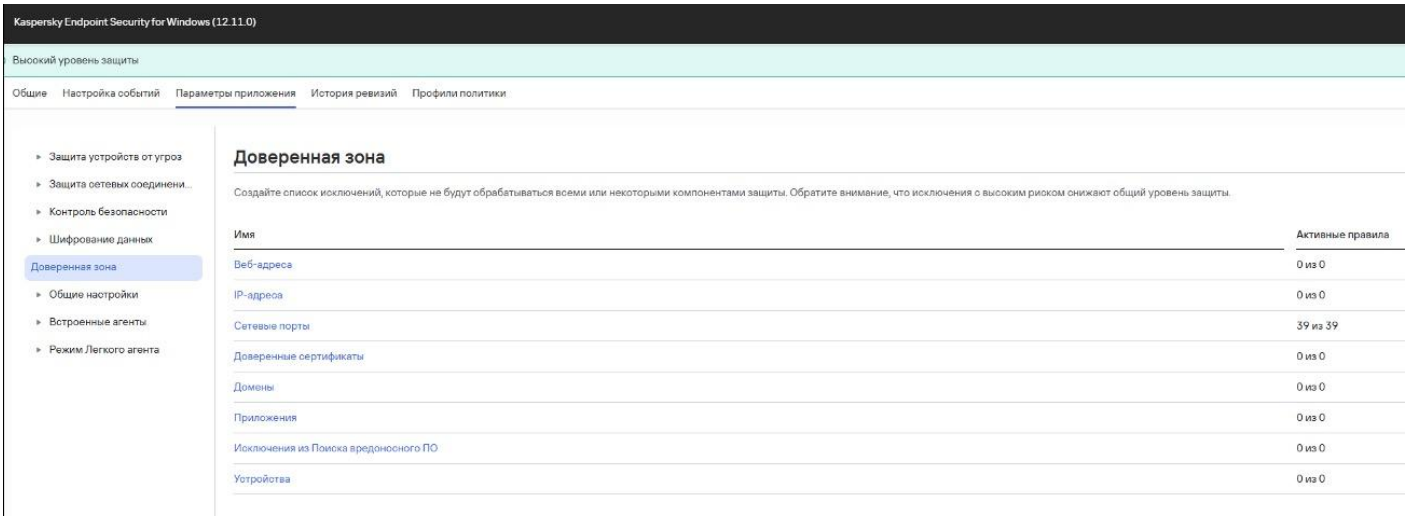
????????? ??????????? KES Windows

???????????

- Исключения KES Windows
  - Исключения файловой проверки
  - Настройка доверенных приложений
  - Добавление доверенных веб-адресов и IP-адресов
  - Добавление доверенных сертификатов
  - Добавление доверенных устройств

???????????? KES Windows

? ???????? KES Windows ??????? ? ?????? 12.11 ????? ????????? ??????????, ???? ? ??????? ?????????? ????, ???? ?????????? ?????????? ??????????? ??????, ????? ??? ?????? ?? ???????? ?????, ????????????? ?????????, ?????? ?????????, ?????? ?? ??????????, ?????? ?? ???????? ?????, ?????? ?? ???-?????, ?????? ?? ??????? ?????, ???????? ?????????



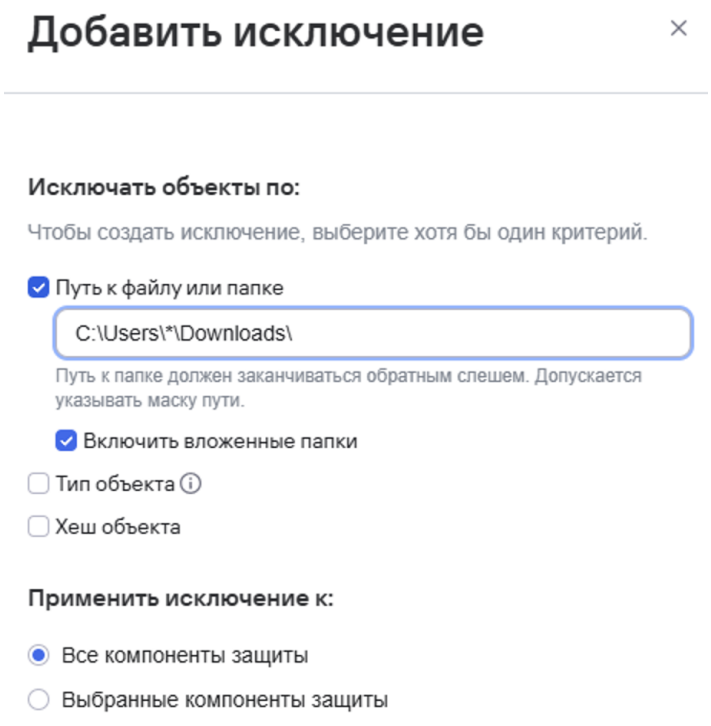
Исключения файловой проверки

Для настройки исключений файловой проверке в политике перейдите в раздел **Параметры приложения → Доверенная зона** и выберите **Исключения из Поиска вредоносного ПО**. Нажав **Добавить** появятся следующие варианты:

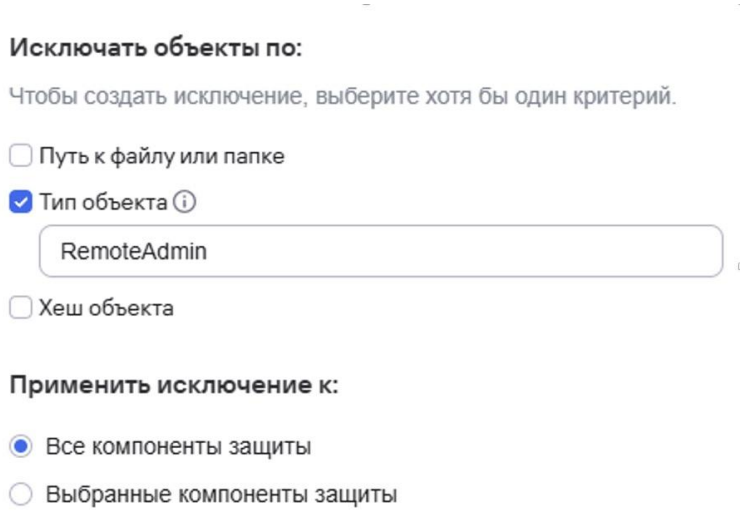
- **Категория** – позволяет создать новую категорию, в которую затем можно будет наполнять исключениями, т.е. позволяет группировать наборы отдельных исключений, например, относящихся к одной подсистеме или программе;
- **Новое исключение** – позволяет создать единичное исключение;
- **Выбрать исключение из списка** – позволяет выбрать преднастроенные в KES исключения для **файлов** некоторых программ.

