????????? ??????????? KES Linux

- Исключения KES Linux
  - Исключения защиты от файловых угроз
  - Настройка доверенных веб-адресов
  - Исключения защиты от сетевых угроз
  - Исключения защиты от шифрования
  - Исключения для анализа поведения
  - Добавление доверенных устройств

??????????? KES Linux

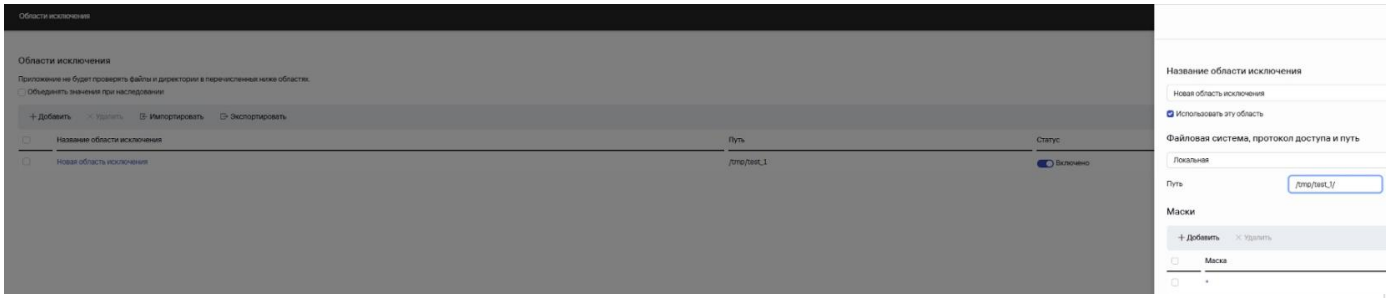
? KESL ?????????? ????????????? ???????? ? ?????? ??????????, ? ????? ???? ??????????? ????????? ????? ?????????? ??? ???? ??????????? ????? ???????? ?????????? ??????????.

Исключения защиты от файловых угроз

Для настройки исключений в работе компонента Защита от файловых угроз. Необходимо перейти в политику KESL в раздел **Параметры приложения → Базовая защита → Исключения Защиты от файловых угроз.** Здесь можно настроить следующие форматы исключений:

- **Области исключения**, где будут указаны необходимые пути для исключения. KESL не проверяет файлы и директории, расположенные по указанным в таблице путям.

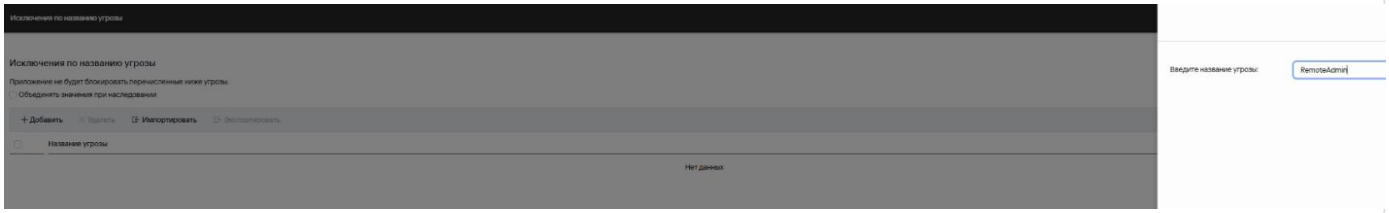
Нажав **Добавить** можно указать необходимый путь. Также в выпадающем списке под заголовком Файловая система, протокол доступа и путь можно указать смонтированные области исключения. При необходимости более гибкой настройки исключения в указанной директории можно добавить маску, по умолчанию используется «*».



