Как перейти на Kaspersky Security для Windows Server версии 10.1

К разделу "Общая информация"

2018 апр 03 ID: 14312

Kaspersky Security для Windows Server 10.1 поддерживает переход со следующих версий:

- Антивирус Касперского 8.0 для Windows Servers Enterprise Edition (8.0.0.559).
- Антивирус Касперского 8.0 для Windows Servers Enterprise Edition MR1 (8.0.1.923).
- Антивирус Касперского 8.0 для Windows Servers Enterprise Edition MR2 (8.0.2.213).
- Kaspersky Security для Windows Server (10.0.0.486).

Миграция настроек программы

Без изменения значений сохраняются и импортируются следующие параметры:

- Настроенные параметры компонентов и задач.
- Журналы выполнения задач и системного аудита.
- Содержимое Карантина и Резервного хранилища.
- Учетные записи, с правами которых запускаются задачи.
- Права на управление программой.
- Уведомления о работе задач программы.

При переходе на новую версию сбрасываются следующие параметры:

- Все счетчики, в том числе статусы состояния антивирусных баз и необходимость обновлений.
- Информация об установленных обновлениях программных модулей и антивирусных баз.
- Статусы выполнения задач.
- Права на управление службой Kaspersky Security.
- Параметры программы и программных компонентов, настроенные через реестр.
- Параметры программы и программных компонентов, измененные и настроенные критическими исправлениями.

Также при установке версии Kaspersky Security 10.1 для Windows Server поверх версий Антивируса Каспесркого 8.0 для Windows Servers Enterprise Edition отключается вывод событий программы, публикуемых в Журнал событий Windows, через оснастку Просмотра событий Windows. Чтобы включить вывод событий программы через оснастку Просмотра событий Windows, перезапустите службу Журнал событий или защищаемый сервер.

Правила контроля запуска программ

При миграции на новую версию программа сохраняет заданные списки правил контроля запуска программ без изменений. Повторное формирование списков правил не требуется. Вы также можете импортировать конфигурационный файл, созданный на основе списков правил предыдущих версий программы, в параметры задачи Контроль запуска программ в новой версии Kaspersky Security для Windows Server.

При выполнении миграции мы рекомендуем останавливать задачу Контроль запуска программ, если она запущена в активном режиме, или переводить задачу в режим Только статистика. А после миграции проверить обновленные списки правил и их срабатывания в режиме Только статистика.

Список недоверенных компьютеров

В новой версии программы изменен механизм блокирования клиентских компьютеров, со стороны которых была обнаружена вредоносная файловая активность или активность шифрования:

- Отсутствует задача Блокирование доступа к сетевым файловым ресурсам.

- Активация блокирования выполняется изменением режима работы задач Постоянная защита файлов и задач защиты от шифрования.
- Списки скомпрометированных клиентских компьютеров хранятся в Хранилище заблокированных узлов.
- Параметры автоматической разблокировки доступа для скомпрометированного клиентского компьютера настраиваются в свойствах Хранилища заблокированных узлов.

После миграции на новую версию программы не сохраняются списки заблокированных компьютеров. Программа начнет работать в режиме активного блокирования доступа к сетевым файловым ресурсам в соответствии с параметрами по умолчанию для задач защиты, которые используют Хранилище заблокированных узлов.

Параметры автоматической разблокировки доступа к заблокированным сетевым файловым ресурсам сохраняются после миграции.

Обновление средств управления

Плагин управления Kaspersky Security для Windows Server 10.1 не обновляет плагины предыдущих версий. Политики и групповые задачи, созданные для предыдущих версий программы, не будут автоматически применены к компьютерам под управлением Kaspersky Security для Windows Server 10.1. Вы можете импортировать созданные политики и групповые задачи вручную при создании политики или групповой задачи для Kaspersky Security для Windows Server 10.1 с помощью консоли Сервера Администрирования.

Консоль Kaspersky Security 10.1 устанавливается поверх консолей предыдущих обновляемых версий и заменяет их.

Совместимость версии 10.1 с консолями и плагинами предыдущих версий:

- Программа версии 10.1 не может управляться Плагинами предыдущих версий программы.
- Плагин версии 10.1 не может управлять программой предыдущих версий.
- Программа версии 10.1 может управляться Консолью предыдущих версий.
- Консоль версии 10.1 может управлять программами предыдущих версий.

Лицензионное соглашение и политика конфиденциальности

Условия Лицензионного соглашения для Kaspersky Security 10.1 для Windows Server отличаются от условий, которые описаны для предыдущих версий программы. Для выполнения миграции на версию Kaspersky Security 10.1 для Windows Server обязательно требуется прочитать и принять условия Лицензионного соглашения.

Также для установки Kaspersky Security 10.1 для Windows Server требуется прочитать и принять Политику конфиденциальности, которая описывает обработку данных. Текст Политики конфиденциальности доступен в Мастере установки, в составе дистрибутива программы, а также на сайте «Лаборатории Касперского».

Положение о Kaspersky Security Network

Условия Положения о Kaspersky Security Network для Kaspersky Security 10.1 для Windows Server отличаются от условий, которые описаны для предыдущих версий программы. Чтобы продолжить использование облачных инфраструктур KSN для защиты сервера после миграции на версию Kaspersky Security 10.1 для Windows Server, требуется прочитать и принять условия новой версии Положения о Kaspersky Security Network.

Текст Положения о Kaspersky Security Network для Kaspersky Security 10.1 для Windows Server доступен в интерфейсе программы при настройке параметров задачи или политики Использование KSN.

Лицензирование

Программа автоматически применяет лицензионный ключ обновляемых версий для активации версии 10.1, если на момент выполнения миграции срок действия лицензии не истек.

При активации программы версии 10.1 с помощью лицензионного ключа предыдущих версий программы использование новых компонентов доступно частично.

Любой ключ, который применялся для активации предыдущих версий программы, дает право на использование следующих новых компонентов:

- Защита от эксплойтов.
- Управление сетевым экраном.

Следующие новые компоненты доступны в зависимости от используемого решения:

- Компоненты Мониторинг файловых операций и Анализ журналов доступны в составе решения для файловых серверов.
- Компонент Контроль устройств доступен в составе решений Advanced, Total, для файловых серверов, для сетевых хранилищ данных.
- Компонент Защита трафика (включая расширение для Microsoft Outlook) доступен в составе решений Advanced, Total, для файловых серверов.
- Компонент Защита трафика для внешних прокси-серверов доступен в составе решений Total, для сетевых хранилищ данных.
- Компонент Защита от шифрования для NetApp доступен в составе решения для сетевых хранилищ данных.

Параметры установки при миграции

Установка поверх предыдущей версии не требует перезагрузки компьютера.

По умолчанию программа создает новую папку установки на основе пути к существующей папке установки: по возможности программа создает папку по имени новой версии с сохранением пути к этой папке. Вы можете задать новый путь для папки установки вручную.