В данном случае будет рассматриваться базовый сценарий выбора пункта **Новое исключение**, после выбора которого будет предложено выбрать критерий (-ии) исключения:

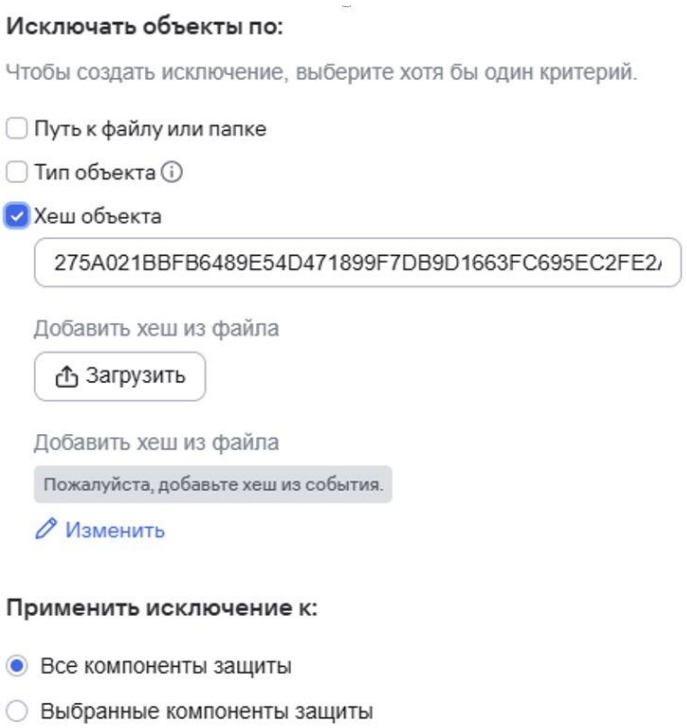
- Путь к файлу или папке – позволяет указать путь к необходимому объекту. Путь к папке должен заканчиваться обратным слешем. Возможно включить проверку вложенных папок и использование масок:
  - Символ *, который заменяет любой набор символов, в том числе пустой, кроме символов \ и /;
  - Два введенных подряд символа * заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы \ и /;
  - Символ **?**, который заменяет любой один символ, кроме символов \ и /;
  - Примеры использования масок.



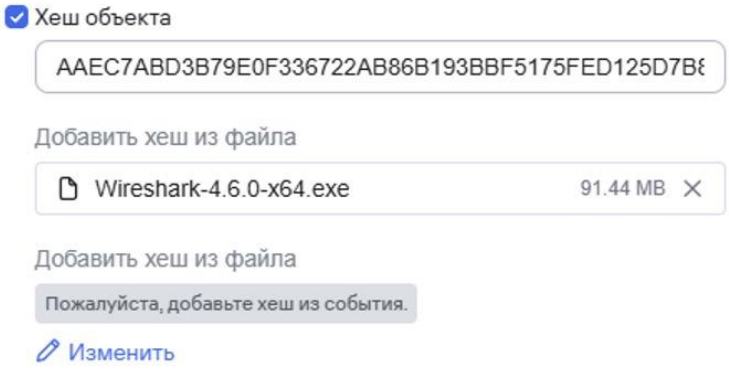
- Тип объекта – позволяет указать тип файла согласно вирусной энциклопедии, например, «RemoteAdmin».



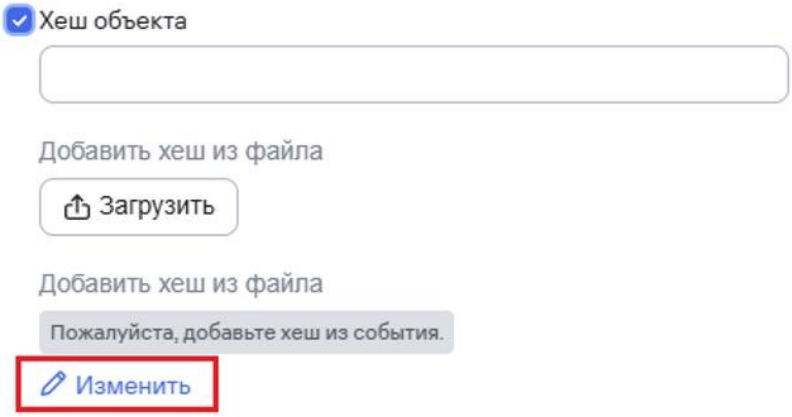
- Хеш объекта – позволяет указать SHA-256 хеш-сумму:
  - Вручную;

