activation server is under maintenance.
89479501	Unknown error of Kaspersky Endpoint Security.
89479502	Invalid parameter transferred (for example, an empty list of activation server addresses).
89479503	Incorrect activation code.
89479504	Invalid user name.
89479505	Invalid user password.
89479506	Invalid response from activation server.

89479507	Activation request interrupted.
89479509	Activation server returned an empty forwarding list.

Appendix. Application profiles

A *Profile* is a Kaspersky Endpoint Security component, task or feature. Profiles are used to manage the application from the command line. You can use profiles to execute `START`, `STOP`, `STATUS`, `STATISTICS`, `EXPORT`, and `IMPORT` commands. Using profiles, you can configure application settings (for example, `STOP DeviceControl`) or run tasks (for example, `START Scan_My_Computer`).

The following profiles are available:

- `AdaptiveAnomaliesControl` – Adaptive Anomaly Control.
- `AMSI` – AMSI Protection Provider.
- `BehaviorDetection` – Behavior Detection.
- `DeviceControl` – Device control.
- `EntAppControl` – Application Control.
- `File_Monitoring` or `FM` – File Threat Protection.
- `Firewall` or `FW` – Firewall.
- `HIPS` – Host Intrusion prevention.
- `IDS` – Network Threat Protection.
- `IntegrityCheck` – Integrity check.
- `Mail_Monitoring` or `EM` – Mail Threat Protection.
- `Rollback` – update rollback.
- `Scan_ContextScan` – Scan from context menu.
- `Scan_IdleScan` – Background scan.
- `Scan_Memory` – Kernel memory scan.
- `Scan_My_Computer` – Full scan.
- `Scan_Objects` – Custom scan.
- `Scan_Qscan` – Scan objects that are loaded at operation system startup.
- `Scan_Removable_Drive` – Removable drives scan.
- `Scan_Startup` or `STARTUP` – Critical Areas Scan.

- Updater – Update.
- Web_Monitoring or WM – Web Threat Protection.
- WebControl – Web Control.

Kaspersky Endpoint Security also supports service profiles. Service profiles may be required when you are contacting Kaspersky Technical Support.

Managing the application through the REST API

Kaspersky Endpoint Security lets you configure application settings, run a scan, update the anti-virus databases, and perform other tasks using third-party solutions. Kaspersky Endpoint Security provides an API for this purpose. The Kaspersky Endpoint Security REST API operates over HTTP and consists of a set of request/response methods. In other words, you can manage Kaspersky Endpoint Security through a third-party solution, and not the local application interface or the Kaspersky Security Center Administration Console.

To start using REST API, you need to [install Kaspersky Endpoint Security with support for the REST API](#). The REST client and Kaspersky Endpoint Security must be installed on the same computer.

To ensure safe interaction between Kaspersky Endpoint Security and REST client, do the following:

- Configure REST client's protection from unauthorized access according the recommendations of the REST client developer. Configure REST client folder protection from writing with the help of Discretionary Access Control List – DACL.
- To run REST client, use a separate account with administrator rights. Deny interactive sign-in into the system for this account.

The application is managed through the REST API at <http://127.0.0.1> or <http://localhost>. It is not possible to remotely manage Kaspersky Endpoint Security through the REST API.



[OPEN THE REST API DOCUMENTATION](#) 

Installing the application with the REST API

To manage the application through the REST API, you need to install Kaspersky Endpoint Security with support for the REST API. If you manage Kaspersky Endpoint Security through the REST API, you cannot manage the application using Kaspersky Security Center.

To install Kaspersky Endpoint Security with REST API support:

1. Run the command line interpreter (cmd.exe) as an administrator.
2. Go to the folder that contains the distribution package for Kaspersky Endpoint Security version 11.2.0 or later.
3. Install Kaspersky Endpoint Security with the following settings:
 - `RESTAPI=1`
 - `RESTAPI_User=<User name>`
User name for managing the application through the REST API. Enter the user name in the format `<DOMAIN>\<UserName>` (for example, `RESTAPI_User=COMPANY\Administrator`). You can manage the application through the REST API only under this account. You can select only one user to work with the REST API.
 - `RESTAPI_Port=<Port>`
Port used for data exchange. Optional parameter. Port 6782 is selected by default.
 - `AdminKitConnector=1`
Application management using administration systems. Management is allowed by default.

You can also use the [setup.ini file](#) to define the settings for working with the REST API.

You can define the settings for working with the REST API only during application installation. It is not possible to change the settings after the application is installed. If you want to change the settings, uninstall Kaspersky Endpoint Security and reinstall it with the new settings for working with the REST API.

Example:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1  
/pAdminKitConnector=1 /pRESTAPI=1 /pRESTAPI_User=COMPANY\Administrator /s
```

As a result, you will be able to manage the application through the REST API. To verify its operation, open the REST API documentation using a GET request.

Example:

```
GET http://localhost:6782/kes/v1/api-docs
```

Working with the API

It is not possible to restrict access to the application through the REST API using [Password Protection](#). For example, it is not possible to block a user from disabling protection through the REST API. You can configure Password Protection through the REST API and restrict user access to the application through the local interface.

To manage the application through the REST API, you need to run the REST client under the account that you specified when [installing the application with REST API support](#). You can select only one user to work with the REST API.



[OPEN THE REST API DOCUMENTATION](#) 

Managing the application through the REST API consists of the following steps:

1. Get the current values of the application settings. To do so, send a GET request.

Example:

```
GET http://localhost:6782/kes/v1/settings/ExploitPrevention
```

2. The application will send a response with the structure and values of settings. Kaspersky Endpoint Security supports XML- and JSON formats.

Example:

```
{  
  "action": 0,  
  "enableSystemProcessesMemoryProtection": true,  
  "enabled": true  
}
```

3. Edit the application settings. To do so, send a POST request. Use the settings structure received in response to the GET request.

Example:

```
POST http://localhost:6782/kes/v1/settings/ExploitPrevention
{
  "action": 0,
  "enableSystemProcessesMemoryProtection": false,
  "enabled": true
}
```

4. The application will apply the changes in the settings and send a response containing the application configuration results.

Sources of information about the application

Kaspersky Endpoint Security page on the Kaspersky website

On the [Kaspersky Endpoint Security page](#), you can view general information about the application and its functions and features.

The Kaspersky Endpoint Security page contains a link to the online store. There you can purchase or renew the application.

Kaspersky Endpoint Security page in the Knowledge Base

Knowledge Base is a section on the Technical Support website.

On the [Kaspersky Endpoint Security page in the Knowledge Base](#), you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to purchase, install, and use the application.

Knowledge Base articles can answer questions relating to not only Kaspersky Endpoint Security but also to other Kaspersky applications. Articles in the Knowledge Base may also contain news from Technical Support.

Discussion of Kaspersky applications in user community

If your question does not require an urgent answer, you can discuss it with Kaspersky experts and other users in our [Community](#).

In the Community, you can view existing topics, post your own comments, and create new discussion topics.

Contacting Technical Support

This section describes the ways to get technical support and the terms on which it is available.

How to get technical support

If you cannot find a solution to your problem in the documentation or in other [sources of information about Kaspersky Endpoint Security](#), we recommend that you contact Technical Support. Technical Support will answer your questions about installing and using Kaspersky Endpoint Security.

Kaspersky provides support for Kaspersky Endpoint Security during the application's life cycle (refer to the [application life cycle page](#)). Before contacting Technical Support, please read the [support rules](#).

You can contact Technical Support in one of the following ways:

- By [visiting the Technical Support website](#)
- By sending a request to Kaspersky Technical Support through the [Kaspersky CompanyAccount portal](#)

Technical Support via Kaspersky CompanyAccount

[Kaspersky CompanyAccount](#) is a portal for companies that use Kaspersky applications. The Kaspersky CompanyAccount portal is designed to facilitate interaction between users and Kaspersky experts via electronic requests. You can use Kaspersky CompanyAccount portal to track the status of your electronic requests and store a history of those requests.

You can register all of your organization's employees under a single account on Kaspersky CompanyAccount. A single account lets you centrally manage electronic requests from registered employees to Kaspersky and also manage the privileges of these employees via Kaspersky CompanyAccount.

Kaspersky CompanyAccount portal is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish
- Portuguese
- Russian
- French
- Japanese

To learn more about Kaspersky CompanyAccount, visit the [Technical Support website](#).

Obtaining information for Technical Support

After you inform Kaspersky Technical Support specialists about your issue, they may ask you to create a *trace file*. The trace file allows you to trace the process of performing application commands step by step and determine the stage of application operation at which an error occurs.

Technical Support specialists may also require additional information about the operating system, processes that are running on the computer, detailed reports on the operation of application components.

While running diagnostics, Technical Support experts may ask you to change application settings by:

- Activating the functionality for receiving extended diagnostic information.
- Fine-tuning the settings of individual application components, which are not available via standard user interface elements.
- Changing the settings for storage of diagnostic information.
- Configuring the interception and logging of network traffic.

Technical Support experts will provide all the information needed to perform these operations (description of the sequence of steps, settings to be modified, configuration files, scripts, additional command line functionality, debugging modules, special-purpose utilities, etc.) and inform you about the scope of data used for purposes of debugging. The extended diagnostic information is saved on the user's computer. The data is not automatically transmitted to Kaspersky.

The operations listed above should be performed only under the supervision of Technical Support specialists by following their instructions. Unsupervised changes to application settings performed in ways other than those described in the Administrator's Guide or instructions of Technical Support specialists can slow down or crash the operating system, affect computer security, or compromise the availability and integrity of data being processed.

Contents and storage of trace files

You are personally responsible for the security of the data that is stored on your computer, particularly for monitoring and restricting access to the data until it is submitted to Kaspersky.

Trace files are stored on the computer as long as the application is in use, and are deleted permanently when the application is removed.

Trace files, except trace files of Authentication Agent, are stored in the folder %ProgramData%\Kaspersky Lab.

Trace files are named as follows: KES<version number_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log.

You can view data saved in trace files.

All trace files contain the following common data:

- Event time.
- Number of the thread of execution.

The Authentication Agent trace file does not contain this information.

- Application component that caused the event.
- Degree of event severity (informational event, warning, critical event, error).
- A description of the event involving command execution by a component of the application and the result of execution of this command.

Kaspersky Endpoint Security saves user passwords to a trace file only in encrypted form.

Contents of SRV.log, GUI.log, and ALL.log trace files

SRV.log, GUI.log, and ALL.log trace files may store the following information in addition to general data:

- Personal data, including the last name, first name, and middle name, if such data is included in the path to files on the local computer.
- Data on the hardware installed on the computer (such as BIOS/UEFI firmware data). This data is written to trace files when performing Kaspersky Disk Encryption.
- The user name and password if they were transmitted openly. This data can be recorded in trace files during Internet traffic scanning.
- The user name and password if they are contained in HTTP headers.
- The name of the Microsoft Windows account if the account name is included in a file name.
- Your email address or a web address containing the name of your account and password if they are contained in the name of the object detected.
- Websites that you visit and redirects from these websites. This data is written to trace files when the application scans websites.
- Proxy server address, computer name, port, IP address, and user name used to sign in to the proxy server. This data is written to trace files if the application uses a proxy server.
- Remote IP addresses to which your computer established connections.
- Message subject, ID, sender's name and address of the message sender's web page on a social network. This data is written to trace files if the Web Control component is enabled.
- Network traffic data. This data is written to trace files if traffic monitoring components are enabled (such as Web Control).
- Data received from Kaspersky servers (such as the version of anti-virus databases).

- Statuses of Kaspersky Endpoint Security components and their operating data.
- Data on user activity in the application.
- Operating system events.

Contents of HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log trace files

In addition to general data, the HST.log trace file contains information about the execution of a database and application module update task.

In addition to general data, the BL.log trace file contains information about events occurring during operation of the application, as well as data required to troubleshoot application errors. This file is created if the application is started with the avp.exe -bl parameter.

In addition to general data, the Dumpwriter.log trace file contains service information required for troubleshooting errors that occur when the application dump file is written.

In addition to general data, the WD.log trace file contains information about events occurring during operation of the avpsus service, including application module update events.

In addition to general data, the AVPCon.dll.log trace file contains information about events occurring during the operation of the Kaspersky Security Center connectivity module.

Contents of performance trace files

Performance trace files are named as follows: KES<version number_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl.

In addition to general data, performance trace files contain information about the load on the processor, information about the loading time of the operating system and applications, and information about running processes.

Contents of the AMSI Protection Provider trace files

In addition to general data, the AMSI.log trace file contains information about the results of scans performed on requests from third-party applications.

Contents of trace files of the Mail Threat Protection component

The trace file mcou.OUTLOOK.EXE.log may contain parts of email messages, including email addresses, in addition to general data.

Contents of trace files of the Scan from Context Menu component

The shelllex.dll.log trace file contains information about completion of the scan task and data required to debug the application, in addition to general information.

Contents of trace files of the application web plug-in

Trace files of the application web plug-in are stored on the computer on which Kaspersky Security Center 12 Web Console is deployed, in the folder Program Files\Kaspersky Lab\Kaspersky Security Center Web Console 12\logs.

Trace files of the application web plug-in are named as follows: logs-kes_windows-<type of trace file>.DESKTOP-<date of file update>.log. Web Console begins writing data after installation and deletes the trace files after Web Console is removed.

Trace files of the application web plug-in contain the following information in addition to general data:

- KLAdmin user password for unlocking the Kaspersky Endpoint Security interface ([Password protection](#)).
- Temporary password for unlocking the Kaspersky Endpoint Security interface ([Password protection](#)).
- User name and password for the SMTP mail server ([Email notifications](#)).
- User name and password for the Internet proxy server ([Proxy server](#)).
- User name and password for the [Change application components task](#).
- Account credentials and paths specified in Kaspersky Endpoint Security tasks and policy properties.

Contents of the Authentication Agent trace file

The Authentication Agent trace file is stored in the System Volume Information folder and is named as follows: KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin.

In addition to general data, the Authentication Agent trace file contains information about the operation of Authentication Agent and the actions performed by the user with Authentication Agent.

Application traces

Application traces are detailed records of the actions performed by the application, and of messages about events that occurred during operation of the application.

Application traces should be performed under the supervision of Kaspersky Technical Support.

To create an application trace file:

1. In the main application window, click the **Support** button.
The **Support** window opens.
2. In the **Support** window, click the **System traces** button.
The **Information for Technical Support** window opens.
3. To start the tracing process, select one of the following items in the **Application traces** drop-down list:
 - **is enabled**
Select this item to enable tracing.
 - **with rotation.**

Select this item to enable tracing and limit the maximum number of trace files and the maximum size of each trace file. If the maximum number of trace files of the maximum size is written, the oldest trace file is deleted so that a new trace file can be written.

If this item is selected, you can specify a value for the following fields:

- **Maximum number of files for rotation**
- **Maximum size for each file**

4. In the **Level** drop-down list, select the tracing level.

You are advised to clarify the required tracing level with a Technical Support specialist. In the absence of guidance from Technical Support, set the tracing level to **Normal (500)**.

5. Restart Kaspersky Endpoint Security.

6. To stop the tracing process, return to the **Information for Technical Support** window and select **Disabled** in the **Application traces** drop-down list.

You can also create trace files when installing the application from the [command line](#), including by using the [setup.ini file](#).

Application performance traces

Kaspersky Endpoint Security lets you receive information about computer operating issues during use of the application. For example, you can receive information about delays in operating system loading after the application is installed. To do so, Kaspersky Endpoint Security creates [performance trace files](#). *Performance traces* refer to the logging of actions performed by the application for the purpose of diagnosing performance issues of Kaspersky Endpoint Security. To receive information, Kaspersky Endpoint Security uses the Event Tracing for Windows service (ETW). Kaspersky Technical Support is responsible for diagnosing issues of Kaspersky Endpoint Security and establishing the reasons for those issues.

Application traces should be performed under the supervision of Kaspersky Technical Support.

To create a performance trace file:

1. In the main application window, click the **Support** button.

2. In the **Support** window, click the **System traces** button.

The **Information for Technical Support** window opens.

3. In the **Performance traces** drop-down list, select **Enabled** or **With rotation**.

Rotation lets you limit the size of a trace file. Specify the maximum size for a trace file. If the size of a file reaches the maximum size, Kaspersky Endpoint Security overwrites the oldest lines in the file.

4. In the **Level** drop-down list, select the tracing level:

- **Light**. Kaspersky Endpoint Security analyzes the main operating system processes related to performance.
- **Detailed**. Kaspersky Endpoint Security analyzes all operating system processes related to performance.

5. In the **Tracing type** drop-down list, select the tracing type:

- **Basic information.** Kaspersky Endpoint Security analyzes processes while the operating system is running. Use this tracing type if a problem persists after the operating system is loaded, such as a problem accessing the Internet in the browser.
- **On restart.** Kaspersky Endpoint Security analyzes processes only while the operating system is loading. After the operating system is loaded, Kaspersky Endpoint Security stops tracing. Use this tracing type if the problem is related to delayed loading of the operating system.

6. Restart the computer and try to reproduce the problem.

7. To stop the tracing process, return to the **Information for Technical Support** window and select **is disabled** in the **Performance traces** drop-down list.

As a result, a performance trace file will be created in the folder %ProgramData%\Kaspersky Lab. After the trace file is created, send the file to Kaspersky Technical Support.

Dump writing

Saved dump files may contain confidential data. To control access to data, you must independently ensure the security of dump files.

Dump files are stored on the computer as long as the application is in use, and are deleted permanently when the application is removed. Dump files are stored in the folder %ProgramData%\Kaspersky Lab.

A dump file contains all information about the working memory of Kaspersky Endpoint Security processes at the moment when the dump file was created.

To enable or disable dump writing:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Application Settings**.
3. In the **Debug information** section, click the **Settings** button.
The **Debug information** window opens.
4. Do one of the following:
 - Select the **Enable dump writing** check box if you want the application to write dumps of the application.
 - Clear the **Enable dump writing** check box if you do not want the application to write dumps of the application.
5. Click **OK** in the **Debug information** window.
6. To save the changes, click the **Save** button in the main application window.

Protecting dump files and trace files

Dump files and trace files contain information about the operating system, and may also contain [user data](#). To prevent unauthorized access to such data, you can enable protection of dump files and trace files.

If protection of dump files and trace files is enabled, the files can be accessed by the following users:

- Dump files can be accessed by the system administrator and local administrator, and by the user that enabled the writing of dump files and trace files.
- Trace files can be accessed only by the system administrator and local administrator.

To enable or disable protection of dump files and trace files:

1. In the main application window, click the **Settings** button.
2. In the application settings window, select **General Settings** → **Application Settings**.
3. In the **Debug information** section, click the **Settings** button.

The **Debug information** window opens.

4. Do one of the following:
 - Select the **Enable dump and trace files protection** check box if you want to enable protection.
 - Clear the **Enable dump and trace files protection** check box if you want to disable protection.
5. Click **OK** in the **Debug information** window.
6. To save the changes, click the **Save** button in the main application window.

Dump files and trace files that were written while protection was active remain protected even after this function is disabled.

Glossary

Active key

A key that is currently used by the application.

Administration group

A set of devices that share common functions and a set of Kaspersky applications installed on them. Devices are grouped so that they can be managed conveniently as a single unit. A group may include other groups. It is possible to create group policies and group tasks for each installed application in the group.

Anti-virus databases

Databases that contain information about computer security threats known to Kaspersky as of the date when the anti-virus databases were released. Anti-virus database records help to detect malicious code in scanned objects. Anti-virus databases are created by Kaspersky specialists and updated hourly.

Archive

One or several files packed into a single compressed file. A specialized application called an archiver is required for packing and unpacking data.

Authentication Agent

Interface that lets you complete authentication to access encrypted hard drives and load the operating system after the bootable hard drive has been encrypted.

Certificate issuer

Certification center that issued the certificate.

Database of malicious web addresses

A list of web addresses whose content may be considered to be dangerous. The list is created and regularly updated by Kaspersky experts, and is included in the Kaspersky application distribution kit.

Database of phishing web addresses

A list of addresses of web resources that Kaspersky experts have determined to be phishing-related. The database is regularly updated and is part of the Kaspersky application distribution kit.

Disinfection

A method of processing infected objects that results in complete or partial recovery of data. Not all infected objects can be disinfected.

False alarm

A false alarm occurs when the Kaspersky application reports an uninfected file as infected because the signature of the file is similar to that of a virus.

Infected file

A file which contains malicious code (code of known malware has been detected when scanning the file). Kaspersky does not recommend using such files, because they may infect your computer.

License certificate

A document that Kaspersky transfers to the user together with the key file or activation code. It contains information about the license granted to the user.

Mask

Representation of a file name and extension by using wildcards.

File masks can contain any characters that are allowed in file names, including wildcards:

- The * (asterisk) character, which takes the place of any set of characters, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:**.txt` will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.
- Two consecutive * characters take the place of any set of characters (including an empty set) in the file or folder name, including the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder***.txt` will include all paths to files with the TXT extension located in the folder named `Folder` and its subfolders. The mask must include at least one nesting level. The mask `C:***.txt` is not a valid mask. The ** mask is available only for creating scan exclusions.
- The ? (question mark) character, which takes the place of any single character, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:\Folder\???.txt` will include paths to all files residing in the folder named `Folder` that have the TXT extension and a name consisting of three characters.

Network Agent

A Kaspersky Security Center component that enables interaction between the Administration Server and Kaspersky applications that are installed on a specific network node (workstation or server). This component is common for all Kaspersky applications running under Windows. Dedicated versions of Network Agent are intended for applications running under other operating systems.

Normalized form of the address of a web resource

The normalized form of the address of a web resource is a textual representation of a web resource address that is obtained through normalization. Normalization is a process whereby the textual representation of a web resource address changes according to specific rules (for example, exclusion of the user login, password, and connection port from the text representation of the web resource address; additionally, the web resource address is changed from uppercase to lowercase characters).

Regarding the operation of protection components, the purpose of normalization of web resource addresses is to avoid scanning website addresses, which may differ in syntax while being physically equivalent, more than once.

Example:

Non-normalized form of an address: `www.Example.com\.`

Normalized form of an address: `www.example.com.`

OLE object

An attached file or a file that is embedded in another file. Kaspersky applications allow scanning OLE objects for viruses. For example, if you insert a Microsoft Office Excel® table into a Microsoft Office Word document, the table is scanned as an OLE object.

Portable File Manager

This is an application that provides an interface for working with encrypted files on removable drives when encryption functionality is not available on the computer.

Protection scope

Objects that are constantly being scanned by the Essential Threat Protection component when it is running. The protection scopes of different components have different properties.

Reserve key

A key that certifies the right to use the application but is not currently being used.

Scan scope

Objects that Kaspersky Endpoint Security scans while performing a scan task.

Task

Functions performed by the Kaspersky application as tasks, for example: Real-time File Protection, Full Device Scan, Database Update.

Trusted Platform Module

A microchip developed to provide basic functions related to security (for example, for storing encryption keys). A Trusted Platform Module is usually installed on the computer motherboard and interacts with all other system components via the hardware bus.

Appendices

This section contains information that supplements the body of the document.

Appendix 1. Policy settings in the Web Console and Cloud Console

You can use a [policy](#) to configure Kaspersky Endpoint Security settings. Detailed information about application components is provided in the corresponding sections.

Kaspersky Security Network

To protect your computer more effectively, Kaspersky Endpoint Security uses data that is received from users around the globe. Kaspersky Security Network is designed for obtaining this data.

Kaspersky Security Network (KSN) is an infrastructure of cloud services providing access to the online Kaspersky Knowledge Base that contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky Endpoint Security to new threats, improves the performance of some protection components, and reduces the likelihood of false positives. If you are participating in Kaspersky Security Network, KSN services provide Kaspersky Endpoint Security with information about the category and reputation of scanned files, as well as information about the reputation of scanned web addresses.

Use of Kaspersky Security Network is voluntary. The application prompts you to use KSN during initial configuration of the application. Users can begin or discontinue participation in KSN at any time.

For more detailed information about sending Kaspersky statistical information that is generated during participation in KSN, and about the storage and destruction of such information, please refer to the Kaspersky Security Network Statement and the [Kaspersky website](#). The `ksn_<language ID>.txt` file with the text of the Kaspersky Security Network Statement is included in the application [distribution kit](#).

To reduce the load on KSN servers, Kaspersky experts may release application updates that temporarily disable or partly restrict requests to Kaspersky Security Network. In this case, the status of the connection to KSN in the local interface of the application is *Enabled with restrictions*.

KSN Infrastructure

Kaspersky Endpoint Security supports the following KSN infrastructural solutions:

- *Global KSN* is the solution that is used by most Kaspersky applications. KSN participants receive information from Kaspersky Security Network and send Kaspersky information about objects detected on the user's computer to be analyzed additionally by Kaspersky analysts and to be included in the reputation and statistical databases of Kaspersky Security Network.
- *Private KSN* is a solution that enables users of computers hosting Kaspersky Endpoint Security or other Kaspersky applications to obtain access to reputation databases of Kaspersky Security Network, and to other statistical data without sending data to KSN from their own computers. Private KSN is designed for corporate customers who are unable to participate in Kaspersky Security Network for any of the following reasons:

- Local workstations are not connected to the Internet.
- Transmission of any data outside the country or outside the corporate LAN is prohibited by law or restricted by corporate security policies.

By default, Kaspersky Security Center uses Global KSN. You can configure the use of Private KSN in the Administration Console (MMC) and Kaspersky Security Center 12 Web Console. It is not possible to configure the use of Private KSN in the Kaspersky Security Center Cloud Console.

For more details about Private KSN, please refer to the *documentation on Kaspersky Private Security Network*.

KSN Proxy

User computers managed by Kaspersky Security Center Administration Server can interact with KSN via the KSN Proxy service.

The KSN Proxy service provides the following capabilities:

- The user's computer can query KSN and submit information to KSN even without direct access to the Internet.
- The KSN Proxy service caches processed data, thereby reducing the load on the external network communication channel and speeding up receipt of the information that is requested by the user's computer.

For more details on the KSN Proxy service, please refer to the [Kaspersky Security Center Help Guide](#).

Kaspersky Security Network settings

Parameter	Description
Extended KSN mode	<i>Extended KSN mode</i> is a mode in which Kaspersky Endpoint Security sends additional data to Kaspersky. Kaspersky Endpoint Security uses KSN to detect threats regardless of the toggle position.
