Коммерческий релиз Kaspersky Security 10.1 для Windows Server (версия 10.1.0.622)

К разделу "Информация о версиях"

2018 мар 20 ID: 14283

Коммерческий релиз Kaspersky Security 10.1 для Windows Server состоялся 20 марта 2018 года. Полный номер версии 10.1.0.622.

Kaspersky Security 10.1 для Windows Server (ранее Антивирус Касперского для Windows Servers Enterprise Edition) — решение для защиты корпоративных серверов и систем хранения данных. Область защиты и набор функциональных компонентов зависит от типа лицензии.

Что нового в Kaspersky Security 10.1 для Windows Server

В новой версии Kaspersky Security 10.1 для Windows Server появились следующие возможности:

- Добавлен компонент Защита трафика: теперь вы можете защитить сервер от веб-угроз, передающихся через HTTP или HTTPS-трафик, а также от почтовых угроз. Новый компонент поддерживает следующие сценарии защиты:
  - Антивирусная и антифишинговая защита почтового трафика с помощью расширения для почтового клиента Microsoft Outlook.
  - Антивирусная и антифишинговая защита веб-трафика.
  - Проверка веб-ссылок по базам вредоносных веб-адресов.
  - Проверка веб-ссылок по облачным базам вредоносных веб-адресов.
  - Веб-контроль с помощью правил для веб-ссылок и сертификатов.
  - Контроль веб-ресурсов по категориям.
  - Контроль сертификатов веб-серверов при подключении.
- Защита трафика может быть сконфигурирована в одном из трех вариантов:
  - Внешний прокси-сервер с использованием ICAP-службы: анализ перенаправленного трафика от внешнего прокси-сервера (без сетевого драйвера).
  - Перенаправление трафика: анализ перенаправленного трафика от браузеров, запущенных в терминальной сессии (без сетевого драйвера). Программа функционирует в режиме внутренней системной прокси.
  - Драйверный перехват: перехват трафика с помощью сетевого драйвера в терминальных сессиях защищаемого сервера.
- Добавлен компонент Защита от шифрования для NetApp: теперь вы можете использовать сервер с установленным Kaspersky Security 10.1 для Windows Server для защиты кластерного подключаемого сетевого хранилища данных NetApp версий 8.2 и выше от вредоносного шифрования.
- Добавлен компонент Контроль устройств: теперь вы можете формировать списки правил, на основе которых программа разрешает или запрещает файловый обмен с внешними устройствами хранения данных (запоминающие устройства USB и MTP, CD/DVD-устройства).
- Добавлен компонент Защита от эксплойтов: теперь вы можете настраивать параметры защиты памяти процессов от эксплуатации уязвимостей на основе распространенных техник митигации.
- Добавлен компонент Мониторинг файловых операций: теперь вы можете указывать объекты, за целостностью которых вы хотите следить.
- Добавлен компонент Анализ журналов: теперь вы можете формировать правила анализа журналов событий Windows, а также настраивать применение эвристического анализатора для анализа журналов событий Windows.