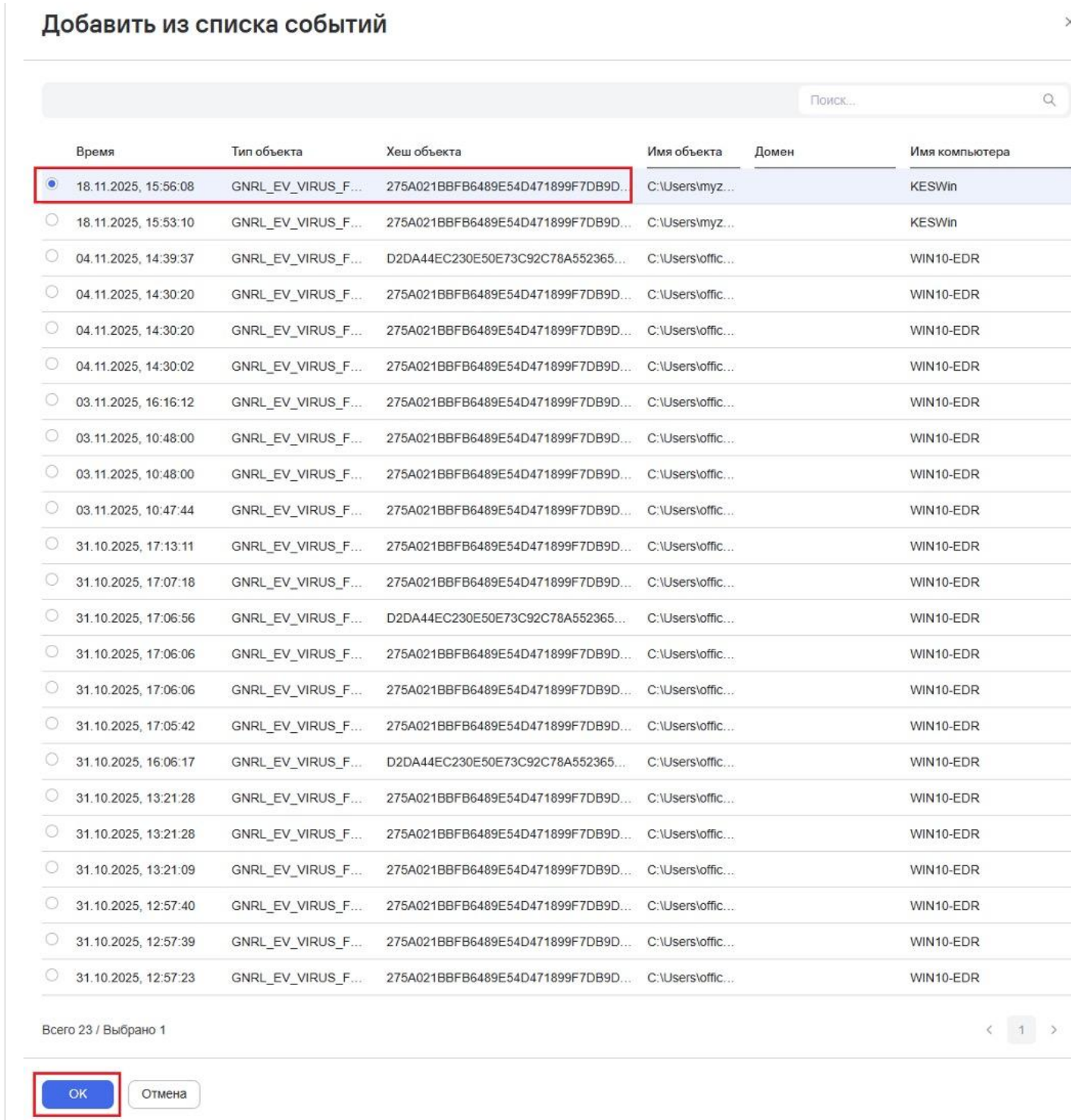


- Из выбранного файла при нажатии кнопки **Выбрать**;



- Из файла, на который ранее была сработка. При нажатии на **Изменить** появится список заблокированных KES’ом файлов и их хеш-суммы.

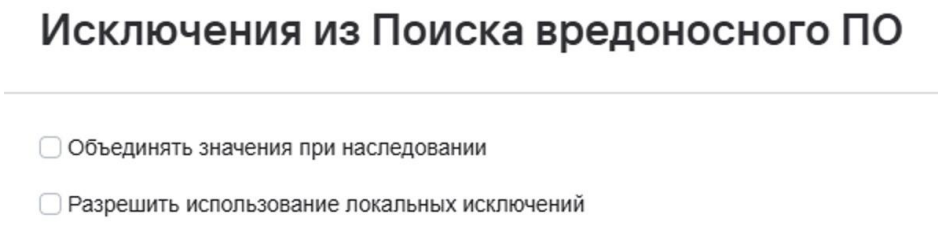




Также для файловых исключений можно использовать параметры:

- **Объединять значения при наследовании** – в таком случае исключения из родительской политики отображаются в дочерних политиках и доступны для просмотра. Таким образом, вы можете, например, создать общий исключений для всей организации. Если исключения дочерней и родительской политик совпадают, то эти элементы отображаются как один элемент родительской политики;

- **Разрешить использование локальных исключений** – в таком случае пользователь сможет сам добавлять исключения в локальном интерфейсе KES.



Настройка доверенных приложений

Список доверенных приложений – это список приложений, у которых **KES не контролирует файловую и сетевую активности** (в том числе и вредоносную), а также обращения этих приложений к системному реестру. По умолчанию KES контролирует объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех приложений и создаваемый ими сетевой трафик. После добавления приложения в список доверенных приложений KES перестает контролировать активность приложения.

Отличие исключений из проверки от доверенных приложений заключается в том, что для исключений KES не проверяет файлы, а для доверенных приложений инициируемые процессы. То есть, если доверенное приложение создаст вредоносный файл в папке, которая не включена в исключения, KES обнаружит этот файл и устранит угрозу. Если папка добавлена в исключения, KES пропустит этот файл.

Например, если вы считаете объекты, используемые приложением Microsoft Windows Блокнот, безопасными, то есть доверяете этому приложению, вам следует добавить приложение Microsoft Windows Блокнот в список доверенных приложений, чтобы не контролировать объекты, используемые этим приложением. Это позволит увеличить производительность компьютера, что особенно важно при использовании серверных приложений.

Кроме того, некоторые действия, которые KES классифицирует как подозрительные, могут быть безопасны в рамках функциональности ряда приложений. Например, перехват текста, который вы вводите с клавиатуры, является штатным действием приложения автоматического переключения раскладок клавиатуры (например, Punto Switcher). Чтобы учесть специфику таких приложений и отключить контроль их активности, рекомендуется добавить их в список доверенных приложений.

Доверенные приложения позволяют избежать проблемы совместимости KES с другими приложениями (например, проблемы двойной проверки сетевого трафика стороннего компьютера KES и другого антивирусного приложения).

В то же время исполняемый файл и процесс доверенного приложения по-прежнему проверяются на наличие в них вирусов и других приложений, представляющих угрозу. Для полного исключения приложения из проверки KES следует пользоваться исключениями из проверки.

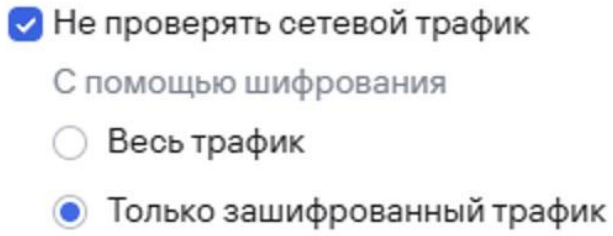
Для настройки доверенных приложений в политике перейдите в раздел **Параметры приложения → Доверенная зона** и выберите **Доверенные приложения**. Нажав **Добавить** появятся следующие варианты:

- **Категория** – позволяет создать новую категорию, которую затем можно будет наполнять доверенными приложениями, т.е. позволяет группировать наборы отдельных исполняемых файлов, например, относящихся к одной подсистеме;
- **Новое исключение** – позволяет создать единичное исключение;
- **Выбрать исключение из списка** – позволяет выбрать преднастроенные в KES исключения для **исполняемых файлов** некоторых программ.