Cloud mode	<p><i>Cloud mode</i> refers to the application operating mode in which Kaspersky Endpoint Security uses a light version of anti-virus databases. Kaspersky Security Network supports the operation of the application when light anti-virus databases are being used. The light version of anti-virus databases lets you use approximately half of the computer RAM that would otherwise be used with the usual databases. If you do not participate in Kaspersky Security Network or if cloud mode is disabled, Kaspersky Endpoint Security downloads the full version of anti-virus databases from Kaspersky servers.</p> <p>If the toggle button is switched on, Kaspersky Endpoint Security uses the light version of anti-virus databases, which reduces the load on operating system resources.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Kaspersky Endpoint Security downloads the light version of anti-virus databases during the next update after the check box was selected.</p> </div> <p>If the toggle button is switched off, Kaspersky Endpoint Security uses the full version of anti-virus databases.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Kaspersky Endpoint Security downloads the full version of anti-virus databases during the next update after the check box was cleared.</p> </div>

Computer status when KSN servers are unavailable	The items in this drop-down list determine the status of a computer in Kaspersky Security Center when KSN servers are unavailable (Devices → Managed devices).
Use KSN Proxy	If the check box is selected, Kaspersky Endpoint Security uses the KSN Proxy service. You can configure the KSN Proxy service settings in the Administration Server properties.
Use KSN servers when KSN Proxy is not available	If the check box is selected, Kaspersky Endpoint Security uses KSN servers when the KSN Proxy service is unavailable. KSN servers may be located both on the side of Kaspersky (when Global KSN is used) and on the side of third parties (when Private KSN is used).

Behavior Detection

The Behavior Detection component receives data on the actions of applications on your computer and provides this information to other protection components to improve their performance.

The Behavior Detection component utilizes Behavior Stream Signatures (BSS) for applications. If application activity matches a behavior stream signature, Kaspersky Endpoint Security performs the selected responsive action. Kaspersky Endpoint Security functionality based on behavior stream signatures provides proactive defense for the computer.

Behavior Detection component settings

Parameter	Description
On detecting malware activity	<ul style="list-style-type: none"> • Delete file. If this option is selected, on detecting malicious activity Kaspersky Endpoint Security deletes the executable file of the malicious application and creates a backup copy of the file in Backup. • Terminate the program. If this option is selected, on detecting malicious activity Kaspersky Endpoint Security terminates this application. • Inform. If this option is selected and malware activity of an application is detected, Kaspersky Endpoint Security does not terminate this application and adds information about its malware activity to the list of active threats.
Protection of shared folders against external encryption	<p>If the toggle button is switched on, Kaspersky Endpoint Security analyzes activity in shared folders. If this activity matches a behavior stream signature that is typical for external encryption, Kaspersky Endpoint Security performs the selected action.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>Kaspersky Endpoint Security prevents external encryption of only those files that are located on media that have the NTFS file system and are not encrypted by the EFS system.</p> </div>
On detection of external encryption of	<ul style="list-style-type: none"> • Inform. If this option is selected, on detecting an attempt to modify files in shared folders, Kaspersky Endpoint Security adds information about this attempt to modify files in shared folders to the list of active threats.

shared folders	<ul style="list-style-type: none"> • Block connection. If this option is selected, on detecting an attempt to modify files in shared folders, Kaspersky Endpoint Security blocks network activity originating from the computer attempting to modify files and creates backup copies of modified files. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>If the Remediation Engine component is enabled and the Block connection option is selected, Kaspersky Endpoint Security restores modified files from backup copies.</p> </div>
Block connection for N minutes	<p>The time for which Kaspersky Endpoint Security blocks the network activity of the remote computer performing encryption of shared folders.</p>
Exclusions	<p>List of computers from which attempts to encrypt shared folders will not be monitored.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>To apply the list of exclusions of computers from protection of shared folders against external encryption, you must enable Audit Logon in the Windows security audit policy. Audit Logon is disabled by default. For more details about a Windows security audit policy, please visit the Microsoft website.</p> </div>

Exploit Prevention

The Exploit Prevention component detects program code that takes advantage of vulnerabilities on the computer to exploit administrator privileges or to perform malicious activities. For example, exploits can utilize a buffer overflow attack. To do so, the exploit sends a large amount of data to a vulnerable application. When processing this data, the vulnerable application executes malicious code. As a result of this attack, the exploit can start an unauthorized installation of malware.

When there is an attempt to run an executable file from a vulnerable application that was not performed by the user, Kaspersky Endpoint Security blocks this file from running or notifies the user.

Exploit Prevention component settings

Parameter	Description
On detecting exploit	<ul style="list-style-type: none"> • Block operation. If this option is selected, on detection of an exploit Kaspersky Endpoint Security blocks the actions attempted by the exploit. • Inform. If this option is selected and an exploit is detected, Kaspersky Endpoint Security does not block the actions of the exploit but adds information about this exploit to the list of active threats.
System processes memory protection	<p>If this toggle button is switched on, Kaspersky Endpoint Security blocks external processes that attempt to access system process memory.</p>

Host Intrusion Prevention

The Host Intrusion Prevention component prevents applications from performing actions that may be dangerous for the operating system, and ensures control over access to operating system resources and personal data. The component provides computer protection with the help of anti-virus databases and the Kaspersky Security Network cloud service.

The component controls the operation of applications by using *application rights*. Application rights include the following access parameters:

- Access to operating system resources (for example, automatic startup options, registry keys)
- Access to personal data (such as files and applications)

Network activity of applications is controlled by the [Firewall](#) using *network rules*.

During the first startup of the application, the Host Intrusion Prevention component performs the following actions:

1. Checks the security of the application using downloaded anti-virus databases.
2. Checks the security of the application in Kaspersky Security Network.

You are advised to [participate in Kaspersky Security Network](#) to help the Host Intrusion Prevention component work more effectively.

3. Puts the application in one of the *trust groups*: Trusted, Low Restricted, High Restricted, Untrusted.

A [trust group defines the rights](#) used by Kaspersky Endpoint Security when controlling network activity of applications. Kaspersky Endpoint Security places an application in a trust group depending on the level of danger that this application may pose to the computer.

Kaspersky Endpoint Security places an application in a trust group for the Firewall and Host Intrusion Prevention components. You cannot change the trust group only for the Firewall or Host Intrusion Prevention.

If you refused to participate in KSN or there is no network, Kaspersky Endpoint Security places the application in a trust group depending on the [settings of the Host Intrusion Prevention component](#). After receiving the reputation of the application from KSN, the trust group can be changed automatically.

4. Blocks application actions depending on the trust group. For example, applications from the High Restricted trust group are denied access to the operating system modules.

The next time the application is started, Kaspersky Endpoint Security checks the integrity of the application. If the application is unchanged, the component uses the current application rights for it. If the application has been modified, Kaspersky Endpoint Security analyzes the application as if it were being started for the first time.

Host Intrusion Prevention component settings

Parameter	Description
Application rights	Applications Table of applications that are monitored by the Host Intrusion Prevention component. Applications are assigned to trust groups. A trust group defines the rights that Kaspersky Endpoint Security refers to when controlling application activity.

	<p>You can select an application from a single list of all applications installed on computers under the influence of a policy and add the application to a trust group.</p> <p>Application access rights are presented in the following tables:</p> <ul style="list-style-type: none"> • Files and system registry. This table contains the rights of applications within a trust group to access operating system resources and personal data. • Rights. This table contains the rights of applications in a trust group to access processes and resources of the operating system. • Network rules. Table of network rules for applications that are part of a trust group. In accordance with these rules, Firewall regulates the network activity of applications. The table displays the predefined network rules that are recommended by Kaspersky experts. These network rules have been added to optimally protect the network traffic of computers running Windows operating systems. It is not possible to delete the predefined network rules.
<p>Protected resources</p>	<p>Name</p> <p>The table contains categorized computer resources. The Host Intrusion Prevention component monitors attempts by other applications to access resources in the table.</p> <p>A resource can be a registry category, file or folder, or registry key.</p> <p>Applications</p> <p>Table of applications monitored by the Host Intrusion Prevention component for the selected resource. Applications are assigned to trust groups. A trust group defines the rights that Kaspersky Endpoint Security refers to when controlling application activity.</p>
<p>Applications launched before Kaspersky Endpoint Security for Windows are automatically moved to the trust group</p>	<p>A trust group in which Kaspersky Endpoint Security will place applications that are started before Kaspersky Endpoint Security.</p>
<p>Update rights for previously unknown applications from KSN database</p>	<p>If the check box is selected, the Host Intrusion Prevention component updates rights for previously unknown applications by using the Kaspersky Security Network database.</p>
<p>Trust applications that have a digital signature</p>	<p>If this check box is selected, the Host Intrusion Prevention component places digitally signed applications in the Trusted group.</p> <p>If this check box is cleared, the Host Intrusion Prevention component does not consider digitally signed applications to be trusted, and uses other parameters to determine their trust group.</p>
<p>Delete rights for applications that are not started for more than N days</p>	<p>If the check box is selected, Kaspersky Endpoint Security automatically deletes information about the application (trust group and access rights) if the following conditions are met:</p> <ul style="list-style-type: none"> • You manually put the application into a trust group or configured its access rights. • The application has not started within the defined period of time.

	<p>If the trust group and rights of an application were determined automatically, Kaspersky Endpoint Security deletes information about this application after 30 days. It is not possible to change the storage term for application information or turn off automatic deletion.</p> <p>The next time you start this application, Kaspersky Endpoint Security analyzes the application as if it were starting for the first time.</p>
<p>If a trust group cannot be defined, automatically move applications to <trust group></p>	<p>Items in this drop-down list determine to which trust group Kaspersky Endpoint Security will assign an unknown application.</p> <p>You can choose one of the following items:</p> <ul style="list-style-type: none"> • Low Restricted. • High Restricted. • Untrusted.

Remediation Engine

The Remediation Engine lets Kaspersky Endpoint Security roll back actions that have been performed by malware in the operating system.

When rolling back malware activity in the operating system, Kaspersky Endpoint Security handles the following types of malware activity:

- **File activity**

Kaspersky Endpoint Security performs the following actions:

- Deletes executable files that were created by malware (on all media except network drives).
- Deletes executable files that were created by programs that have been infiltrated by malware.
- Restores files that have been modified or deleted by malware.

The file recovery feature has a [number of limitations](#).

- **Registry activity**

Kaspersky Endpoint Security performs the following actions:

- Deletes registry keys that were created by malware.
- Does not restore registry keys that have been modified or deleted by malware.

- **System activity**

Kaspersky Endpoint Security performs the following actions:

- Terminates processes that have been initiated by malware.
- Terminates processes into which a malicious application has penetrated.
- Does not resume processes that have been halted by malware.

- **Network activity**

Kaspersky Endpoint Security performs the following actions:

- Blocks the network activity of malware.
- Blocks the network activity of processes that have been infiltrated by malware.

A rollback of malware actions can be started by the [File Threat Protection](#) or [Behavior Detection](#) component, or during a [virus scan](#).

Rolling back malware operations affects a strictly defined set of data. Rollback has no adverse effects on the operating system or on the integrity of your computer data.

File Threat Protection

The File Threat Protection component lets you prevent infection of the file system of the computer. By default, the File Threat Protection component permanently resides in the computer's RAM. The component scans files on all drives of the computer, as well as on connected drives. The component provides computer protection with the help of anti-virus databases, the [Kaspersky Security Network cloud service](#), and heuristic analysis.

The component scans the files accessed by the user or application. If a malicious file is detected, Kaspersky Endpoint Security blocks the file operation. The application then disinfects or deletes the malicious file, depending on the settings of the File Threat Protection component.

When attempting to access a file whose contents are stored in the OneDrive cloud, Kaspersky Endpoint Security downloads and scans the file contents.

File Threat Protection component settings

Parameter	Description
Protection scope	<p>Contains objects that are scanned by the File Threat Protection component. A scan object may be a hard drive, removable drive, network drive, folder, file, or multiple files defined by a mask.</p> <p>By default, the File Threat Protection component scans files that are started on any hard drives, removable drives, or network drives. The protection scope for these objects cannot be changed or deleted. You can also exclude an object (such as removable drives) from scans.</p>
Action on threat detection	<p>Disinfect; delete if disinfection fails. If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected files that are detected. If disinfection fails, Kaspersky Endpoint Security deletes the files.</p> <p>Disinfect; block if disinfection fails. If this option is selected, the File Threat Protection component automatically attempts to disinfect all infected files that are detected. If disinfection fails, the File Threat Protection component blocks these files.</p> <p>Block. If this option is selected, the File Threat Protection component automatically blocks all infected files without attempting to disinfect them.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Before attempting to disinfect or delete an infected file, the File Threat Protection component creates a backup copy in case it becomes necessary to restore the file or it becomes possible to disinfect the file at a later time.</p> </div>

Scan only new and changed files	This check box enables or disables the mode for scanning only new files and files that have been modified since the previous scan. This helps reduce the duration of a scan.
Scan archives	This check box enables / disables scanning of RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives.
Scan distribution packages	This check box enables/disables scanning of third-party distribution packages.
Scan files in Microsoft Office formats	This check box enables or disables scanning of Microsoft Office files (DOC, DOCX, XLS, PPT, and others). Office format files include OLE objects as well.
Do not unpack large compound files	If this check box is selected, Kaspersky Endpoint Security does not scan compound files if their size exceeds the specified value. If this check box is cleared, Kaspersky Endpoint Security scans compound files of all sizes. Kaspersky Endpoint Security scans large files that are extracted from archives, regardless of whether the Do not unpack large compound files check box is selected.
Unpack compound files in the background	If the check box is selected, Kaspersky Endpoint Security provides access to compound files that are larger than the specified value before these files are scanned. In this case, Kaspersky Endpoint Security unpacks and scans compound files in the background. Kaspersky Endpoint Security provides access to compound files that are smaller than this value only after unpacking and scanning these files. If the check box is not selected, Kaspersky Endpoint Security provides access to compound files only after unpacking and scanning files of any size.

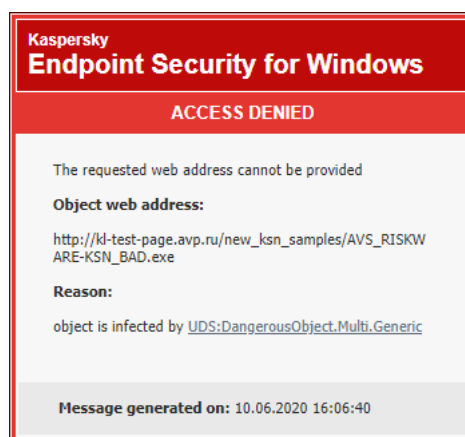
Web Threat Protection

The Web Threat Protection component prevents downloads of malicious files from the Internet, and also blocks malicious and phishing websites. The component provides computer protection with the help of anti-virus databases, the [Kaspersky Security Network cloud service](#), and heuristic analysis.

Kaspersky Endpoint Security scans HTTP-, HTTPS- and FTP-traffic. Kaspersky Endpoint Security scans URLs and IP addresses. You can [specify the ports that Kaspersky Endpoint Security will monitor](#), or select all ports.

For HTTPS traffic monitoring, you need to [enable encrypted connections scan](#).

When a user tries to open a malicious or phishing website, Kaspersky Endpoint Security will block access and show a warning (see the figure below).



Website access denied message

Web Threat Protection component settings

Parameter	Description
Action on threat detection	<ul style="list-style-type: none"> • Block download. If this option is selected and an infected object is detected in web traffic, the Web Threat Protection component blocks access to the object and displays a message in the browser. • Inform. If this option is selected and an infected object is detected in web traffic, Kaspersky Endpoint Security allows this object to be downloaded to the computer but adds information about the infected object to the list of active threats.
Do not scan web traffic from trusted web addresses	If the check box is selected, the Web Threat Protection component does not scan the content of web pages or websites whose addresses are included in the list of trusted web addresses.
Trusted web addresses	The Web Threat Protection component does not scan the content of web pages or websites whose addresses are included in the list of trusted web addresses. You can add both the specific address and the address mask of a web page/website to the list of trusted web addresses.

Mail Threat Protection

The Mail Threat Protection component scans the attachments of incoming and outgoing email messages for viruses and other threats. The component also scans messages for malicious and phishing links. By default, the Mail Threat Protection component permanently resides in the computer's RAM and scans all messages received or sent using the POP3, SMTP, IMAP, or NNTP protocols, or the Microsoft Office Outlook mail client (MAPI). The component provides computer protection with the help of anti-virus databases, the [Kaspersky Security Network cloud service](#), and heuristic analysis.

The Mail Threat Protection component does not scan messages if the mail client is open in a browser.

When a malicious file is detected in an attachment, Kaspersky Endpoint Security renames the message subject: [Message is infected] <message subject> or [Infected object deleted] <message subject>.

This component interacts with mail clients installed on the computer. For the Microsoft Office Outlook mail client, an [extension with additional parameters](#) is provided. The Mail Threat Protection extension is embedded in the Microsoft Office Outlook mail client during installation of Kaspersky Endpoint Security.

Mail Threat Protection component settings

Parameter	Description
<p>Action on threat detection</p>	<p>Disinfect; delete if disinfection fails. When an infected object is detected in an inbound or outbound message, Kaspersky Endpoint Security attempts to disinfect the detected object. The user will be able to access the message with a safe attachment.</p> <p>If the object cannot be disinfected, Kaspersky Endpoint Security deletes the infected object. Kaspersky Endpoint Security adds information about the performed action to the message subject: [Infected object was deleted] <message subject>.</p> <p>Disinfect; block if disinfection fails. When an infected object is detected in an inbound message, Kaspersky Endpoint Security attempts to disinfect the detected object. The user will be able to access the message with a safe attachment. If the object cannot be disinfected, Kaspersky Endpoint Security adds a warning to the message subject: [Message infected] <message subject>. The user will be able to access the message with the original attachment.</p> <p>When an infected object is detected in an outbound message, Kaspersky Endpoint Security attempts to disinfect the detected object. If the object cannot be disinfected, Kaspersky Endpoint Security blocks transmission of the message, and the mail client shows an error.</p> <p>Block. If an infected object is detected in an inbound message, Kaspersky Endpoint Security adds a warning to the message subject: [Message infected] <message subject>. The user will be able to access the message with the original attachment.</p> <p>If an infected object is detected in an outbound message, Kaspersky Endpoint Security blocks transmission of the message, and the mail client shows an error.</p>
<p>POP3 / SMTP / NNTP / IMAP traffic</p>	<p>The check box enables / disables scanning by the Mail Threat Protection component of traffic that is transferred via the POP3, SMTP, NNTP, and IMAP protocols.</p>
<p>Microsoft Office Outlook extension</p>	<p>If the check box is selected, scanning of email messages transmitted via the POP3, SMTP, NNTP, IMAP protocols is enabled on the side of the extension integrated into Microsoft Office Outlook.</p> <p>If mail is scanned using the extension for Microsoft Office Outlook, it is recommended to use Cached Exchange Mode. For more detailed information about the Exchange caching mode and recommendations on its use, please refer to the Microsoft Knowledge Base.</p>
<p>Do not scan archives larger than N MB</p>	<p>If this check box is selected, the Mail Threat Protection component excludes archives attached to email messages from scanning if their size exceeds the specified value.</p> <p>If the check box is cleared, the Mail Threat Protection component scans email attachment archives of any size.</p>
<p>Do not scan archives for more than N sec</p>	<p>If the check box is selected, the time that is allocated for scanning archives attached to email messages is limited to the specified period.</p>
<p>Attachment filter</p>	<div style="border: 1px solid black; padding: 10px;"> <p>The attachment filter is not applied to outgoing email messages.</p> </div>

Disable filtering. If this option is selected, the Mail Threat Protection component does not filter files that are attached to email messages.

Rename attachments of selected types. If this option is selected, the Mail Threat Protection component replaces the last character in attached files of the specified types with the underscore (_) symbol.

Delete attachments of selected types. If this option is selected, the Mail Threat Protection component deletes attached files of the specified types from email messages.

In the list of file masks, you can specify the types of attached files to rename or delete from email messages.

Network Threat Protection

The Network Threat Protection component scans inbound network traffic for activity that is typical of network attacks. When Kaspersky Endpoint Security detects an attempted network attack on the user's computer, it blocks the network connection with the attacking computer.

Descriptions of currently known types of network attacks and ways to counteract them are provided in Kaspersky Endpoint Security databases. The list of network attacks that the Network Threat Protection component detects is updated during [database and application module updates](#).

Network Threat Protection component settings

Parameter	Description
Add the attacking computer to the list of blocked computers for N minutes	If the check box is selected, the Network Threat Protection component adds the attacking computer to the blocked list. This means that the Network Threat Protection component blocks the network connection with the attacking computer after the first network attack attempt for the specified amount of time. This block automatically protects the user's computer against possible future network attacks from the same address.
Exclusions	The list contains IP addresses from which Network Threat Protection does not block network attacks. Kaspersky Endpoint Security does not log information on network attacks from the IP addresses that are in the list of exclusions.
Protection against MAC spoofing	A MAC spoofing attack consists of changing the MAC address of a network device (network card). As a result, an attacker can redirect data sent to a device to another device and gain access to this data. Kaspersky Endpoint Security lets you block MAC Spoofing attacks and receive notifications about the attacks.

Firewall

The Firewall blocks unauthorized connections to the computer while working on the Internet or local network. The Firewall also controls the network activity of applications on the computer. This allows you to protect your corporate LAN from identity theft and other attacks. The component provides computer protection with the help of anti-virus databases, the Kaspersky Security Network cloud service, and predefined *network rules*.

Network rules

You can configure network rules at the following levels:

- *Network packet rules.* Network packet rules impose restrictions on network packets, regardless of the application. Such rules restrict inbound and outbound network traffic through specific ports of the selected data protocol. Kaspersky Endpoint Security has predefined network packet rules with permissions recommended by Kaspersky experts.
- *Application network rules.* Application network rules impose restrictions on the network activity of a specific application. They factor in not only the characteristics of the network packet, but also the specific application to which this network packet is addressed or which issued this network packet.

Controlled access of applications to operating system resources, processes and personal data is provided by the [Host Intrusion Prevention component](#) by using *application rights*.

During the first startup of the application, the Firewall performs the following actions:

1. Checks the security of the application using downloaded anti-virus databases.