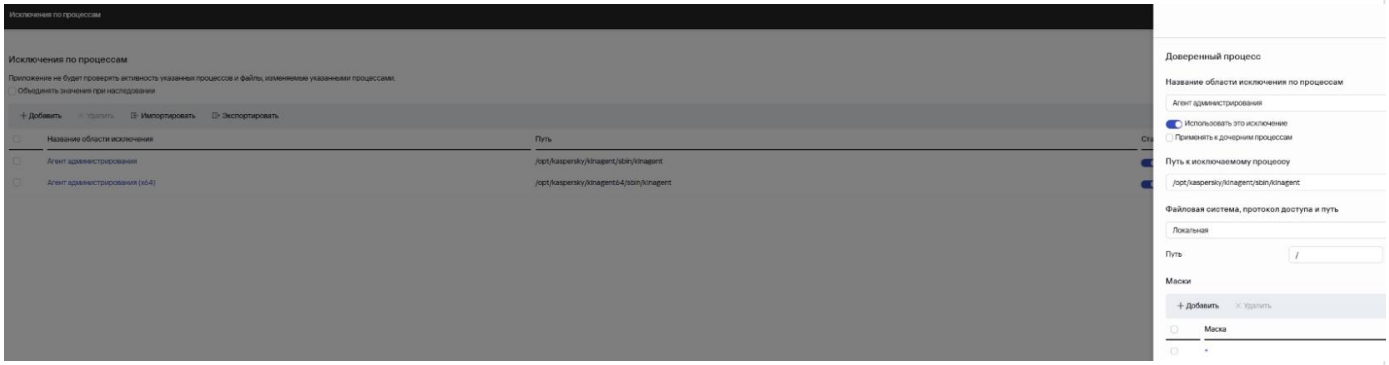
- **Исключения по маске** – KESL не будет проверять файлы с названиями, подходящими под перечисленные ниже маски. Для настройки необходимо в соответствующем разделе выбрать **Добавить** и указать необходимую маску



- **Исключения по названию угрозы** – здесь можно указать исключения по конкретным угрозам согласно [вирусной энциклопедии](). Для настройки необходимо в соответствующем разделе выбрать **Добавить** и указать необходимую угрозу или её маску



- **Исключения по процессам** – позволяет не контролировать активность указанных процессов и файлы, которые они изменяют, а также дочерние процессы. Для настройки необходимо в соответствующем разделе выбрать **Добавить,** указать название и указать путь к процессу