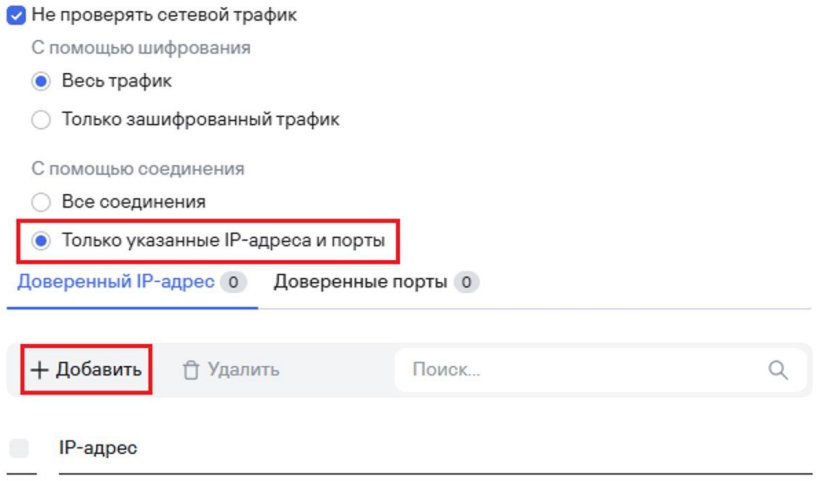
В данном случае будет рассматриваться базовый сценарий выбора пункта **Новое исключение**, после выбора которого будет предложено указать путь или маску пути к приложению и указать параметры исключения:

- Не проверять открываемые файлы – KES исключает из проверки все файлы, открываемые с помощью приложения;
- Не перехватывать изменения файлов – KES не отслеживает изменения файлов приложением;
- Не перехватывать изменения реестра – KES не отслеживает изменения реестра приложением;
- Не контролировать активность приложений – KES не контролирует файловую и сетевую активности приложения в операционной системе;
  - **Не контролировать для компонентов защиты и контроля** – отключает контроль за приложением следующих компонентов: Анализ поведения, Защита от эксплойтов, Предотвращение вторжений, Откат вредоносных действий и Сетевой экран;
  - **Не контролировать для Managed Detection and Response и Endpoint Detection and Response** – отключает контроль за активностью приложения со стороны встроенных агентов MDR и EDR (KATA);
    - Не перехватывать консольный ввод для Endpoint Detection and Response – KES не отправляет данные телеметрии об управлении приложением через консоль в EDR (KATA);
- **Не контролировать активность дочерних приложений** – KES не контролирует файловую и сетевую активности приложений, которые запускает указанное приложение. Вы можете применить исключение рекурсивно. То есть приложение не контролирует активность всей цепочки дочерних приложений;
- **Не наследовать ограничения родительского процесса (приложения)** – KES не применяет ограничения, которые настроены для родительского процесса к указанному процессу. Родительский процесс запускает приложение, для

которого настроены права приложения (Предотвращение вторжений) и сетевые правила приложения (Сетевой экран);
- **Разрешить взаимодействие с интерфейсом Kaspersky Endpoint Security** –самозащита KES не блокирует попытки управления службами приложения с удаленного компьютера. Приложению удаленного доступа к компьютеру разрешено управлять параметрами KES;
- **Не блокировать взаимодействие с компонентом AMSI-защита** – KES не контролирует запросы доверенного приложения на проверку объектов компонентом AMSI-защита.
- **Не проверять сетевой трафик** – KES исключает из проверки сетевой трафик, инициируемый приложением.
  - Можно исключить весь трафик, либо только зашифрованный трафик.



- Можно исключить точечно указанные соединения выбрав **Только указанные IP-адреса и порты**



Также для доверенный приложений можно использовать параметры:

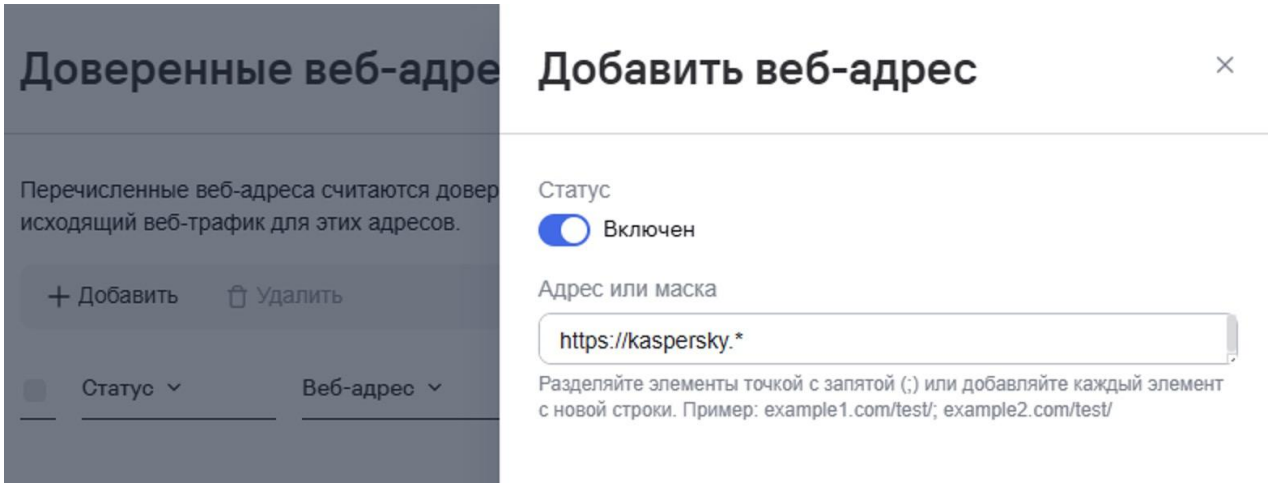
- **Объединять значения при наследовании** – в таком случае исключения из родительской политики отображаются в дочерних политиках и доступны для просмотра. Таким образом, вы можете, например, создать общий список доверенных приложений для всей организации. Если исключения дочерней и родительской политик совпадают, то эти элементы отображаются как один элемент родительской политики;

- **Разрешить использование локальных исключений** – в таком случае пользователь сможет сам добавлять доверенные приложения в локальном интерфейсе KES.