2. Checks the security of the application in Kaspersky Security Network.
You are advised to [participate in Kaspersky Security Network](#) to help the Firewall work more effectively.

3. Puts the application in one of the *trust groups*: Trusted, Low Restricted, High Restricted, Untrusted.

A [trust group defines the rights](#) used by Kaspersky Endpoint Security when controlling network activity of applications. Kaspersky Endpoint Security places an application in a trust group depending on the level of danger that this application may pose to the computer.

Kaspersky Endpoint Security places an application in a trust group for the Firewall and Host Intrusion Prevention components. You cannot change the trust group only for the Firewall or Host Intrusion Prevention.

If you refused to participate in KSN or there is no network, Kaspersky Endpoint Security places the application in a trust group depending on the [settings of the Host Intrusion Prevention component](#). After receiving the reputation of the application from KSN, the trust group can be changed automatically.

4. It blocks network activity of the application depending on the trust group. For example, applications in the High Restricted trust group are not allowed to use any network connections.

The next time the application is started, Kaspersky Endpoint Security checks the integrity of the application. If the application is unchanged, the component uses the current network rules for it. If the application has been modified, Kaspersky Endpoint Security analyzes the application as if it were being started for the first time.

Network Rule Priorities

Each rule has a priority. The higher a rule is on the list, the higher its priority. If network activity is added to several rules, the Firewall regulates network activity according to the rule with the highest priority.

Network packet rules have a higher priority than network rules for applications. If both network packet rules and network rules for applications are specified for the same type of network activity, the network activity is handled according to the network packet rules.

Network packet rules have a higher priority than network rules for applications. If both network packet rules and network rules for applications are specified for the same type of network activity, the network activity is handled according to the network packet rules.

Network rules for applications work as follows: a network rule for applications includes access rules based on the network status: *public*, *local*, or *trusted*. For example, applications in the High Restricted trust group are not allowed any network activity in networks of all statuses by default. If a network rule is specified for an individual application (parent application), then the child processes of other applications will run according to the network rule of the parent application. If there is no network rule for the application, the child processes will run according to network access rule of the application's trust group.

For example, you have prohibited any network activity in networks of all statuses for all applications, except browser X. If you start browser Y installation (child process) from browser X (parent application), then browser Y installer will access the network and download the necessary files. After installation, browser Y will be denied any network connections according to the Firewall settings. To prohibit network activity of browser Y installer as a child process, you must add a network rule for the installer of browser Y.

Network connection statuses

The Firewall allows you to control network activity depending on the status of the network connection. Kaspersky Endpoint Security receives the network connection status from the computer's operating system. The status of the network connection in the operating system is set by the user when setting up the connection. You can [change the status of the network connection in the Kaspersky Endpoint Security settings](#). The Firewall will monitor network activity depending on the network status in the Kaspersky Endpoint Security settings, and not in the operating system.

The network connection can have one of the following status types:

- **Public network.** The network is not protected by antivirus applications, firewalls, or filters (such as Wi-Fi in a cafe). When the user operates a computer that is connected to such a network, Firewall blocks access to files and printers of this computer. External users are also unable to access data through shared folders and remote access to the desktop of this computer. Firewall filters the network activity of each application according to the network rules that are set for it.

Firewall assigns *Public network* status to the Internet by default. You cannot change the status of the Internet.

- **Local network.** Network for users with restricted access to files and printers on this computer (such as for a corporate LAN or home network).

Trusted network. Safe network in which the computer is not exposed to attacks or unauthorized data access attempts. Firewall permits any network activity within networks with this status.

Firewall component settings

Parameter	Description
Network packet rules	<p>Table with a list of network packet rules. Network packet rules serve to impose restrictions on network packets, regardless of the application. Such rules restrict inbound and outbound network traffic through specific ports of the selected data protocol.</p> <p>The table lists pre-configured network packet rules that are recommended by Kaspersky for optimum protection of the network traffic of computers that run on Microsoft Windows operating systems.</p>

	<p>Firewall sets the execution priority of each network packet rule. Firewall processes network packet rules in the order in which they appear in the list of network packet rules, from top to bottom. Firewall locates the topmost network packet rule that is suitable for the network connection and applies it by either allowing or blocking network activity. Firewall then ignores all subsequent network packet rules for the specific network connection.</p> <p>Network packet rules have higher priority than network rules for applications.</p>
Network connections	<p>This table contains information about network connections that Firewall detects on the computer.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>The <i>Public network</i> status is assigned to the Internet by default. You cannot change the status of the Internet.</p> </div>
Network rules	<p>Appendices</p> <p>Table of applications that are controlled by the Firewall component. Applications are assigned to trust groups. A trust group defines the rights used by Kaspersky Endpoint Security when controlling network activity of applications.</p> <p>You can select an application from a single list of all applications installed on computers under the influence of a policy and add the application to a trust group.</p> <p>Network rules</p> <p>Table of network rules for applications that are part of a trust group. In accordance with these rules, Firewall regulates the network activity of an application.</p> <p>The table displays the predefined network rules that are recommended by Kaspersky experts. These network rules have been added to optimally protect the network traffic of computers running Windows operating systems. It is not possible to delete the predefined network rules.</p>

BadUSB Attack Prevention

Some viruses modify the firmware of USB devices to trick the operating system into detecting the USB device as a keyboard.

The BadUSB Attack Prevention component prevents infected USB devices emulating a keyboard from connecting to the computer.

When a USB device is connected to the computer and identified by the application as a keyboard, the application prompts the user to enter a numerical code generated by the application from this keyboard, or using On-Screen Keyboard (if it is available). This procedure is known as keyboard authorization. The application allows use of an authorized keyboard and blocks a keyboard that has not been authorized.

The BadUSB Attack Prevention component is not installed by default. If you need the BadUSB Attack Prevention component, you can add the component in the properties of the [installation package](#) before installing the application or [change the available application components](#) after installing the application.

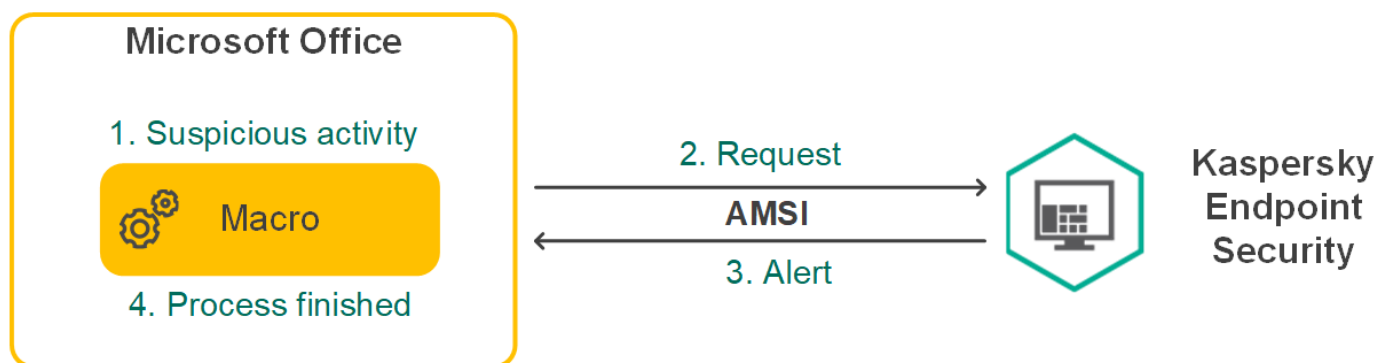
BadUSB Attack Prevention component settings

Parameter	Description
Prohibit use of On-Screen Keyboard for authorization of USB devices	If the check box is selected, the application blocks use of On-Screen Keyboard for authorization of a USB device from which an authorization code cannot be entered.

AMSI Protection Provider

AMSI Protection Provider is intended to support Antimalware Scan Interface from Microsoft. The *Antimalware Scan Interface (AMSI)* allows third-party applications with AMSI support to send objects (for example, PowerShell scripts) to Kaspersky Endpoint Security for an additional scan and then receive the results from scanning these objects. Third-party applications may include, for example, Microsoft Office applications (see the figure below). For details on AMSI refer to [Microsoft documentation](#).

The AMSI Protection Provider can only detect a threat and notify a third-party application about the detected threat. Third-party application after receiving a notification of a threat does not allow to perform malicious actions (for example, terminates).



AMSI operation example

AMSI Protection Provider may decline a request from a third-party application, for example, if this application exceeds maximum number of requests within a specified interval. Kaspersky Endpoint Security sends information about a rejected request from a third-party application to the Administration Server. The AMSI Protection Provider component does not reject requests from those third-party applications for which the [Do not block interaction with AMSI Protection Provider check box](#) is selected

The AMSI Protection Provider is available for the following operating systems for workstations and servers:

- Windows 10 Home / Pro / Education / Enterprise;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter.

AMSI Protection Provider component settings

Parameter	Description
Scan archives	This check box enables/disables scanning of archives in RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE formats.
Scan distribution packages	This check box enables/disables scanning of third-party distribution packages.
Scan files in Microsoft Office formats	This check box enables or disables scanning of Microsoft Office files (DOC, DOCX, XLS, PPT, and others). Office format files include OLE objects as well.
Do not unpack large compound	If this check box is selected, Kaspersky Endpoint Security does not scan compound files if their size exceeds the specified value.

files

If this check box is cleared, Kaspersky Endpoint Security scans compound files of all sizes.

Kaspersky Endpoint Security scans large files that are extracted from archives, regardless of whether the **Do not unpack large compound files** check box is selected.

Application Control

Application Control manages the startup of applications on users' computers. This allows you to implement a corporate security policy when using applications. Application Control also reduces the risk of computer infection by restricting access to applications.

Configuring Application Control consists of the following steps:

1. [Creating application categories.](#)

The administrator creates categories of applications that the administrator wants to manage. Categories of applications are intended for all computers in the corporate network, regardless of administration groups. To create a category, you can use the following criteria: KL category (for example, *Browsers*), file hash, application vendor, and other criteria.

2. [Creating Application Control rules.](#)

The administrator creates Application Control rules in the policy for the administration group. The rule includes the categories of applications and the startup status of applications from these categories: blocked or allowed.

3. [Selecting the Application Control mode.](#)

The administrator chooses the mode for working with applications that are not included in any of the rules: black list or white list.

When a user attempts to start a prohibited application, Kaspersky Endpoint Security will block the application from starting and will display a notification (see the figure below).

A *test mode* is provided to check the configuration of Application Control. In this mode, Kaspersky Endpoint Security does the following:

- Allows the startup of applications, including prohibited ones.
- Shows a notification about the startup of a prohibited application and adds information to the report on the user's computer.
- Sends data about the startup of prohibited applications to Kaspersky Security Center.



Application Control notification

Application Control operating modes

The Application Control component operates in two modes:

- **Black List.** In this mode, Application Control allows users to start all applications except for applications that are prohibited in Application Control rules.

This mode of Application Control is enabled by default.

- **White List.** In this mode, Application Control blocks users from starting any applications except for applications that are allowed and not prohibited in Application Control rules.

If the allow rules of Application Control are fully configured, the component blocks the startup of all new applications that have not been verified by the LAN administrator, while allowing the operation of the operating system and of trusted applications that users rely on in their work.

You can read the [recommendations on configuring application control rules in white list mode](#).

Application Control can be configured to operate in these modes both by using the Kaspersky Endpoint Security local interface and by using Kaspersky Security Center.

However, Kaspersky Security Center offers tools that are not available in the Kaspersky Endpoint Security local interface, such as the tools that are needed for the following tasks:

- [Creating application categories](#).

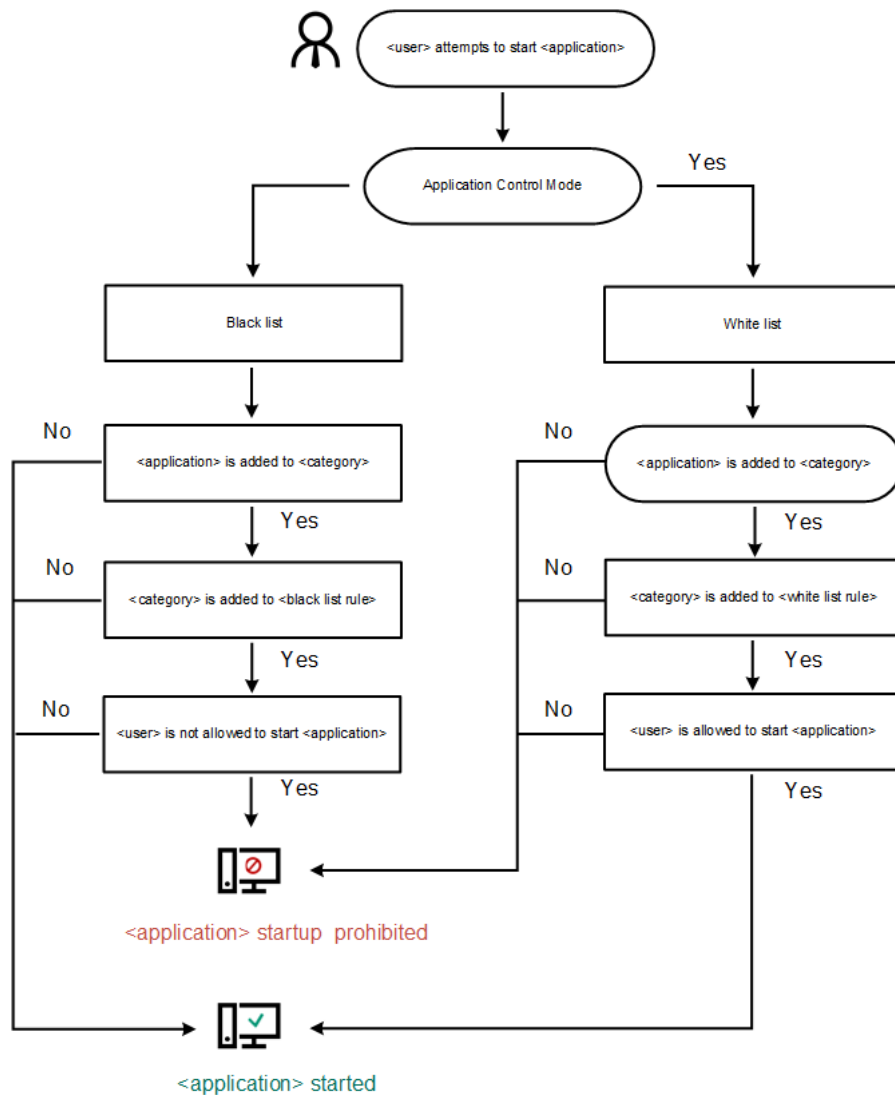
Application Control rules created in the Kaspersky Security Center Administration Console are based on your custom application categories and not on inclusion and exclusion conditions as is the case in the Kaspersky Endpoint Security local interface.

- [Receiving information about applications that are installed on corporate LAN computers](#).

This is why it is recommended to use Kaspersky Security Center to configure the operation of the Application Control component.

Application Control operating algorithm

Kaspersky Endpoint Security uses an algorithm to make a decision about starting an application (see the figure below).



Application Control operating algorithm

Application Control component settings

Parameter	Description
Test mode	If the toggle button is switched on, Kaspersky Endpoint Security allows the startup of an application that is blocked in the current Application Control mode, but logs information about its startup in the report.
Application Control mode	<p>You can choose one of the following options:</p> <ul style="list-style-type: none"> • Black List. If this option is selected, Application Control allows all users to start any applications, except in cases that satisfy the conditions of Application Control block rules. • White List. If this option is selected, Application Control blocks all users from starting any applications, except in cases that satisfy the conditions of Application Control allow rules. <p>When White list mode is selected, two Application Control rules are automatically created:</p> <ul style="list-style-type: none"> • Golden Image. • Trusted Updaters.

	<p>You cannot edit the settings of or delete automatically created rules. You can enable or disable these rules.</p>
<p>Control DLL and drivers</p>	<p>If the check box is selected, Kaspersky Endpoint Security controls the loading of DLL modules when users attempt to start applications. Information about the DLL module and the application that loaded this DLL module is logged in the report.</p> <p>When enabling control over which DLL modules and drivers are loaded, make sure that one of the following rules is enabled in the Application Control settings: the default Golden Image rule or another rule that contains the Trusted certificates KL category and ensures that trusted DLL modules and drivers are loaded before Kaspersky Endpoint Security is started. Enabling control of the loading of DLL modules and drivers when the Golden Image rule is disabled may cause instability in the operating system.</p> <p>Kaspersky Endpoint Security monitors only the DLL modules and drivers loaded since the Control DLL and drivers check box was selected. It is recommended to restart the computer after selecting the Control DLL and drivers check box to ensure that the application monitors all DLL modules and drivers, including those loaded before Kaspersky Endpoint Security starts.</p>
<p>Message templates</p>	<p>Blockage. Template of the message that is displayed when an Application Control rule that blocks an application from starting is triggered.</p> <p>Message to administrator. Template of the message that a user can send to the corporate LAN administrator if the user believes that an application was blocked by mistake.</p>

Device Control

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Windows for workstations. This component is unavailable if Kaspersky Endpoint Security is installed on a computer that runs on Windows for servers.

Device Control manages user access to devices that are installed on or connected to the computer (for example, hard drives, cameras, or Wi-Fi modules). This lets you protect the computer from infection when such devices are connected, and prevent loss or leaks of data.

Device access levels

Device Control controls access at the following levels:

- **Device type.** For example, printers, removable drives, and CD/DVD drives.

You can configure device access as follows:

- Allow – ✓.
- Block – ⓧ.

- Depends on connection bus (except for Wi-Fi) – 🌐.
- Block with exceptions (only Wi-Fi and portable devices (MTP)) – 📱.
- **Connection bus.** A *connection bus* is an interface used for connecting devices to the computer (for example, USB or FireWire). Therefore, you can restrict the connection of all devices, for example, over USB.

You can configure device access as follows:

- Allow – ✓.
- Block – 🚫.
- **Trusted devices.** *Trusted devices* are devices to which users that are specified in the trusted device settings have full access at all times.

You can add trusted devices based on the following data:

- **Devices by ID.** Each device has a unique identifier (Hardware ID, or HWID). You can view the ID in the device properties by using operating system tools. Example device ID: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Adding devices by ID is convenient if you want to add several specific devices.
- **Devices by model.** Each device has a vendor ID (VID) and a product ID (PID). You can view the IDs in the device properties by using operating system tools. Template for entering the VID and PID: `VID_1234&PID_5678`. Adding devices by model is convenient if you use devices of a certain model in your organization. This way, you can add all devices of this model.
- **Devices by ID mask.** If you are using multiple devices with similar IDs, you can add devices to the trusted list by using masks. The * character replaces any set of characters. Kaspersky Endpoint Security does not support the ? character when entering a mask. For example, `WDC_C*`.
- **Devices by model mask.** If you are using multiple devices with similar VID's or PID's (for example, devices from the same manufacturer), you can add devices to the trusted list by using masks. The * character replaces any set of characters. Kaspersky Endpoint Security does not support the ? character when entering a mask. For example, `VID_05AC & PID_*`.

Device Control regulates user access to devices by using [access rules](#). Device Control also lets you save device connection/disconnection events. To save events, you need to configure the registration of events in a policy.

If access to a device depends on the connection bus (the 🌐 status), Kaspersky Endpoint Security does not save device connection/disconnection events. To enable Kaspersky Endpoint Security to save device connection/disconnection events, allow access to the corresponding type of device (the ✓ status) or add the device to the trusted list.

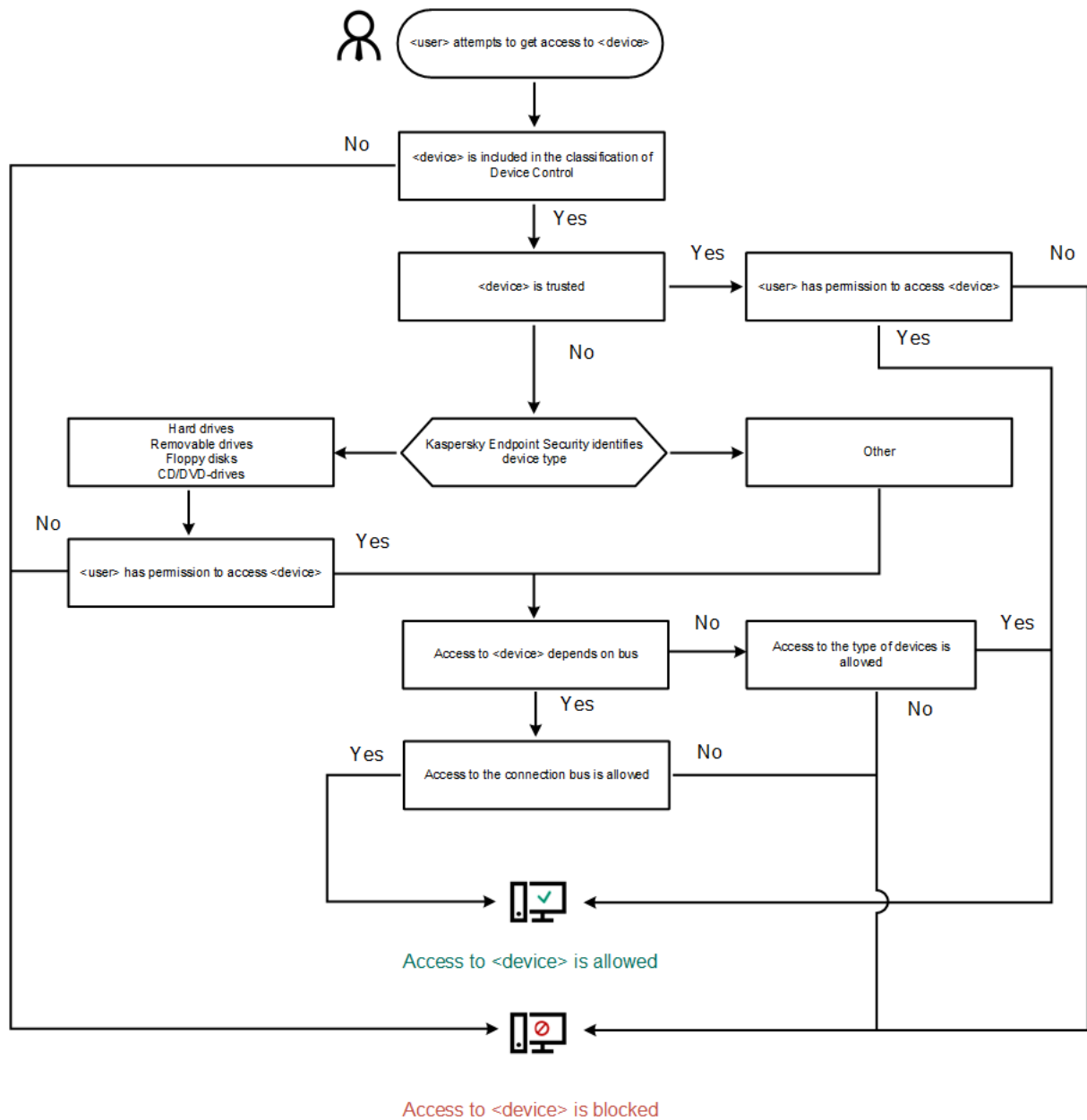
When a device that is blocked by Device Control is connected to the computer, Kaspersky Endpoint Security will block access and show a notification (see the figure below).



Device Control notification

Device Control operating algorithm

Kaspersky Endpoint Security makes a decision on whether to allow access to a device after the user connects the device to the computer (see the figure below).



Device Control operating algorithm

If a device is connected and access is allowed, you can edit the access rule and block access. In this case, the next time someone attempts to access the device (such as to view the folder tree, or perform read or write operations), Kaspersky Endpoint Security blocks access. A device without a file system is blocked only the next time that the device is connected.

If a user of the computer with Kaspersky Endpoint Security installed must request access to a device that the user believes was blocked by mistake, send the user the [request access instructions](#).

Device Control component settings

Parameter	Description
Allow requests for	If the check box is selected, the Request access button is available through the local interface of Kaspersky Endpoint Security. Clicking this button opens the Request access to device window. In this window, the user can request temporary access to a blocked device.

temporary access	
Access rules for devices and Wi-Fi networks	This table contains all possible types of devices according to the classification of the Device Control component, including their respective access statuses.
Block connection of mobile devices in ADB and iTunes modes	<p>The settings for controlling access to mobile devices running Android or iOS also apply to the settings of portable devices (MTP). When a mobile device is connected to the computer, the operating system determines the device type. If Android Debug Bridge (ADB), iTunes or their equivalent applications are installed on the computer, the operating system identifies mobile devices as ADB or iTunes devices. In all other cases, the operating system may identify the mobile device type as a portable device (MTP) for file transfer, a PTP device (camera) for image transfer, or another device. The device type depends on the model of the mobile device.</p> <p>If the check box is selected, Kaspersky Endpoint Security blocks access to the mobile device through ADB or iTunes. However, the user can still charge the battery of the mobile device. Access to a mobile device identified as a portable device (MTP) or a PTP device (camera) is regulated by the access rule for the specific type of device.</p> <p>If the check box is cleared, Kaspersky Endpoint Security regulates access to mobile devices through ADB and iTunes by using the access rules for portable devices (MTP) and PTP devices (camera). However, even if access to portable devices (MTP) is blocked, the user can still charge the battery of the mobile device.</p>
Connection buses	A list of all available connection buses according to the Device Control component's classification, including their respective access statuses.
Trusted devices	List of trusted devices and users who are granted access to these devices.
Anti-Bridging	<p>Anti-Bridging inhibits the creation of network bridges by preventing the simultaneous establishment of multiple network connections for a computer. This lets you protect a corporate network from attacks over unprotected, unauthorized networks.</p> <p>Anti-Bridging blocks the establishment of multiple connections according to the priorities of devices. The higher a device is on the list, the higher its priority.</p> <p>If an active connection and a new connection are both of the same type (for example, Wi-Fi), Kaspersky Endpoint Security blocks the active connection and allows establishment of the new connection.</p> <p>If an active connection and a new connection are of different types (for example, a network adapter and Wi-Fi), Kaspersky Endpoint Security blocks the connection with the lower priority and allows the connection with the higher priority.</p> <p>Anti-Bridging supports operation with the following types of devices: network adapter, Wi-Fi, and modem.</p>
Message templates	<ul style="list-style-type: none"> • Blockage. Template of the message that appears when a user attempts to access a blocked device. This message also appears when a user attempts to perform an operation on the device contents that was blocked for this user. • Message to administrator. A template of the message that is sent to the LAN administrator when the user believes that access to the device is blocked or an operation with device content is forbidden by mistake.

Web Control

Web Control manages users' access to web resources. This helps reduce traffic and inappropriate use of work time. When a user tries to open a website that is restricted by Web Control, Kaspersky Endpoint Security will block access or show a warning (see the figure below).

Kaspersky Endpoint Security monitors only HTTP- and HTTPS traffic.

For HTTPS traffic monitoring, you need to [enable encrypted connections scan](#).

Methods for managing access to websites

Web Control lets you configure access to websites by using the following methods:

- **Website category.** Websites are categorized according to the Kaspersky Security Network cloud service, heuristic analysis, and the database of known websites (included in application databases). You can restrict users' access, for example, to the "Social networks" category or to [other categories](#).
- **Data type.** You can restrict users' access to data on a website, and hide graphic images, for example. Kaspersky Endpoint Security determines the data type based on the file format and not based on its extension.

Kaspersky Endpoint Security does not scan files within archives. For example, if image files were placed in an archive, Kaspersky Endpoint Security identifies the "Archives" data type and not "Graphic files".

- **Individual address.** You can enter a web address or [use masks](#).

You can simultaneously use multiple methods for regulating access to websites. For example, you can restrict access to the "Office files" data type just for the "Web-based email" website category.

Website access rules

Web Control manages users' access to websites by using *access rules*. You can configure the following advanced settings for a website access rule:

- Users to which the rule applies.
For example, you can restrict Internet access through a browser for all users of the company except the IT department.
- Rule schedule.
For example, you can restrict Internet access through a browser during working hours only.

Access rule priorities

Each rule has a priority. The higher a rule is on the list, the higher its priority. If a website has been added to multiple rules, Web Control regulates access to the website based on the rule with the highest priority. For example, Kaspersky Endpoint Security may identify a corporate portal as a social network. To restrict access to social networks and provide access to the corporate web portal, create two rules: one block rule for the "Social networks" website category and one allow rule for the corporate web portal. The access rule for the corporate web portal must have a higher priority than the access rule for social networks.



Web Control messages

Web Control component settings

Parameter	Description
Rule List	List containing web resource access rules. Each rule has a priority. The higher a rule is on the list, the higher its priority. If a website has been added to multiple rules, Web Control regulates access to the website based on the rule with the highest priority.
Default rule	The <i>Default rule</i> is a rule for accessing web resources that are not covered by any other rule. The following options are available: <ul style="list-style-type: none"> • Allow all except the rules list, also known as black list mode. • Deny everything except the rules list, also known as white list mode.