- Добавлена функциональность защиты и контроля контейнеров Microsoft Windows Server 2016: теперь вы можете обеспечить защиту контейнеров Microsoft Windows Server 2016 с помощью следующих технологий:
    - Защита от файловых угроз в реальном времени. Требуется установка Kaspersky Security 10.1 для Windows Server на узле с развернутыми контейнерами Microsoft Windows Server 2016.
    - Контроль запусков программ в контейнере в соответствии с заданными списками правил задачи Контроль запуска программ. Требуется установка Kaspersky Security 10.1 для Windows Server с компонентом Контроль запуска программ на узле с развернутыми контейнерами Microsoft Windows Server 2016.
    - Защита памяти процессов, запущенных в контейнере, от эксплойтов. Требуется установка Kaspersky Security 10.1 для Windows Server с компонентом Защита от эксплойтов внутри контейнера Microsoft Windows Server 2016.
- Добавлен компонент Compact Diagnostic Interface: теперь вы можете контролировать статус защиты сервера, просматривать важные маркеры состояния программы, а также управлять записью диагностических данных без установки Средств Администрирования. Компактный интерфейс (Compact Diagnostic Interface) устанавливается в составе компонента Tray Icon и выполняет некоторые важные диагностические функции Консоли Kaspersky Security 10.1.
- Поддержана интеграция с сервисами Kaspersky Managed Protection: теперь вы можете усилить защиту сети с помощью сервисов круглосуточного анализа и отчетности по событиям информационной безопасности от экспертов «Лаборатории Касперского».
- Поддержана интеграция с Microsoft Operations Management Suite.
- Добавлена функциональность интеграции с внешними SIEM-системами: теперь вы можете настраивать параметры экспорта журналов программы в сторонние системы агрегации событий по протоколу syslog.
- Добавлена функциональность отслеживания подключений к защищаемому устройству по шине USB: теперь вы можете настроить параметры нотификации о фактах подключений различных типов устройств к защищаемому серверу по шине USB.
- Реализован Журнал нарушений безопасности: теперь вы можете просматривать все события, фиксируемые компонентами программы и свидетельствующие о потенциальной компрометации защищаемой системы, в одном журнале.
- Добавлен компонент Управление сетевым экраном: теперь вы можете контролировать правила сетевого экрана Windows через графический интерфейс Kaspersky Security 10.1 для Windows Server.
- Добавлена функциональность проверки запоминающих USB устройств: теперь вы можете выполнять автоматическую проверку запоминающих устройств при их подключении к защищаемому компьютеру.
- Добавлена функциональность защиты паролем для доступа к управлению программой: теперь вы можете дополнительно защитить Kaspersky Security 10.1 для Windows Server и ограничить доступ к критичным операциям с помощью пароля.
- Добавлена функциональность автоматического разрешения запуска программ по доверенным пакетам установки: теперь вы можете добавить исключения для пакетов установки, чтобы упростить разрешение запуска файлов при установке или обновлении программного обеспечения в параметрах задачи Контроль запуска программ.
- Упрощена функциональность блокирования доступа к сетевым файловым ресурсам: теперь компоненты защиты от шифрования и задача Постоянная защита файлов помещают идентификаторы скомпрометированных узлов в Хранилище заблокированных узлов. Вы можете отключить наполнение Хранилища заблокированных узлов в параметрах задач защиты. Кроме того, теперь вы можете просмотреть информацию обо всех заблокированных узлах в централизованном списке Консоли Сервера Администрирования.
- Оптимизированы возможности формирования списка правил доверенных процессов для Доверенной зоны: теперь вы можете использовать в качестве критерия исключения процесса только хеш-сумму, только путь или путь с хеш-суммой. Также теперь вы можете добавить несколько процессов в список доверенных одновременно.
- Упрощен и расширен механизм наполнения списков правил контроля запуска программ: добавлена возможность совмещенного использования списков правил, настроенных на локальных хостах и в политике, а также реализован механизм формирования правил на основе событий работы задачи в Kaspersky Security Center.

- Оптимизирован режим Default Allow для задачи Контроля запуска программ: теперь вы можете использовать функциональность контроля запуска программ в режиме разрешения всех запусков, кроме запрещенных программ.

Ограничения и известные ошибки

Защита трафика:

- Мы не рекомендуем включать в область защиты задачи VPN-трафик (порт 1723).
- Браузер Opera Presto Engine сообщает о попытке подключения по недоверенному сертификату, если Kaspersky Security 10.1 для Windows Server применяется для защиты HTTPS-трафика.
- Не выполняется проверка трафика по IP-адресам в формате IPv6.
- Компонент защиты трафика доступен только на версиях операционных систем Microsoft Windows Server 2008 R2 и выше.
- Программа работает только с TCP-трафиком.
- Агент администрирования обнаруживает компонент защиты трафика при попытке соединения с Сервером администрирования, поэтому мы рекомендуем установить Агент администрирования до разворачивания компонента Защита трафика. Если установка компонента и запуск задачи Защита трафика были выполнены до установки Агента администрирования, перезапустите задачу Защита трафика.

Проверка по требованию, защита от файловых угроз и угроз шифрования, защита памяти процессов:

- Недоступна антивирусная проверка MTP-устройств при подключении.
- Недоступна проверка архивных объектов без проверки SFX-архивов: если в параметрах безопасности Kaspersky Security 10.1 для Windows Server применяется режим проверки архивов, программа автоматически проверяет объекты как в архивах, так и объекты в SFX-архивах. Проверка SFX-архивов без проверки архивов доступна.
- Исключения Доверенной зоны не применяются при выполнении проверок в контейнерах Windows Server 2016.
- Технология iSwift не применяется при выполнении проверок в контейнерах Windows Server 2016.
- Компонент Защита от эксплойтов не защищает приложения, установленные через Microsoft Store, на операционных системах Windows Server 2012 и Windows Server 2012 R2.

Контроль компьютера и диагностика:

- Задача Анализ журналов обнаруживает потенциальные паттерны атаки Kerberos (MS14-068) только на компьютерах под управлением операционных систем Windows Server 2008 и выше в роли доменного контроллера с установленными обновлениями.
- Задача Контроль устройств блокирует любые подключения MTP-устройства при выполнении в Активном режиме.