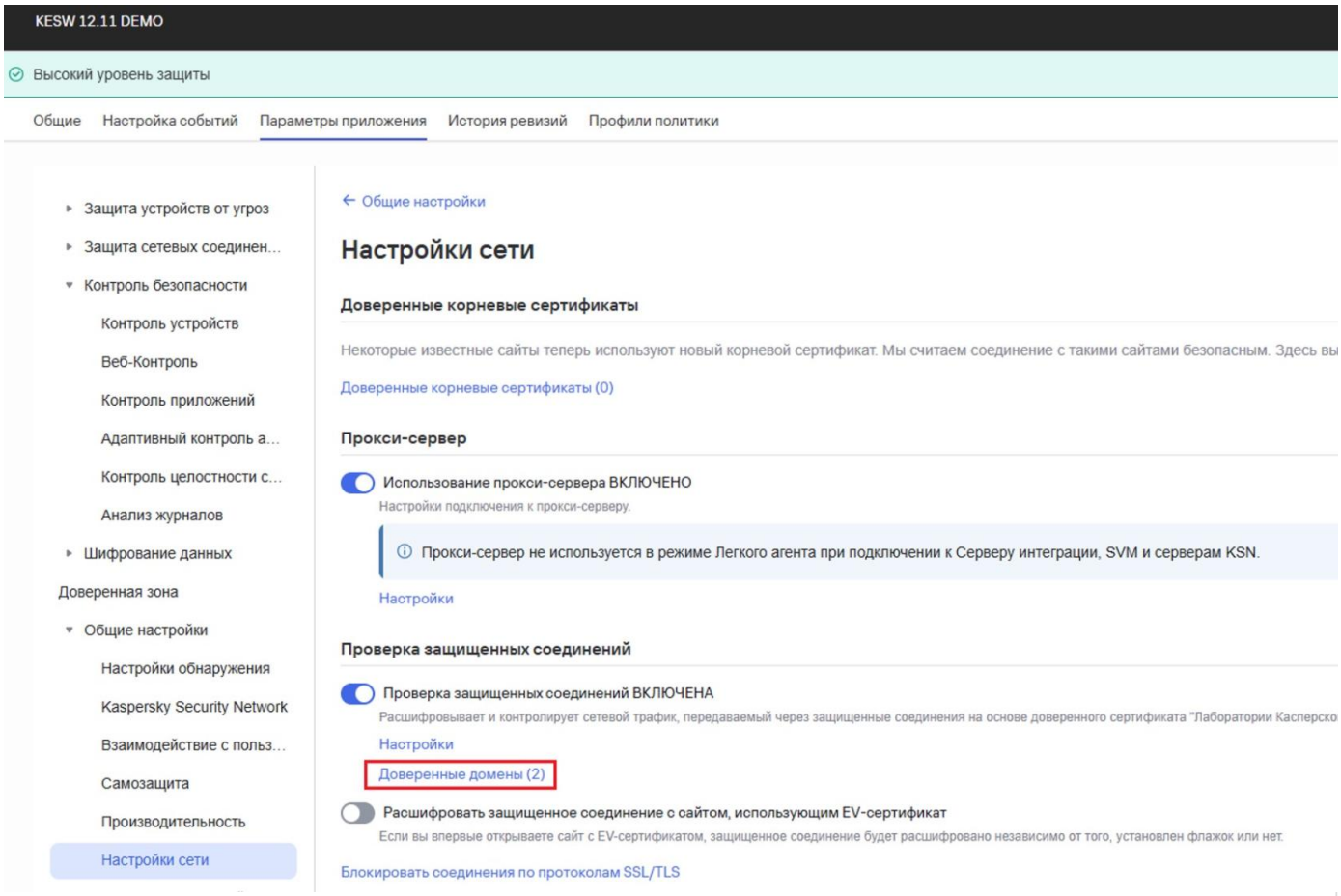
Добавление доверенных веб-адресов и IP-адресов

Для исключения веб-адресов из списка проверки компонентом защита от веб угроз необходимо создать исключения для соответствующих адресов.

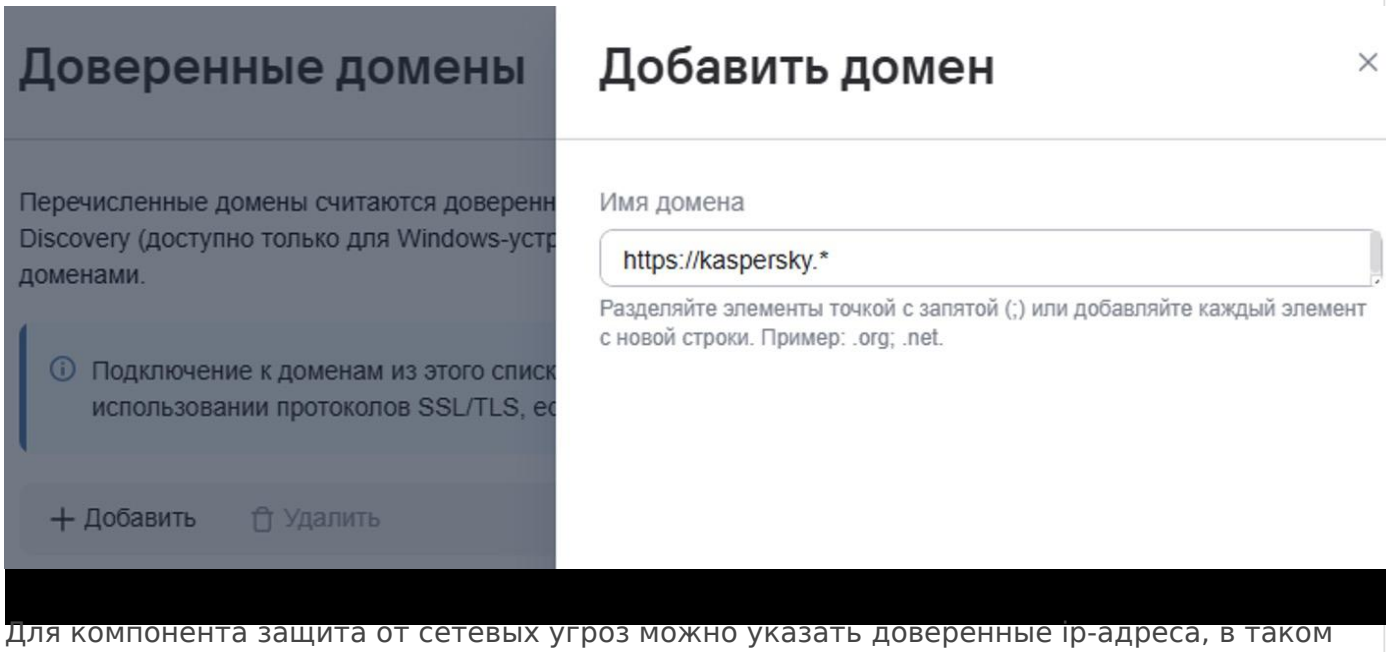
Для настройки доверенных веб-адресов в политике перейдите в раздел **Параметры приложения → Доверенная зона** и выберите **Веб-адреса**. Затем нажав **Добавить** укажите необходимые адреса. Поддерживается использование масок и добавление сразу нескольких адресов в исключение.



Также для работы некоторых веб приложений может потребоваться добавление исключения на проверку KES’ом зашифрованных соединений. Для этого в политике KES перейдите в раздел **Параметры приложения → Общие настройки → Настройки сети** и выберите **Доверенные домены** в блоке **Проверка защищенных соединений.** (Также доступно в разделе **Доверенная зона → Домены**).