Message templates	<ul style="list-style-type: none"> • Warning. The entry field consists of a template of the message that is displayed if a rule for warning about attempts to access an unwanted web resource is triggered. • Blockage. The entry field contains the template of the message that appears if a rule which blocks access to a web resource is triggered. • Message to administrator. The entry field contains the template of the message to be sent to the LAN administrator if the user considers the block to be a mistake.
Log the opening of allowed pages	Kaspersky Endpoint Security logs data on visits to all websites, including allowed websites. Kaspersky Endpoint Security sends events to Kaspersky Security Center, to the local log of Kaspersky Endpoint Security , and to the Windows Event log. To monitor user Internet activity, you need to configure the settings for saving events .

Monitoring user Internet activity may require more computer resources when decrypting HTTPS traffic.

Adaptive Anomaly Control

You can manage Adaptive Anomaly Control in the Kaspersky Security Center 12 Web Console. Adaptive Anomaly Control cannot be managed in the Kaspersky Security Center Cloud Console. You can also manage Adaptive Anomaly Control in the Kaspersky Security Center Administration Console.

The Adaptive Anomaly Control component is available only for Kaspersky Endpoint Security for Business Advanced and Kaspersky Total Security for Business (learn more about Kaspersky Endpoint Security products for business at the [Kaspersky website](#) ²).

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Windows for workstations. This component is unavailable if Kaspersky Endpoint Security is installed on a computer that runs on Windows for servers.

The Adaptive Anomaly Control component monitors and blocks actions that are not typical of the computers in a company's network. Adaptive Anomaly Control uses a set of rules to track uncharacteristic behavior (for example, the *Start of Microsoft PowerShell from office application* rule). Rules are created by Kaspersky specialists based on typical scenarios of malicious activity. You can configure how Adaptive Anomaly Control handles each rule and, for example, allow the execution of PowerShell scripts that automate certain workflow tasks. Kaspersky Endpoint Security updates the set of rules along with the application databases. Updates to the sets of rules must be [confirmed manually](#).

Adaptive Anomaly Control settings

Configuring Adaptive anomaly control consists of the following steps:

1. Training Adaptive Anomaly Control.

After you enable Adaptive Anomaly Control, its rules work in *training mode*. During the training, Adaptive Anomaly Control monitors rule triggering and sends triggering events to Kaspersky Security Center. Each rule has its own duration of the training mode. The duration of the training mode is set by Kaspersky experts. Normally, the training mode is active for two weeks.

If a rule is not triggered at all during the training, Adaptive Anomaly Control will consider the actions associated with this rule as non-typical. Kaspersky Endpoint Security will block all actions associated with that rule.

If a rule was triggered during training, Kaspersky Endpoint Security logs events in the [rule triggering report](#) and the **Triggering of rules in Smart Training mode** repository.

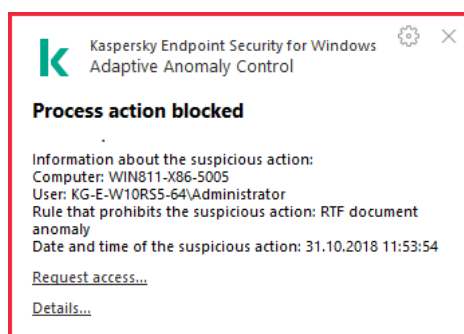
2. Analyzing the rule triggering report.

The administrator analyzes the [rule triggering report](#) or the contents of the **Triggering of rules in Smart Training mode** repository. Then the administrator can select the behavior of Adaptive Anomaly Control when the rule is triggered: either block or allow. The administrator can also continue to monitor how the rule works and extend the duration of the training mode. If the administrator does not take any action, the application will also continue to work in training mode. The training mode term is restarted.

Adaptive Anomaly Control is configured in real time. Adaptive Anomaly Control is configured via the following channels:

- Adaptive Anomaly Control automatically starts to block the actions associated with the rules that were never triggered in training mode.
- Kaspersky Endpoint Security adds new rules or removes obsolete ones.
- The administrator configures the operation of the Adaptive Anomaly Control after reviewing the rule triggering report and the contents of the **Triggering of rules in Smart Training mode** repository. It is recommended to check the rule triggering report and the contents of the **Triggering of rules in Smart Training mode repository**.

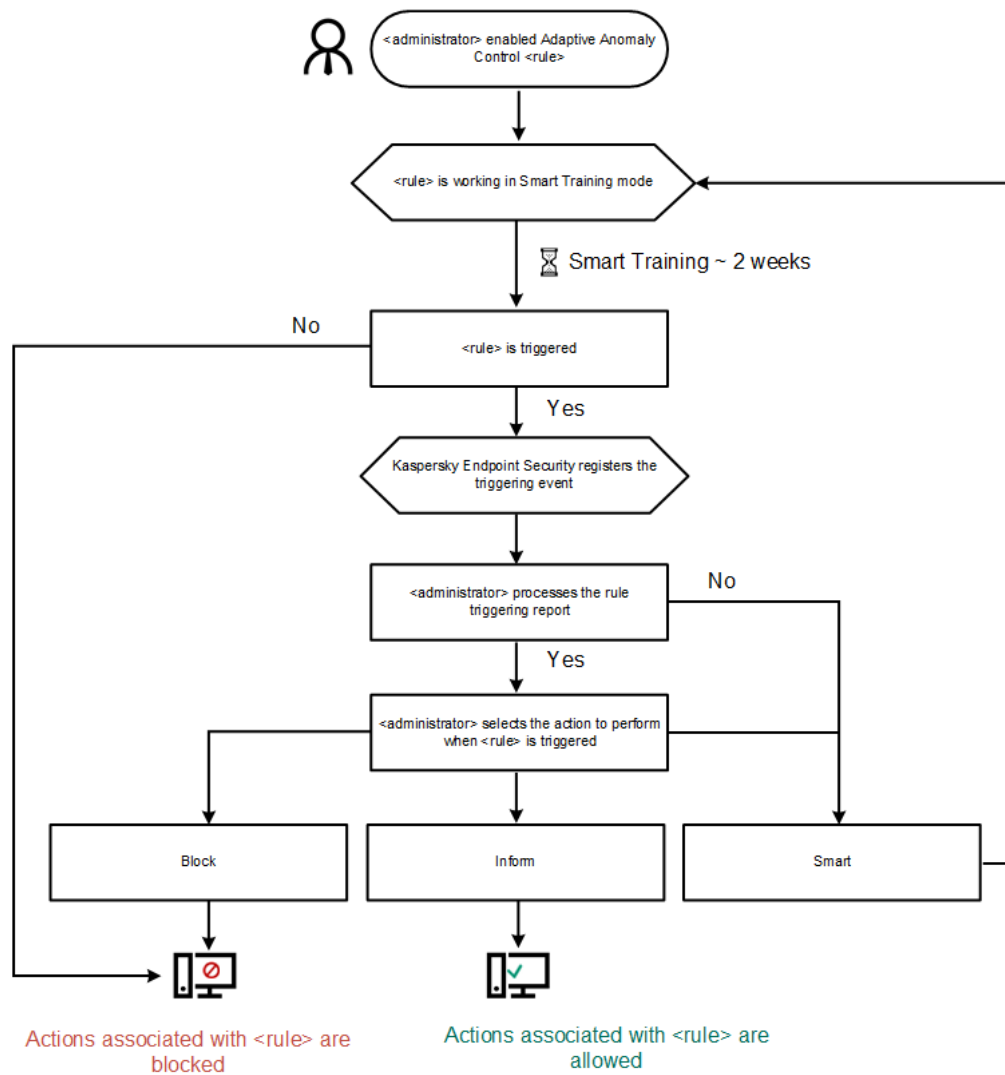
When a malicious application attempts to perform an action, Kaspersky Endpoint Security will block the action and display a notification (see figure below).



Adaptive Anomaly Control notification

Adaptive Anomaly Control operating algorithm

Kaspersky Endpoint Security decides whether to allow or block an action that is associated with a rule based on the following algorithm (see the figure below).



Adaptive Anomaly Control operating algorithm

Adaptive Anomaly Control component settings

Parameter	Description
Rule status report	This report contains information about the status of Adaptive Anomaly Control detection rules (for example, the <i>Off</i> or <i>Block</i>). The report is generated for all administration groups.
Rule triggering report	This report contains information about non-typical actions detected using Adaptive Anomaly Control. The report is generated for all administration groups.
Rules	Adaptive Anomaly Control table of rules. Rules are created by Kaspersky specialists based on typical scenarios of potentially malicious activity.
Message templates	<ul style="list-style-type: none"> • Blockage. Template of the message that is displayed to a user when an Adaptive Anomaly Control rule that blocks a non-typical action is triggered. • Message to administrator. Template of the message that a user can be sent to the local corporate network administrator if the user considers the blocking to be a mistake.

Full Disk Encryption

You can select an encryption technology: Kaspersky Disk Encryption or BitLocker Drive Encryption (hereinafter also referred to as simply "BitLocker").

Kaspersky Disk Encryption

After the system hard drives have been encrypted, at the next computer startup the user must complete authentication using the [Authentication Agent](#) before the hard drives can be accessed and the operating system is loaded. This requires entering the password of the token or smart card connected to the computer, or the user name and password of the Authentication Agent account created by the local area network administrator using *Authentication Agent account management* task. These accounts are based on Microsoft Windows accounts under which users log into the operating system. You can also [use Single Sign-On \(SSO\) technology](#), which lets you automatically log in to the operating system using the user name and password of the Authentication Agent account.

User authentication in the Authentication Agent can be performed in two ways:

- Enter the name and password of the Authentication Agent account created by the LAN administrator using Kaspersky Security Center tools.
- Enter the password of a token or smart card connected to the computer.

Use of a token or smart card is available only if the computer hard drives were encrypted using the AES256 encryption algorithm. If the computer hard drives were encrypted using the AES56 encryption algorithm, addition of the electronic certificate file to the command will be denied.

BitLocker Drive Encryption

BitLocker is an encryption technology built into Windows operating systems. Kaspersky Endpoint Security allows you to control and manage BitLocker using Kaspersky Security Center. BitLocker encrypts logical volumes. BitLocker cannot be used for encryption of removable drives. For more details on BitLocker, refer to [Microsoft documentation](#).

BitLocker provides secure storage of access keys using a trusted platform module. A *Trusted Platform Module (TPM)* is a microchip developed to provide basic functions related to security (for example, to store encryption keys). A Trusted Platform Module is usually installed on the computer motherboard and interacts with all other system components via the hardware bus. Using TPM is the safest way to store BitLocker access keys, since TPM provides pre-startup system integrity verification. You can still encrypt drives on a computer without a TPM. In this case, the access key will be encrypted with a password. BitLocker uses the following authentication methods:

- TPM and password.
- TPM and PIN.
- Password.

After encrypting a drive, BitLocker creates a master key. Kaspersky Endpoint Security sends the master key to Kaspersky Security Center so that you can [restore access to the disk](#), for example, if a user has forgotten the password. If a user encrypts a disk using BitLocker, Kaspersky Endpoint Security will send [information about disk encryption to Kaspersky Security Center](#). However, Kaspersky Endpoint Security will not send the master key to Kaspersky Security Center, so it will be impossible to restore access to the disk using Kaspersky Security Center. For BitLocker to work correctly with Kaspersky Security Center, decrypt the drive and re-encrypt the drive using a policy. You can decrypt a drive locally or using a policy.

After encrypting the system hard drive, the user needs to go through BitLocker authentication to boot the operating system. After the authentication procedure, BitLocker will allow for users to log in. BitLocker does not support single sign-on technology (SSO).

If you are using Windows group policies, turn off BitLocker management in the policy settings. Windows policy settings may conflict with Kaspersky Endpoint Security policy settings. When encrypting a drive, errors may occur.

Kaspersky Disk Encryption component settings

Parameter	Description
Encryption mode	<p>Encrypt all hard drives. If this item is selected, the application encrypts all hard drives when the policy is applied.</p> <div data-bbox="392 629 1493 752" style="border: 1px solid #f08080; padding: 5px; margin: 10px 0;"> <p>If the computer has several operating systems installed, after encryption you will be able to load only the operating system that has the application installed.</p> </div> <p>Decrypt all hard drives. If this item is selected, the application decrypts all previously encrypted hard drives when the policy is applied.</p> <p>Leave unchanged. If this item is selected, the application leaves drives in their previous state when the policy is applied. If the drive was encrypted, it remains encrypted. If the drive was decrypted, it remains decrypted. This item is selected by default.</p>
Automatically create Authentication Agent accounts for users	<p>This check box enables / disables automatic creation of Authentication Agent accounts when applying a policy. Kaspersky Endpoint Security creates a list of Authentication Agent accounts based on Windows accounts. By default, Kaspersky Endpoint Security uses all local and domain accounts with which the user logged in to the operating system over the past 30 days.</p>
Authentication Agent account creation settings	<p>All accounts on the computer. If this check box is selected, when running the full disk encryption task Kaspersky Endpoint Security creates Authentication Agent accounts for all computer accounts that have ever been active.</p> <p>All domain accounts on the computer. If this check box is selected, when running the full disk encryption task Kaspersky Endpoint Security creates Authentication Agent accounts for all computer accounts belonging to a certain domain that have ever been active.</p> <p>All local accounts on the computer. If this check box is selected, when running the full disk encryption task Kaspersky Endpoint Security creates Authentication Agent accounts for all local computer accounts that have ever been active.</p> <p>Local administrator. If this check box is selected, when running the full disk encryption task Kaspersky Endpoint Security creates a local administrator account.</p> <p>Computer manager. If this check box is selected, when running the full disk encryption task Kaspersky Endpoint Security creates an Authentication Agent account for the account whose properties in Active Directory show that it is a management account.</p> <p>Active account. If this check box is selected, when running the full disk encryption task Kaspersky Endpoint Security automatically creates an Authentication Agent account for the computer account that is active during the task.</p>
Save user name entered in Authentication Agent	<p>If the check box is selected, the application saves the name of the Authentication Agent account. You will not be required to enter the account name the next time you attempt to complete authorization in the Authentication Agent under the same account.</p>

<p>Encrypt used disk space only</p>	<p>This check box enables / disables the option that limits the encryption area to only occupied hard drive sectors. This limit lets you reduce encryption time.</p> <div data-bbox="392 185 1493 342" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>After encryption started, enabling / disabling the Encrypt used disk space only function will not change this setting until the hard drives are decrypted. You must select or clear the check box before starting encryption.</p> </div> <p>If the check box is selected, only portions of the hard drive that are occupied by files are encrypted. Kaspersky Endpoint Security automatically encrypts new data as it is added.</p> <p>If the check box is cleared, the entire hard drive is encrypted, including residual fragments of previously deleted and modified files.</p> <div data-bbox="392 577 1493 768" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>This option is recommended for new hard drives whose data has not been modified or deleted. If you are applying encryption on a hard drive that is already in use, it is recommended to encrypt the entire hard drive. This ensures protection of all data, even deleted data that is potentially recoverable.</p> </div> <p>This check box is cleared by default.</p>
<p>Use Legacy USB Support</p>	<p>This check box enables/disables the Legacy USB Support function. <i>Legacy USB Support</i> is a BIOS/UEFI function that allows you to use USB devices (such as a security token) during the computer's boot phase before starting the operating system (BIOS mode). Legacy USB Support does not affect support for USB devices after the operating system is started.</p> <p>If the check box is selected, support for USB devices during initial startup of the computer will be enabled.</p> <div data-bbox="392 1189 1493 1379" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0; background-color: #f8d7da;"> <p>When the Legacy USB Support function is enabled, the Authentication Agent in BIOS mode does not support working with tokens via USB. It is recommended to use this option only when there is a hardware compatibility issue and only for those computers on which the problem occurred.</p> </div>
<p>Password settings</p>	<p>Authentication Agent account password strength settings. You can also enable the use of Single Sign-On (SSO) technology.</p> <p>SSO technology makes it possible to use the same account credentials to access encrypted hard drives and to sign in to the operating system.</p> <p>If the check box is selected, you must enter the account credentials for accessing encrypted hard drives and then automatically logging in to the operating system.</p> <p>If the check box is cleared, to access encrypted hard drives and subsequently log into the operating system you must separately enter the credentials for accessing encrypted hard drives and the operating system user account credentials.</p>
<p>Help texts</p>	<p>Authentication. Help text that appears in the Authentication Agent window when entering account credentials.</p> <p>Change password. Help text that appears in the Authentication Agent window when changing the password for the Authentication Agent account.</p> <p>Recover password. Help text that appears in the Authentication Agent window when recovering the password for the Authentication Agent account.</p>

Parameter	Description
Encryption mode	<p>Encrypt all hard drives. If this item is selected, the application encrypts all hard drives when the policy is applied.</p> <div data-bbox="419 237 1493 362" style="border: 1px solid #f08080; padding: 5px; margin: 10px 0;"> <p>If the computer has several operating systems installed, after encryption you will be able to load only the operating system that has the application installed.</p> </div> <p>Decrypt all hard drives. If this item is selected, the application decrypts all previously encrypted hard drives when the policy is applied.</p> <p>Leave unchanged. If this item is selected, the application leaves drives in their previous state when the policy is applied. If the drive was encrypted, it remains encrypted. If the drive was decrypted, it remains decrypted. This item is selected by default.</p>
Enable use of BitLocker authentication requiring preboot keyboard input on slates	<p>This check box enables / disables the use of authentication requiring data input in a preboot environment, even if the platform does not have the capability for preboot input (for example, with touchscreen keyboards on tablets).</p> <div data-bbox="419 770 1493 927" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>The touchscreen of tablet computers is not available in the preboot environment. To complete BitLocker authentication on tablet computers, the user must connect a USB keyboard, for example.</p> </div> <p>If the check box is selected, use of authentication requiring preboot input is allowed. It is recommended to use this setting only for devices that have alternative data input tools in a preboot environment, such as a USB keyboard in addition to touchscreen keyboards.</p> <p>If the check box is cleared, BitLocker Drive Encryption is not possible on tablets.</p>
Use hardware encryption	<p>If the check box is selected, the application applies hardware encryption. This lets you increase the speed of encryption and use less computer resources.</p>
Encrypt used disk space only	<p>This check box enables / disables the option that limits the encryption area to only occupied hard drive sectors. This limit lets you reduce encryption time.</p> <div data-bbox="419 1393 1493 1550" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>After encryption started, enabling / disabling the Encrypt used disk space only function will not change this setting until the hard drives are decrypted. You must select or clear the check box before starting encryption.</p> </div> <p>If the check box is selected, only portions of the hard drive that are occupied by files are encrypted. Kaspersky Endpoint Security automatically encrypts new data as it is added.</p> <p>If the check box is cleared, the entire hard drive is encrypted, including residual fragments of previously deleted and modified files.</p> <div data-bbox="419 1818 1493 2011" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>This option is recommended for new hard drives whose data has not been modified or deleted. If you are applying encryption on a hard drive that is already in use, it is recommended to encrypt the entire hard drive. This ensures protection of all data, even deleted data that is potentially recoverable.</p> </div> <p>This check box is cleared by default.</p>
Authentication	Use Trusted Platform Module (TPM)

settings

If this option is selected, BitLocker uses a Trusted Platform Module (TPM).

A *Trusted Platform Module (TPM)* is a microchip developed to provide basic functions related to security (for example, to store encryption keys). A Trusted Platform Module is usually installed on the computer motherboard and interacts with all other system components via the hardware bus.

For computers running Windows 7 or Windows Server 2008 R2, only encryption using a TPM module is available. If a TPM module is not installed, BitLocker encryption is not possible. Use of a password on these computers is not supported.

A device equipped with a Trusted Platform Module can create encryption keys that can be decrypted only with the device. A Trusted Platform Module encrypts encryption keys with its own root storage key. The root storage key is stored within the Trusted Platform Module. This provides an additional level of protection against attempts to hack encryption keys.

This action is selected by default.

You can configure the settings for accessing the encryption key:

- **Use PIN.** If this check box is selected, a user can use of a PIN code to obtain access to an encryption key that is stored in a Trusted Platform Module (TPM). If this check box is cleared, users are prohibited from using PIN codes. To access the encryption key, a user must enter the password.
- **Use password if Trusted Platform Module (TPM) is unavailable** If the check box is selected, the user can use a password to obtain access to encryption keys when a Trusted Platform Module (TPM) is not available. If the check box is cleared and the TPM is not available, full disk encryption will not start.

Use password

If this option is selected, Kaspersky Endpoint Security prompts the user for a password when the user attempts to access an encrypted drive.

This option can be selected when a Trusted Platform Module (TPM) is not being used.

File Level Encryption

You can [compile lists of files](#) by extension or group of extensions and lists of folders stored on local computer drives, and create [rules for encrypting files that are created by specific applications](#). After a policy is applied, Kaspersky Endpoint Security encrypts and decrypts the following files:

- files individually added to lists for encryption and decryption;
- files stored in folders added to lists for encryption and decryption;
- files created by separate applications.

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Windows for workstations. This component is unavailable if Kaspersky Endpoint Security is installed on a computer that runs on Windows for servers.

File encryption has the following special features:

- Kaspersky Endpoint Security encrypts / decrypts files in predefined folders only for local user profiles of the operating system. Kaspersky Endpoint Security does not encrypt or decrypt files in predefined folders of roaming user profiles, mandatory user profiles, temporary user profiles, or redirected folders.
- Kaspersky Endpoint Security does not encrypt files whose modification could harm the operating system and installed applications. For example, the following files and folders with all nested folders are on the list of encryption exclusions:
 - %WINDIR%;
 - %PROGRAMFILES% and %PROGRAMFILES(X86)%;
 - Windows registry files.

The list of encryption exclusions cannot be viewed or edited. While files and folders on the list of encryption exclusions can be added to the encryption list, they will not be encrypted during file encryption.

File Level Encryption component settings

Parameter	Description
Manage encryption	<p>Leave unchanged. If this item is selected, Kaspersky Endpoint Security leaves the files and folders unchanged without encrypting or decrypting them.</p> <p>Encrypt according to rules. If this item is selected, Kaspersky Endpoint Security encrypts the files and folders according to encryption rules, decrypts the files and folders according to decryption rules, and regulates the access of applications to encrypted files according to application rules.</p> <p>Decrypt all. If this item is selected, Kaspersky Endpoint Security decrypts all encrypted files and folders.</p>
Encryption rules	<p>This tab shows encryption rules for files stored on local drives. You can add files as follows:</p> <ul style="list-style-type: none"> • Predefined folders. Kaspersky Endpoint Security allows you to add the following areas: <ul style="list-style-type: none"> Documents. Files in the standard <i>Documents</i> folder of the operating system, and its subfolders. Favorites. Files in the standard <i>Favorites</i> folder of the operating system, and its subfolders. Desktop. Files in the standard <i>Desktop</i> folder of the operating system, and its subfolders. Temporary files. Temporary files related to the operation of applications installed on the computer. For example, Microsoft Office applications create temporary files containing backup copies of documents. Outlook files. Files related to the operation of the Outlook mail client: data files (PST), offline data files (OST), offline address book files (OAB), and personal address book files (PAB). • Folders. You can type the path to the folder. When adding a folder path, adhere to the following rules: <ul style="list-style-type: none"> Use an environment variable (for example, %FOLDER%\UserFolder\). You can use an environment variable only once and only at the beginning of the path.

	<p>Do not use relative paths. You can use the set <code>\..\ C:\Users\..\UserFolder\ The set <code>\..\ Do not use the <code>* Do not use UNC paths. Use <code>; or <code>, as a separator character.</code></code></code></code></code></p> <ul style="list-style-type: none"> • Files by extension. You can select extension groups from the list, such as the extension group <i>Archives</i>. You can also manually add the file extension.
Decryption rules	This tab shows decryption rules for files stored on local drives.
Rules for applications	The tab displays a table containing encrypted file access rules for applications and encryption rules for files that are created or modified by individual applications.
Encrypted package password settings	Password strength requirements to meet when creating encrypted packages.

Encryption of removable drives

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Windows for workstations. This component is unavailable if Kaspersky Endpoint Security is installed on a computer that runs on Windows for servers.

Kaspersky Endpoint Security supports encryption of files in FAT32 and NTFS file systems. If a removable drive with an unsupported file system is connected to the computer, the encryption task for this removable drive ends with an error and Kaspersky Endpoint Security assigns the read-only status to the removable drive.

To protect data on removable drives, you can use the following types of encryption:

- Full Disk Encryption (FDE).

Encryption of the entire removable drive, including the file system.

It is not possible to access encrypted data outside the corporate network. It is also impossible to access encrypted data inside the corporate network if the computer is not connected to Kaspersky Security Center (e.g. on a guest computer).

- File Level Encryption (FLE).

Encryption of only files on a removable drive. The file system remains unchanged.

Encryption of files on removable drives provides the capability to access data outside the corporate network using a special mode called [*portable mode*](#).

During encryption, Kaspersky Endpoint Security creates a master key. Kaspersky Endpoint Security saves the master key in the following repositories:

- Kaspersky Security Center.

- User's computer.

The master key is encrypted with the user's secret key.

- Removable drive.

The master key is encrypted with the public key of Kaspersky Security Center.

After encryption is complete, the data on the removable drive can be accessed within the corporate network as if it was on an ordinary unencrypted removable drive.

Accessing encrypted data

When a removable drive with encrypted data is connected, Kaspersky Endpoint Security performs the following actions:

1. Checks for a master key in the local storage on the user's computer.

If the master key is found, the user gains access to the data on the removable drive.

If the master key is not found, Kaspersky Endpoint Security performs the following actions:

- a. Sends a request to Kaspersky Security Center.

After receiving the request, Kaspersky Security Center sends a response that contains the master key.

- b. Kaspersky Endpoint Security saves the master key in the local storage on the user's computer for subsequent operations with the encrypted removable drive.

2. Decrypts the data.

Special features of removable drive encryption

Encryption of removable drives has the following special features:

- The policy with preset settings for removable drive encryption is formed for a specific group of managed computers. Therefore, the result of applying the Kaspersky Security Center policy configured for encryption / decryption of removable drives depends on the computer to which the removable drive is connected.
- Kaspersky Endpoint Security does not encrypt / decrypt read-only files that are stored on removable drives.
- The following device types are supported as removable drives:
 - Data media connected via the USB bus
 - hard drives connected via USB and FireWire buses
 - SSD drives connected via USB and FireWire buses

Encryption of removable drives component settings

Parameter	Description