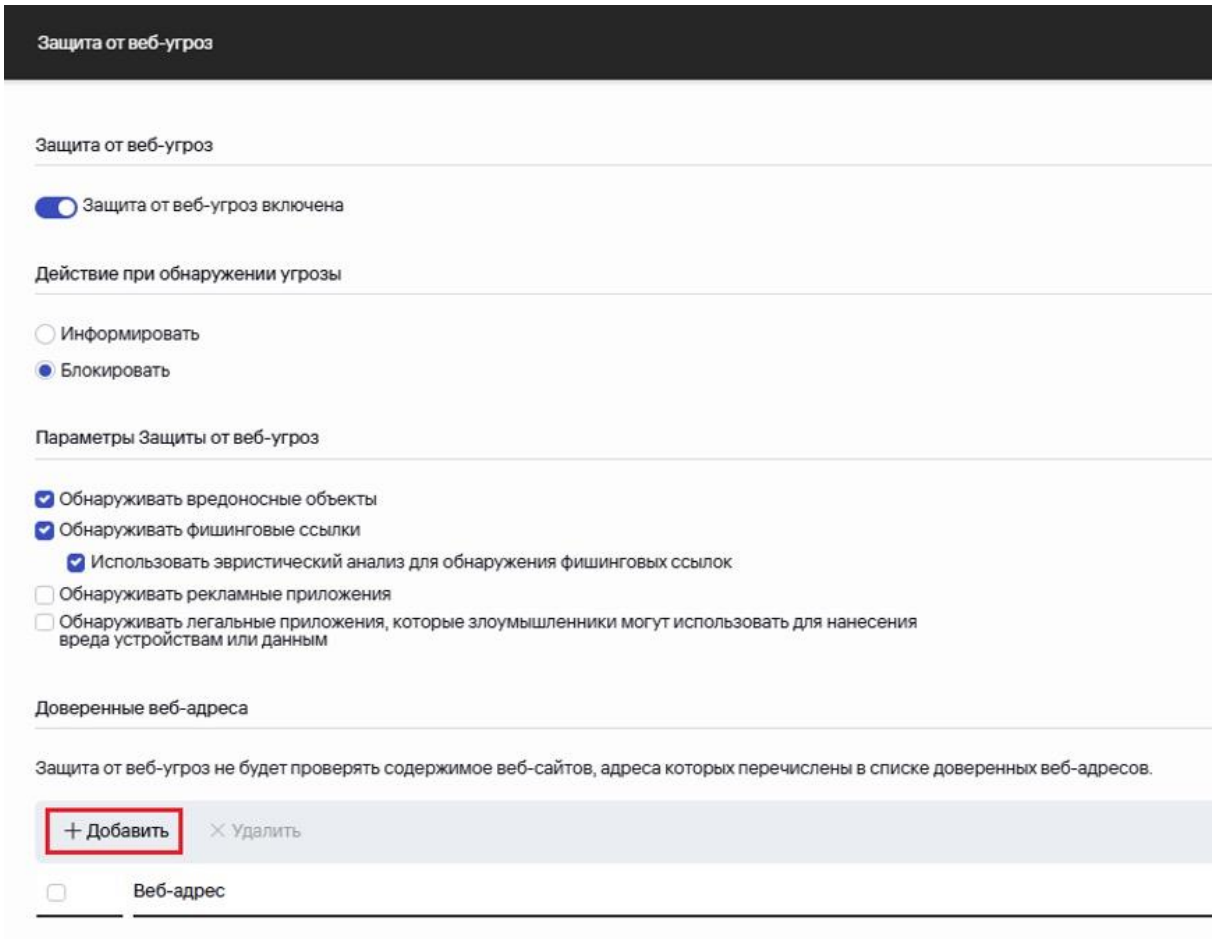


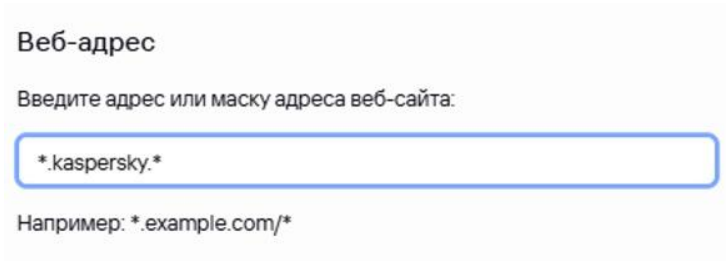
Также для каждого из перечисленных типов исключения можно активировать параметр **Объединять значения при наследовании.** В таком случае исключения из

родительской политики отображаются в дочерних политиках и доступны для просмотра. Если исключения дочерней и родительской политик совпадают, то эти элементы отображаются как один элемент родительской политики.

Настройка доверенных веб-адресов

Для создания исключения компонента Защита от веб-угроз необходимо в политике KESL в компоненте Защита от веб-угроз выбрать **Добавить** в блоке **Доверенные веб-адреса** и указать необходимый адрес, возможно использование масок.



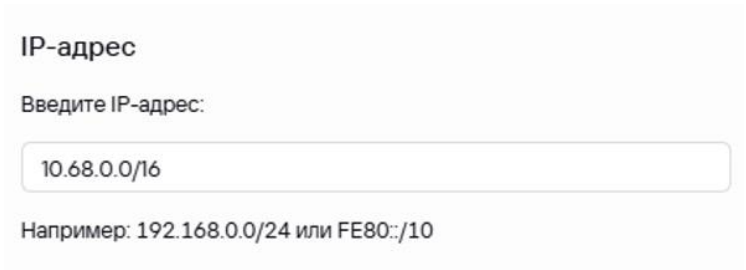


На указанных веб-сайтах не будет производиться проверка их содержимого

Исключения защиты от сетевых угроз

В случае ложных срабатываний компонента **Защита от сетевых угроз** и блокировок соединений, необходимо добавить соответствующее исключение в для этого компонента в политике KESL нажав **Добавить** и указать необходимый адрес или маску сети



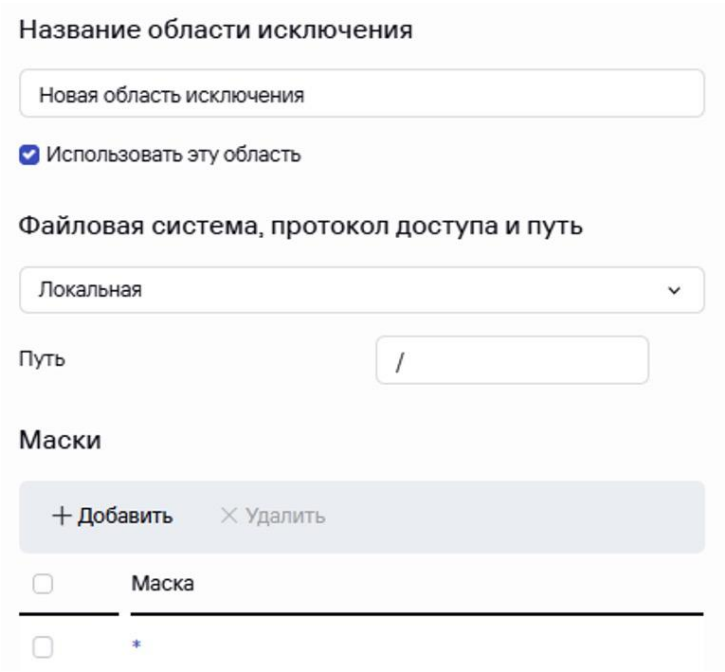


Исключения защиты от шифрования

В данном случае речь идёт о возможности исключения работы компонента **Защита от шифрования** для файловых ресурсов, расположенных в общих сетевых директориях защищаемого устройства. Для добавления исключения необходимо перейти в соответствующий компонент в политике KESL. Для обоих типов исключений работает функционал объединения значений при наследовании политик.