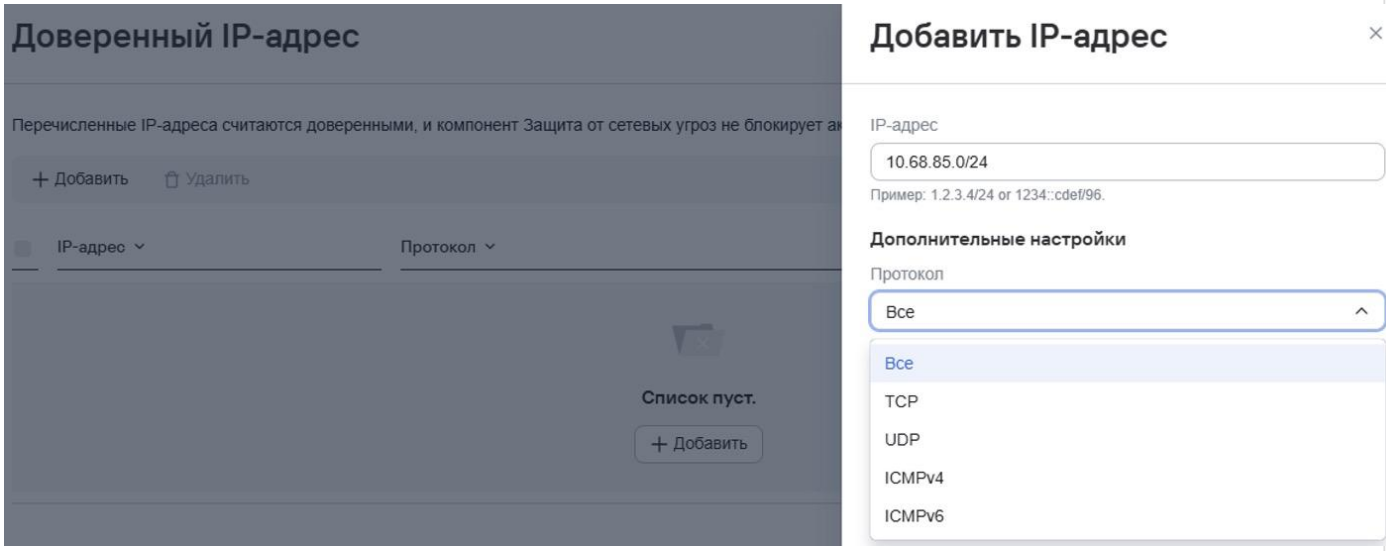


Выбрав **Добавить** укажите веб-адреса для которых не будет производиться проверка зашифрованного трафика. Поддерживается использование масок и добавление сразу нескольких адресов в исключение.

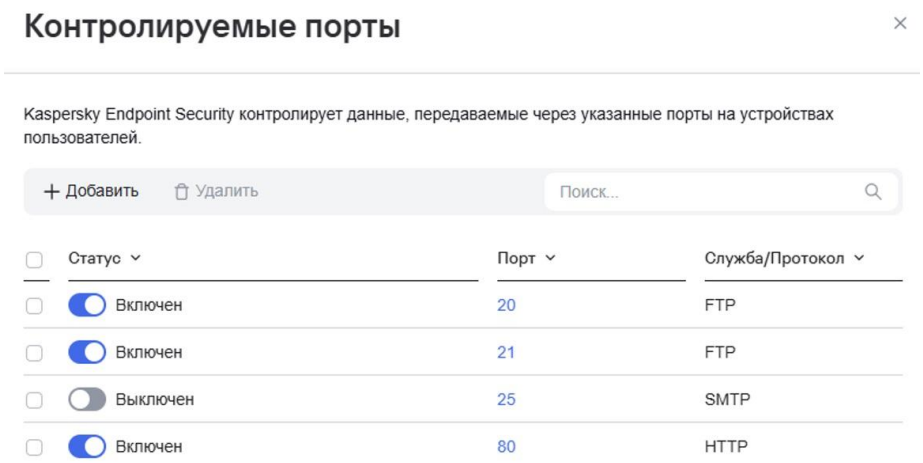


Для компонента защита от сетевых угроз можно указать доверенные ip-адреса, в таком случае компонент не будет блокировать активность с данных адресов. Для добавления исключения в политике перейдите в раздел **Параметры приложения → Доверенная зона** и выберите **IP-адреса**. Затем нажав **Добавить** укажите необходимые адреса. Поддерживается использование масок сети. Дополнительно можно указать протокол и

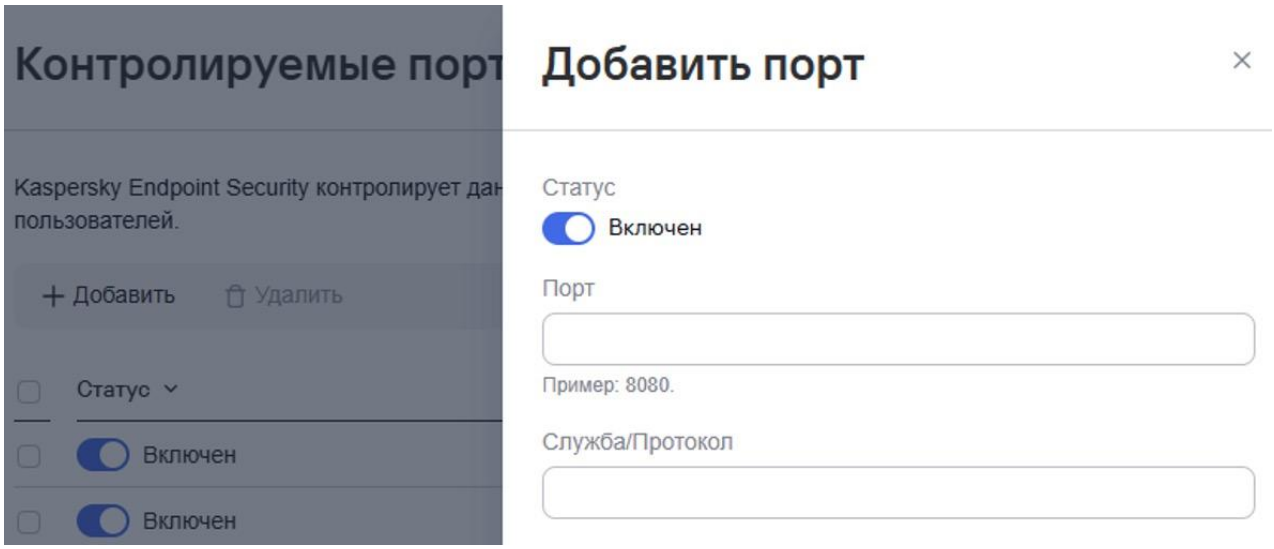
порт.