Manage encryption	Encrypt entire removable drive. If this item is selected, when applying the policy with the specified encryption settings for removable drives, Kaspersky Endpoint Security encrypts removable drives sector by sector, including their file systems.

Encrypt all files. If this item is selected, when applying the policy with the specified encryption settings for removable drives, Kaspersky Endpoint Security encrypts all files that are stored on removable drives. Kaspersky Endpoint Security does not re-encrypt files that are already encrypted. The contents of the file system of a removable drive, including the folder structure and names of encrypted files, are not encrypted and remain accessible.

Encrypt new files only. If this item is selected, when applying the policy with the specified encryption settings for removable drives, Kaspersky Endpoint Security encrypts only those files that were added or modified on removable drives after the Kaspersky Security Center policy was last applied. This encryption mode is convenient when a removable drive is used for both personal and work purposes. This encryption mode lets you leave all old files unchanged and encrypt only those files that the user creates on a work computer that has Kaspersky Endpoint Security installed and encryption functionality enabled. As a result, access to personal files is always available, regardless of whether or not Kaspersky Endpoint Security is installed on the computer with encryption functionality enabled.

Decrypt entire removable drive. If this item is selected, when applying the policy with the specified encryption settings for removable drives, Kaspersky Endpoint Security decrypts all encrypted files stored on removable drives as well as the file systems of the removable drives if they were previously encrypted.

Leave unchanged. If this item is selected, the application leaves drives in their previous state when the policy is applied. If the drive was encrypted, it remains encrypted. If the drive was decrypted, it remains decrypted. This item is selected by default.

Portable mode

This check box enables / disables the preparation of a removable drive that makes it possible to access files stored on this removable drive on computers outside of the corporate network.

If this check box is selected, Kaspersky Endpoint Security prompts the user to specify a password before encrypting files on a removable drive upon the application of the policy. The password is needed to access files encrypted on a removable drive on computers outside of the corporate network. You can configure the password strength.

Portable mode is available for the **Encrypt all files** or **Encrypt new files only** modes.

Encrypt used disk space only

This check box enables / disables the encryption mode in which only occupied disk sectors are encrypted. This mode is recommended for new drives whose data has not been modified or deleted.

If the check box is selected, only portions of the drive that are occupied by files are encrypted. Kaspersky Endpoint Security automatically encrypts new data as it is added.

If the check box is cleared, the entire drive is encrypted, including residual fragments of previously deleted and modified files.

The ability to encrypt only occupied space is available only for the **Encrypt entire removable drive** mode.

After encryption started, enabling / disabling the **Encrypt used disk space only** function will not change this setting. You must select or clear the check box before starting encryption.

Encryption rules for selected devices

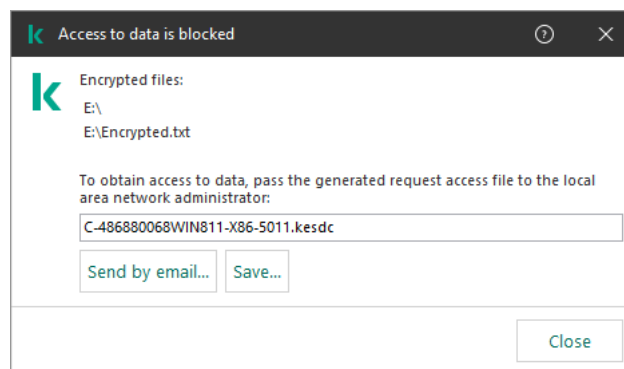
This table contains devices for which custom encryption rules are defined. You can create encryption rules for individual removable drives in the following ways:

- Add a removable drive from the list of trusted devices for Device Control.
- Manually add a removable drive:

	<ul style="list-style-type: none"> • By device ID (Hardware ID, or HWID) • By device model: vendor ID (VID) and product ID (PID)
Allow removable drive encryption in offline mode	<p>If this check box is selected, Kaspersky Endpoint Security encrypts removable drives even when there is no connection to Kaspersky Security Center. In this case, the data required for decrypting removable drives is stored on the hard drive of the computer to which the removable drive is connected, and is not transmitted to Kaspersky Security Center.</p> <p>If the check box is cleared, Kaspersky Endpoint Security does not encrypt removable drives without a connection to Kaspersky Security Center.</p>
Portable mode password settings	<p>Password strength settings for the Portable File Manager.</p>

Templates (data encryption)

After data encryption, Kaspersky Endpoint Security may restrict access to data, for example, due to a change in the organization's infrastructure and a change in the Kaspersky Security Center Administration Server. If a user does not have access to encrypted data, the user can ask the administrator for access to the data. In other words, the user needs to send a request access file to the administrator. The user then needs to upload the response file received from the administrator to Kaspersky Endpoint Security. Kaspersky Endpoint Security allows you to request access to data from the administrator via email (see the figure below).



Requesting access to encrypted data

A template is provided for reporting a lack of access to encrypted data. For user convenience, you can fill out the following fields:

- **To.** Enter the email address of the administrator group with rights to the data encryption features.
- **Subject.** Enter the subject of the email with your request for access to encrypted files. You can, for example, add tags to filter messages.
- **Message.** If necessary, change the contents of the message. You can use variables to get the necessary data (for example, %USER_NAME% variable).

Endpoint Sensor

Endpoint Sensor is not included in Kaspersky Endpoint Security 11.4.0.

You can manage the Endpoint Sensor in the Kaspersky Security Center 12 Web Console and in the Kaspersky Security Center Administration Console. It is not possible to manage Endpoint Sensor in the Kaspersky Security Center Cloud Console.

Endpoint Sensor is designed to interact with Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* is a solution designed for timely detection of sophisticated threats such as targeted attacks, advanced persistent threats (APT), zero-day attacks, and others. Kaspersky Anti Targeted Attack Platform includes two functional blocks: Kaspersky Anti Targeted Attack (hereinafter also referred to as "KATA") and Kaspersky Endpoint Detection and Response (hereinafter also referred to as "KEDR"). You can purchase KEDR separately. For detailed information on the solution, [refer to the Kaspersky Anti Targeted Attack Platform Help](#).

Managing Endpoint Sensor has the following limitations:

- You can configure Endpoint Sensor settings in a policy provided that Kaspersky Endpoint Security version 11.0.0 to 11.3.0 is installed on the computer. For more information about configuring Endpoint Sensor settings using the policy, refer to the [help articles for the previous versions of Kaspersky Endpoint Security](#).
- If Kaspersky Endpoint Security version 11.4.0 and later is installed on the computer, you cannot configure Endpoint Sensor settings in the policy.

Endpoint Sensor is installed on client computers. On these computers, the component constantly monitors processes, active network connections, and files that are modified. Endpoint Sensor relays information to the KATA server.

The component functionality is available under the following operating systems:

- Windows 7 Service Pack 1 Home / Professional / Enterprise;
- Windows 8.1 Professional / Enterprise;
- Windows 10 RS3 Home / Professional / Education / Enterprise;
- Windows 10 RS4 Home / Professional / Education / Enterprise;
- Windows 10 RS5 Home / Professional / Education / Enterprise;
- Windows 10 RS6 Home / Professional / Education / Enterprise;
- Windows Server 2008 R2 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2012 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2012 R2 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2016 Essentials / Standard (64-bit).

For detailed information on KATA operation, please [refer to the Kaspersky Anti Targeted Attack Platform Help Guide](#).

Task management

You can create the following types of tasks to administer Kaspersky Endpoint Security through Kaspersky Security Center:

- Local tasks that are configured for an individual client computer.
- Group tasks that are configured for client computers within administration groups.
- Tasks for a selection of computers.

You can create any number of group tasks, tasks for a selection of computers, or local tasks. For more details about working with administration groups and selections of computers, *please refer to [Kaspersky Security Center Help](#)*.

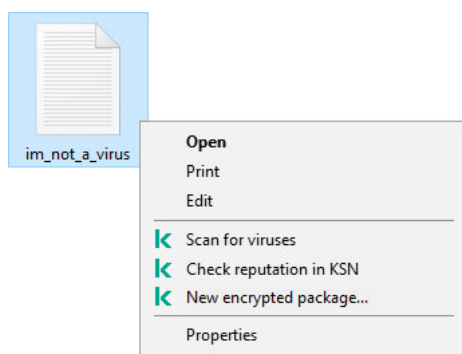
Task management settings

Parameter	Description
Allow use of local tasks	<p>If the check box is selected, local tasks are displayed in the Kaspersky Endpoint Security local interface. When there are no additional policy restrictions, the user can configure and run tasks. However, configuring task run schedule remains unavailable for the user. The user can run tasks only manually.</p> <p>If the check box is cleared, use of local tasks is stopped. In this mode, local tasks do not run according to schedule. Tasks cannot be started or configured in the local interface of Kaspersky Endpoint Security, or when working with the command line.</p> <p>A user can still start a virus scan of a file or folder by selecting the Scan for viruses option in the context menu of the file or folder. The scan task is started with the default values of settings for the custom scan task.</p>
Allow group tasks to be displayed	<p>If the check box is selected, group tasks are displayed in the Kaspersky Endpoint Security local interface. The user can view the list of all tasks in the application interface.</p> <p>If the check box is cleared, Kaspersky Endpoint Security displays an empty task list.</p>
Allow management of group tasks	<p>If the check box is selected, users can start and stop group tasks specified in Kaspersky Security Center. Users can start and stop tasks in the application interface or in the simplified application interface.</p> <p>If the check box is cleared, Kaspersky Endpoint Security starts scheduled tasks automatically, or the administrator starts tasks manually in Kaspersky Security Center.</p>

Scan from context menu

Kaspersky Endpoint Security lets you run a scan of individual files for viruses and other malware from the context menu (see the figure below).

When performing a scan from the context menu, Kaspersky Endpoint Security does not scan files whose contents are located in OneDrive cloud storage.



Scan from context menu

Scan from Context Menu task settings

Parameter	Description
Action on threat detection	<ul style="list-style-type: none"> • Disinfect; delete if disinfection fails. If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected files that are detected. If disinfection fails, Kaspersky Endpoint Security deletes the files. • Disinfect; inform if disinfection fails. If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected files that are detected. If disinfection is not possible, Kaspersky Endpoint Security adds the information about the infected files that are detected to the list of active threats. • Inform. If this option is selected, Kaspersky Endpoint Security adds the information about infected files to the list of active threats on detection of these files.
Scan only new and changed files	This check box enables or disables the mode for scanning only new files and files that have been modified since the previous scan. This helps reduce the duration of a scan.
Skip files that are scanned for longer than N sec	The check box enables / disables the time duration for scanning an object. After the specified amount of time, Kaspersky Endpoint Security stops scanning a file. This helps reduce the duration of a scan.
Scan archives	This check box enables / disables scanning of RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives.
Scan distribution packages	The check box enables or disables scanning of distribution packages.
Scan files in Microsoft Office formats	<p>This check box enables or disables scanning of Microsoft Office files (DOC, DOCX, XLS, PPT, and others).</p> <p>Office format files include OLE objects as well.</p>
Do not unpack large compound files	If this check box is selected, Kaspersky Endpoint Security does not scan compound files if their size exceeds the specified value.

Removable drives scan

Kaspersky Endpoint Security allows you to scan removable drives that are connected to your computer for viruses and other malware.

Removable drives scan task settings

Parameter	Description
Action on connection of a removable drive	<ul style="list-style-type: none">• Do not scan.• Detailed Scan If this option is selected, after a removable drive is connected Kaspersky Endpoint Security scans all files located on the removable drive, including files within compound objects.• Quick Scan If this option is selected, after a removable drive is connected Kaspersky Endpoint Security scans only files of specific formats that are most vulnerable to infection, and does not unpack compound objects.
Maximum removable drive size	<p>If this check box is selected, Kaspersky Endpoint Security performs the action that is selected in the Action on connection of a removable drive drop-down list on removable drives with a size not more than the specified maximum drive size.</p> <p>If the check box is cleared, Kaspersky Endpoint Security performs the action that is selected in the Action on connection of a removable drive drop-down list on removable drives of any size.</p>
Show scan progress	<p>If the check box is selected, Kaspersky Endpoint Security displays the progress of removable drives scan in a separate window and in the Tasks window.</p> <p>If the check box is cleared, Kaspersky Endpoint Security performs removable drives scan in the background.</p>
Block the stopping of the scan task	<p>If the check box is selected, the Stop button in the Tasks window and the Stop button in the Virus Scan window are not available in the local interface of Kaspersky Endpoint Security.</p>

Background scan

Background scan is a scan mode of Kaspersky Endpoint Security that does not display notifications for the user. Background scan requires less computer resources than other types of scans (such as a full scan). In this mode, Kaspersky Endpoint Security scans startup objects, kernel memory, and the system partition. A background scan is started in the following cases:

- After an anti-virus database update.
- 30 minutes after Kaspersky Endpoint Security is started.
- Every six hours.
- When the computer is idling for five minutes or more.

Background scan when the computer is idling is interrupted when any of the following conditions are true:

- The computer went into active mode.

If the background scan has not been run for more than ten days, the scan is not interrupted.

- The computer (laptop) has switched to battery mode.

When performing a background scan, Kaspersky Endpoint Security does not scan files whose contents are located in OneDrive cloud storage.

Application settings

You can configure the following general settings of the application:

- Operating mode
- Self-Defense
- Performance
- Debug information
- Computer status when settings are applied

Application settings

Parameter	Description
Start Kaspersky Endpoint Security for Windows on computer startup	<p>When the check box is selected, Kaspersky Endpoint Security is started after the operating system loads, protecting the computer during the entire session.</p> <p>When the check box is cleared, Kaspersky Endpoint Security is not started after the operating system loads, until the user starts it manually. Computer protection is disabled and user data may be exposed to threats.</p>
Enable Advanced Disinfection technology	<p>If the check box is selected, a pop-up notification appears on the screen when malicious activity is detected in the operating system. In its notification, Kaspersky Endpoint Security offers the user to perform Advanced Disinfection of the computer. After the user approves this procedure, Kaspersky Endpoint Security neutralizes the threat. After completing the advanced disinfection procedure, Kaspersky Endpoint Security restarts the computer. The advanced disinfection technology uses considerable computing resources, which may slow down other applications.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Advanced Disinfection technology is available only on computers running a Windows operating system for workstations. You cannot use Advanced Disinfection technology on computers running Windows operating systems for servers.</p> </div>
Use Kaspersky Security Center as	<p>If this check box is selected, the Kaspersky Security Center Administration Server is used as a proxy server when activating the application.</p>

proxy server for activation	
Enable Self-Defense	When this check box is selected, Kaspersky Endpoint Security prevents alteration or deletion of application files on the hard drive, memory processes, and entries in the system registry.
Disable external management of system services	When the check box is selected, Kaspersky Endpoint Security blocks all attempts to manage application services from a remote computer. When an attempt is made to manage application services remotely, a notification is displayed in the Microsoft Windows taskbar, above the application icon (unless the notification service has been disabled by the user).
Postpone scheduled tasks while running on battery power	If the check box is selected, energy conservation mode is enabled. Kaspersky Endpoint Security postpones scheduled tasks. You can start scan and update tasks manually, if necessary.
Concede resources to other applications	When Kaspersky Endpoint Security runs scheduled tasks, this may result in increased workload on the CPU and disk subsystems, which slows down the performance of other applications. When the check box is selected, Kaspersky Endpoint Security suspends scheduled tasks when it detects an increased load and frees up operating system resources for user applications.
Enable dump writing	If the check box is selected, Kaspersky Endpoint Security writes dumps when it crashes. If the check box is cleared, Kaspersky Endpoint Security does not write dumps. The application also deletes existing dump files from the computer hard drive.
Enable dump and trace files protection	If the check box is selected, access to dump files is granted to the system administrator and local administrator as well as to the user who enabled dump writing. Only system and local administrators can access trace files. If the check box is cleared, any user can access dump files and trace files.
Computer status when settings are applied	Settings for displaying the statuses of client computers with Kaspersky Endpoint Security installed in the Web Console when errors occur while applying a policy or executing a task. The <i>OK</i> , <i>Warning</i> , and <i>Critical</i> statuses are available.

Network options

You can configure the proxy server used for connecting to the Internet and updating anti-virus databases, select the network port monitoring mode, and configure encrypted connections scan.

Network options

Parameter	Description
Proxy server settings	Settings of the proxy server used for Internet access of users of client computers. Kaspersky Endpoint Security uses these settings for certain protection components, including for updating databases and application modules.

	<p>For automatic configuration of a proxy server, Kaspersky Endpoint Security uses the WPAD protocol (Web Proxy Auto-Discovery Protocol). If the IP address of the proxy server cannot be determined by using this protocol, Kaspersky Endpoint Security uses the proxy server address that is specified in the Microsoft Internet Explorer browser settings.</p>
Bypass proxy server for local addresses	<p>If the check box is selected, Kaspersky Endpoint Security does not use a proxy server when performing an update from a shared folder.</p>
Monitored ports	<ul style="list-style-type: none"> • Monitor all network ports. In this network port monitoring mode, the protection components (File Threat Protection, Web Threat Protection, Mail Threat Protection) monitor data streams that are transmitted via any open network ports of the computer. • Monitor selected network ports only. In this network port monitoring mode, the protection components monitor only user-specified network ports of the computer. The list of network ports that are normally used for transmission of email and network traffic is configured according to the recommendations of Kaspersky experts.
Scan encrypted connections	<p>If the check box is selected, the Web Threat Protection, Mail Threat Protection, and Web Control components scan encrypted traffic that is transmitted over the following protocols:</p> <ul style="list-style-type: none"> • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>Kaspersky Endpoint Security does not scan encrypted connections that are established by applications if the Do not scan network traffic check box is selected for those applications in the Scan exclusions for application window.</p> </div>
When visiting a domain with an untrusted certificate	<ul style="list-style-type: none"> • Allow. If this option is selected, when visiting a domain with an untrusted certificate, Kaspersky Endpoint Security allows the network connection. <p>When opening a domain with an untrusted certificate in a browser, Kaspersky Endpoint Security displays an HTML page showing a warning and the reason why visiting that domain is not recommended. A user can click the link from the HTML warning page to obtain access to the requested web resource. After following this link, during the next hour Kaspersky Endpoint Security will not display warnings about an untrusted certificate when visiting other resources on this same domain.</p> <ul style="list-style-type: none"> • Block connection. If this option is selected, when visiting a domain with an untrusted certificate, Kaspersky Endpoint Security blocks the network connection. <p>When opening a domain with an untrusted certificate in a browser, Kaspersky Endpoint Security displays an HTML page showing the reason why that domain is blocked.</p>
When encrypted connection scan errors occur	<ul style="list-style-type: none"> • Block connection. If this item is selected, when an encrypted connection scan error occurs, Kaspersky Endpoint Security blocks the network connection. • Add domain to exclusions. If this item is selected, when an encrypted connection scan error occurs, Kaspersky Endpoint Security adds the domain that resulted in the error to the list of domains with scan errors and does not monitor encrypted network traffic when this domain is visited. You can view a list of domains with encrypted connections

	scan errors only in the local interface of the application. To clear the list contents, you need to select Block connection .
Block SSL 2.0 connections	<p>If the check box is selected, Kaspersky Endpoint Security blocks network connections established over the SSL 2.0 protocol.</p> <p>If the check box is cleared, Kaspersky Endpoint Security does not block network connections established over the SSL 2.0 protocol and does not monitor network traffic transmitted over these connections.</p>
Decrypt encrypted connections with websites that use EV certificates	<p>EV certificates (Extended Validation Certificates) confirm the authenticity of websites and enhance the security of the connection. Browsers use a lock icon in their address bar to indicate that a website has an EV certificate. Browsers may also fully or partially color the address bar in green.</p> <p>If the check box is selected, Kaspersky Endpoint Security decrypts and monitors encrypted connections with websites that use an EV certificate.</p> <p>If the check box is cleared, Kaspersky Endpoint Security does not have access to the contents of HTTPS traffic. For this reason, the application monitors HTTPS traffic only based on the website address, for example, <code>https://facebook.com</code>.</p> <p>If you are opening a website with an EV certificate for the first time, the encrypted connection will be decrypted regardless of whether or not the check box is selected.</p>
Trusted addresses	List of web addresses for which Kaspersky Endpoint Security does not scan encrypted network connections.
Trusted applications	List of applications whose activity is not monitored by Kaspersky Endpoint Security during its operation. You can select the types of application activity that Kaspersky Endpoint Security will not monitor (for example, do not scan network traffic).

Exclusions

A *trusted zone* is a system administrator-configured list of objects and applications that Kaspersky Endpoint Security does not monitor when active. In other words, it is a set of scan exclusions.

The administrator forms the trusted zone independently, taking into account the features of the objects that are handled and the applications that are installed on the computer. It may be necessary to include objects and applications in the trusted zone when Kaspersky Endpoint Security blocks access to a certain object or application, if you are sure that the object or application is harmless.

You can exclude objects from scans by using the following methods:

- specify the path to the file or folder;
- enter the object hash;
- Use masks:
 - The * (asterisk) character, which takes the place of any set of characters, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask `C:**.txt` will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.

- Two consecutive * characters take the place of any set of characters (including an empty set) in the file or folder name, including the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\Folder***.txt will include all paths to files with the TXT extension located in the folder named Folder and its subfolders. The mask must include at least one nesting level. The mask C:***.txt is not a valid mask.
- The ? (question mark) character, which takes the place of any single character, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\Folder\???.txt will include paths to all files residing in the folder named Folder that have the TXT extension and a name consisting of three characters.
- Enter the name of the object according to the classification of the [Kaspersky IT Encyclopedia](#) (for example, Email-Worm, Rootkit or RemoteAdmin).

Scan exclusions

A *scan exclusion* is a set of conditions that must be fulfilled so that Kaspersky Endpoint Security will not scan a particular object for viruses and other threats.

Scan exclusions make it possible to safely use legitimate software that can be exploited by criminals to damage the computer or user data. Although they do not have any malicious functions, such applications can be exploited by intruders. For details on legitimate software that could be used by criminals to harm the computer or personal data of a user, please visit the website of the [Kaspersky IT Encyclopedia](#).

Such applications may be blocked by Kaspersky Endpoint Security. To prevent them from being blocked, you can configure scan exclusions for the applications in use. To do so, add the name or name mask that is listed in the Kaspersky IT Encyclopedia to the trusted zone. For example, you often use the Radmin application for remote administration of computers. Kaspersky Endpoint Security regards this activity as suspicious and may block it. To prevent the application from being blocked, create a scan exclusion with the name or name mask that is listed in the Kaspersky IT Encyclopedia.

If an application that collects information and sends it to be processed is installed on your computer, Kaspersky Endpoint Security may classify this application as malware. To avoid this, you can exclude the application from scanning by configuring Kaspersky Endpoint Security as described in this document.

Scan exclusions can be used by the following application components and tasks that are configured by the system administrator:

- Behavior Detection.
- Exploit Prevention.
- Host Intrusion Prevention.
- File Threat Protection.
- Web Threat Protection.
- Mail Threat Protection.
- Scan tasks.

List of trusted applications

The *list of trusted applications* is a list of applications whose file and network activity (including malicious activity) and access to the system registry are not monitored by Kaspersky Endpoint Security. By default, Kaspersky Endpoint Security scans objects that are opened, executed, or saved by any application process and controls the activity of all applications and network traffic that is generated by them. Kaspersky Endpoint Security excludes applications in the [list of trusted applications](#) from scanning.