Возможно настроить исключение указав нужный путь. При необходимости можно использовать маски для более гибкого исключения, а также указать локальную или смонтированную файловую систему.

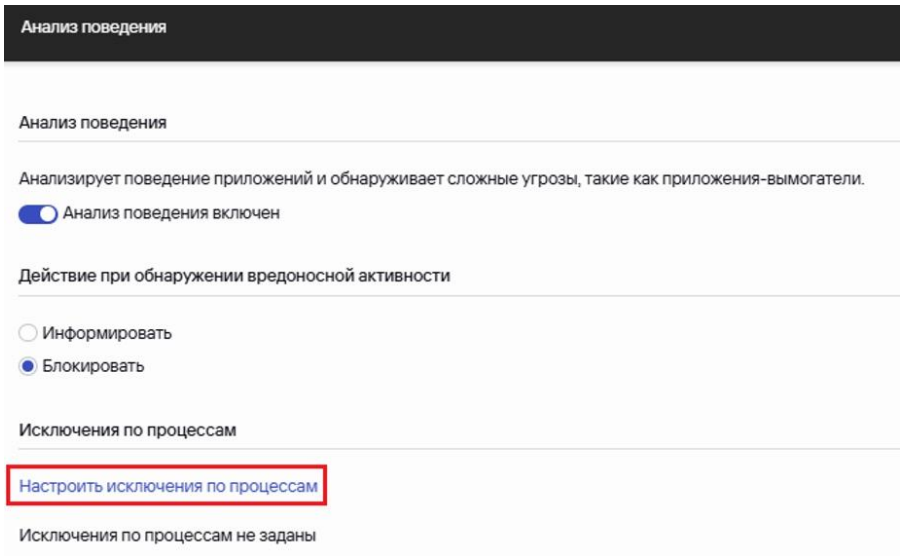


Также возможно настроить исключение работы данного компонента только на указанные файлы

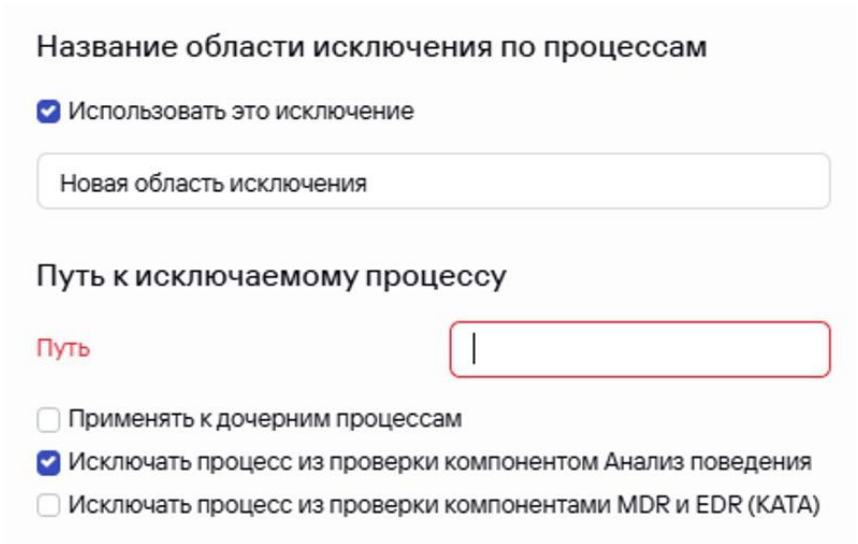


Исключения для анализа поведения

Компонент **Анализ поведения** позволяет контролировать вредоносную активность приложений в операционной системе. При обнаружении вредоносной активности Kaspersky Endpoint Security может завершать процесс приложения, осуществляющего вредоносную активность. При необходимости добавить процесс в исключение для данного компонента необходимо перейти в соответствующий компонент в политике KESL и выбрать **Настроить исключения по процессам**