Также в политике KES в разделе **Параметры приложения → Доверенная зона → Сетевые порты** можно отключить контроль трафика по общеизвестным портам. Для этого необходимо перевести соответствующий переключатель в неактивное положение



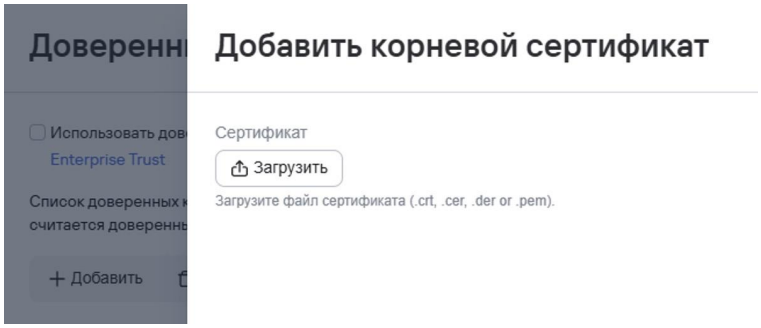
Также в данном разделе можно добавить контролируемые сетевые порты, нажав **Добавить**



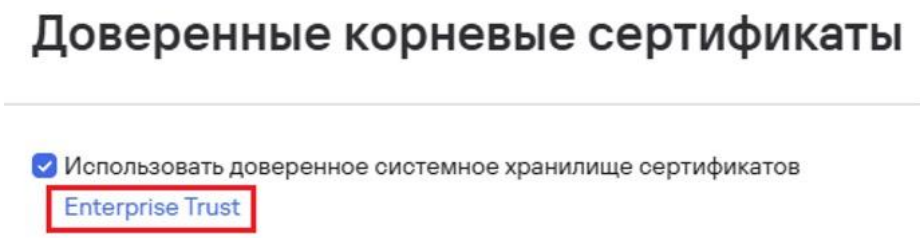
Добавление доверенных сертификатов

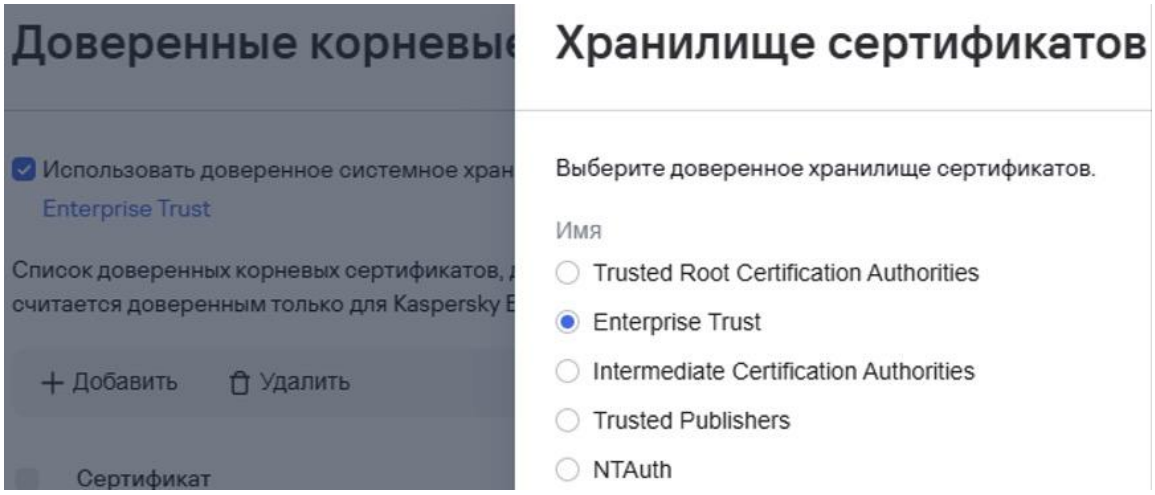
Приложение позволяет добавить сертификат в специальное хранилище сертификатов KES. При этом сертификат будет доверенным только для приложения KES. То есть пользователь будет иметь доступ к веб-сайту с новым сертификатом в браузере. Если другое приложение попытается получить доступ к веб-сайту, вы можете получить ошибку соединения из-за проблем с сертификатом.

Для настройки доверенных сертификатов в политике перейдите в раздел **Параметры приложения → Доверенная зона** и выберите **Доверенные сертификаты**. Затем нажав **Добавить** загрузите необходимый сертификат.



Также можно добавить использование системного хранилища сертификатов. Для этого необходимо поставить соответствующую галочку и выбрать доверенное хранилище сертификатов.