Управление сетевым экраном:

- Недоступна работа с IP-адресами в формате IPv6 при указании области применения правила, состоящей из одного адреса.
- При запуске задачи Управление сетевым экраном в параметрах сетевого экрана операционной системы автоматически удаляются заданные правила следующих типов:
  - запрещающие правила;
  - правила контроля исходящего трафика.
- Предварительно заданные правила политики Управление сетевым экраном обеспечивают выполнение основных сценариев взаимодействия локальных компьютеров с Сервером администрирования. Для полного использования функциональности Kaspersky Security Center требуется вручную задать правила для разрешения портов. Информацию о номерах портов, протоколах и их функциях читайте в статье.
- Программа не контролирует изменения правил и групп правил брандмауэра Windows при ежеминутном опросе задачи Управление сетевым экраном, если эти правила и группы

были добавлены в параметры задачи при установке программы. Для обновления статуса и наличия таких правил требуется перезапуск задачи Управление сетевым экраном.
- Для операционных систем Microsoft Windows Server 2008 и выше: перед установкой компонента Управление сетевым экраном требуется запустить сервис брандмауэра Windows (запущен по умолчанию).
- Для операционной системы Microsoft Windows Server 2003: для работы брандмауэра Windows требуется запущенная служба SharedAccess. По умолчанию служба остановлена и запуск службы выполняется только с правами Администратора. Если компонент Управление сетевым экраном запущен при остановленной службе SharedAccess, программа показывает недействительное состояние компонента: визуально задача активна и выполняется, но брандмауэр Windows не запущен и сетевые правила не применяются. Для корректной работы компонента Управление сетевым экраном запустите службу SharedAccess.

Установка:

- Во время установки программы возникает предупреждение о слишком длинном пути, если полный путь к папке установки Kaspersky Security 10.1 для Windows Server содержит более 150 символов. Предупреждение не влияет на процесс: установка Kaspersky Security 10.1 для Windows Server и дальнейшее функционирование программы выполняются успешно.
- Для установки компонента Поддержка SNMP требуется наличие службы SNMP на защищаемом сервере.
- Для установки компонента Поддержка SNMP протокола требуется перезапуск службы SNMP, если эта служба запущена.
- Недоступна установка Средств администрирования Kaspersky Security 10.1 для Windows Server через групповые политики Microsoft Active Directory.
- При установке программы на компьютеры под управлением устаревших операционных систем, не имеющих возможности получать регулярные обновления, необходимо проверить наличие следующих корневых сертификатов: DigiCert Assured ID Root CA, DigiCert_High_Assurance_EV_Root_CA, DigiCertAssuredIDRootCA. Отсутствие указанных сертификатов может привести к некорректной работе программы. Рекомендуется установить указанные сертификаты любым доступным способом. Инструкция по скачиванию и применению актуальных сертификатов доступна в статье.

Лицензирование:

- Недоступна активация программы с помощью ключа из мастера установки программы, если файл ключа расположен на диске, созданном с помощью команды SUBST, или если указан сетевой путь к файлу ключа.

Обновления:

- После установки критических обновлений модулей Kaspersky Security 10.1 для Windows Server значок Kaspersky Security 10.1 для Windows Server по умолчанию скрыт.

Интерфейс:

- В Консоли Kaspersky Security 10.1 для Windows Server при использовании фильтра в узлах Карантин, Резервное хранилище, Журнал системного аудита, Журналы выполнения задач требуется соблюдать регистр.
- При настройке области защиты и области проверки в Консоли Kaspersky Security 10.1 возможно использование только одной маски в пути и только в конце пути. Примеры правильного задания маски: "C:\Temp\Temp*", или "C:\Temp\Temp???.doc", или "C:\Temp\Temp*.doc". Ограничение не распространяется на параметры Доверенной зоны.

Интеграция с Kaspersky Security Center:

- Сервер администрирования проверяет корректность обновлений баз программы по их получении и перед распространением на компьютеры сети. Проверка корректности полученных обновлений модулей программы на стороне Сервера администрирования не выполняется.
- При работе с компонентами, передающими динамически изменяющиеся данные в Kaspersky Security Center с помощью сетевых списков (Карантин, Резервное хранилище), убедитесь, что в параметрах взаимодействия с Сервером администрирования установлены соответствующие флажки.

Другие функции:

- При использовании утилиты командной строки отображение специальных символов доступно, если региональные настройки операционной системы совпадают с используемой локализацией Kaspersky Security 10.1 для Windows Server.
- При использовании базовой аутентификации на прокси-сервере возможно возникновение ошибок аутентификации, если имя пользователя или пароль заданы в мультибайтной кодировке.
- При восстановлении файла из Карантина или Резервного хранилища не восстанавливается значение «Encrypted» атрибута файла.
- Недоступно использование зеркального сервера при подключении к syslog-серверу по протоколу UDP.
- Тип устройства может быть не распознан при генерации события о подключении к USB-шине. В этом случае событие будет содержать только GUID устройства.
- Значения Device Instance Path указываются в разных форматах для компонента Контроль устройств и функциональности отслеживания подключений по шине USB.