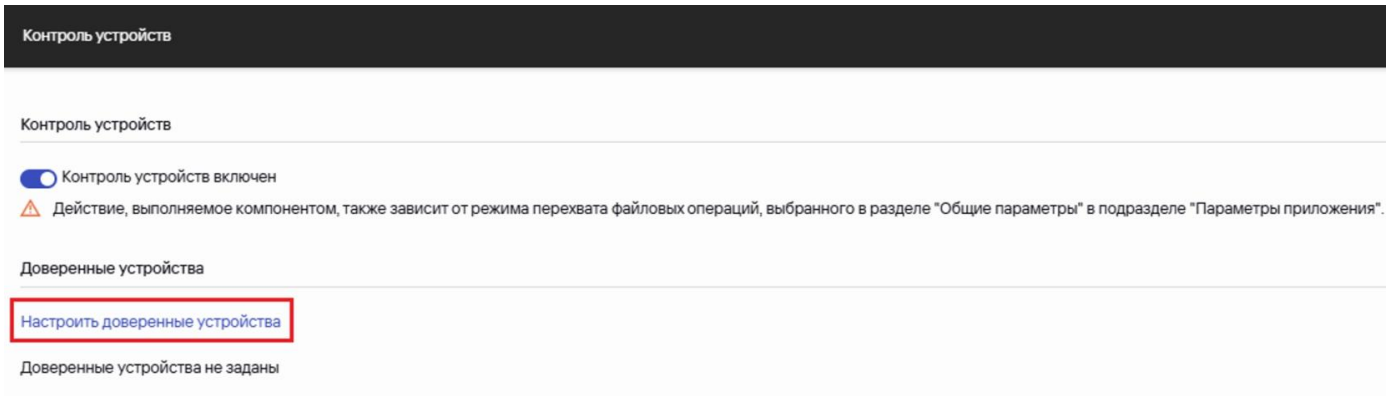
В открывшемся окне можно будет добавить исключение, где будет необходимо указать путь и выбрать галочку «Исключать процесс из проверки компонентом Анализ поведения». Также можно применять исключение к дочерним процессам и исключить процесс из проверки компонентами MDR и EDR. При необходимости можно объединять значения при наследовании политик



Добавление доверенных устройств

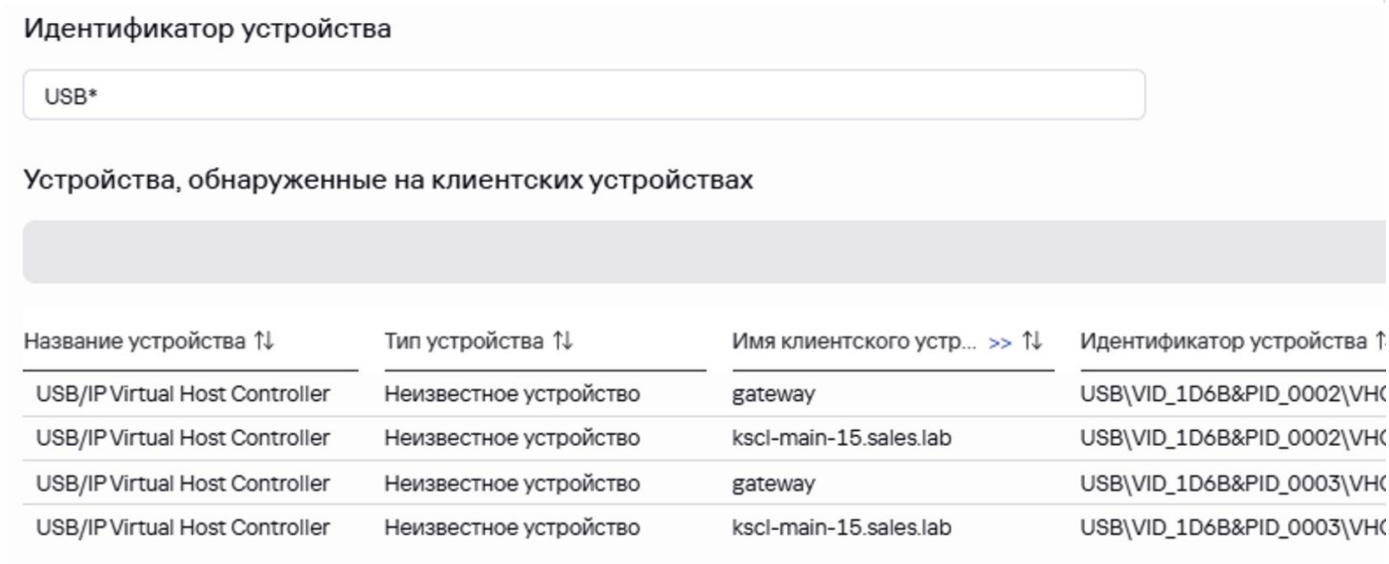
Доверенные устройства – это устройства, к которым у пользователей есть полный доступ. Например, вы можете разрешить доступ к конкретным USB-устройствам или только к USB-накопителям, при этом доступ к остальным USB-устройства будет запрещен. Кроме того, вы можете указать пользователей или группы пользователей, для которых устройства будут доверенными.