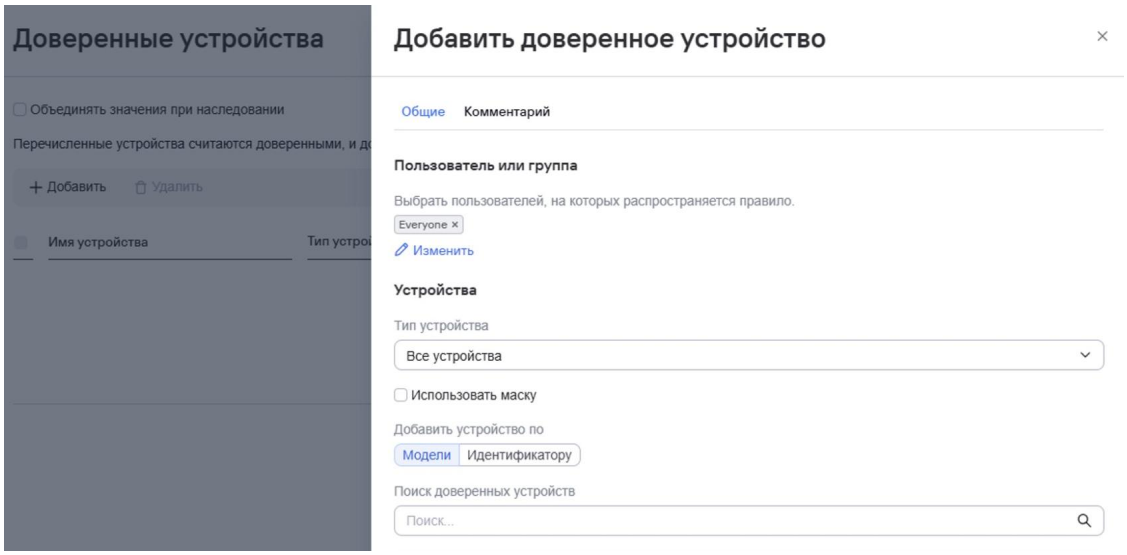




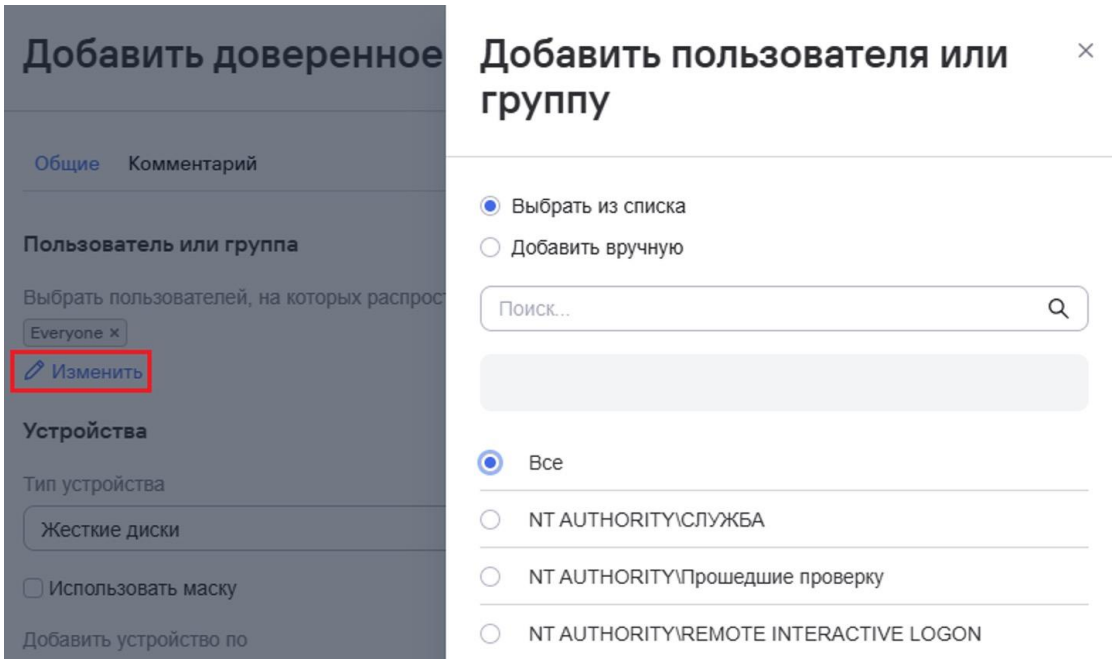
Добавление доверенных устройств

Доверенные устройства – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

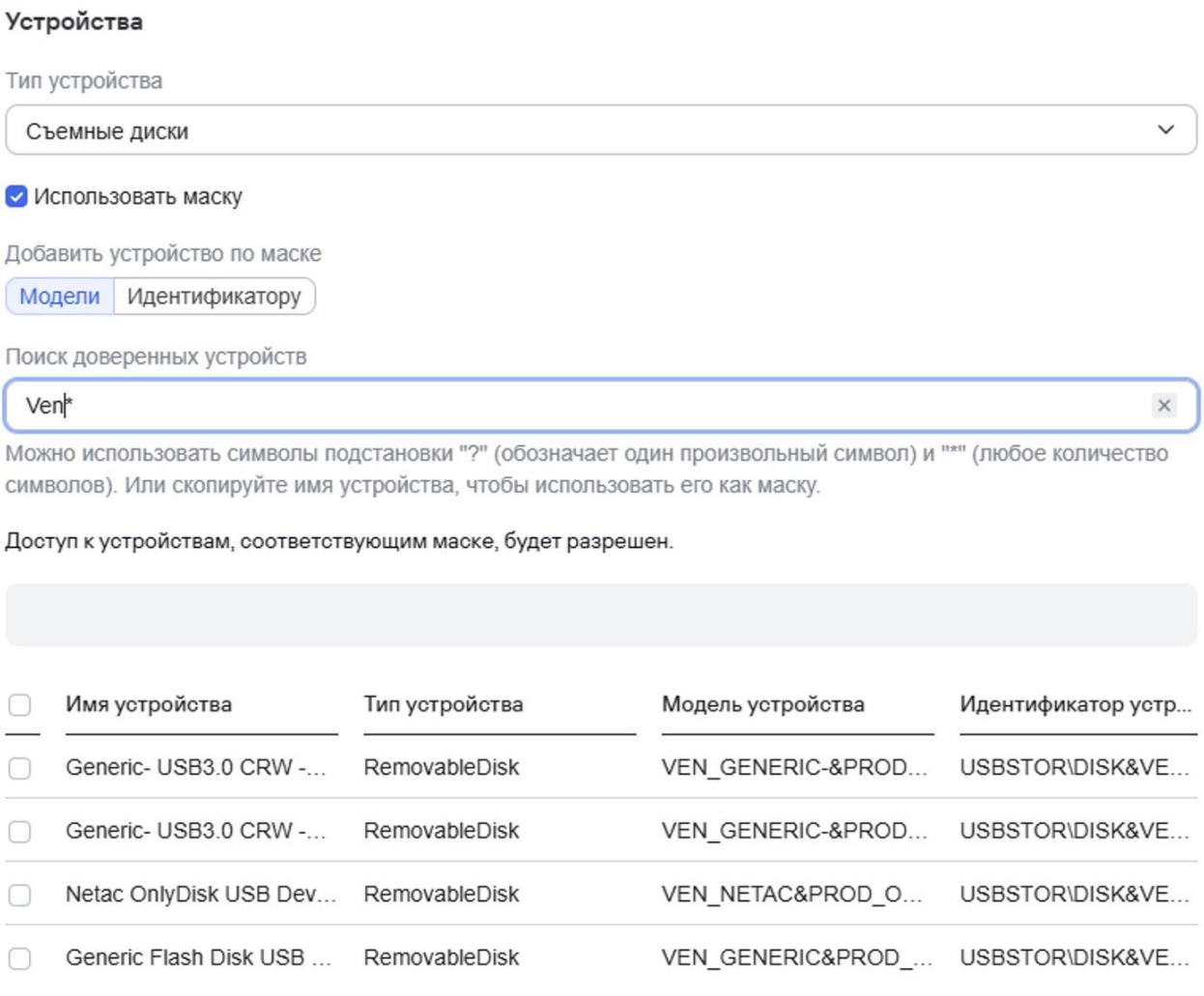
Для добавления доверенных устройств в политике перейдите в раздел **Параметры приложения → Доверенная зона** и выберите **Устройства**. Затем нажав **Добавить** появится меню добавления устройства.



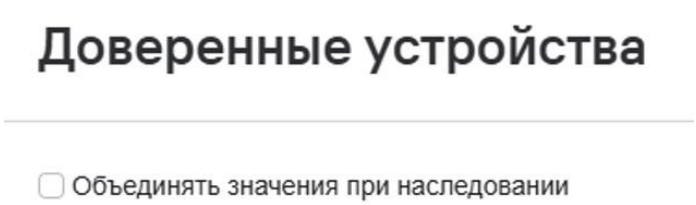
Необходимо указать пользователя (-ей), на которых распространяется правило, по умолчанию разрешение распространяется на всех пользователей. Нажмите изменить для выбора пользователя или группы. Для удобства можно использовать поиск.



Затем необходимо выбрать сами устройства. Для удобства можно выбрать конкретный тип устройства из предложенного списка, использовать маску модели или идентификатора, а также использовать поиск устройства



Также для доверенных устройств можно **Объединять значения при наследовании**. В таком случае исключения из родительской политики отображаются в дочерних политиках и доступны для просмотра. Таким образом, вы можете, например, создать общий исключений для всей организации. Если исключения дочерней и родительской политик совпадают, то эти элементы отображаются как один элемент родительской политики.



Revision #7
Created 25 June 2026 16:17:38 by Сергей
Updated 26 June 2026 15:42:16 by Сергей