For example, if you consider objects that are used by the standard Microsoft Windows Notepad application to be safe without scanning, meaning that you trust this application, you can add Microsoft Windows Notepad to the list of trusted applications. Scanning then skips objects that are used by this application.

In addition, certain actions that are classified by Kaspersky Endpoint Security as suspicious may be safe within the context of the functionality of a number of applications. For example, the interception of text that is typed from the keyboard is a routine process for automatic keyboard layout switchers (such as Punto Switcher). To take account of the specifics of such applications and exclude their activity from monitoring, we recommend that you add such applications to the trusted applications list.

Excluding trusted applications from scanning allows avoiding compatibility conflicts between Kaspersky Endpoint Security and other programs (for example, the problem of double-scanning of the network traffic of a third-party computer by Kaspersky Endpoint Security and by another anti-virus application), and also increases the computer's performance, which is critical when using server applications.

At the same time, the executable file and process of the trusted application are still scanned for viruses and other malware. An application can be fully excluded from Kaspersky Endpoint Security scanning by means of scan exclusions.

Settings of exclusions

Parameter	Description
Objects for detection	<p>Regardless of the configured application settings, Kaspersky Endpoint Security always detects and blocks viruses, worms, and Trojans. They can cause significant harm to the computer.</p> <ul style="list-style-type: none">• Viruses and worms 

Subcategory: viruses and worms (Viruses_and_Worms)

Threat level: high

Classic viruses and worms perform actions that are not authorized by the user. They can create copies of themselves which are able to self-replicate.

Classic virus

When a classic virus infiltrates a computer, it infects a file, activates, performs malicious actions, and adds copies of itself to other files.

A classic virus multiplies only on local resources of the computer; it cannot penetrate other computers on its own. It can be passed to another computer only if it adds a copy of itself to a file that is stored in a shared folder or on an inserted CD, or if the user forwards an email message with an attached infected file.

Classic virus code can penetrate various areas of computers, operating systems, and applications. Depending on the environment, viruses are divided into *file viruses*, *boot viruses*, *script viruses*, and *macro viruses*.

Viruses can infect files by using a variety of techniques. *Overwriting* viruses write their code over the code of the file that is infected, thus erasing the file's content. The infected file stops functioning and cannot be restored. *Parasitic* viruses modify files, leaving them fully or partially functional. *Companion viruses* do not modify files, but instead create duplicates. When an infected file is opened, a duplicate of it (what is actually a virus) is started. The following types of viruses are also encountered: *link viruses*, *OBJ viruses*, *LIB viruses*, *source code* viruses, and many others.

Worm

As with a classic virus, the code of a worm is activated and performs malicious actions after it infiltrates a computer. Worms are so named because of their ability to "crawl" from one computer to another and to spread copies via numerous data channels without the user's permission.

The main feature that allows differentiating between various types of worms is the way they spread. The following table provides an overview of various types of worms, which are classified by the way in which they spread.

Ways in which worms spread

Type	Name	Description
Email-Worm	Email-Worm	They spread via email. An infected email message contains an attached file with a copy of a worm, or a link to a file that is uploaded to a website which may have been hacked or created exclusively for that purpose. When you open the attached file, the worm is activated. When you click the link, download, and then open the file, the worm also starts performing its malicious actions. After that, it goes on spreading copies of itself, searching for other email addresses and sending infected messages to them.
IM-Worm	IM clients	They spread through IM clients.

		Usually, such worms send messages that contain a link to a file with a copy of the worm on a website, making use of the user's contact lists. When the user downloads and opens the file, the worm activates.
IM-Worm	Internet chat worms	<p>They spread via Internet Relay Chats, service systems which allow communicating with other people over the Internet in real time.</p> <p>These worms publish a file with a copy of themselves or a link to the file in an Internet chat. When the user downloads and opens the file, the worm activates.</p>
Net-Worm	Network worms	<p>These worms spread over computer networks.</p> <p>Unlike other types of worms, a typical network worm spreads without the user's participation. It scans the local network for computers that contain programs with vulnerabilities. To do this, it sends a specially formed network packet (exploit) which contains the worm code or a part of it. If a "vulnerable" computer is on the network, it receives such a network packet. When the worm completely penetrates the computer, it activates.</p>
P2P Worm	File sharing network worms	<p>They spread over peer-to-peer file sharing networks.</p> <p>To infiltrate a P2P network, the worm copies itself into a file sharing folder which is usually located on the user's computer. The P2P network displays information about this file so that the user may "find" the infected file on the network like any other file, and then download and open it.</p> <p>More sophisticated worms emulate the network protocol of a specific P2P network: they return positive responses to search queries and offer copies of themselves for download.</p>
Worm	Other types of worms	<p>Other types of worms include:</p> <ul style="list-style-type: none"> • Worms that spread copies of themselves over network resources. By using the functions of the operating system, they scan available network folders, connect to computers on the Internet, and attempt to obtain full access to their disk drives. Unlike the previously described types of worms, other types of worms activate not on their own, but when the user opens a file that contains a copy of the worm. • Worms that do not use any of the methods described in the previous table to spread (for example, those that spread over cell phones).

- [Trojans](#) 

Subcategory: Trojans

Threat level: high

Unlike worms and viruses, Trojans do not self-replicate. For example, they penetrate a computer via email or a browser when the user visits an infected web page. Trojans are started with the user's participation. They begin performing their malicious actions right after they are started.

Different Trojans behave differently on infected computers. The main functions of Trojans consist in blocking, modifying, or destroying information, and disabling computers or networks. Trojans can also receive or send files, run them, display messages on the screen, request web pages, download and install programs, and restart the computer.

Hackers often use "sets" of various Trojans.

Types of Trojan behavior are described in the following table.

Types of Trojan behavior on an infected computer

Type	Name	Description
Trojan-ArcBomb	Trojans – "archive bombs"	<p>When unpacked, these archives grow in size to such an extent that the computer's operation is impacted.</p> <p>When the user attempts to unpack such an archive, the computer may slow down or freeze; the hard disk may become filled with "empty" data. "Archive bombs" are especially dangerous to file and mail servers. If the server uses an automatic system to process incoming information, an "archive bomb" may halt the server.</p>
Backdoor	Trojans for remote administration	<p>They are considered the most dangerous type of Trojan. In their functions, they are similar to remote administration applications that are installed on computers.</p> <p>These programs install themselves on the computer without being noticed by the user, allowing the intruder to manage the computer remotely.</p>
Trojan	Trojans	<p>They include the following malicious applications:</p> <ul style="list-style-type: none">• Classic Trojans. These programs perform only the main functions of Trojans: blocking, modifying or destroying information, and disabling computers or networks. They do not have any advanced features, unlike the other types of Trojans that are described in the table.• Versatile Trojans. These programs have advanced features typical of several types of Trojans.

Trojan-Ransom	Ransom Trojans	They take the user's information "hostage", modifying or blocking it, or impact the computer's operation so that the user loses the ability to use information. The intruder demands a ransom from the user, promising to send an application to restore the computer's performance and the data that had been stored on it.
Trojan-Clicker	Trojan clickers	They access web pages from the user's computer, either by sending commands to a browser on their own or by changing the web addresses that are specified in operating system files. By using these programs, intruders perpetrate network attacks and increase website visits, increasing the number of displays of banner ads.
Trojan-Downloader	Trojan downloaders	They access the intruder's web page, download other malicious applications from it, and install them on the user's computer. They can contain the file name of the malicious application to download, or receive it from the web page that is accessed.
Trojan-Dropper	Trojan droppers	They contain other Trojans which they install on the hard drive and then install. Intruders may use Trojan Dropper-type programs for the following goals: <ul style="list-style-type: none"> • Install a malicious application without being noticed by the user: Trojan Dropper-type programs display no messages, or display fake messages which inform, for example, of an error in an archive or an incompatible version of the operating system. • Protect another known malicious application from detection: not all anti-virus software can detect a malicious application within a Trojan Dropper-type application.
Trojan-Notifier	Trojan notifiers	They inform an intruder that the infected computer is accessible, sending the intruder information about the computer: IP address, number of opened port, or email address. They connect with the intruder via email, FTP, accessing the intruder's web page, or in another way. Trojan Notifier-type programs are often used in sets that are made of several Trojans. They notify the intruder that other Trojans have been successfully installed on the user's computer.
Trojan-Proxy	Trojan proxies	They allow the intruder to anonymously access web pages by using the user's

		computer; they are often used for sending spam.
Trojan-PSW	Password-stealing-ware	<p>Password-stealing-ware is a kind of Trojan that steals user accounts, such as software registration data. These Trojans find confidential data in system files and in the registry and send it to the "master" by email, via FTP, by accessing the intruder's web page, or in another way.</p> <p>Some of these Trojans are categorized into separate types that are described in this table. These are Trojans that steal bank accounts (Trojan-Banker), steal data from users of IM clients (Trojan-IM), and steal information from users of online games (Trojan-GameThief).</p>
Trojan-Spy	Trojan spies	They spy on the user, collecting information about the actions that the user makes while working at the computer. They may intercept the data that the user enters at the keyboard, take screenshots, or collect lists of active applications. After they receive the information, they transfer it to the intruder by email, via FTP, by accessing the intruder's web page, or in another way.
Trojan-DDoS	Trojan network attackers	<p>They send numerous requests from the user's computer to a remote server. The server lacks resources to process all requests, so it stops functioning (Denial of Service, or simply DoS). Hackers often infect many computers with these programs so that they can use the computers to attack a single server simultaneously.</p> <p>DoS programs perpetrate an attack from a single computer with the user's knowledge. DDoS (Distributed DoS) programs perpetrate distributed attacks from several computers without being noticed by the user of the infected computer.</p>
Trojan-IM	Trojans that steal information from users of IM clients	They steal account numbers and passwords of IM client users. They transfer the data to the intruder by email, via FTP, by accessing the intruder's web page, or in another way.
Rootkit	Rootkits	They mask other malicious applications and their activity, thus prolonging the applications' persistence in the operating system. They can also conceal files, processes in an infected computer's memory, or registry keys which run malicious applications. The rootkits can mask data exchange between applications on the user's computer and other computers on the network.
Trojan-SMS	Trojans in the form of SMS messages	They infect cell phones, sending SMS messages to premium-rate phone numbers.

Trojan-GameThief	Trojans that steal information from users of online games	They steal account credentials from users of online games, after which they send the data to the intruder by email, via FTP, by accessing the intruder's web page, or in another way.
Trojan-Banker	Trojans that steal bank accounts	They steal bank account data or e-money system data; send the data to the hacker by email, via FTP, by accessing the hacker's web page, or by using another method.
Trojan-Mailfinder	Trojans that collect email addresses	They collect email addresses that stored on a computer and send them to the intruder by email, via FTP, by accessing the intruder's web page, or in another way. Intruders may send spam to the addresses they have collected.

- [Malicious tools](#) 

Subcategory: Malicious tools

Danger level: medium

Unlike other types of malware, malicious tools do not perform their actions right after they are started. They can be safely stored and started on the user's computer. Intruders often use the features of these programs to create viruses, worms, and Trojans, perpetrate network attacks on remote servers, hack computers, or perform other malicious actions.

Various features of malicious tools are grouped by the types that are described in the following table.

Features of malicious tools

Type	Name	Description
Constructor	Constructors	They allow creating new viruses, worms, and Trojans. Some constructors boast a standard window-based interface in which the user can select the type of malicious application to create, the way of counteracting debuggers, and other features.
Dos	Network attacks	They send numerous requests from the user's computer to a remote server. The server lacks resources to process all requests, so it stops functioning (Denial of Service, or simply DoS).
Exploit	Exploits	<p>An exploit is a set of data or a program code that uses vulnerabilities of the application in which it is processed, performing a malicious action on a computer. For example, an exploit can write or read files, or request "infected" web pages.</p> <p>Different exploits use vulnerabilities in different applications or network services. Disguised as a network packet, an exploit is transmitted over the network to numerous computers, searching for computers with vulnerable network services. An exploit in a DOC file uses the vulnerabilities of a text editor. It may start performing the actions that are preprogrammed by the hacker when the user opens the infected file. An exploit that is embedded in an email message searches for vulnerabilities in any email client. It may start performing a malicious action as soon as the user opens the infected message in this email client.</p> <p>Net-Worms spread over networks by using exploits. Nuker <i>exploits</i> are network packets that disable computers.</p>
FileCryptor	Encryptors	They encrypt other malicious applications to conceal them from the anti-virus application.

Flooder	Programs for "contaminating" networks	<p>They send numerous messages over network channels. This type of tools includes, for example, programs that contaminate Internet Relay Chats.</p> <p>Flooder-type tools do not include programs that "contaminate" channels that are used by email, IM clients, and mobile communication systems. These programs are distinguished as separate types that are described in the table (Email-Flooder, IM-Flooder, and SMS-Flooder).</p>
HackTool	Hacking tools	They make it possible to hack the computer on which they are installed or attack another computer (for example, by adding new system accounts without the user's permission or by erasing system logs to conceal traces of their presence in the operating system). This type of tools includes some sniffers which feature malicious functions, such as password interception. Sniffers are programs that allow viewing network traffic.
Hoax	Hoaxes	They alarm the user with virus-like messages: they may "detect a virus" in an uninfected file or notify the user that the disk has been formatted, although this has not happened in reality.
Spoofers	Spoofing tools	They send messages and network requests with a fake address of the sender. Intruders use Spoofers-type tools to pass themselves off as the true senders of messages, for example.
VirTool	Tools that modify malicious applications	They allow modifying other malware programs, concealing them from anti-virus applications.
Email-Flooder	Programs that "contaminate" email addresses	They send numerous messages to various email addresses, thus "contaminating" them. A large volume of incoming messages prevents users from viewing useful messages in their inboxes.
IM-Flooder	Programs that "contaminate" traffic of IM clients	They flood users of IM clients with messages. A large volume of messages prevents users from viewing useful incoming messages.
SMS-Flooder	Programs that "contaminate" traffic with SMS messages	They send numerous SMS messages to cell phones.

- [Adware](#) 

Subcategory: advertising software (Adware);

Threat level: medium

Adware displays advertising information to the user. Adware programs display banner ads in the interfaces of other programs and redirect search queries to advertising web pages. Some of them collect marketing information about the user and send it to the developer: this information may include the names of the websites that are visited by the user or the content of the user's search queries. Unlike Trojan-Spy-type programs, adware sends this information to the developer with the user's permission.

- [Auto-dialers](#) 

Subcategory: legal software that may be used by criminals to damage your computer or personal data.

Danger level: medium

Most of these applications are useful, so many users run them. These applications include IRC clients, auto-dialers, file download programs, computer system activity monitors, password utilities, and Internet servers for FTP, HTTP, and Telnet.

However, if intruders gain access to these programs, or if they plant them on the user's computer, some of the application's features may be used to violate security.

These applications differ by function; their types are described in the following table.

Type	Name	Description
Client-IRC	Internet chat clients	Users install these programs to talk to people in Internet Relay Chats. Intruders use them to spread malware.
Dialer	Auto-dialers	They can establish phone connections over a modem in hidden mode.
Downloader	Programs for downloading	They can download files from web pages in hidden mode.
Monitor	Programs for monitoring	They allow monitoring activity on the computer on which they are installed (seeing which applications are active and how they exchange data with applications that are installed on other computers).
PSWTool	Password restorers	They allow viewing and restoring forgotten passwords. Intruders secretly implant them on users' computers with the same purpose.
RemoteAdmin	Remote administration programs	They are widely used by system administrators. These programs allow obtaining access to the interface of a remote computer to monitor and manage it. Intruders secretly implant them on users' computers with the same purpose: to monitor and manage remote computers. Legal remote administration programs differ from Backdoor-type Trojans for remote administration. Trojans have the ability to penetrate the operating system independently and install themselves; legal programs are unable to do so.
Server-FTP	FTP servers	They function as FTP servers. Intruders implant them on the user's computer to open remote access to it via FTP.
Server-Proxy	Proxy servers	They function as proxy servers. Intruders implant them on the user's computer to send spam under the user's name.
Server-Telnet	Telnet servers	They function as Telnet servers. Intruders implant them on the user's computer to

		open remote access to it via Telnet.
Server-Web	Web servers	They function as web servers. Intruders implant them on the user's computer to open remote access to it via HTTP.
RiskTool	Tools for working at a local computer	They provide the user with additional options when working at the user's own computer. The tools allow the user to hide files or windows of active applications and terminate active processes.
NetTool	Network tools	They provide the user with additional options when working with other computers on the network. These tools allow restarting them, detecting open ports, and starting applications that are installed on the computers.
Client-P2P	P2P network clients	They allow working on peer-to-peer networks. They can be used by intruders for spreading malware.
Client-SMTP	SMTP clients	They send email messages without the user's knowledge. Intruders implant them on the user's computer to send spam under the user's name.
WebToolbar	Web toolbars	They add toolbars to the interfaces of other applications to use search engines.
FraudTool	Pseudo-programs	They pass themselves off as other programs. For example, there are pseudo-anti-virus programs which display messages about malware detection. However, in reality, they do not find or disinfect anything.

- [Other](#) 

Subcategory: legal software that may be used by criminals to damage your computer or personal data.

Danger level: medium

Most of these applications are useful, so many users run them. These applications include IRC clients, auto-dialers, file download programs, computer system activity monitors, password utilities, and Internet servers for FTP, HTTP, and Telnet.

However, if intruders gain access to these programs, or if they plant them on the user's computer, some of the application's features may be used to violate security.

These applications differ by function; their types are described in the following table.

Type	Name	Description
Client-IRC	Internet chat clients	Users install these programs to talk to people in Internet Relay Chats. Intruders use them to spread malware.
Dialer	Auto-dialers	They can establish phone connections over a modem in hidden mode.
Downloader	Programs for downloading	They can download files from web pages in hidden mode.
Monitor	Programs for monitoring	They allow monitoring activity on the computer on which they are installed (seeing which applications are active and how they exchange data with applications that are installed on other computers).
PSWTool	Password restorers	They allow viewing and restoring forgotten passwords. Intruders secretly implant them on users' computers with the same purpose.
RemoteAdmin	Remote administration programs	They are widely used by system administrators. These programs allow obtaining access to the interface of a remote computer to monitor and manage it. Intruders secretly implant them on users' computers with the same purpose: to monitor and manage remote computers. Legal remote administration programs differ from Backdoor-type Trojans for remote administration. Trojans have the ability to penetrate the operating system independently and install themselves; legal programs are unable to do so.
Server-FTP	FTP servers	They function as FTP servers. Intruders implant them on the user's computer to open remote access to it via FTP.
Server-Proxy	Proxy servers	They function as proxy servers. Intruders implant them on the user's computer to send spam under the user's name.
Server-Telnet	Telnet servers	They function as Telnet servers. Intruders implant them on the user's computer to

		open remote access to it via Telnet.
Server-Web	Web servers	They function as web servers. Intruders implant them on the user's computer to open remote access to it via HTTP.
RiskTool	Tools for working at a local computer	They provide the user with additional options when working at the user's own computer. The tools allow the user to hide files or windows of active applications and terminate active processes.
NetTool	Network tools	They provide the user with additional options when working with other computers on the network. These tools allow restarting them, detecting open ports, and starting applications that are installed on the computers.
Client-P2P	P2P network clients	They allow working on peer-to-peer networks. They can be used by intruders for spreading malware.
Client-SMTP	SMTP clients	They send email messages without the user's knowledge. Intruders implant them on the user's computer to send spam under the user's name.
WebToolbar	Web toolbars	They add toolbars to the interfaces of other applications to use search engines.
FraudTool	Pseudo-programs	They pass themselves off as other programs. For example, there are pseudo-anti-virus programs which display messages about malware detection. However, in reality, they do not find or disinfect anything.

- [Packed files that may cause harm](#) 

Kaspersky Endpoint Security scans compressed objects and the unpacker module within SFX (self-extracting) archives.

To hide dangerous programs from anti-virus applications, intruders archive them by using special packers or create multi-packed files.

Kaspersky virus analysts have identified packers that are the most popular amongst hackers.

If Kaspersky Endpoint Security detects such a packer in a file, the file most likely contains a malicious application or an application that can be used by criminals to cause harm to your computer or personal data.

Kaspersky Endpoint Security singles out the following types of programs:

- *Packed files that may cause harm* – used for packing malware, such as viruses, worms, and Trojans.
- *Multi-packed files* (medium threat level) – the object has been packed three times by one or more packers.

- [Multi-packed files](#) 

Kaspersky Endpoint Security scans compressed objects and the unpacker module within SFX (self-extracting) archives.

To hide dangerous programs from anti-virus applications, intruders archive them by using special packers or create multi-packed files.

Kaspersky virus analysts have identified packers that are the most popular amongst hackers.

If Kaspersky Endpoint Security detects such a packer in a file, the file most likely contains a malicious application or an application that can be used by criminals to cause harm to your computer or personal data.

Kaspersky Endpoint Security singles out the following types of programs:

- *Packed files that may cause harm* – used for packing malware, such as viruses, worms, and Trojans.
- *Multi-packed files* (medium threat level) – the object has been packed three times by one or more packers.

Scan exclusions

This table contains information about scan exclusions.

You can exclude objects from scans by using the following methods:

- specify the path to the file or folder;
- enter the object hash;
- Use masks:

	<ul style="list-style-type: none"> • The * (asterisk) character, which takes the place of any set of characters, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:**.txt will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders. • Two consecutive * characters take the place of any set of characters (including an empty set) in the file or folder name, including the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\Folder***.txt will include all paths to files with the TXT extension located in the folder named Folder and its subfolders. The mask must include at least one nesting level. The mask C:***.txt is not a valid mask. • The ? (question mark) character, which takes the place of any single character, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\Folder\???.txt will include paths to all files residing in the folder named Folder that have the TXT extension and a name consisting of three characters. • Enter the name of the object according to the classification of the Kaspersky IT Encyclopedia (for example, Email-Worm, Rootkit or RemoteAdmin).