Для добавление доверенных устройств перейдите в раздел **Контроль устройств** политики KESL и выберите **Настроить доверенные устройства**



В открывшемся окне будет доступно 2 способа добавления доверенных устройств:

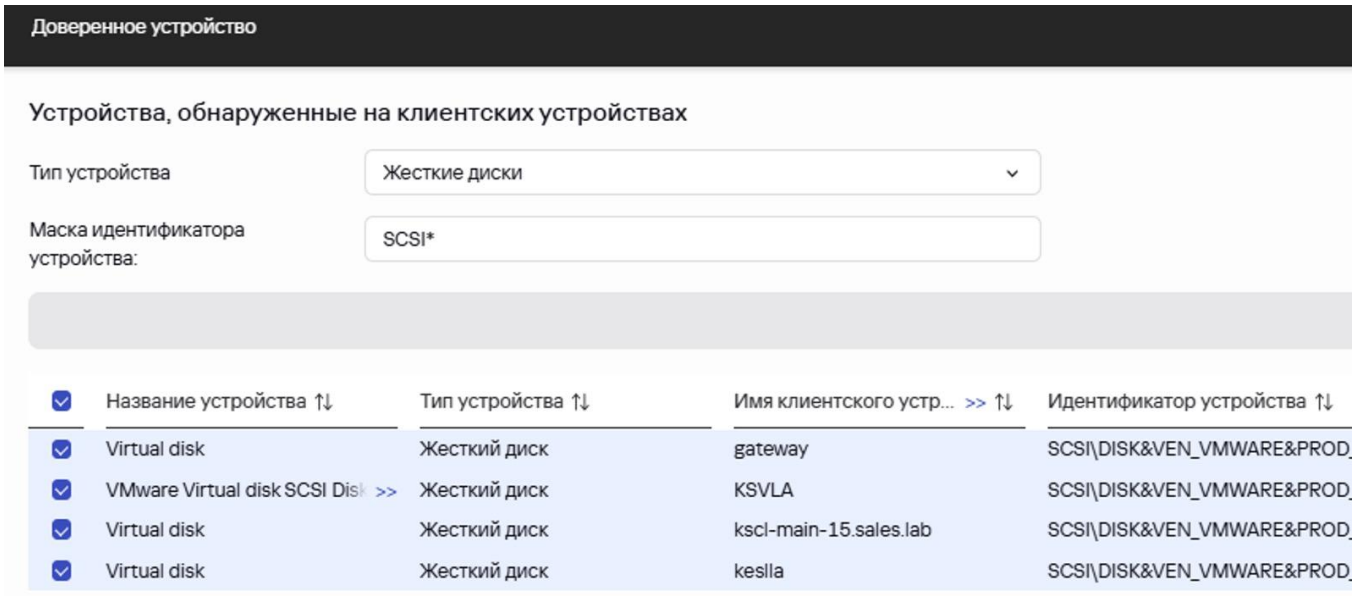
- **Добавить по идентификатору** – позволяет указать маску идентификатора устройства (либо полностью).



Затем будет необходимо указать пользователей или группы для которых будут доступны данные устройства (вручную, либо из списка), после этого можно будет добавить комментарий к исключению(опционально)



- **Выбрать существующее устройство** – позволяет указать конкретные устройства, которые уже известны KSC. Для удобства поиска можно изменить тип устройства и использовать маску идентификатора. Можно выбрать несколько устройств при необходимости.



Затем будет необходимо указать пользователей или группы для которых будут доступны данные устройства (вручную, либо из списка), после этого можно будет добавить комментарий к исключению(опционально)



Таким образом выбранные доверенные устройства не будут блокироваться для выбранных пользователей, что можно использовать, в том числе и для более точечного и гибкого ограничения на работу с внешними носителями информации.

Revision #2
Created 26 June 2026 15:29:49 by Сергей
Updated 26 June 2026 15:46:19 by Сергей