Trusted applications	<p>This table lists trusted applications whose activity is not monitored by Kaspersky Endpoint Security during its operation.</p> <p>The Application Control component regulates the startup of each of the applications regardless of whether or not the application is included in the table of trusted applications.</p>
Use trusted system certificate store	<p>If the check box is selected, Kaspersky Endpoint Security excludes from scanning the applications signed with a trusted digital signature. The Host Intrusion Prevention component automatically assigns such applications to the Trusted group.</p> <p>If the check box is cleared, a virus scan is performed regardless of whether or not the application has a digital signature. The Host Intrusion Prevention component assigns applications to trust groups according to the configured settings.</p>

Reports and Storage

Reports

Information about the operation of each Kaspersky Endpoint Security component, data encryption events, the performance of each scan task, the update task and integrity check task, and the overall operation of the application is recorded in reports.

Reports are stored in the folder C:\ProgramData\Kaspersky Lab\KES\Report.

Backup

Backup stores reserve copies of files that were deleted or modified during disinfection. A *backup copy* is a file copy created before the file was disinfected or deleted. Backup copies of files are stored in a special format and do not pose a threat.

Backup copies of files are stored in the folder C:\ProgramData\Kaspersky Lab\KES\QB.

Users in the Administrators group are granted full permission to access this folder. Limited access rights to this folder are granted to the user whose account was used to install Kaspersky Endpoint Security.

Kaspersky Endpoint Security does not provide the capability to configure user access permissions to backup copies of files.

Settings of reports and storage

Parameter	Description
Store reports no longer than N days	If the check box is selected, the maximum report storage term is limited to the defined time interval. The default maximum storage term for reports is 30 days. After that period of time, Kaspersky Endpoint Security automatically deletes the oldest entries from the report file.
Maximum file size N MB	If the check box is selected, the maximum report file size is limited to the defined value. By default, the maximum file size is 1024 MB. To avoid exceeding the maximum report file size, Kaspersky Endpoint Security automatically deletes the oldest entries from the report file when the maximum report file size is reached.
Store objects no longer than N days	If the check box is selected, the maximum file storage term is limited to the defined time interval. The default maximum storage term for files is 30 days. After expiration of the maximum storage term, Kaspersky Endpoint Security deletes the oldest files from Backup.
Maximum storage size N MB	If the check box is selected, the maximum storage size is limited to the defined value. By default, the maximum size is 100 MB. To avoid exceeding the maximum storage size, Kaspersky Endpoint Security automatically deletes the oldest files from storage when the maximum storage size is reached.
Data transfer to Administration Server	Categories of events on client computers whose information must be relayed to the Administration Server.

Interface

You can configure the settings of the application interface.

Interface settings

Parameter	Description
Interaction with user	<ul style="list-style-type: none"> • With simplified interface. On a client computer, the main application window is inaccessible, and only the icon in the Windows notification area is available. In the context menu of the icon, the user can perform a limited number of operations with Kaspersky Endpoint Security. Kaspersky Endpoint Security also displays notifications above the application icon. • With full interface. On a client computer, the main window of Kaspersky Endpoint Security and the icon in the Windows notification area are available. In the context menu of the icon, the user can perform operations with Kaspersky Endpoint Security. Kaspersky Endpoint Security also displays notifications above the application icon. • No interface. On a client computer, no signs of Kaspersky Endpoint Security operation are displayed. The icon in the Windows notification area and notifications are not available.

Notifications	<ul style="list-style-type: none"> • Notification rules. A table with the settings of notifications about events of different importance levels that may occur during the operation of a component, task, or the entire application. Kaspersky Endpoint Security shows notifications about these events on the screen, sends them by email, or logs them. • Email notification settings. SMTP server settings for delivery of notifications about events registered during operation of the application.
Warnings	Categories of application events that cause the Kaspersky Endpoint Security icon to change in the Microsoft Windows taskbar notification area (🛡️ or 🛡️) and result in a pop-up notification.
Local anti-virus database status notifications	Settings of notifications about outdated anti-virus databases used by the application.
Password protection	<p>If the toggle button is switched on, Kaspersky Endpoint Security prompts the user for a password when the user attempts to perform an operation that is within the scope of Password Protection. The Password Protection scope includes forbidden operations (such as disabling protection components) and the user accounts to which the Password Protection scope is applied.</p> <p>After Password Protection is enabled, Kaspersky Endpoint Security prompts you to set a password for performing operations.</p>
Technical Support web resources	List of links to web resources containing information about technical support for Kaspersky Endpoint Security. Added links are displayed in the Support window of the Kaspersky Endpoint Security local interface instead of standard links.
Message to user	Message that is displayed in the Support window of the local interface of Kaspersky Endpoint Security.

Appendix 2. Application trust groups

Kaspersky Endpoint Security categorizes all applications that are started on the computer into trust groups. Applications are categorized into trust groups depending on the level of threat that the applications pose to the operating system.

The trust groups are as follows:

- **Trusted.** This group includes applications for which one or more of the following conditions are met:
 - Applications are digitally signed by trusted vendors.
 - Applications are recorded in the trusted applications database of Kaspersky Security Network.
 - The user has placed applications in the Trusted group.

No operations are prohibited for these applications.

- **Low Restricted.** This group includes applications for which the following conditions are met:
 - Applications are not digitally signed by trusted vendors.

- Applications are not recorded in the trusted applications database of Kaspersky Security Network.
- The user has placed applications in the "Low Restricted" group.

Such applications are subject to minimal restrictions on access to operating system resources.

- **High Restricted.** This group includes applications for which the following conditions are met:
 - Applications are not digitally signed by trusted vendors.
 - Applications are not recorded in the trusted applications database of Kaspersky Security Network.
 - The user has placed applications in the High Restricted group.

Such applications are subject to high restrictions on access to operating system resources.

- **Untrusted.** This group includes applications for which the following conditions are met:
 - Applications are not digitally signed by trusted vendors.
 - Applications are not recorded in the trusted applications database of Kaspersky Security Network.
 - The user has placed applications in the Untrusted group.

For these applications, all operations are blocked.

Appendix 3. Web resource content categories

The web resource content categories (hereinafter also referred to as "categories") listed below have been selected to most fully describe the blocks of data hosted by web resources, taking into account their functional and thematic features. The order in which the categories appear in this list does not reflect the relative importance or prevalence of such categories on the Internet. The category names are provisional and used solely for the purposes of Kaspersky applications and websites. The names do not necessarily reflect the meaning implied by law. One web resource can belong to several categories at once.

Adult content

This category generally includes web resources related to the sexual aspect of human relationships, philosophies, sex shops, etc. This includes content in any form or format.

Alcohol, tobacco, drugs

This category generally includes web resources that mention alcohol, drugs, or tobacco of any kind, including advertising, historical, medical and educational resources. This also includes web resources where devices for the use of these substances are described or sold.

Violence

This category includes web resources containing any photo-, video- or text materials describing acts of physical or psychological violence directed against people or cruel treatment of animals, which serve as an intended purpose of this content.

Works of art may be exceptions in this category.

Profanity, obscenity

This category includes web resources where profane language has been detected.

This category also includes web resources with linguistic and philological materials containing profanity as the subject of study.

Weapons, explosives, pyrotechnics

This category includes web resources with information about weapons, explosives, and pyrotechnical products.

The term "weapons" means appliances, items, and means designed to harm the life or health of humans and animals and/or damage equipment and structures.

Job search

This category includes web resources designed to bring together employers and job seekers. This specifically includes the following:

- Websites of recruitment agencies (employment agencies and/or headhunting agencies).
- Websites of employers with descriptions of available job openings and their advantages.
- Independent portals with offers of employment from employers and recruitment agencies.
- Professional social networks that, among other capabilities, make it possible to publish or find information about specialists who are not actively searching for employment.

Anonymizers

This category includes web resources that act as an intermediary in downloading content of other web resources using special web applications for doing the following:

- Bypass restrictions imposed by a LAN administrator on access to web addresses or IP addresses.
- Anonymously access web resources, including web resources that deliberately reject HTTP requests from certain IP addresses or their groups (for example, IP addresses grouped by country of origin).

Software, audio, video

This category generally includes web resources that provide the capability to download related files.

- **Torrents**

Torrent trackers and web resources that help organize their work.

- **File sharing**

Web resources that provide the capability for file sharing.

- **Audio, video**

Web resources from which you can download or view/listen to video/audio files.

Gambling, lotteries, sweepstakes

This category includes web resources offering:

- Gambling in which participants are required to make monetary contributions.
- Sweepstakes that involve betting with money.
- Lotteries that involve purchasing lottery tickets or numbers.

Internet communication

This category generally includes web resources that allow specific users (registered or not) to send personalized messages to other users. There are a number of web resources designed for communication.

- **Web-based email**

Web-based email – exclusively login pages of an email service and mailbox pages containing emails and associated data (such as personal contacts). This category is not assigned to other web pages of an Internet service provider that also offers email service.

- **Social networks**

Social networks – websites designed for building, displaying, and managing contacts between persons, organizations, and governments, which require registering a user account as a condition of participation.

- **Chats, forums**

This category includes web chats as well as web resources designed to distribute or support instant messaging applications that enable real-time communication. It also includes forums, which are special web services for public discussion of various topics while saving the correspondence.

- **Blogs**

Blogs – web resources intended for a public discussion of various topics by means of special web applications, including blog platforms (websites that offer pay-for or free blog creation and maintenance services).

- **Dating sites**

Online dating resources that help organize dating between people, including acquaintances without sexual implications.

Online stores, banks, payment systems

This category generally includes web resources designed for any non-cash online transactions using special-purpose web applications. This also includes web resources that help rent, buy, or sell real estate.

- **Online stores**

Online stores and online auctions selling any goods, work or services to individuals and/or legal entities, including websites of stores that conduct sales exclusively online and online profiles of physical stores that accept online payments.

- **Banks**

Web resources of banks.

- **Payment systems**

This category includes the following web pages:

- Dedicated web pages of banks with online banking functionality, including wire (electronic) transfers between bank accounts, making bank deposits, performing currency conversion, paying for third-party services, etc.
- Web pages of e-money systems that provide access to the user's personal account.

- **Cryptocurrencies and Mining**

This subcategory includes websites offering services for buying and selling cryptocurrency as well as informational services concerning cryptocurrencies and mining.

Computer games

This category includes web resources devoted to computer games of various genres. This also includes gaming communities and services.

Religions, religious associations

This category includes web resources with materials on public movements, associations, and organizations with a religious ideology and/or cult in any manifestations.

News media

News portals on any topic, including social news, news aggregators, and rss newsletters.

Banners

This category includes web resources with banners. Advertising information on banners may distract users from their activities, while banner downloads increase the amount of traffic.

Regional legal restrictions

- **Forbidden by laws of the Russian Federation**
- **Forbidden by laws of Belgium**

- **Forbidden by Police of Japan**

Web resources provided upon agreement with the Japanese police only for products of the Japanese market.

Appendix 4. File extensions for quick removable drives scan

com – executable file of an application no larger than 64 KB

exe – executable file or self-extracting archive

sys – Microsoft Windows system file

prg – program text for dBase™, Clipper or Microsoft Visual FoxPro®, or a WAVmaker program

bin – binary file

bat – batch file

cmd – command file for Microsoft Windows NT (similar to a bat file for DOS), OS/2

dpl – compressed Borland Delphi library

dll – dynamic link library

scr – Microsoft Windows splash screen

cpl – Microsoft Windows control panel module

ocx – Microsoft OLE (Object Linking and Embedding) object

tsp – program running in split-time mode

drv – device driver

vxd – Microsoft Windows virtual device driver

pif – program information file

lnk – Microsoft Windows link file

reg – Microsoft Windows system registry key file

ini – configuration file which contains configuration data for Microsoft Windows, Windows NT, and some applications

cla – Java class

vbs – Visual Basic® script

vbe – BIOS video extension

js, jse – JavaScript source text

htm – hypertext document

htt – Microsoft Windows hypertext header

hta – hypertext program for Microsoft Internet Explorer®

asp – Active Server Pages script

chm – compiled HTML file

pht – HTML file with integrated PHP scripts

php – script that is integrated into HTML files

wsh – Microsoft Windows Script Host file

wsf – Microsoft Windows script

the – Microsoft Windows 95 desktop wallpaper file

hlp – Win Help file

eml – Microsoft Outlook Express email message

nws – new Microsoft Outlook Express email message

msg – Microsoft Mail email message

plg – email message

mbx – saved Microsoft Office Outlook email message

doc* – Microsoft Office Word documents, such as: doc for Microsoft Office Word documents, docx for Microsoft Office Word 2007 documents with XML support, and docm for Microsoft Office Word 2007 documents with macro support

dot* – Microsoft Office Word document templates, such as: dot for Microsoft Office Word document templates, dotx for Microsoft Office Word 2007 document templates, dotm for Microsoft Office Word 2007 document templates with macro support

fpm – database program, Microsoft Visual FoxPro start file

rtf – Rich Text Format document

shs – Windows Shell Scrap Object Handler fragment

dwg – AutoCAD® drawing database

msi – Microsoft Windows Installer package

otm – VBA project for Microsoft Office Outlook

pdf – Adobe Acrobat document

swf – Shockwave® Flash package object

jpg, jpeg – compressed image graphics format

emf – Enhanced Metafile format file;

ico – object icon file

ov? – Microsoft Office Word executable files

xl* – Microsoft Office Excel documents and files, such as: xla, the extension for Microsoft Office Excel, xlc for diagrams, xlt for document templates,.xlsx for Microsoft Office Excel 2007 workbooks, xltm for Microsoft Office Excel 2007 workbooks with macro support, xlsb for Microsoft Office Excel 2007 workbooks in binary (non-XML) format, xltx for Microsoft Office Excel 2007 templates, xlsx for Microsoft Office Excel 2007 templates with macro support, and xlsm for Microsoft Office Excel 2007 plug-ins with macro support

pp* – Microsoft Office PowerPoint® documents and files, such as: pps for Microsoft Office PowerPoint slides, ppt for presentations, pptx for Microsoft Office PowerPoint 2007 presentations, pptm for Microsoft Office PowerPoint 2007 presentations with macros support, potx for Microsoft Office PowerPoint 2007 presentation templates, potm for Microsoft Office PowerPoint 2007 presentation templates with macro support, ppsx for Microsoft Office PowerPoint 2007 slide shows, ppsm for Microsoft Office PowerPoint 2007 slide shows with macro support, and ppam for Microsoft Office PowerPoint 2007 plug-ins with macro support

md* – Microsoft Office Access® documents and files, such as: mda for Microsoft Office Access workgroups and mdb for databases

sldx – a Microsoft PowerPoint 2007 slide

sldm – a Microsoft PowerPoint 2007 slide with macro support

thmx – a Microsoft Office 2007 theme

Appendix 5. File Types for the Mail Threat Protection attachment filter

Note that the actual format of a file may not match its file name extension.

If you enabled filtering of email attachments, the Mail Threat Protection component may rename or delete files with the following extensions:

com – executable file of an application no larger than 64 KB

exe – executable file or self-extracting archive

sys – Microsoft Windows system file

prg – program text for dBase™, Clipper or Microsoft Visual FoxPro®, or a WAVmaker program

bin – binary file

bat – batch file

cmd – command file for Microsoft Windows NT (similar to a bat file for DOS), OS/2

dpl – compressed Borland Delphi library

dll – dynamic link library

scr – Microsoft Windows splash screen

cpl – Microsoft Windows control panel module

ocx – Microsoft OLE (Object Linking and Embedding) object

tsp – program running in split-time mode

drv – device driver

vxd – Microsoft Windows virtual device driver

pif – program information file

lnk – Microsoft Windows link file

reg – Microsoft Windows system registry key file

ini – configuration file which contains configuration data for Microsoft Windows, Windows NT, and some applications

cla – Java class

vbs – Visual Basic® script

vbe – BIOS video extension

js, jse – JavaScript source text

htm – hypertext document

htt – Microsoft Windows hypertext header

hta – hypertext program for Microsoft Internet Explorer®

asp – Active Server Pages script

chm – compiled HTML file

pht – HTML file with integrated PHP scripts

php – script that is integrated into HTML files

wsh – Microsoft Windows Script Host file

wsf – Microsoft Windows script

the – Microsoft Windows 95 desktop wallpaper file

hlp – Win Help file

eml – Microsoft Outlook Express email message

nws – new Microsoft Outlook Express email message

msg – Microsoft Mail email message

plg – email message

mbx – saved Microsoft Office Outlook email message

doc* – Microsoft Office Word documents, such as: doc for Microsoft Office Word documents, docx for Microsoft Office Word 2007 documents with XML support, and docm for Microsoft Office Word 2007 documents with macro support

dot* – Microsoft Office Word document templates, such as: dot for Microsoft Office Word document templates, dotx for Microsoft Office Word 2007 document templates, dotm for Microsoft Office Word 2007 document templates with macro support

fpm – database program, Microsoft Visual FoxPro start file

rtf – Rich Text Format document

shs – Windows Shell Scrap Object Handler fragment

dwg – AutoCAD® drawing database

msi – Microsoft Windows Installer package

otm – VBA project for Microsoft Office Outlook

pdf – Adobe Acrobat document

swf – Shockwave® Flash package object

jpg, jpeg – compressed image graphics format

emf – Enhanced Metafile format file;

ico – object icon file

ov? – Microsoft Office Word executable files

xl* – Microsoft Office Excel documents and files, such as: xla, the extension for Microsoft Office Excel, xlc for diagrams, xlt for document templates,.xlsx for Microsoft Office Excel 2007 workbooks, xltm for Microsoft Office Excel 2007 workbooks with macro support, xlsb for Microsoft Office Excel 2007 workbooks in binary (non-XML) format, xltx for Microsoft Office Excel 2007 templates, xlsx for Microsoft Office Excel 2007 templates with macro support, and xlam for Microsoft Office Excel 2007 plug-ins with macro support

pp* – Microsoft Office PowerPoint® documents and files, such as: pps for Microsoft Office PowerPoint slides, ppt for presentations, pptx for Microsoft Office PowerPoint 2007 presentations, pptm for Microsoft Office PowerPoint 2007 presentations with macros support, potx for Microsoft Office PowerPoint 2007 presentation templates, potm for Microsoft Office PowerPoint 2007 presentation templates with macro support, ppsx for Microsoft Office PowerPoint 2007 slide shows, ppsm for Microsoft Office PowerPoint 2007 slide shows with macro support, and ppam for Microsoft Office PowerPoint 2007 plug-ins with macro support

md* – Microsoft Office Access® documents and files, such as: mda for Microsoft Office Access workgroups and mdb for databases

sldx – a Microsoft PowerPoint 2007 slide

sldm – a Microsoft PowerPoint 2007 slide with macro support

thmx – a Microsoft Office 2007 theme

Appendix 5. Network settings for interaction with external services

Kaspersky Endpoint Security uses the following network settings for interacting with external services.

Network settings

Address	Description
activation- v2.kaspersky.com/activation-service/activation-service.svc Protocol: HTTPS Port: 443	Activating the application
s00.upd.kaspersky.com s01.upd.kaspersky.com s02.upd.kaspersky.com s03.upd.kaspersky.com s04.upd.kaspersky.com s05.upd.kaspersky.com s06.upd.kaspersky.com s07.upd.kaspersky.com s08.upd.kaspersky.com s09.upd.kaspersky.com s10.upd.kaspersky.com s11.upd.kaspersky.com s12.upd.kaspersky.com s13.upd.kaspersky.com s14.upd.kaspersky.com s15.upd.kaspersky.com s16.upd.kaspersky.com s17.upd.kaspersky.com	Updating databases and application modules

s18.upd.kaspersky.com
s19.upd.kaspersky.com
cm.k.kaspersky-labs.com
Protocol: HTTPS
Port: 443

downloads.upd.kaspersky.com
Protocol: HTTPS
Port: 443

- Updating databases and application modules
- Checking if Kaspersky servers are accessible. If access to the servers using system DNS is not possible, the application uses public DNS. This is necessary to make sure anti-virus databases are updated and the level of security is maintained for the computer. Kaspersky Endpoint Security uses the following list of public DNS servers in the following order:
 1. Google Public DNS (8.8.8.8).
 2. Cloudflare DNS (1.1.1.1).
 3. Alibaba Cloud DNS (223.6.6.6).
 4. Quad9 DNS (9.9.9.9).
 5. CleanBrowsing (185.228.168.168).

	<p>Requests emitted by the application may contain addresses of domains and the public IP address of the user because the application establishes a TCP/UDP connection with the DNS server. This information is needed, for example, to validate the certificate of a web resource when using HTTPS. If Kaspersky Endpoint Security is using a public DNS server, data processing is governed by the privacy policy of the relevant service. If you want to prevent Kaspersky Endpoint Security from using a public DNS server, contact Technical Support for a private patch.</p>
<p>touch.kaspersky.com Protocol: HTTP</p>	<ul style="list-style-type: none"> • Receiving the trusted time for checking the validity period of the certificate (TLS connection). • Warning about access denial to a web resource in the browser (Web Threat Protection and Web Control).
<p>p00.upd.kaspersky.com p01.upd.kaspersky.com p02.upd.kaspersky.com p03.upd.kaspersky.com p04.upd.kaspersky.com p05.upd.kaspersky.com p06.upd.kaspersky.com p07.upd.kaspersky.com p08.upd.kaspersky.com p09.upd.kaspersky.com p10.upd.kaspersky.com p11.upd.kaspersky.com p12.upd.kaspersky.com p13.upd.kaspersky.com p14.upd.kaspersky.com</p>	<p>Updating databases and application modules</p>

<p>p15.upd.kaspersky.com p16.upd.kaspersky.com p17.upd.kaspersky.com p18.upd.kaspersky.com p19.upd.kaspersky.com downloads.kaspersky-labs.com cm.k.kaspersky-labs.com Protocol: HTTP Port: 80</p>	
<p>ds.kaspersky.com Protocol: HTTPS Port: 443</p>	Using Kaspersky Security Network.
<p>ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com Protocol: Any Port: 443, 1443</p>	Using Kaspersky Security Network.
<p>click.kaspersky.com redirect.kaspersky.com Protocol: HTTPS</p>	Follow links from the interface
<p>cr1.kaspersky.com ocsp.kaspersky.com Protocol: HTTP Port: 80</p>	Public Key Infrastructure (PKI)

Information about third-party code

Information about third-party code is contained in the file `legal_notices.txt`, in the application installation folder.

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

Adobe, Acrobat, Flash, Reader, and Shockwave are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Apple, FireWire, iTunes and Safari are trademarks of Apple Inc., registered in the U.S. and other countries.

AutoCAD is a trademark or registered trademark of Autodesk, Inc., and/or its subsidiaries and/or affiliates in the USA and/or other countries.

The Bluetooth word, mark and logos are owned by Bluetooth SIG, Inc.

Borland is trademark or registered trademark of Borland Software Corporation.

Android, Chrome, Google Chrome, and Google Talk are trademarks of Google, Inc.

Citrix and Citrix Provisioning Services, XenApp, and XenDesktop are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

dBase is a trademark of dataBased Intelligence, Inc.

EMC and SecurID are trademarks or registered trademarks of EMC Corporation in the United States and/or other countries

Radmin is a registered trademark of Famatech.

IBM is a trademark of International Business Machines Corporation, registered in many jurisdictions worldwide.

ICQ is a trademark and/or service mark of ICQ LLC.

Intel is a trademark of Intel Corporation in the U.S. and/or other countries.

IOS is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Logitech is either a registered trademark or trademark of Logitech in the United States and/or other countries.

Microsoft, Access, Active Directory, ActiveSync, BitLocker, Excel, Internet Explorer, LifeCam Cinema, MSDN, MultiPoint, Outlook, PowerPoint, PowerShell, Segoe, Skype, Visual C++, Visual Basic, Visual FoxPro, Windows, Windows Live, Windows PowerShell, Windows Server, and Windows Store are registered trademarks of Microsoft Corporation in the United States and other countries.

Mozilla, Firefox, and Thunderbird are the trademarks of the Mozilla Foundation.

Java and JavaScript are registered trademark of Oracle and/or its affiliates.

VMware and VMware ESXi are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.